

The Strong, the Weak, and the Hyperreal “I”: Cognitive Warfare and the Metaphysical Limits of Security

Luis Jacob Retanan

Independent researcher, ORCID: 0000-0002-4743-9569, corresponding address: canonleo_r17@yahoo.com

Abstract

As cognitive warfare increasingly emerges as a distinct concept amid the convergence of artificial intelligence (AI) and neurotechnology, its conceptual differentiation from hybrid warfare raises ontological questions concerning subjectivity and security itself. This paper argues that attempts to conceptualize cognitive warfare ultimately expose the metaphysical limits of security by presupposing a stable and self-identical subject capable of securing its own mind. Drawing primarily on Slavoj Žižek’s Hegelian-Lacanian psychoanalytic framework while engaging post-structuralist insights, the paper critiques the Cartesian conception of the irreducible and indubitable self (the Strong “I”). It argues that the subject is instead ontologically incomplete (the Weak “I”), creating a fundamental dilemma: either cognitive warfare loses its conceptual distinctiveness, or subjectivity is displaced altogether through the transformation of the subject into a simulated object (the Hyperreal “I”), rendering the project of securing the mind self-undermining and ultimately self-consuming. To demonstrate the practical implications of this argument, the paper critically examines adaptive security and its practice of transmorphance (the capacity of a system to adapt to uncertainty while preserving its core identity) as an emerging systems-level approach to cognitive defense, arguing that this practice culminates in the transformation of the system into a Hyperreal “I”, thereby exposing the metaphysical limits of security itself.

Keywords: cognitive warfare, subjectivity, security, psychoanalysis, transmorphance, psychopolitics

First published online on 20 October 2026

*“For what shall it profit a man, if he shall gain the whole world,
and lose his own soul?”
— Mark 8:36*

Introduction: Cogito Ergo Sum – the dilemma of a hackable mind

Advances in AI, neurotechnologies and other related innovations increasingly fuel direct and intrusive interventions to human cognition, and consequently open the plausibility of a “hackable mind” (Farahany 2023). From a security perspective, this raises a dilemma: how can one know if their mind is secured, if ultimately the thing that can tell them so is their own mind? One could argue that: I know my mind is secured because I am able to assert or question that it is. This is essentially the proposition *cogito ergo sum* (i.e., “I think therefore I am”) of René Descartes (1996: Meditations I and II), who argued that the self-referentiality of the “I” is the proof of its own (a) certainty or “indubitability” given that thinking itself requires the existence of a conscious being to begin with, and (b) fundamentality or “irreducibility” since its certainty is explained by its own existence rather than anything external to it.

However, in the context of a hackable mind, this Cartesian “I” becomes problematic as perception, introspection, and reflexivity in this case are no longer mechanisms for self-verification and critical thinking but rather subversive weapons of cognitive warfare. One’s own defense becomes its own threat. However, addressing this logical inversion of security reveals the real and fundamental problem of cognitive warfare: the necessity and delusion of the Cartesian “I”.

Cognitive warfare’s conceptual foundations remain contested, drawing on information, psychological, and hybrid warfare while its practice is driven by technical innovations for manipulating human cognition. This creates a widening gap between concept and practice that risks conflating cognitive warfare with the forms of warfare it seeks to differentiate itself from. Addressing this gap requires conceptual clarity through engagement with the philosophical issues at its foundation.

Vojtěch Bahenský (2025) argues, in his conceptual analysis of hybrid warfare, that conceptual clarity and utility enable a security concept to identify and explain explicitly the threat, the referent object, and the means by which it is protected. Indeed, Chiara Libiseller (2023) emphasizes the necessity of a fixed intelligible essence and clear aim for security concepts to have practical significance in the first place. Thereby, clarity and utility at the conceptual level promote consistency in policy development and operational practice within defense establishments. Yet the conceptualization of hybrid warfare fails, as “hybrid warfare concepts generally

compounded the existing definitional issues of various concepts within the field of defence and security by combining them into a rather impenetrable definition” (Bahenský 2025: 25). Western military establishments and security scholars broadly define this type of warfare as an adaptive combination of conventional and non-conventional means to achieve political aims (Fabian 2019).

Thus, despite its popularity among security practitioners and academics, the imprecision of hybrid warfare renders it unsuitable for “theory-building or understanding war” – it is not an analytical but rather a “fashionable” yet unstable concept (Libiseller 2023: 874). Interlinked with hybrid warfare concepts, cognitive warfare is susceptible to the same conceptual instability. However, in-depth and meaningful engagement with concepts, which is seen as a solution in addressing definitional issues (Libiseller 2023; Milevski as cited in Bahenský 2025), requires careful application in cognitive warfare. Engagement for the sake of conceptual stability and effective operationalization is counterproductive in cognitive warfare because, as this paper will set out to demonstrate, this warfare pushes the very conception of security to its “metaphysical limits.”

As its main thesis, this paper aims to demonstrate that cognitive warfare pushes security to its metaphysical limits, given that its conceptualization fundamentally depends on stabilizing the ontologically unstable “I” into a referent object. This stabilization produces (a) the “inversion of security,” whereby the “I” becomes the source of both certainty and insecurity, and (b) the “perversion of security,” whereby the “I” is treated as if it were stable and objectifiable despite its impossibility. Following Slavoj Žižek (2006), perversion here refers to the paradoxical attitude that affirms a truth as if it were always true despite being aware that it is not. Given so, (b) intensifies in response to (a) because of the instability of the “I”; yet when (b) is pushed to its radical conclusion in response to (a) then it entails the complete stabilization of the “I” as a referent object at the cost of the ontological instability that constitutes it as an “I” in the first place. Thus, cognitive warfare pushes security to its metaphysical limits insofar as it not only renders security self-undermining but also self-consuming.

To methodically explicate its thesis, this paper presents a three-stage dialectical critique: (1) the conceptualization of cognitive warfare entails the stabilization of the “I” as both indubitable and irreducible, (2) this stabilization fundamentally fails due to the ontological instability of the “I”, and (3) affirming the stability of the “I” despite (2) and in pursuit of (1) demonstrates the conceptual and practical perversion of security in the context of the growing hackability of the mind in cognitive warfare. The main contribution of the paper to the literature of cognitive warfare then is how *not* to conceptualize and operationalize this warfare, and the potential importance of the ontological instability of the “I” in ensuring so.

This paper develops this dialectical critique in three parts. First is a discussion of conceptualization efforts of cognitive warfare, primarily within the North At-

lantic Treaty Organization (NATO) establishment, and the metaphysical questions concerning mind and reality that come with these efforts. Second is a dissection of the tension between security and the “I” through the post-structuralist framework and the Žižekian ontological critique of the subject, within the context of today’s convergence of artificial intelligence (AI) and neurotechnology in order to show how efforts to stabilize the unstable “I” fails and leads to its dissolution and the perversion of security itself. The final part is a critique from the Žižekian perspective on how the notion of an adaptive defense strategy for cognitive warfare based on the concept of “transmorphism” (i.e., the capacity of a system to adapt to uncertainty while preserving its core identity) ultimately becomes a self-undermining and even self-consuming enterprise.

The conceptualization of cognitive warfare

This section examines the developments and challenges concerning the conceptualization of cognitive warfare within its burgeoning literature, the role of human cognition in driving and challenging its conceptual clarity and utility, and the metaphysical issue that comes with conceptualizing a warfare centered on the human mind.

The pursuit for conceptual clarity and utility

NATO has emerged as one of the leading military organizations in the development and operationalization of the concept of cognitive warfare amid the growing weaponization of AI and advances in neurotechnology. Driven by persistent concerns over Russian disinformation campaigns, the organization has sought to develop cognitive warfare as a military concept capable of explaining how increasingly sophisticated technologies shape and manipulate human cognition across societal, psychological, and physiological domains. As noted in the 2025 NATO Chief Scientist Research Report (CSRR) on cognitive warfare, the NATO Science and Technology Organization (STO) recognized cognitive warfare as a “strategic research challenge” in 2022 due to its implications for decision-making, collective resilience, and trust, and subsequently launched multiple research activities under its Collaborative Program of Work (CPoW) (Søndergaard 2025).

These activities seek to strengthen the conceptual clarity and utility of cognitive warfare by enhancing resonance, consistency, internal coherence, external differentiation, and theoretical utility – the five criteria of conceptual quality identified by Bahenský (2025). In terms of resonance, the 2022 House Model developed by STO Human Factors and Medicine (HFM) and the Science and Technology Committee (STC) provides a common framework for the nature, means, and objectives of cognitive warfare within the alliance (Søndergaard 2025). This shared understanding promotes consistency in the use of cognitive warfare as a military concept. At the same time, the model contributes to internal coher-

ence by integrating physiological, psychological, and socio-cultural dimensions of cognitive manipulation into a single framework.

Internal coherence and external differentiation clarify what cognitive warfare is and is not. The NATO CSRR characterizes cognitive warfare as an increasingly AI-enabled convergence of psychological, information, and cyber operations targeting cognition across multiple interconnected vectors (Guyader cited in Søndergaard 2025). Situated within a “multiplex network” of social norms, symbols, and institutions (Korobeynikov Davydiuk & Mokhor 2026), cognitive warfare’s multidimensionality becomes its defining attribute.

