BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

Cognitive Warfare and Strategic Uncertainty: Planning under the Threshold in Open Societies

Luis VAZ, MSc*
LTC Cav Pedro FERREIRA, PhD**
*Portuguese Military Academy Research Centre
e-mail: lvazsantos@gmail.com
**Portuguese Military Academy Research Centre
e-mail: ferreira.pna@exercito.pt

Abstract

This article examines the way in which open societies can design long-range strategy in the cognitive domain under conditions of strategic uncertainty and persistent sub-threshold competition. Using a conceptual-doctrinal research design grounded in strategic analysis, future-oriented synthesis, and selected operational illustrations from contemporary information competition, the article develops a framework for understanding Cognitive Warfare (CogWar) as a contest over tempo, attention, legitimacy, and decision quality. The analysis advances a double diagnosis. First, the openness paradox: unprecedented connectivity and information abundance coexist with fragmentation, polarisation, and degraded collective sensemaking. Second, the deterrence paradox: a strategic culture centred on the avoidance of escalation incentivises adversaries to employ indirect, deniable methods, operating below the threshold of armed conflict. Drawing on classical strategic theory, information operations literature, and contemporary examples including election interference, synthetic media, and crisis-driven narrative competition, the article argues that cognition has become both the strategic centre of gravity and a principal vulnerability in liberal democracies.
The article contributes in three ways. First, it reframes CogWar less as narrative control and more as a struggle over decision tempo and institutional orientation. Second, it connects deterrence theory and the indirect approach to contemporary socio-technical battlefields shaped by algorithmic acceleration and ambiguity. Third, it proposes doctrinal design principles for cognitive defence compatible with democratic governance, emphasising legitimacy, anticipation, coalition interoperability, and institutional coherence. The article concludes that effective cognitive defence depends less on information dominance than on the ability of open societies to sustain lawful speed, strategic orientation, and public trust under conditions of persistent uncertainty.

Keywords:
Cognitive Warfare; Sub-Threshold Competition; Strategic Foresight; Futures Studies; OODA Loop; Cognitive Security.

Article info
Received: 31 March 2026; Revised: 3 April 2026; Accepted: 21 May 2026; Available online: 30 June 2026

Citation: Vaz, L., and P. Ferreira. 2026. "Cognitive Warfare and Strategic Uncertainty: Planning under the Threshold in Open Societies." *Bulletin of "Carol I" National Defence University*, 15(2): 229-256. https://doi.org/10.53477/2284-9378-26-26

Introduction

This article examines the way in which open societies can design long-range strategy in the Cognitive Warfare (CogWar) domain under conditions of strategic uncertainty, persistent sub-threshold competition, and accelerating technological change. The relevance of the problem rests on a double paradox. First, liberal-democratic societies have never been more connected or information-rich, yet public space is increasingly fragmented, polarised, and exposed to degraded collective sensemaking. Second, the openness that sustains innovation, pluralism, and civic participation also creates vulnerabilities exploitable by adversaries operating through ambiguity, deniability, and information asymmetry. In this environment, cognition – understood as the capacity of societies and institutions to orient, decide, and sustain legitimacy under pressure – emerges simultaneously as a strategic centre of gravity and a principal vulnerability.

The strategic significance of this shift has become increasingly visible across recent crises and geopolitical disputes. Russian interference campaigns in electoral processes, the information contestation surrounding the COVID-19 pandemic, and the rapid circulation of synthetic media during ongoing conflicts such as the war in Ukraine illustrate how contemporary competition increasingly targets perception, orientation, and decision tempo rather than territorial control alone. These operations frequently unfold below the threshold of armed conflict, exploiting legal ambiguity, institutional seams, and the slower deliberative rhythms of open societies.

At the same time, technological acceleration is compressing the interval between signal generation, narrative amplification, and strategic effect. AI-assisted content production, automated distribution systems, algorithmic engagement mechanisms, and synthetic media have significantly reduced the cost and time required to shape public attention and distort institutional orientation (Chesney and Citron 2019; Singer and Brooking 2018). In practical terms, this means that the decisive variable is often no longer the factual superiority of information itself, but the speed with which coherent interpretations can be formed, legitimised, and operationalised.

Read through a Clausewitzian lens, the character of conflict adapts to socio-technical transformation while remaining subordinate to political purpose (Clausewitz 1976). Contemporary cognitive competition, therefore, does not reflect the disappearance of strategic logic, but its migration into increasingly dilated battlefields extending across institutions, media ecosystems, digital platforms, and everyday social practices. Under these conditions, the strategic problem is no longer reducible to "countering disinformation" as an isolated activity, but concerns the broader capacity of open societies to sustain orientation, legitimacy, and decision quality under persistent information pressure.