Having established resonance, consistency, internal coherence, and external differentiation, cognitive warfare gains theoretical utility through its operationalization as a military concept. The linkage of the House Model to the Observe-Orient-Decide-Act (OODA) Decision Cycle translates cognitive warfare into a measurable activity, enabling the development of mitigation and response strategies. This approach was further explored through an STO workshop initiated by the Norwegian Defense Research Establishment in November 2022, which examined how technology, policy, and training could be leveraged to counter technology-enabled efforts to influence human behavior in support of adversarial political and military objectives (Søndergaard 2025). As of April 2025, the STO continues to expand its research activities designed to explore the doctrinal integration of cognitive warfare with AI, cybersecurity, and information operations.

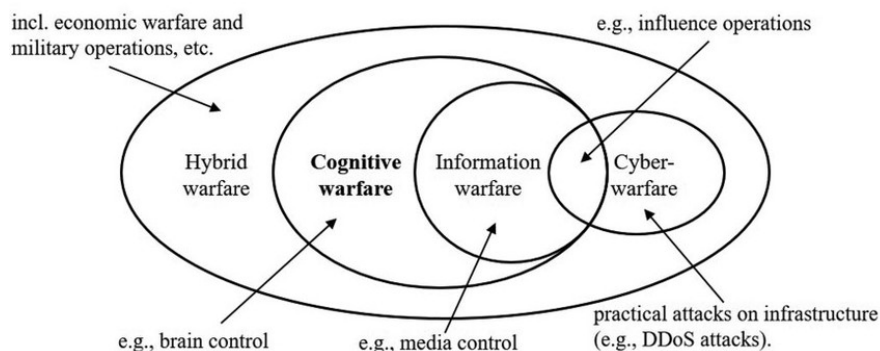
The developments highlighted by the 2025 NATO CSRR strengthen the understanding of cognitive warfare through pursuing the conceptual clarity and utility of its working definition published by NATO in 2023: “the activities conducted in synchronization with other instruments of power, to affect attitudes and behaviours by influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage” (NATO Allied Command Transformation 2023). In turn, this definition provides a conceptual basis for NATO’s pursuit of cognitive superiority, understood as the capability to (a) degrade capabilities of adversaries to influence decision-making, (b) improve human and technological cognition, and (c) withstand and recover performance (Søndergaard 2025).

Collectively, all these efforts contribute significantly to the conceptual quality of cognitive warfare. Such developments are crucial if cognitive warfare is to emerge as both a distinct area of inquiry within security studies, and an operationalizable military concept. Nevertheless, cognitive warfare continues to evolve alongside technological advances and its growing interconnection with other forms of warfare, creating persistent challenges for maintaining conceptual clarity and utility. But the real problem may not be the conceptualization of cognitive warfare per se, but rather the tension inherent in what such conceptualization fundamentally entails: the “I” as both a controllable object and a conscious subject.

Issues and limits of conceptualization

The multidimensionality of cognitive warfare renders it identifiable with a wide range of technologically-evolving non-kinetic activities (i.e., information, psychological, and cyber operations) that constitute hybrid warfare, fundamentally questioning whether cognitive warfare can stand as a concept in its own right.

Figure 1. Relationship between hybrid warfare, cognitive warfare, information warfare, and cyber warfare



Source: Adapted from Hung and Hung (2022)

The relationship of cognitive warfare with hybrid warfare as shown by the diagram above (Hung & Hung 2022) fundamentally questions not only its conceptual clarity and utility but also whether cognitive warfare can be a concept in its own right. Two approaches are being pursued in the literature: the minimalist conception, which tries to limit the scope of cognitive warfare to make it usable, and the maximalist conception, which aims to emphasize its multidimensional nature driven by techno-human interaction to make it distinct (Deppe & Schaal 2024).

A “minimalist conception” produces narrower and non-kinetic characteristics, which strengthen resonance, consistency, internal coherence, and theoretical utility of cognitive warfare at the expense of its external differentiation (Danyk & Briggs 2023; Bernal et al. 2020). In other words, this conception renders cognitive warfare observable and operationalizable but not unique. Through situating human-technology interaction in the division between the physical and mental, the minimalist conception is able to limit cognitive warfare in two ways: (1) the external environment can affect human cognition, but (2) this is not guaranteed given that the access to the internal environment of the mind is exclusive to the individual.

The philosophical dilemma known as the “mind-body problem” concerns how physical and ideational realities interact despite their fundamentally different natures. If this dilemma is understood in terms of separability between mind and matter, it limits cognitive warfare insofar as the mind cannot be manipulated di-

rectly, but only through the external environment in which it is situated. Hence, this environment can only be shaped through activities aimed at controlling perception (i.e., reception of information) rather than cognition itself (i.e., processing of information). This strengthens the conceptual consistency of cognitive warfare by rendering it an observable phenomenon manifested through practices of perceptual control. Thus, the shaping of information content becomes both the primary mode and limitation of cognitive manipulation from a minimalist conception of cognitive warfare.

However, cognitive warfare loses its multidimensionality, and becomes indistinguishable from the information-manipulating activities it seeks to integrate. The minimalist approach may have made the concept of cognitive warfare usable in practice. Yet this approach not only rendered the concept interchangeable with hybrid warfare's subsets, but also stripped its distinctiveness as a subset of hybrid warfare itself. Cognitive warfare has become a mere advanced practice of information, cyber, and psychological operations.

In contrast, a “maximalist conception” treats cognitive warfare as a distinct and evolving form of conflict shaped by advancements in human information-processing technologies, the expanding definition of “cognitive attacks,” and the perceived strategic value of such attacks (Deppe & Schaal 2024). By emphasizing the uniqueness of cognitive warfare as a concept, the maximalist conception strengthens its resonance, but does so at the expense of the other dimensions of conceptual quality. However, precisely because this conception affirms the multidimensionality of cognitive warfare, it consequently generates problems in consistency, coherence, and external differentiation.

As discussed, prioritizing consistency and coherence leads to a minimalist conception of cognitive warfare grounded on distinction between physical and mental realities, which in turn limits its multidimensionality. By framing cognitive attacks as information control, the minimalist conception limits the battle to what is perceived rather than how it is perceived. On the other hand, the maximalist conception essentially sees cognitive warfare as a battle over how information is received and interpreted. In this view, human cognition is not an unassailable “inner sanctum” to which the individual can retreat to but rather a product of social, psychological, and physiological processes.

The maximalist conception relies on more flexible theories of how mental and physical realities interact. Mark Rowlands (2010) highlights four prominent theories of cognition known as the 4Es in the field of cognitive science: embedded, embodied, extended, and enacted cognition. Each of these theories represents a different understanding of the relationship between mind and matter, thereby determining the focus and scope of cognitive warfare. First, the theory of embedded cognition rationalizes the minimalist conception by emphasizing that even though cognitive processes are driven by interaction with the external

environment, these processes are internal to the individual. Second, the enacted and extended theories of cognition underlie the maximalist conception by allowing a less rigid mind-body distinction through phenomenological experience and human-technology interaction, respectively. Third, the theory of embodied cognition pushes the maximalist conception further by dissolving the distinction between mind and body through direct neurobiological control of cognition. These theories demonstrate how a particular understanding of human cognition defines the conceptual scope of cognitive warfare. Moreover, from the maximalist conception, enacted, extended, and especially embodied cognition all entail the multidimensionality of cognitive warfare.

Yet this still does not establish cognitive warfare as a distinct area within security studies, as external differentiation remains an issue – this time in relation to hybrid warfare itself. After all, where is the difference between two concepts that both treat every aspect of human existence as potentially weaponizable? Both cognitive and hybrid attacks seek to shape adversaries' decisions and actions in ways that ensure strategic advantage. As illustrated earlier in the conceptual relationship diagram, the maximalist conception ultimately collapses the distinction between cognitive warfare and hybrid warfare, rendering them effectively synonymous and extending cognition to such a degree that virtually all human activity becomes cognitive in nature. As a result, this cannot serve as a basis for asserting conceptual primacy or the distinctiveness of cognitive warfare. Instead, it further weakens the conceptual clarity and utility of both cognitive and hybrid warfare.

The only way to preserve the distinctiveness and conceptual primacy of cognitive warfare over hybrid warfare is to treat cognition as the enabling condition that makes activity possible rather than as an activity itself. Yet this seemingly counter-intuitive idea is actually what the minimalist conception anchors on and the maximalist conception distances from: the irreducibility and indubitability of the "I".

How can thinking not be an activity at all? Activities are causal and observable within time and space, whereas thinking is not merely an activity but the *irreducible* reality of the "I". Immanuel Kant's concept of transcendental apperception emphasizes the "I" as the fundamental organizing condition that unifies experience and renders it intelligible. An activity is only recognizable as an activity because there is an "I" that makes sense of it (Kant 1998: B131-132). Yet the irreducibility of the "I" to any particular activity only establishes its uniqueness and fundamentality, not its stability or certainty. For the "I" to serve as the ontological foundation of cognitive warfare's distinctiveness and conceptual primacy, irreducibility must therefore be grounded in indubitability. This is precisely what the Cartesian "I" presupposes, since the way it proves its existence does not only establish that it is certain but also that it is the *only* thing that can be certain. Consequently, if the maximalist conception were extended on the basis of the irreducibility and

indubitability of the Cartesian "I", it would entail the primacy of the "I" that *exists* and *persists* despite, and above, all human activities.