Research Design and Methodological Approach

This article adopts a conceptual-doctrinal and exploratory research design grounded in strategic analysis, future-oriented synthesis, and interdisciplinary literature integration. Rather than pursuing empirical causal testing or operational modelling, the study seeks to clarify how defence institutions in open societies can think about long-range cognitive strategy under conditions of uncertainty and sub-threshold competition.

Methodologically, the article combines four analytical pillars. First, it draws on classical strategic theory, particularly the Clausewitzian concepts of war, deterrence theory, and the indirect approach (Clausewitz 1976; Hart 1967; Schelling 1966; Beaufre 1965). Second, it incorporates contemporary literature on information operations, media ecosystems, algorithmic amplification, and disinformation dynamics (Benkler, Faris, and Roberts 2018; Rid 2020; Singer and Brooking 2018). Third, it integrates conceptual perspectives associated with strategic foresight and Futures Studies, particularly regarding uncertainty, horizon scanning, and anticipatory governance (Schoemaker 1995; Cascio 2020). Finally, the article engages selected operational illustrations from contemporary crises and geopolitical disputes – including electoral interference, pandemic-related narrative competition, and synthetic media proliferation – not as formal case studies, but as analytical examples intended to ground the conceptual discussion in observable strategic dynamics.

The article employs a limited and practice-oriented Futures Studies perspective. The purpose is not predictive forecasting, but the development of anticipatory orientation mechanisms capable of reducing strategic surprise and preserving institutional adaptability under volatile conditions. Accordingly, the proposed approach emphasises horizon scanning, alternative scenarios, signposts, and iterative reassessment integrated into institutional decision cycles.

Several limitations should be acknowledged. Given its conceptual and doctrinal nature, the article does not propose an operational playbook for tactical execution units, nor does it rely on classified material, quantitative modelling, or field-based empirical research. Its primary focus remains at the level of governance, strategic culture, and institutional design within NATO and EU-oriented open societies. The article, therefore, prioritises analytical coherence and doctrinal applicability over predictive precision or operational prescription.

Conceptual Boundaries and Contribution

For the purposes of this article, Cognitive Warfare refers to activities intended to influence, degrade, or disrupt perception, orientation, and decision-making processes across civil-military environments. The concept is treated not merely as strategic communication or disinformation, but as a broader contest over tempo, attention, legitimacy, and institutional coherence. Open societies are understood as liberal-democratic systems characterised by plural media ecosystems, legal constraints on state authority, institutional transparency, and politically contested public spaces.

The article contributes in four ways. First, it reframes CogWar less as a struggle for narrative dominance and more as a contest over decision tempo and strategic orientation. Second, it links the contemporary return of the indirect approach to the deterrence logic and escalation constraints that structure sub-threshold competition in open societies. Third, it integrates Futures Studies and strategic foresight into the cognitive domain through a lightweight anticipatory framework compatible with democratic governance. Finally, it proposes doctrinal design principles centred on legitimacy, lawful speed, coalition interoperability, and institutional coherence as foundations for long-range cognitive defence.

Structure of the Article

The article proceeds in four sections. The first section, "Double Paradoxes: Establishing the Problem in Open Societies," develops the openness paradox and the deterrence paradox as the structural conditions shaping contemporary cognitive competition. The second section, "Deterrence Fixation and the Return of the Indirect Approach in Dilating Battlefields," examines how ambiguity, deniability, and tempo function within sub-threshold strategic competition. The third section analyses the techno-operational environment of CogWar, focusing on speed, scale, scope, attribution challenges, and planning horizons. The fourth section, "From Method to Doctrine," develops doctrinal principles for cognitive defence in open societies, emphasising legitimacy, anticipation, institutional coordination, and coalition alignment.

Rather than offering technological solutions or operational recipes, the article argues that effective cognitive defence ultimately depends on the ability of open societies to sustain strategic orientation, lawful speed, and public legitimacy under conditions of persistent uncertainty and accelerated information competition.

Double Paradoxes: Establishing the Problem in Open Societies

This section develops the article's central analytical diagnosis: contemporary CogWar emerges from the interaction between two structural paradoxes shaping open societies in accelerated information environments. The first is the openness paradox: the same conditions that enable democratic pluralism, innovation, and large-scale participation also generate fragmentation, information volatility, and vulnerabilities exploitable through manipulation and ambiguity. The second is the deterrence paradox: the long strategic emphasis on escalation avoidance and deterrence stability has incentivised adversaries to pursue indirect, deniable, and sub-threshold forms of competition designed to erode orientation and decision quality without triggering conventional military response.

Taken together, these paradoxes relocate the strategic centre of gravity from primarily physical assets toward societal cognition and institutional decision-making. The decisive contest increasingly concerns not only military capabilities or territorial control, but the ability of open societies to sustain coherent orientation, legitimacy, and operational tempo under persistent information pressure.