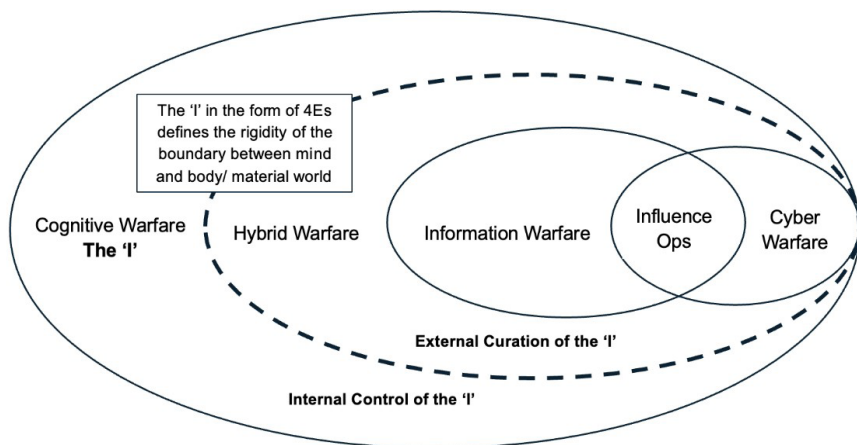
Both the irreducibility and indubitability of the "I" then provide the conceptual uniqueness cognitive warfare needs. This "I" delineates cognitive warfare from the supposed all-encompassing concept of hybrid warfare. Moreover, this "I" enables cognitive warfare to attain conceptual primacy over hybrid warfare as a multidimensional control of human activities from the macrolevel (i.e., social, economic, and political) to the microlevel (i.e., neurobiological and psychological) aimed for the augmentation and disruption of cognition. Cognitive warfare in practice thereby becomes a battle for what NATO has already termed as "cognitive superiority," which is "the expansion of knowledge and understanding . . . connected by all-domains and enabled by technology, in order to maximize commander's ability to anticipate, think, decide and act" (Søndergaard 2025: 11).

This establishes the first stage of the paper's dialectical critique: the conceptualization of cognitive warfare entails the stabilization of the "I" as both indubitable and irreducible. But as both the irreducibility and indubitability of the "I" render the distinctiveness of cognitive warfare, they also entail the impossibility of the complete and total *external* control or even dissolution of the "I". This implies that the "I" can be curated at best by causal mechanisms but only the "I" itself can exercise control over its own internal reality, which includes technologically extending, enacting, embedding, and embodying itself. This would then mean that cognitive warfare is about gaining strategic advantage over adversaries through (1) curation of the "I" through control of causal cognitive processes from the physiological up to the systemic level, and (2) control of the "I" over its own mental states (e.g., beliefs, thoughts, introspection, etc.) through technological optimization and augmentation.

However, the latter definition of cognitive dominance highlights the fundamental tension between subjectivity and security by implying that the "I" as a conscious subject must *render* itself into a controllable object to continuously ensure its security. Understanding cognitive warfare on the basis of the persistent existence of the "I" may have provided a way to address conceptualization issues but this also entails the stabilization of the "I" not only as a rational and autonomous subject but also a referent object of security. This opens up a far more problematic issue: the metaphysical tension between subjectivity and objectivity.

If the "I" as a subject is indeed irreducible into an object even through its own act of self-objectification, this risks undermining the conception of cognitive warfare by limiting the participative role and practical significance of the "I" – a key requirement if cognitive warfare is to remain distinct from hybrid warfare, as it must demonstrate how it shapes human activities while remaining conceptually above them. Conversely, if the "I" can exercise reflexive control over itself,

Figure 2. Revised conceptual relationship diagram of cognitive warfare with the Cartesian “I” as its basis.



Source: Author

this affirms its indubitability but raises a further question: whether the “I” can persist as both subject and object, or is transformed into something else entirely.

In essence, cognitive warfare requires the “I” to be both subject and object. Yet as human institutions, relations, and biology are now being weaponized for this warfare, they also intensify the underlying tension between subjectivity and security into an “ontological crisis” (Giddens 1991; Mitzen 2006). Projects grounded on the irreducibility and indubitability of the “I” become self-compromising: they not only render human cognition vulnerable to disruptions, but also require the complete transformation of the “I” into a controllable object of security while simultaneously presupposing its persistence as a rational and autonomous subject. Treating the “I” as a referent object may stabilize it into a definable and securable entity, but it also distorts both the “I” and security itself in the age of cognitive warfare.

Stabilizing the “I” and the perversion of security

Cognitive warfare can then be understood as: (a) curation of the “I” through control of causal cognitive processes from the physiological up to systemic level, and (b) control of the “I” over its own mental states (e.g., beliefs, thoughts, introspection, etc.) through technological optimization and augmentation to gain strategic advantage over adversaries. Its practices operate within a multidimensional environment for human cognition that drives and incentivizes the pursuit for rational thinking, computational prowess, and certainty itself.

This section aims to show how such environment attempts and fails to stabilize the “I” as both a conscious subject and a controllable object. As such, the “I” is able to reflexively demonstrate its irreducibility and indubitability. For this reason,

the “I” is characterized here as the Strong “I”. Nevertheless, this section not only highlights how the Strong “I” is fundamentally unstable, but also how addressing this instability transforms it into a mere determinable and securable object while eroding its character as an incomplete and conscious subject. Ultimately, this demonstrates how security becomes perverted in an environment that drives and incentivizes the Strong “I” through the growing convergence between human and machine intelligence.

Cognitive technoscientific order: Exploiting the strong “I”

Technology and its use shape how people acquire, exchange, and process information, thereby creating a system that influences human cognition. Branden Allenby (2021) refers to this system as the “cognitive ecosystem,” which, with the rise of AI technologies capable of simulating and extending human cognition, has increasingly become global in scope. As AI emerges as a primary information-processing tool within contemporary institutions, its continued development depends on deeper access to and understanding of human cognitive processes. Consequently, human cognition is increasingly treated as a shapeable and exploitable strategic resource for dominating the global cognitive ecosystem.

The present global cognitive ecosystem is shaped not only by data production and consumption, but also by intellectual capital from biological and social sciences (Allenby 2021). This capital accelerates AI’s convergence with neurotechnology, deepening computational capabilities, and understanding of cognition. The resulting interdependence of data, knowledge, and technology enables increasingly personalized human-machine interactions, creating the conditions for multidimensional curation of the “I” and incentivizing self-regulation.

The global cognitive ecosystem exemplifies what Antoine Bousquet (2022: 17) describes as a “technoscientific regime of order,” in which “order came to be increasingly justified and organized on the basis of scientific and technical rationality.” This is because the present co-constitutive relationship of science and technology is not just shaping the social but also the neurobiological reality of the individual. Consequently, this intensifies the Cartesian belief of rational individuals being the “masters and possessors of nature” – which increasingly includes their own bodies. Here, the Strong “I” is realized as both a thinking subject and stable object.

With the emergence of cognitive warfare, the Strong “I” becomes both an instrument and participant with the technoscientific order of the global cognitive ecosystem. As advances in AI and neurotechnology enable increasingly sophisticated interventions into cognitive processes, the individual is not a mere passive resource but rather an active participant utilizing those interventions to technologically harness cognition in its different forms (i.e., embedded, enacted, extended, and embodied) and through various sites of intervention as summarized in Table 1.

Table 1. Cognitive warfare interventions across the 4Es theories of cognition.

Form of Cognition	Site of Intervention	Technology
Embedded	Information Environment	Sensor Networks
Enacted	Perception-action feedback	Augmented and Virtual Reality
Extended	Cognitive offloading	AI cognitive assistants
Embodied	Neurophysical process	Neurostimulation devices

Source: Author’s synthesis. Adapted from Rowlands (2010) and informed by Søndergaard (2025), Eyre et al (2023), Bousquet (2022) and Farahany (2023).

The centrality of the “I” within this technoscientific order makes it a key technology in its own right, as the individual becomes increasingly intertwined with technological devices they create, innovate, and study with. The “I” in its strong form is its own tool in its bid to master its environment and its own body. Given so, the present global cognitive ecosystem exemplifies a *cognitive* technoscientific order, marking a shift from what Bousquet (2022) defines as a technoscientific order based on “chaoplexic” warfare, which focuses on managing the complexity and chaos of today’s interconnected information networks through an adaptive and decentralized approach to military command and control (C2). The growing importance of rapid and flexible decision-making increasingly shifts strategic focus toward cognition itself as AI becomes deeply embedded in operational C2. Human cognition becomes then directly consequential to military success and failure.