The Openness Paradox: Abundance with Fragmentation

Over recent decades, networked digital infrastructures have dramatically expanded access to information and participation in public discourse. Generally speaking, such openness should strengthen democratic accountability, diversify knowledge production, and improve collective learning. Yet, the same technological transformations have also altered the conditions under which public reasoning occurs. Information itself is no longer scarce; attention has become the limiting strategic resource (Simon 1971).

Contemporary digital platforms operate according to engagement-driven logics that prioritise salience, emotional activation, and continuous interaction rather than epistemic quality or coherence. Algorithmic systems amplify content capable of generating rapid behavioural responses, frequently rewarding novelty, outrage, identity affirmation, and emotional polarisation (Sunstein 2009; Pariser 2011). Over time, these dynamics contribute to fragmented information ecosystems in which different social groups increasingly operate within partially disconnected interpretive environments.

The strategic significance of this fragmentation lies not merely in the circulation of false information but in the degradation of shared orientation mechanisms. Public discourse becomes more volatile and temporally compressed, while institutional processes – investigation, verification, deliberation, and consensus-building – retain comparatively slower rhythms. In operational terms, this creates widening asymmetries between the speed of narrative circulation and the speed of institutional sensemaking.

The COVID-19 pandemic illustrated this dynamic with unusual clarity. During the global health crisis, institutional communication competed simultaneously against conspiracy narratives, peer-to-peer amplification, emotionally charged content, and conflicting expert interpretations circulating across digital platforms. The World Health Organisation itself characterised the phenomenon as an "infodemic," recognising that the challenge extended beyond misinformation narrowly understood and involved the broader erosion of orientation under conditions of information abundance and accelerated uncertainty (World Health Organization 2020).

Competing narratives regarding vaccines, public health restrictions, and institutional credibility frequently spread faster than formal verification processes, contributing to distrust, polarisation, and difficulties in coordinated policy implementation.

Research on "network propaganda" further suggests that contemporary manipulation often succeeds less through direct persuasion than through salience disruption and interpretive overload (Benkler, Faris, and Roberts 2018). In many cases, the objective is not to convince the public of a coherent alternative reality, but to fragment attention, increase uncertainty, and degrade confidence in institutional arbiters. Under such conditions, the strategic contest increasingly concerns who frames first, who sustains interpretive tempo, and whose orientation mechanisms remain operational under stress.

Technological acceleration amplifies these vulnerabilities. AI-assisted content generation, synthetic media, automated amplification systems, and low-cost distribution infrastructures significantly reduce barriers to influence operations (Chesney and Citron 2019). Content that once required substantial organisational resources to produce and disseminate can now be generated rapidly and circulated globally at a marginal cost close to zero. The proliferation of deepfake technologies and AI-generated political material during electoral cycles and geopolitical crises further compresses verification windows, increasing pressure on institutions already operating under time constraints.

Yet openness remains simultaneously a vulnerability and a strategic strength. Open societies possess capacities for redundancy, distributed scrutiny, peer correction, and adaptive learning unavailable to more centralised systems. Independent media, plural institutions, civil society networks, and coalition-based verification mechanisms can increase resilience – provided that institutional legitimacy and decisional tempo are preserved. The openness paradox, therefore, does not imply that democratic systems are inherently weaker, but rather that their resilience depends increasingly on the quality and speed of collective orientation under accelerated information conditions.

The Deterrence Paradox: Escalation Avoidance and Sub-threshold Strategy

The second paradox emerges from the strategic logic of deterrence and escalation management that has shaped Western security thinking since 1945. Nuclear deterrence and escalation avoidance contributed significantly to preventing direct great-power confrontation. However, this strategic success also displaced competition into domains operating below the threshold of conventional armed conflict, where ambiguity, deniability, and incremental pressure could be employed at lower political and strategic cost (Freedman 2013; Mazarr 2015).

Contemporary adversaries increasingly exploit this environment through indirect approaches combining information, cyber, diplomatic, economic, and psychological instruments calibrated to remain beneath formal escalation thresholds. In these contexts, ambiguity itself becomes operationally valuable. Attribution uncertainty slows institutional response, complicates coalition coordination, and raises the political costs associated with retaliation or escalation.

Russian interference campaigns in Western electoral processes exemplify this logic, particularly in the 2016 U.S. elections, where official investigations documented a coordinated active-measures campaign combining cyber activity, social media manipulation, and political interference (U.S. Senate Select Committee on Intelligence 2020). Rather than relying on direct coercion, such operations frequently combined plausible deniability, proxy actors, coordinated amplification networks, selective leaks, and information disruption strategies designed to increase political friction and institutional hesitation. Similarly, information operations preceding and accompanying the war in Ukraine demonstrated how narrative pre-positioning, synthetic media

circulation, and digitally accelerated influence ecosystems could shape international interpretation windows before conventional military events fully unfolded.
Thomas Schelling's concept of coercion as the manipulation of expectations through uncertainty and risk remains particularly relevant in this context (Schelling 1966). Under sub-threshold conditions, adversaries frequently seek not decisive persuasion, but hesitation, distraction, delay, and cumulative erosion of orientation. The operational objective is often to stretch institutional decision cycles, exploit legal and bureaucratic seams, and impose disproportionate cognitive and political costs on defenders.