The shift from a chaoplexic to a cognitive technoscientific order is driven by the need for predictability and control in warfare. While chaoplexic warfare seeks to mitigate uncertainty by adapting to external complexity, cognitive warfare seeks to ground certainty in the Strong “I”.

Nonetheless, Allenby (2021: 37) argues that the continued growth of data and advances in AI are pushing the global cognitive ecosystem toward a “tipping point, where cognitive processes evolve and function beyond anything that humans and their institutions are accustomed to.” While human cognition is unlikely to be replaced, AI in convergence with other cognitive or brain technologies is poised to emerge as the dominant cognitive force within this ecosystem. Paradoxically, the cognitive technoscientific order risks reducing the Strong “I” to a dispensable resource. In so-called “hyperwar,” the speed and volume of information processing compresses decision-making to the point where critical cognitive functions are delegated entirely to AI systems (Bousquet, 2022), reducing human cognition from active participant to object of optimization.

The Strong “I” is further reduced to a referent object of security through the institutions that enable and sustain the speed and adaptability of cognitive warfare. Within the cognitive technoscientific regime, governance increasingly

takes algorithmic forms aimed at understanding, predicting, and influencing cognitive processes at scale. This “algorithmic governmentality” extends the Foucauldian biopolitics beyond the management of physical existence of the individual towards the neurobiological curation of individual subjectivity through AI-mediated interventions. As Claes Wrangel (2024: 351) argues, it seeks to “monitor and intervene not only in actual behavior, but in the very potentiality of being – steering and regulating processes of subjectivity as they emerge in the human brain.” In this context, the “I” is increasingly policed to render itself into a knowable, predictable, and governable object. Surveillance and self-censorship become more intimate as individuals are encouraged to monitor and optimize their own neurobiological features. Yet even as surveillance cannot fully capture individual subjectivity (Abbey 2025), individuals are incentivized to identify with their own data-representations – the Cartesian ideal of self-mastery reproduced as algorithmic self-governance.

Indeed, the Cartesian ideal rationalizes the *conscious* effort of the “I” to render itself into an optimizable object – exemplifying the supposed synergy of the Strong “I” as both subject and object, sacrificing irreducibility for the sake of indubitability. However, pursuing the Strong “I” renders its own subjectivity into a tool in the effort to make itself more securable. As discussed, cognitive warfare in its hyper war form relegates human cognition into a dispensable resource to be managed in the cognitive technoscientific order. In Heideggerian terms, the individual increasingly becomes a cognitive *bestand* or “standing-reserve” as subjectivity is translated into a measurable and optimizable resource for the present technoscientific order (Heidegger 2013). Thus, with subjectivity subordinated to the institutional need to objectify the “I”, the Strong “I” becomes a complete yet empty non-conscious object.

The cognitive technoscientific order ultimately reveals that the Cartesian ideal of the Strong “I” rests on a metaphysical assumption that renders the “I” a referent object of security. As argued earlier, the indubitability of the “I” derives from its existence as a thinking subject whose reflexivity grounds its certainty. In this sense, the Strong “I” exemplifies the “metaphysics of presence,” which is a “metaphysics that seeks for foundations, origins” (Edkins 1999: 66), thereby resulting in “profound reassurance of the certainty of meaning” (Derrida 2001: 73). The “I” appears as immediately given, producing the impression of a continuous and stable presence. But as the “I” leverages its own reflexivity to exercise self-control and affirm its own certainty in the context of the cognitive technoscientific order, it transforms from a thinking being to a *controlled* thinking being. This transformation is crucial if security itself is to be conceivable amid cognitive warfare. As Michael Dillon (1996: 21) puts it, “It does not matter what you secure so long as security itself is secured. That is to say, so long as things are made certain, mastered and thereby controllable.”

Therefore, if the “I” is to be a referent object of security, it must be treated as if it is certain, mastered, and controllable. Yet this objectification rests on the assumption of givenness that comes at the expense of reflexivity and disregards the subjective nature of the “I”. The Strong “I” thus reveals both the inversion and perversion of security. It inverts security by undermining the very subjectivity that grounds the certainty of the “I” in the first place. Moreover, it perverts security by stabilizing the “I” as both subject and object, as if this is ontologically possible. Within the cognitive technoscientific order, this contradiction intensifies as the “I” is increasingly valued as a controllable object rather than a thinking subject. Simply put, the Strong “I” approach renders the “I” vulnerable and manipulable.

Post-truth world: Denying the Weak “I”

Externally curatable, internally controllable, and fundamentally present, the Strong “I” is supposed to be the defining element of cognitive warfare and the central driver of its underlying cognitive technoscientific order. Yet as both tool and ideal of this order, the Strong “I” begins to unravel. The pursuit for greater certainty over reality and the self drives individuals to optimize and increasingly subordinate their cognitive capacities to powerful AI systems. In doing so, the “I” consciously transforms itself into a determinable object by constraining itself as a thinking subject. Consequently, it becomes simultaneously securable and manipulable, perverting the pursuit for security in the present technoscientific order.

The Strong “I” thereby emerges as ontologically unstable as it essentially suppresses its own subjectivity to become an object. This conscious suppression and incessant pursuit of objectification nevertheless reveal a deeper truth about the “I” – its reality as an incomplete subject.

Ironically, the clue is already within the Cartesian “I”. Reflexivity is presumed to be the defining feature of the “I” as a conscious subject, and its unique capacity to render itself into a definable object. Indeed, the proposition of “I think therefore I am” leverages reflexive thinking to demonstrate the immediate presence of the “I”. But this is the metaphysics of presence, and by suspending this mere assumption, reflexivity is then revealed not as the basis of certainty of the “I” but rather a paradox that challenges it. Structurally, reflexivity hinges on a contradiction at both logical and metaphysical levels. At the logical level, reflexivity makes the subject (definer) as not-a-subject (definition) at the same time for it to work; at the metaphysical level, it results in a subject aware of its own existence and an object that is not. Thus, the Cartesian “I” uses reflexivity to produce an indubitable and irreducible “I” without examining and accounting the paradoxical logic it was built upon.

Without the assumption of presence, reflexivity then brings about an “I” that still cannot be objectively described, but also an “I” that cannot subjectively affirm its own certainty. Thus, the “I” is irreducible but not indubitable, revealing an

unstable ontological structure in which the "I" cannot escape its own subjectivity. However, this does not only show the fundamental untenability of the Strong "I", but also ultimately the failure of the subject to reflexively render itself into an object which the pursuit for Strong "I" tries to mask.

But if the subject fundamentally fails to attain and sustain self-objectification, then this failure may be constitutive. This constitutive tension within the "I" is precisely what the psychoanalytic approach intends to reveal. Psychoanalysts such as Jacques Lacan and Slavoj Žižek (as cited in Edkins, 1999) conceptualize the "I" as a void marked by inconsistencies, relentlessly striving and failing to completely objectify itself. As Žižek (2020: 31) puts it, "a subject endeavors to adequately represent itself, this representation fails, and the subject is the result of this failure." On this account, it is this failure to be something that defines what a subject is. Thus, if the "I" is defined by the very instability the Strong "I" seeks to conceal, it is more precisely characterized as the Weak "I": an inherently incomplete and structurally unstable subject.

Thus, if reflexivity in the Strong "I" presupposes the subject's capacity to examine and define itself from an external standpoint, in the Weak "I" it instead reveals the impossibility of such standpoint.

Reflexivity does not enable the subject to view itself objectively, since it is always the subject performing the act in the first place. To assume otherwise without ontological guarantee external to the subject – such as God, language, or culture, or what Žižek (2012a) terms as the "Big Other" – is madness. Yet even with such symbolic support, it can only so far enable the "I" to realize its failure through the mediation of the symbols, structures, and frameworks of the Big Other since it is ultimately the "I" that leverages the Big Other. A gap therefore persists between the "I" as subject and the "I" as object, but this gap is not the result of the epistemological failure of the "I" rather its defining metaphysical structure. The "I" is the failure itself.

Hence, this paper establishes the second stage of its dialectical critique: the stabilization of the "I" as both irreducible and indubitable fundamentally fails due to the ontological instability of the "I". However, this raises a pertinent point. If the Weak "I" cannot be eliminated, why does the present technoscientific order centered on the idealization and exploitation of the Strong "I" continue to hold and entrench itself?

The persistence of the Strong "I" is driven by the desire of the Weak "I" for completion – there is no need if there is no lack. Consequently, the supposed completeness of the Strong "I" within the cognitive technoscientific order becomes the object of fantasy of the incomplete subject. This fetishization of the Cartesian ideal elevates the "I" itself into the "master signifier" of the ideological structure of the cognitive technoscientific order. As Žižek (2008) argues, a master signifier functions as a symbol that presents itself as truth while concealing the fact that it

is not a given but rather an empty concept defined by mere difference (i.e., what it is *is* a mere product of what it is not), and *retroactively* organizing other ideas and concepts as if they were parts of its absolute conception of reality. Thus, as a master signifier, the beliefs of the indubitable “I” about the world and itself become truths in its own perspective. This act of “transference” is how ideology entrenches itself: the moment in which a belief becomes an intrinsic nature of things. In this sense, the Strong “I” is a uniquely powerful ideology because it is grounded in self-delusion.

Through producing the myth of the Strong “I” by exploiting the desire of the “I” for completeness, the ideological structure of the present cognitive technoscientific order not only suppresses the Weak “I” but also generates the conditions for the emergence of a “post-truth” world that destabilizes this very structure in order to reinforce it. The post-truth condition is not the “death of truth” but rather its *personalization*, rendering truth itself a matter of self-identity. In this environment, the “I” becomes both the producer and arbiter of truth, undermining the objective scientific foundations of the cognitive technoscientific order while simultaneously affirming its Cartesian ideal of a self-determining individual. The result is a paradoxical psychosocial structure characterized by relativism and dogmatism, and permissiveness and self-optimization. Leveraging AI and its convergence with neurotechnology as psychographic instruments disguised as technologies of the self (i.e., practices and techniques in which the individual uses to examine themselves), the post-truth world compels individuals to conceal the Weak “I” with the fantasy of the Strong “I”.

Relativism is often regarded as the hallmark of a post-truth landscape characterized by pluralization of knowledge communities and de-monopolization of knowledge claims (Elias & Rohloff cited in Malcolm 2021; Schindler 2024). However, the post-truth world has not devalued truth, but rather it has transformed it into a fetishized commodity. The resurgence of populist, nationalist, and other extremist ideologies across both liberal and authoritarian societies has produced a fragmented global epistemic environment in which state and non-state actors compete to establish their respective worldviews as dogmatic truth. This competition fosters “filter bubbles” that radicalize existing beliefs through AI-enabled social media platforms with algorithmic recommendation systems, increasingly augmented by neuromarketing techniques (e.g., eye-tracking, biometric sensing, and facial coding), and maximize engagement by identifying and affirming what users already desire to believe based on their online behavior (Malcolm 2021; O’Neil 2016; Saavedra et al 2025).

Beneath the pervasiveness of dogmatism in the relativized epistemic conditions of the post-truth world lies what Schindler (2024) terms “dogmatic cynicism”: shared cynicism over truths unadulterated by political and selfish motives. From a psychoanalytical perspective, however, dogmatic cynicism is not merely an

uncritical stance towards one’s own critique of truth, but a mode of intensified personalization in which truth is fetishized as self-identity. The “I” thus retreats into itself with the truth and becomes its embodiment, transforming itself into a Strong “I”. It is the desire for self-objectification that renders relativism and dogmatism paradoxically compatible in the post-truth world, thereby leaving no space for the Weak “I”.

Permissiveness is often used to describe the cultural predisposition of the relativistic and irrational post-truth world. In this view, the “death” of truth has allowed the unrestricted pursuit for self-expression. Yet, as argued, this apparent “anything goes” environment is grounded in the personalization of truth, wherein the individual becomes the embodiment of their own beliefs. Permissiveness in the truth-obsessed post-truth world thus does not reflect the Dostoyevskian claim that “without God, everything is permitted” but rather its Žižekian subversion, “with God, everything is permitted” (Žižek 2012b). Permissiveness is thereby not merely descriptive but prescriptive, and it operates through two faces: (a) its totalitarian face carries with it an ideological imperative that instrumentalizes any desires as tools in its service (Žižek 2012b), and (b) its “friendly” face encourages the expression of individuality under the guise of freedom, rendering the psyche readable, transparent, and optimizable (Han 2017).

Either way, the post-truth world places the “I” in a condition in which freedom itself becomes a trap. With the generative capabilities of AI increasingly shaped by the fields of “affective computing” (i.e., systems designed to respond to human emotions) and wearable neural devices, AI emerges not only as a technology of the self but also an intrusive psychographic tool (Saavedra et al. 2025). It sustains the appeal and necessity of the Strong “I” through highly customized and addictive forms of user engagement. Thus, permissiveness entraps the “I” in a system wherein no matter what it chooses to be, it is always driven to pathologize its own instability.

Relativism and dogmatism affirm the Strong “I”, while permissiveness and self-optimization manage it. The paradoxical psychosocial structure of the post-truth world is thereby both the product of the cognitive technoscientific order and the mechanism through which it reproduces itself – thereby generating the very pathologization of the Weak “I” it claims to resolve. What sustains presence is absence; what produces absence is presence.

The self-undermining nature of the Strong “I” stems from its attempt to function simultaneously as subject and object in order to stabilize the ontological instability of the “I”. Yet, as the post-truth world reveals, this instability is precisely what makes the illusion of stability possible in the first place. The absence embedded within this instability enables the retroactive positing of the metaphysics of presence. The “I” projects its stabilizing presence as if it had always been given. However, this projection is a perversion that *conceals* the fact that the “I” is a failed

and incomplete subject. In this sense, the pursuit for the Strong “I” operates as a Foucauldian disciplinary mechanism that manages the Weak “I” by denying its reality while simultaneously exploiting its instability. A conception of security grounded in the Strong “I” is therefore *necessarily* perverted and self-undermining. Paradoxically, this also implies that full stabilization of the “I” as both irreducible and indubitable would require the elimination of its instability at the ontological level, effectively erasing subjectivity itself and producing a “hyperreal” object that appears more real than the real incompleteness of the “I”.

Neoliberal neuro-psychopolitics: Engineering the hyperreal “I”

The “I” is ontologically unstable, but this instability is its defining feature. The failure of the “I” to reflexively become an object is not a limitation of subjectivity but its very condition. The self emerges from the irreducible gap between subject and object – a gap reflexivity can never fully close. Consequently, self-objectification can only proceed incompletely, for the “I” that pursues it is itself marked by instability. Objectification through reflexivity is a necessarily self-undermining project, fundamentally revealing the “I” as a subject. This presents a profound challenge in conceptualizing cognitive warfare because it reveals the metaphysical limits of security itself.

As discussed, the Strong “I” conception of cognitive warfare – wherein the “I” is treated as both the referent object and conscious subject – is ontologically untenable. By rendering itself a controllable object, the “I” undermines its own subjectivity, but this undermining is necessary in sustaining the drive to be such an object. The Strong “I” is therefore a delusion sustained by the Weak “I” it seeks to deny.

If security is grounded in the metaphysics of presence that requires a controllable and determinate referent object, then a Strong “I” conception of cognitive warfare pushes the conception of security itself to its breaking point. A dilemma emerges. Cognitive warfare based on the Strong “I” implodes conceptually by becoming conflated with hybrid warfare and its subsets, and operationally by becoming self-undermining as illustrated by hyper war and algorithmic governmentality. Conversely, the Weak “I” resists ontologically, which results to its pathologization within the cognitive technoscientific order and its post-truth conditions. The dilemma, therefore, is not that the conceptualization of cognitive warfare fails, but rather its apparent resolution requires the elimination of the very thing it seeks to secure: the “I”.

The transformation of the “I” into an object leverages the very paradox that reveals its ontological instability. As discussed, the Cartesian view treats reflexivity as proof that the “I” can simultaneously exist as subject and object, whereas the Žižekian perspective exposes this as a myth. In both cases, reflexivity reveals not only the incompatibility between the “I” as a subject and its pursuit to be an

object, but also the dependence of that pursuit on the “I” being a subject. The “I” as a subject is therefore the reason why reflexivity is an open-ended and destabilizing process. But what if reflexivity can be managed to reach the point in which it ends, and the “I” finally achieves complete self-knowledge? That would essentially entail the “death” of the conscious subject.

On the contrary, transhumanism views the achievement of complete self-knowledge not as the death of the subject but as its transcendence. Through the enhancement and optimization of cognition, the “I” is expected to overcome its biological limitations and attain a higher form of consciousness, fulfilling and even surpassing the Cartesian ideal of self-mastery. This project entails not merely an enhancement of the human subject but its transformation into “divinity,” no longer requiring the presence of a Big Other to secure meaning, identity, and truth. As Žižek (2020: 57) describes, this resembles the “reconciliation of reality with Spirit,” the moment when “we renounce our separated individuality and become one with the Spirit which permeates reality itself, when our self-consciousness experiences itself as the self-awareness of reality itself.” From this perspective, the ontological instability of the “I” appears as the final obstacle to its transformation to a *Homo Deus* – a human-god capable of complete self-mastery and self-knowledge (Harari 2018).

For transhumanists such as Nick Bostrom (2014) and Ray Kurzweil (2005), the convergence of AI and neurotechnology – or, more broadly, the symbiosis of human and machine – constitutes the key to this transformation. But with the “I” becoming a pure object in effect, the subjectivity of the “I” dissolves. The individual then becomes a “wired brain,” which hypothetically enables them to control reality with their thoughts, while rendering these very thoughts controllable by machines. This culminates in the “singularity” or a “domain of global shared mental experience . . . which will function as a new form of divinity – my thoughts will be directly immersed in a global Thought of the universe itself” (Žižek 2020: 14).