The deterrence paradox, therefore, resides in the unintended strategic consequences of escalation avoidance itself. The more costly and dangerous overt confrontation becomes, the greater the incentives for indirect competition exploiting ambiguity and deniability. Conventional deterrence models – structured around visible force, attribution clarity, and proportional response – map imperfectly onto environments where effects are cumulative, diffuse, and politically internalised over time.

Reinterpreted through a Clausewitzian perspective, this does not represent a departure from strategic logic, but an adaptation of the conflict's character to socio-technical conditions (Clausewitz 1976; Gray 2010). Political objectives remain central, yet the relevant battlespace increasingly extends across media ecosystems, institutional processes, digital platforms, and social trust structures. Under such conditions, time itself becomes a strategic variable: whoever imposes orientation delays and interpretive instability gains operational advantage without necessarily crossing conventional thresholds of war.

Centre of Gravity in Open Societies: Cohesion and Decision Quality
Taken together, the openness and deterrence paradoxes reposition societal cognition as a central strategic variable in liberal democracies. The critical capability increasingly concerns whether institutions and publics can sustain coherent orientation, legitimate decision-making, and adaptive coordination under conditions of uncertainty, information saturation, and persistent cognitive pressure.
In this context, the centre of gravity of open societies lies less in information control than in the preservation of decision quality and societal cohesion. Three interrelated vulnerabilities become particularly significant.

First, decision latency emerges as a strategic risk. If investigative, legal, and communicative processes cannot operate at sufficient speed relative to narrative circulation, opportunities for pre-emptive framing and coordinated response are lost. Delayed orientation allows ambiguity and emotionally charged interpretations to stabilise before institutional clarification becomes effective.
Second, cohesion gaps create exploitable fractures across social, regional, political, or information lines. Cognitive operations frequently target bridging institutions and trust relationships – electoral/political and judicial systems, public health authorities,

armed forces, scientific expertise, or media credibility – precisely because disruption at these points can generate disproportionate societal effects.

Third, legitimacy erosion undermines the long-term capacity of institutions to sustain compliance and collective action. In open societies, legitimacy functions not merely as a normative value, but as an operational capability. Responses perceived as disproportionate, opaque, or procedurally inconsistent may achieve temporary tactical effects while degrading long-term trust and institutional resilience.

TABLE 1. The three linked vulnerabilities

Vulnerabilities	Definition
Decision Latency	If investigative, legal, and communicative processes cannot keep pace with the speed of narrative formation and diffusion, opportunities for pre-emptive framing and coordinated response are lost. Latency can reflect process design (e.g., clearance bottlenecks), resource limits, or inter-agency coordination gaps
Cohesion Gaps	Where publics segment along social, regional, or informational lines, adversaries can target bridging points (e.g., electoral administration, public-health compliance, military credibility) to produce outsized disruption. Cohesion does not imply unanimity; it implies sufficient cross-group trust to sustain contested decisions
Legitimacy Erosion	Even when decisions are substantively sound, deficits in transparency and proportionality can degrade acceptance, making subsequent decisions harder. In open societies, legitimacy is a capability to be designed and maintained—not a by-product to be assumed

Source: Author's own elaboration.

Importantly, these vulnerabilities are cumulative rather than isolated. Delayed decisions can intensify fragmentation; fragmentation can weaken legitimacy; weakened legitimacy further slows coordinated response. Cognitive competition, therefore, exploits systemic interactions across institutional, technological, and societal layers simultaneously.

Time, Ambiguity, and the Shifting Cost Curve

A defining feature of contemporary CogWar is the increasing strategic utility of time and ambiguity. Technological acceleration alters operational cost curves in at least three ways.

First, speed. AI-assisted content production, automated scheduling systems, and algorithmic amplification dramatically reduce the interval between conception, dissemination, and strategic effect. Early framing advantages accumulate rapidly because initial interpretations frequently anchor subsequent public understanding.

Second, scale. Digital infrastructures enable near-zero marginal distribution costs and highly targeted dissemination strategies. Coordinated influence campaigns can therefore achieve disproportionate visibility relative to their resource base, particularly when amplified through emotionally engaging content and algorithmically optimised interaction loops.

Third, scope. Contemporary operations move fluidly across domains and

jurisdictions, linking online discourse, diaspora networks, economic concerns, security debates, and physical-world behaviour. Information effects increasingly ricochet between digital and physical environments, generating complex feedback loops difficult to isolate or contain.