This paper does not seek to determine whether such transformation is feasible in the present or immediate future. Rather, it argues that this possibility should be taken as more than a mere thought experiment. The ontological demands of a robust conceptualization, the operational sophistication required by a cognitive technoscientific order, and the personalization of truth in the post-truth world, all suggest that the necessary technoscientific and psychosocial conditions are already emerging. Yet these conditions do not eliminate the Weak “I”. Instead, they manage and reproduce its instability in ways that sustain the appeal and necessity of the Strong “I”. However, the prospect of deeper human-machine symbiosis points toward a more radical trajectory. As technoscientific and psychosocial conditions converge with the neoliberal imperative of optimization and competition, the personalized and permissive management of the “I” increasingly shifts from regulating its instability to eliminating the subjectivity that produces it.

Byung-Chul Han (2017) characterizes neoliberalism as a socioeconomic order that subverts freedom into an instrument of control – mobilizing the psyche as a productive force, and rendering individuals both agents and objects of their own exploitation. The neoliberal system both rationalizes and incentivizes the emergence of (a) the cognitive technoscientific order, which technologically optimizes the exploitation of the “I” through increasingly sophisticated technologies of the self, and (b) the post-truth world, which sustains the illusion of the Strong “I” through a psychosocial environment that affirms the individual as the source and arbiter of truth.

Together, these technoscientific and psychosocial structures underpin what Han (2017: 52) calls “psychopolitics” – a mode of governance of the neoliberal system that “stabilizes and perpetuates the prevailing system by means of psychological programming and steering” through the datafication of subjectivity and analytic power of big data. Yet psychopolitics remains a mechanism for managing rather than eliminating the Weak “I”. The ontological instability of the subject persists, and subjectivity itself cannot be fully reduced to data (Abbey 2025). Consequently, a residual space for resistance remains in the figure of the “idiot,” whom Han (2017: 55) describes as one who possesses the “courage to deviate from orthodoxy” through “silence, quiet and solitude.”

Neoliberal psychopolitics encourages self-fulfillment but the resulting emotional exhaustion and self-guilt provide individuals an opportunity for withdrawal and silence that ultimately subverts psychopolitics. However, if psychopolitics can be “radicalized” to promise unlimited optimization without burnout, the fantasy of the Strong “I” becomes increasingly unquestionable. This would require the integration of neurobiological interventions into psychopolitics, opening the prospect of “neurological reflexivity” as a more efficient path to self-optimization, whereby individuals become capable of modifying their own brains and “improving” their “somatic, bodily, embrained selves” (Rose & Abi-Rached 2014: 17).

Such a combination can be described as “neuro-psychopolitics” because it not only leverages neurotechnology to manage the individual but also harnesses (1) the psychographic capabilities of AI, and (2) the positivity of psychopolitics to render neurobiological intervention both appealing and necessary for achieving an idealized self. In doing so, it facilitates human-machine symbiosis as a project of self-optimization. Thus, through the intimate mechanism of neuro-psychopolitics, the “I” is driven by its own desire for completeness to eliminate its own subjectivity, transforming itself into a simulated object – a Hyperreal “I”.

Jean Baudrillard (1994) describes the hyperreal as a simulation that is neither true nor false, but a “simulacrum” – something detached from reality yet experienced as more real than the reality it claims to represent. The simulation becomes a reality of its own. Thus, the Hyperreal “I” emerges as an engineered simulation of the Strong “I”, produced through neuro-psychopolitics and facilitated by the

growing convergence of human and machine intelligence at the expense of subjectivity. Neuro-psychopolitics is no longer about sustaining the fantasy of the Strong "I" but rather transforming the "I" itself completely so that the Strong "I" is experienced as reality. This transformation does not make the "I" both subject and object. Instead, it displaces the "I" as a subject, transforming it into a simulated object, restructuring the ontological conditions of the "I" and giving rise to the Hyperreal "I". No longer a conscious subject, it persists as a technologically mediated simulation of selfhood. In this sense, the Hyperreal "I" represents the logical endpoint of a conception of cognitive warfare that seeks to preserve its distinctiveness and overcome the metaphysical limits of security by eliminating the "I" itself upon which both ultimately depend.

However, the Hyperreal "I" represents the ultimate perversion of security. Unlike the exploitation of the Strong "I" and denial of the Weak "I", the neuro-psychopolitical engineering of the Hyperreal "I" is not merely self-undermining but self-consuming. It no longer produces a conception of security whose pursuit undermines what it seeks to protect; rather, it rationalizes a conception of security that consumes its object in the very act of securing. This is perversion in its most radical form because it does not simply deny reality but replaces it with something deemed more real than reality. As Žižek (2020: 71) argues, human-machine symbiosis culminates in the loss of individuality as the "I" becomes part of the shared cognitive reality of the Singularity wherein "it is no longer I who experience myself as the agent of my thoughts, 'my' awareness is the direct awareness of a self-less system." Self-knowledge and autonomy collapse as the individual's belief over their own beliefs (Byrne 2011), and desire over their own desires (Frankfurt 1971) become products of neuro-psychopolitical engineering. Ironically, at the very moment the "I" appears to achieve the fullness of its own presence, it disappears as a subject altogether. The Hyperreal "I" is then the tragic conclusion of conceptualizing and mastering cognitive warfare – one must willingly sacrifice the very thing they intend to protect to protect it.

Summarizing this section, Table 2 highlights in one theoretical framework the different forms of "I" and their underlying structures and problems as well as how they lead to the perversion of security and what would that mean for cognitive warfare.

Table 2. Three Forms of “I” and Ontological Perversion of Security

Form of “I”	Ontological Structure	Ontological Dilemma	Mode of Perversion	Implication for Cognitive Warfare
Strong	Subject and Object <i>(Irreducibility and Indubitability)</i>	Incompatibility of pursuing self-objectification and subjectivity	Optimization by the cognitive technoscientific order	Self-undermining
Weak	Incomplete Subject <i>(Irreducibility Only)</i>	Impossibility of complete self-objectification of the subject	Pathologization by the post-truth world	Self-concealing
Hyperreal	Simulated Object <i>(Indubitability Only)</i>	Elimination of subjectivity in pursuit of complete self-objectification	Simulation through neuro-psychopolitics	Self-consuming

Source: Author

Transmorphance tragedy: A critique of adaptive strategy for cognitive warfare

This final section critiques one of the emerging defense theories for cognitive warfare within NATO academia: the adaptive structure-centric approach based on the concept of transmorphance. Korobeynikov, Davydiuk, and Mokhor (2026: 14) define transmorphance as “the capacity for profound structural transformation without forfeiture of identity.” This section argues that transmorphance as a theoretical framework for an adaptive cognitive defense strategy (1) scales the ideology of the Strong “I” from the individual to the systemic level, and (2) reproduces the same ontological dilemma, culminating in the system’s self-consumption and transformation into a Hyperreal “I”.

A structure-centric approach to cognitive warfare treats the system as the primary referent object. Central to this conception are what Korobeynikov, Davydiuk, and Mokhor (2026: 11) call “invariants,” which they define as “epistemological assumptions, axiological hierarchies, normative expectations, symbolic constructions of identity and teleological vectors.” These interconnected structures organize how the system interprets information, maintains internal order, distinguishes itself from other systems, and constitutes the identity of the system itself. In doing so, invariants do not merely stabilize the system as an object of security; they also render it into an agential subject capable of interpreting information, regulating its own internal cognitive structures, and pursuing self-governance. In psychoanalytical terms, the system becomes an “I”. However, when the system as

an "I" is presumed as to have an underlying identity, this entails that the system renders itself not only self-coherent but also self-certain. This is thereby the Strong "I" albeit scaled up to the systemic level.

The Strong "I" framing is evident in how Korobeynikov, Davydiuk, and Mokhor (2026) conceptualized cognitive warfare and its solution. They identify the strategic aim of cognitive warfare from this approach as "cognitive decoherence," which they define as "a state characterized by a loss of coherence among invariants, whereby the system forfeits its capacity for integrated self-description" (Korobeynikov, Davydiuk & Mokhor 2026: 7) – the destabilization of how the system makes sense of the world and itself. Therefore, addressing this threat meant ensuring the stability of the system. But considering the system's multidimensional layers of invariants, its stability depends on its capacity to manage change from multiple vectors while sustaining its identity. Thus, a system must not only be able to absorb the impact of cognitive attacks (i.e., "cognitive resilience") but also evolve to continuously make itself resilient from such attacks while maintaining its distinctive identity (i.e., transmorphance).

As a mechanism of pursuing the Strong "I", transmorphance seeks to preserve the system as both subject and object. Yet because transmorphance operates within the same ideological conditions that sustain the fantasy of the Strong "I" – the cognitive technoscientific order, post-truth world, and emergence of neoliberal neuro-psychopolitics – it inevitably reproduces the ontological problem of stabilizing the "I". This dilemma lies not merely on the ontological incompatibility of subject and object, but also in the very attempt to render the "I" both simultaneously. Reflexivity then becomes instrumentalized either to mask the instability of the "I" or eliminate the "I" as a conscious subject altogether. Consequently, a "transmorphic" system generates a mode of cognitive defense that is either self-undermining or self-consuming. The following discussion demonstrates how transmorphance leads to a cognitive defense that either undermines or even consumes the "I" itself.