These transformations lower barriers to entry while increasing the operational advantages associated with ambiguity and rapid iteration. Adversaries can probe institutional reactions, test narratives, and adjust tactics at relatively low cost. Defenders, by contrast, remain constrained by legal standards, attribution requirements, coalition coordination processes, and democratic accountability mechanisms.

The result is a shifting asymmetry in which attackers benefit from low-cost experimentation while defenders bear the heavier burden of verification, proportionality, and legitimacy preservation.

Why Paradoxes Matter for Strategy

The strategic relevance of the double paradox lies in the risk of analytical misdiagnosis.

One risk is over-kinetic framing: interpreting CogWar primarily through models derived from conventional force-on-force conflict. Such approaches may underestimate how small, deniable, and cumulative information actions can generate strategic effects by degrading orientation and slowing decision-making rather than by physically destroying capabilities.

The opposite risk is over-managerial framing: reducing cognitive competition to communication management, reputational defence, or isolated "counter-disinformation" initiatives. These risks obscure the strategic intent underlying sub-threshold operations, which frequently aim to shape alliance behaviour, impose political costs, and weaken institutional confidence over extended periods.

TABLE 2. Strategic Implications of the Double Paradox

Paradox-Driven Risk	Strategic Implications
Over-kinetic framing	If planners default to models suited to physical force-on-force contests, they may overlook how small, deniable interventions generate strategic effect by degrading decision quality rather than by seizing territory. Measures of success tend therefore to require decision latency, recovery time, and indicators of cross-group bridging, not merely message volumes or takedown counts
Over-managerial framing	If, conversely, planners treat CogWar as a purely communicative or reputational problem, they may obscure adversary doctrine and intent. Sub-threshold campaigns are strategic, not accidental: they are designed to impose costs, signal resolve, test alliances, and sow doubts about state capacity
Normative slippage	Attempts to "harden" the information environment may drift toward illiberal practices that undercut legitimacy. In open societies, means and ends are inseparable: proportionality, transparency, and due process must be built into planning from the start. The credibility gained by adhering to such guardrails is itself a deterrent, as it narrows the political space in which adversaries can claim overreach

Source: Author's own elaboration.

A third risk concerns normative slippage. Attempts to "harden" information environments through excessive control, surveillance, or exceptional measures may erode precisely the legitimacy and openness that constitute democratic strategic strengths. In open societies, means and ends cannot be separated cleanly: procedural legitimacy, transparency, and proportionality are not secondary ethical concerns, but operational conditions of long-term resilience.

From Problem to Programme

The double paradox, therefore, establishes the article's central strategic problem: how can open societies preserve decision quality, legitimacy, and operational tempo under conditions of persistent cognitive competition without undermining the democratic principles they seek to defend?

Two implications follow.

First, classical strategic concepts remain highly relevant when reinterpreted for contemporary socio-technical battlefields (Hart 1967; Beaufre 1965; Schelling 1966; Clausewitz 1976; Rid 2020; Gray 2010). Deterrence, coercion, ambiguity, and the indirect approach continue to shape strategic competition, although their operational grammar increasingly unfolds through information, cognitive, legal, and institutional mechanisms rather than purely military confrontation.

Second, the techno-operational environment structurally favours actors capable of integrating anticipation, orientation, and action into repeatable institutional routines. Effective cognitive defence, therefore, depends less on episodic reaction than on anticipatory governance capacities capable of reducing strategic surprise while preserving legitimacy and coalition coherence.

The following sections develop these implications further by examining the return of the indirect approach in sub-threshold competition, the operational conditions imposed by accelerated technological environments, and the doctrinal principles required for long-range cognitive defence in open societies.

Deterrence Fixation and the Return of the Indirect Approach in Dilating Battlefields

The previous section established how openness and deterrence generate structural vulnerabilities exploitable through cognitive competition. This section examines why contemporary strategic rivalry increasingly unfolds below the threshold of armed conflict and why the indirect approach has regained relevance under conditions of information acceleration, attribution ambiguity, and socio-technical complexity.

The central argument is that the long post-1945 emphasis on deterrence stability and escalation avoidance has unintentionally incentivised indirect and deniable forms of competition operating across what may be described as dilating battlefields – operational environments extending beyond conventional military theatres into institutions, digital infrastructures, legal systems, media ecosystems, and everyday social practices. In such environments, strategic effect derives less from territorial

seizure or direct destruction than from the ability to impose delay, uncertainty, fragmentation, and decision friction on adversaries over time.

Deterrence fixation and competition under the threshold

Since the end of the Second World War, Western strategic culture has been profoundly shaped by the imperative of preventing large-scale interstate war. Nuclear deterrence, escalation management, and alliance stability became central organising principles of Euro-Atlantic security architecture. While this strategic orientation contributed significantly to reducing direct great-power confrontation, it also encouraged competitive behaviour to migrate into domains operating below the threshold of conventional war (Freedman 2013; Mazarr 2015).

Contemporary sub-threshold competition exploits precisely those areas where attribution is uncertain, legal thresholds remain contested, and proportional responses are politically difficult to calibrate. Rather than seeking decisive military confrontation, adversaries frequently pursue cumulative strategic gains through information pressure, cyber operations, economic leverage, political disruption, proxy actors, and cognitive manipulation calibrated to remain ambiguous enough to avoid overt escalation.

The annexation of Crimea in 2014 represented a particularly illustrative example of this transition. Russian operations combined military positioning, information operations, political ambiguity, proxy structures, and strategic narrative shaping in ways that complicated attribution, delayed international consensus, and fragmented response coordination. Similar dynamics later emerged in electoral interference campaigns targeting Western democracies, where influence operations relied less on overt persuasion than on amplifying distrust, polarisation, and institutional friction. Such operations reveal an important asymmetry. For defenders operating within democratic and legal constraints, attribution is not merely technical but political. Responses frequently require evidentiary thresholds, coalition coordination, legal justification, and public legitimacy. Adversaries exploiting deniability can therefore impose disproportionate decisional and institutional costs at relatively low operational risk.

Thomas Schelling's analysis of coercion remains particularly relevant in this context (Schelling 1966). Strategic influence increasingly operates through the manipulation of expectations, uncertainty, and escalation perceptions rather than through confrontation alone. The objective is often not immediate persuasion, but hesitation: increasing the political and cognitive costs associated with response while stretching institutional decision cycles.

This dynamic helps explain why contemporary strategic competition increasingly favours persistent, incremental, and ambiguous pressure rather than overt escalation. The strategic success of deterrence at higher levels of conflict has unintentionally expanded the operational attractiveness of the grey zone.

The indirect approach, updated

The contemporary return of the indirect approach reflects this strategic environment. Classical theorists such as B. H. Liddell Hart and André Beaufre argued that

effective strategy often operates most successfully by shaping the adversary's perceptions, orientation, and strategic choices indirectly rather than through frontal confrontation (Hart 1967; Beaufre 1965). Under current conditions, this logic has acquired renewed relevance through digitally mediated and cognitively accelerated forms of competition.

The indirect approach in contemporary CogWar environments seeks not necessarily to impose coherent ideological alternatives, but to increase uncertainty, degrade coordination, and impose cognitive friction across institutional systems. Operationally, this may involve:

- exploiting information asymmetries;
- amplifying social fragmentation;
- targeting alliance cohesion;
- manipulating tempo and attention;
- saturating public discourse with contradictory signals;
- or exploiting legal and bureaucratic seams between institutions.

Importantly, many of these operations function through cumulative rather than spectacular effects. Small-scale information interventions, selective leaks, coordinated amplification campaigns, nuisance cyber incidents, and synthetic media circulation may individually appear insufficient to justify a major response. Yet over time, their aggregated impact can degrade trust, increase decision latency, and weaken institutional coherence.

The war in Ukraine further demonstrated how indirect approaches increasingly combine military and information dimensions into integrated strategic ecosystems, with EU analyses identifying Ukraine as a primary target of Russian foreign information manipulation and interference (European External Action Service 2023). Prior to and during kinetic operations, competing narratives circulated across social media platforms, encrypted communication channels, state-affiliated media systems, and international digital networks. Deepfake videos, manipulated imagery, selective framing, and coordinated amplification efforts illustrated how information operations can shape interpretation windows before facts are fully verified.

This evolution reflects an important doctrinal shift: the indirect approach is no longer confined to military manoeuvre or diplomatic signalling alone. It increasingly unfolds through socio-technical architectures capable of influencing orientation, tempo, and legitimacy simultaneously.

Dilating battlefields: a Clausewitzian reading

A Clausewitzian perspective helps clarify the continuity underlying these transformations. Clausewitz argued that while the nature of war remains enduringly tied to political purpose, friction, and uncertainty, its character evolves according to historical and technological conditions (Clausewitz 1976). Contemporary cognitive competition, therefore does not invalidate classical strategic theory; rather, it demonstrates how strategic interaction adapts to socio-technical change.

Under current conditions, the battlespace becomes increasingly dilated. Strategic interaction extends beyond physical theatres into media infrastructures, digital platforms, institutional procedures, public discourse, economic systems, and social trust networks. These environments are not secondary information "backgrounds" to conflict but operational terrains in their own right.

The decisive effects sought within these dilated battlefields are frequently cognitive and institutional rather than kinetic. Strategic success may manifest as:

- delayed political decisions;
- alliance hesitation;
- fragmented public interpretation;
- reduced institutional legitimacy;
- or increased societal fatigue and uncertainty.