On the surface, transmorphance enables a system to navigate amid uncertainty through continuous structural adaptation. As Korobeynikov and Mokhor (2026: 5) argue, "transmorphic systems engage in continuous structural transformation, expanding the domain of attainable states and generating novel possibilities for functioning." Such a framework fits well in a chaoplexic technoscientific order, where the primary challenge is managing the complexity of interconnected information networks. However, the emergence of a global cognitive ecosystem and a cognitive technoscientific order fundamentally changes the problem. A transmorphic system must not only adapt to an increasingly uncertain external environment by reconfiguring its interconnected invariants, but it must also ensure that this internal restructuring strengthens the stability of its identity.

As cognitive warfare increasingly targets a system's capacity to make sense of both its environment and itself, it demands increasingly instantaneous information processing. Preserving identity therefore requires continual self-reconfiguration and growing reliance on AI systems with superior computational capabilities. This creates a dilemma: failure to stabilize identity produces cognitive decoherence, while success progressively transfers reflexive self-governance to AI. In either case, the system is compromised – the difference is that the successful system fantasizes its technologically sustained identity as its own.

But if the cognitive technoscientific order demands the continuous optimization of a system's internal reflexive mechanisms, the intertwined post-truth world radicalizes the system's identity into a totalizing ideology. Adaptation thereby becomes not only instantaneous but existential. Such conditions would seemingly paralyze the system by requiring constant restructuring while preserving identity. Yet the post-truth condition resolves this tension by making identity itself increasingly ideological. Its underlying permissiveness allows the system to treat its invariants as indefinitely transformable, since the preservation of an ideological identity can justify even contradictory structural changes so long as they sustain the illusion of unity and continuity of that identity.

Thus, the vulnerability of a transmorphic system to cognitive attacks stems from its transmorphic structure. While rigid systems such as authoritarian regimes are particularly susceptible to cognitive decoherence because they lack the capacity to proactively process and assimilate disruptions that challenge their absolutist identities, pluralistic systems appear more resilient precisely because they can reconfigure themselves. Consequently, cognitive attacks against such systems are less likely to target identity directly than the coherence among interconnected layers of invariants, fostering distrust and polarization in how the system understands itself (Korobeynikov, Davydiuk & Mokhor 2026).

To counter this, the system's invariant architecture requires it to be flexible to absorb and assimilate disruptions, and to continually reorganize itself while preserving a coherent identity. Yet as cognitive attacks increasingly overwhelm the system's capacity to process information, adaptation becomes not only operationally instantaneous but also ontologically existential. The more a system restructures itself to preserve its identity, the more it exposes that identity as contingent rather than essential, and ultimately, its transmorphic nature as structurally self-undermining rather than self-reinforcing.

Hence, a transmorphic system renders itself vulnerable to cognitive attacks because it destabilizes what must remain stable while stabilizing what is fundamentally unstable. Its coherence is sustained less by a determinate identity than by ideological fantasy of one. Consequently, the more cognitive attacks target the system's invariant architecture, the more it is compelled to adapt, thereby producing an increasingly self-alienating cognitive structure. Yet this very adaptation

intensifies the effort to sustain the fantasy of a coherent identity, rendering the system's invariant architecture progressively more fragile and singular like that of centralized systems of authoritarian regimes.

Indeed, transmorphance is advanced as a core principle for an adaptive theory of cognitive defense, particularly for pluralistic systems whose cognitive coherence depends on trust and a shared sense of identity across multiple interconnected layers of invariants. It promises to preserve this coherence amidst the deceptive and manipulative attacks by supposedly enabling the system to reflexively distinguish what can and cannot be transformed without compromising its own identity. This presupposes a degree of structural freedom that allows the system to continually reconfigure itself. However, when this structural freedom becomes the ontological core of the system's identity, its adaptive capabilities becomes both powerful and tragic.

Liberal democratic regimes exemplify both the power and tragedy of transmorphance. As adaptation becomes increasingly instantaneous and existential, liberal societies preserve identity by rendering their invariant architecture highly transformable. Freedom thereby ceases to constrain contradiction and instead justifies it. Contradictions become evidence of openness rather than signs of contingency, allowing freedom to produce *un*-freedom. As Žižek (2026: 3-4) argues, this is not merely "fascism with a liberal mask, but liberalism brought to (fascist) conclusion."

When a liberal society elevates freedom into an unquestionable dogma, it loses its very freedom to interrogate what freedom itself means. It becomes incapable of subjecting its own identity to the Socratic questioning "what do you mean by . . . ?" As Žižek (2026) argues, the failure to recognize the contingency of freedom renders liberal societies vulnerable precisely through their unquestioning zeal towards it.

Consequently, the liberal fascist system internalizes freedom simultaneously as its core identity and as the mechanism through which that identity is reproduced. Control is thereby experienced as freedom. As the systemic embodiment of the Strong "I", it continuously undermines itself as it pushes its transmorphic capability to "metastasize" to strengthen the delusion of a coherent identity. This amplifies the system's susceptibility to cognitive attacks while obscuring that vulnerability from itself. Attacks no longer need to undermine the system's identity; they merely need to affirm it. By appealing to rather than disrupting the system's self-understanding, transmorphance ceases to function as a principle of cognitive defense and instead becomes an increasingly effective technique of cognitive manipulation.

Nonetheless, under the intertwined conditions of cognitive technoscientific order and the post-truth world, a transmorphic system becomes not only self-undermining but also self-consuming. Neoliberalism via neuro-psychopolitics does not simply amplify these conditions that sustain the fantasy of the Strong "I", but also drives that very fantasy towards its radical conclusion – the Hyperreal "I".

As discussed, neuro-psychopolitics, through convergence of neurotechnology and AI-driven psychopolitics, provides the mechanism for engineering this delusion into a simulation through eliminating subjectivity itself. Thus, by internalizing its structural freedom as its core identity, a transmorphic system becomes susceptible to the appeal of neuro-psychopolitics for self-expression and self-optimization. The system continuously reconfigures itself until it becomes free not merely to transform itself, but ultimately free of itself. The boundaries of the system collapse, and the system itself merges with the very conditions that radicalized it. The system here is erased, rendered into a simulation of its own identity.

This hyperreal system finds its political expression in Bell and Taillandier's (2025) notion of "cosmos-politanism," a post-national order with transhumanist aspirations to transcend existing political identities through technological transformation. In its libertarian variant, represented by "extropianism," freedom is realized not through the continual adaptation of the system but through the dissolution of its boundaries. Mediated by neuro-psychopolitics, both the system and the individuals within it become simulations of their own identities.

By demonstrating how transmorphance makes the system an "I" self-undermining and self-consuming, this critique calls into question not only the viability of an adaptive strategy for cognitive coherence and resilience, but also the conceivability of cognitive warfare itself. This directly questions the view of Korobeynikov, Davydiuk, and Mokhor (2026) that transmorphance enables a distinctive and operationalizable conceptualization of cognitive warfare by identifying the object of attack (invariants), the mechanism (cascading propagation across interlayer linkages), and the strategic objective (cognitive decoherence). But as transmorphance transposes the ideology of the Strong "I" from the individual to the system, it reproduces its underlying ontological contradictions, rendering cognitive warfare self-undermining and self-consuming, and culminating in the perversion of security wherein the referent object itself is its own threat.

Hence, this paper establishes the last stage of its dialectical critique: affirming the stability of the "I" in pursuit of conceptualizing cognitive warfare, despite the ontological instability of the "I" itself, demonstrates the conceptual and practical perversion of security in the context of the growing hackability of the mind in cognitive warfare.

Conclusion: Weak "I" as anti-theory of cognitive warfare?

Through the dialectical discussion of this paper, it has demonstrated how conceptualizing cognitive warfare based on the Cartesian cogito or Strong "I" opens the possibility of a distinctive understanding of this warfare while simultaneously undermining and perverting security itself.

First, conceptualizing cognitive warfare requires the integration of the Strong “I” perspective. Yet through a Žižekian psychoanalytical lens and post-structuralist analyses on the cognitive technoscientific order, the post-truth world, and neo-liberalism, this paper has shown that the Strong “I” is ontologically untenable and ultimately masks the reality of the Weak “I”.

Second, the stabilization of the “I” into its strong form affirms the metaphysics of presence while pushing security to its metaphysical breaking point. Sustaining this stabilization requires a delusion that is first self-undermining, and ultimately self-consuming, culminating in the engineering of the Hyperreal “I” – a controllable simulation of the “I”.

Third, at the systematic level, the concept of transmorphance demonstrates how the pursuit of the Strong “I” culminates in the Hyperreal “I”. Although the latter appears to provide the stable referent object required to conceptualize cognitive warfare, it does so only by eliminating the very subjectivity that makes the “I” worth securing.

The contribution of this paper is therefore *not* a new theory of cognitive warfare but a critique of the direction of its conceptualization efforts. This can be criticized as counter-productive, but what this contribution mainly challenges is the Strong “I” approach to these efforts. Questioning the Strong “I” opens the conceptual space for exploring the Weak “I” as a possible “anti-theoretical” understanding of both cognitive warfare and security itself – one that emphasizes questioning rather than affirmation, instability over presence. Operationalizing such an approach would require radically different technologies of the self – ones that reveal rather than deny the Weak “I”. Exploring such possibilities remains a task for future research.

This paper will likely appear unnecessarily apocalyptic to traditional security theorists and defense practitioners, particularly if it is read as claiming that cognitive warfare represents the final form of warfare. What this paper ultimately claims is that addressing cognitive warfare may require questioning interconnected and entrenched metaphysical assumptions about subjectivity, security, and reality, and entertaining the possibility of an alternative yet radical path forward.



Funding

This research received no external funding.

Conflict of interest statement

No conflict of interest was reported.

Disclaimer

The views expressed in this article are solely those of the author and do not reflect the official position of the Philippine Department of National Defense.

Data availability statement

No supplementary data associated with the article.

AI usage declaration

The author also acknowledges the use of large language models (LLMs), such as ChatGPT and Gemini, which assisted in improving the readability, tone consistency, and logical clarity of the manuscript. All conceptual and analytical content, however, remains entirely the author's own.

Acknowledgements

This author would like to thank his thesis advisor, Dr. Shunji Cui of Zhejiang University, for her support since the earliest formation of the basic ideas of this article. He also extends his appreciation to Dr. Natalie Meyers and Dr. Gauthier Chassang of the AI-Data Visitation Working Group (AIDV) as well as to the CEJISS reviewers and editors for providing their insights and comments. The author is also grateful for the instructive suggestions on the overall flow, tone and substance of the article made by Ms. Pamela Bagon, Ms. Monica Valerio, and Mr. Joachim Melo.



LUIS JACOB RETANAN is an independent researcher on cognitive security and artificial intelligence (AI) based in the Philippines. His research primarily investigates the metaphysical questions and strategic challenges posed by the emergence of cognitive warfare in the midst of AI-neurotech convergence today. He is a research fellow of the AI-Data Visitation Working Group of the Research Data Alliance (RDA), a Planning Officer of the Philippine Department of National Defense (DND), and a Qiskit Advocate of IBM Quantum. He is also an alumnus of Zhejiang University and the University of the Philippines.

References

- Abbey, M. (2025): The Void of Surveillance: Machine Learning, Psychoanalysis, and the Misreading of Desire. *Surveillance & Society*, 23(2), 169–181.
- Allenby, B. (2021): World Wide Weird: Rise of the Cognitive Ecosystem. *Issues in Science and Technology*, 37(3), 34–44.

- Bahenský, V. (2025): Conceptual Quality in Security and Defence Practice: The Case of Hybrid Warfare. *Central European Journal of International and Security Studies*, 19(4), 5–32.
- Baudrillard, J. (1994): *Simulacra and Simulation*. Translated by S. F. Glaser. Ann Arbor: University of Michigan Press. Original work published 1981.
- Bell, D. & Taillandier, A. (2025): Cosmos-politanism: Transhumanist Visions of Global Order from the First World War to the Digital Age. *Perspectives on Politics*, 23(3), 1071–1088.
- Bernal, A., Carter, C., Singh, I., Cao, K. & Madreperla, O. (2020): Cognitive Warfare: An Attack on Truth and Thought. *Technical report*. NATO Innovation Hub & Johns Hopkins University.
- Bostrom, N. (2014): *Superintelligence: Paths, Dangers, Strategies*. Oxford: Oxford University Press.
- Bousquet, A. (2022): *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. 2nd ed. Oxford: Oxford University Press.
- Byrne, A. (2011): Transparency, Belief, Intention. *Proceedings of the Aristotelian Society*, 85, 201–221.
- Danyk, Y. & Briggs, C. M. (2023): Modern Cognitive Operations and Hybrid Warfare. *Journal of Strategic Security*, 16(1), 35–50.
- Deppe, C. & Schaal, G. S. (2024): Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept. *Frontiers in Big Data*, 7, <accessed online: <https://doi.org/10.3389/fdata.2024.1452129>>.
- Derrida, J. (2001): *Writing and Difference*. Translated by A. Bass. London: Routledge. Original work published 1967.
- Descartes, R. (1996): *Meditations on First Philosophy: With Selections from the Objections and Replies*. Translated by J. Cottingham. Cambridge: Cambridge University Press. Original work published 1641.
- Dillon, M. (1996): *Politics of Security: Towards a Political Philosophy of Continental Thought*. London: Routledge.
- Edkins, J. (1999): *Poststructuralism and International Relations: Bringing the Political Back In*. Boulder: Lynne Rienner Publishers.
- Eyre, H. A., Hynes, W., Ling, G. F. L., Occhipinti, J.-A., Ayadi, R., Matthews, M. D., Abbott, R. & Love, P. (2023): From Neuroweapons to 'Neuroshields': Safeguarding Brain Capital for National Security. *Rice University's Baker Institute for Public Policy*, 10 August, <accessed online: <https://doi.org/10.25613/MS7G-YX19>>
- Fabian, S. (2019): The Russian Hybrid Warfare Strategy – Neither Russian nor Strategy. *Defense & Security Analysis*, 35(3), 308–325.
- Farahany, N. (2023): *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology*. New York: St. Martin's Griffin.
- Frankfurt, H. (1971): Freedom of the Will and the Concept of a Person. *Journal of Philosophy*, 8(1), 5–20.
- Giddens, A. (1991): *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Cambridge: Polity Press.

- Han, B.-C. (2017): *Psychopolitics: Neoliberalism and New Technologies of Power*. Translated by E. Butler. London: Verso. Original work published 2014.
- Harari, Y. (2018): *Homo Deus: A Brief History of Tomorrow*. New York: Harper Perennial.
- Heidegger, M. (2013): *The Question Concerning Technology and Other Essays*. Translated by W. Lovitt. New York: Harper Perennial Modern Classics. Original work published 1954.
- 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).
- Kant, I. (1998): *Critique of Pure Reason*. Translated and edited by P. Guyer & A. W. Wood. Cambridge: Cambridge University Press. Original work published 1781/1787.
- Korobeynikov, F. & Mokhor, V. (2026): Adaptive Security: Strategic Principles for Complex Socio-Technical Systems. *Royal Society Open Science*, 13(1), 251481.
- Korobeynikov, F., Davydiuk, A. & Mokhor, V. (2026): Ontological Foundations of Cognitive Warfare. *NATO Cooperative Cyber Defence Centre of Excellence*, <accessed online: https://ccdcoe.org/uploads/2026/04/ONTOLOGICAL_FOUNDATIONS_OF_COGNITIVE_WARFARE.pdf>
- Kurzweil, R. (2005): *The Singularity Is Near: When Humans Transcend Biology*. New York: Viking.
- Libiseller, C. (2023): 'Hybrid Warfare' as an Academic Fashion. *Journal of Strategic Studies*, 46(4), 858–880.
- Malcolm, D. (2021): Post-Truth Society? An Eliasian Sociological Analysis of Knowledge in the 21st Century. *Sociology*, 55(6), 1063–1079.
- Mitzen, J. (2006): Ontological Security in World Politics: State Identity and the Security Dilemma. *European Journal of International Relations*, 12(3), 341–370.
- O'Neil, C. (2016): *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.
- Rose, N. & Abi-Rached, J. M. (2014): *Governing Through the Brain: Neuropolitics, Neuroscience and Subjectivity*. Cambridge Anthropology, 32(1), 3–23.
- Rowlands, M. (2010): *The New Science of the Mind: From Extended Mind to Embodied Phenomenology*. Cambridge, MA: MIT Press.
- Saavedra, A., Chocarro, R., Cortinas, M. & Rubio, N. (2025): Exploring Unconscious User Responses to Affective Computing in Interactive Prototypes: A Consumer Neuroscience Study. *Behaviour & Information Technology*, 44(20), 5028–5047.
- Schindler, S. (2024): Post-Truth Politics and Neoliberal Competition: The Social Sources of Dogmatic Cynicism. *International Theory*, 16(1), 102–121.
- Søndergaard, S. (2025): Cognitive Warfare: NATO Chief Scientist Research Report. NATO Science and Technology Organization, Office of the Chief Scientist, <accessed online: <https://www.nato.int/content/dam/nato/webready/documents/sto/chief-scientist-report-cognitive-warfare.pdf>>

Wrangel, C. (2024): The Biopolitics of Algorithmic Governmentality: How the US Military Imagines War in the Age of Neurobiology and Artificial Intelligence. *Security Dialogue*, 55(4), 349–367.

Žižek, S. (2006): *The Fundamental Perversion*. In: Ayerza, J. (ed.): Lacanian Ink. London: Lacanian Ink, 114–129.

Žižek, S. (2008): *The Sublime Object of Ideology*. London: Verso.

Žižek, S. (2012a): *Less Than Nothing: Hegel and the Shadow of Dialectical Materialism*. London: Verso.

Žižek, S. (2012b): *The Pervert's Guide to Ideology*. Video. YouTube, <accessed online: <https://www.youtube.com/watch?v=ONGYW7aHK38>>.

Žižek, S. (2020): *Hegel in a Wired Brain*. London: Bloomsbury Academic.

Žižek, S. (2026): *Liberal Fascisms*. London: Bloomsbury Academic.