The relevant variables therefore increasingly concern tempo, orientation, and coherence. In practical terms, a state may retain overwhelming conventional military superiority while nevertheless experiencing strategic paralysis if institutional decision-making becomes sufficiently slowed, fragmented, or delegitimised under persistent information pressure.

This perspective also dissolves simplistic distinctions between "peace" and "war." Cognitive competition frequently unfolds continuously across peacetime, crisis, and conflict phases, with information and psychological shaping operations persisting before, during, and after kinetic escalation. Contemporary strategy must therefore operate across an extended temporal horizon in which orientation and anticipation become continuous rather than episodic activities.

The grammar of sub-threshold coercion

Although contemporary sub-threshold operations vary significantly across actors and theatres, they frequently share a common operational grammar organised around ambiguity, deniability, tempo, and asymmetry.

First, ambiguity is deliberately engineered into operational design. Attribution complexity increases political hesitation and complicates coalition coordination. Cyber incidents, proxy actors, front organisations, commercial intermediaries, and transnational digital networks all contribute to creating uncertainty regarding authorship and intent.

Second, deniability functions as a protective buffer against escalation. By maintaining a plausible distance between sponsor and effect, adversaries reduce the likelihood of proportional retaliation while preserving operational flexibility.

Third, tempo advantage constitutes a central strategic objective. Automated amplification systems, coordinated posting networks, synthetic media generation, and pre-positioned digital ecosystems enable rapid narrative circulation before institutional verification processes can stabilise interpretation. Early framing advantages become particularly powerful under accelerated information conditions because initial narratives frequently shape subsequent public understanding even after corrections emerge.

TABLE 3. The grammar of sub-threshold coercion

Expressions	Definitions
Ambiguity by design	Actions are calibrated to keep motivation and sponsorship contestable. This exploits the evidentiary standards of open societies and buys time
Deniability through indirection	Proxies, front organisations, and cross-border channels create distance between initiator and effect. Attribution becomes a political decision as much as a technical one
Tempo advantage	Content automation, coordinated posting, and pre-positioned channels allow rapid onset. If detection and orientation lag, early frames anchor public interpretation
Seam exploitation	Campaigns look for institutional seams (between ministries, regulators, and courts) and informational seams (between platforms, languages, or jurisdictions). These seams are friction points that can be multiplied at low cost
Cost-imposition asymmetry	Small acts (e.g., a targeted leak, a crafted rumour, a nuisance cyber-incident) impose disproportionate costs on defenders, who must investigate, brief, coordinate, and respond within legal and ethical constraints
Typical effects	Delay, distraction, doubt. Success is often negative: what does not happen (delayed decisions, shelved policies, aborted reforms). Persuasion is not required; uncertainty can be enough

Source: Author's own elaboration.

Fourth, sub-threshold competition systematically exploits institutional seams. Legal jurisdictions, inter-agency coordination gaps, alliance consultation procedures, and differences between public and private governance systems create friction points that can be targeted at relatively low cost. The strategic objective is often less to "win" a narrative outright than to increase institutional complexity, coordination burdens, and decisional fatigue.

Finally, these operations are characterised by cost asymmetry. Relatively small actions can impose disproportionate burdens on defenders required to investigate, coordinate, attribute, communicate, and respond within democratic and legal constraints. This asymmetry favours persistence, experimentation, and iterative adaptation by attackers.

Importantly, the cumulative effects of such operations are frequently negative rather than affirmative. Success may consist not in changing beliefs directly, but in generating sufficient uncertainty, delay, or fragmentation to prevent coherent collective orientation and timely institutional response.

Implications for open societies

For open societies, the return of the indirect approach creates several strategic dilemmas. The first is the temptation to interpret cognitive competition primarily as a communication problem. Such framing risks reducing strategy to messaging or "counter-disinformation" campaigns while neglecting the broader institutional and temporal dimensions of sub-threshold competition. Cognitive operations target not only narratives, but also decision processes, coordination mechanisms, and legitimacy structures.

The second is the opposite temptation: responding through excessive securitisation or illiberal hardening measures that undermine democratic legitimacy and public trust. Attempts to defend openness through opaque control mechanisms, exceptional restrictions, or disproportionate surveillance may ultimately damage the very societal resilience they seek to protect.

A more sustainable approach requires adapting deterrence logic to the cognitive domain without abandoning democratic constraints. This implies acting simultaneously on three interconnected dimensions.

First, reducing attacker payoff windows by shortening institutional detection-to-decision cycles and improving lawful decisional tempo. Second, strengthening societal resilience through credible intermediaries, coalition coordination, and cross-group trust structures capable of reducing fragmentation and interpretive instability. Third, increasing reputational, diplomatic, legal, and political costs associated with covert influence operations, particularly through coalition-based attribution and coordinated transparency measures.

In this context, legitimacy itself becomes a strategic capability. Responses perceived as proportionate, transparent, and procedurally coherent strengthen institutional credibility and reduce opportunities for adversarial exploitation.

Bridge to Sections 3 and 4

If the previous section established cognition as a strategic centre of gravity in open societies, this section has shown why contemporary competition increasingly operates through indirect, deniable, and sub-threshold mechanisms exploiting tempo, ambiguity, and institutional friction across dilating battlefields.

The next section, therefore, examines the techno-operational environment enabling these dynamics. Specifically, it analyses how acceleration, automation, platform architectures, attribution complexity, and transnational information ecosystems reshape operational possibilities and planning horizons in contemporary CogWar environments.

Section 4 subsequently translates these insights into doctrinal design principles for cognitive defence in open societies, focusing on legitimacy, anticipation, institutional coordination, and coalition interoperability as foundations for long-range strategic adaptation.

Techno-Operational Environment of CogWar

Contemporary CogWar unfolds within a techno-operational environment characterised by accelerated information circulation, low barriers to entry, transnational connectivity, and increasingly blurred distinctions between civilian and strategic infrastructures. Under these conditions, the operational advantage frequently belongs not to actors possessing the greatest volume of information, but to those capable of shaping orientation, exploiting tempo asymmetries, and operating effectively across fragmented socio-technical ecosystems.

Three interrelated characteristics are particularly decisive in shaping the contemporary operational environment of CogWar: speed, scale, and scope. Together, they alter the cost structure of influence operations while simultaneously increasing the pressure placed on institutional decision-making processes in open societies.

TABLE 4. Speed–Scale–Scope Matrix: Mechanisms, Effects, and Defensive Implications

Dimension	Mechanisms (enablers)	Operational effects	Implication for defence
Speed	Automation (bots/ schedulers), AI-assisted authoring, synthetic media	Concept→circulation in minutes; first-mover framing anchors later interpretation (Chesney and Citron 2019)	Shorten verification / coordination; institutional readiness to reduce decision latency to prevent decision drift
Scale	Near-zero marginal distribution; programmatic ads; look-alike audiences; coordinated inauthentic behaviour	Attention hijacking via repeated, affect-rich content; simulated mass (Singer and Brooking 2018; Benkler, Faris and Roberts 2018)	Focus on reach/decay metrics; coalition messaging and credible intermediaries to counter saturation
Scope	Cross-platform, encrypted groups, diaspora media; issue transits (health, economy, security)	Online–offline ricochet; more seams (jurisdictional, linguistic, regulatory, institutional)	Pre-aligned cordination across defence, civil authorities, and Allies; institutional mechanisms to manage jurisdictional seams; shared interpretative indicators across the system

Source: Author's own elaboration.

First, speed. AI-assisted content generation, automated distribution systems, coordinated amplification networks, and synthetic media technologies dramatically reduce the interval between narrative conception, dissemination, and strategic effect. Information operations that previously required substantial organisational resources can now be conducted rapidly and iteratively at comparatively low cost. The increasing availability of generative AI tools further compresses production cycles, enabling real-time adaptation of messaging, imagery, and audiovisual manipulation during unfolding crises.

The strategic significance of speed lies in the anchoring effect of early interpretation. Under accelerated information conditions, initial narratives frequently shape subsequent public understanding even when later corrections emerge. During the first phases of the war in Ukraine, for example, competing interpretations circulated globally across digital platforms before many institutional actors had established verified situational awareness. Similar dynamics have appeared during electoral crises, terrorist incidents, and public health emergencies, where rapid emotional framing often precedes institutional clarification.

Second, scale. Contemporary digital infrastructures permit near-zero marginal distribution costs combined with increasingly precise audience targeting

mechanisms. Coordinated inauthentic behaviour, bot amplification systems, programmatic advertising ecosystems, and algorithmic recommendation architectures allow relatively small actors to achieve disproportionate information visibility (Singer and Brooking 2018). Research on networked media ecosystems further suggests that emotionally activating content spreads more efficiently across digital platforms than slower, verification-dependent institutional communication (Benkler, Faris, and Roberts 2018).

This asymmetry creates an operational environment in which repetition, emotional salience, and visibility frequently matter more immediately than factual robustness. Cognitive operations, therefore, exploit the logic of platform amplification itself, using algorithmic engagement incentives to increase interpretive instability and information saturation.

Third, scope. Contemporary CogWar environments operate across increasingly interconnected and transnational information ecosystems. Influence operations no longer remain confined to isolated media channels or national information spaces.

Instead, narratives circulate fluidly across:

- social media platforms;
- encrypted messaging applications;
- diaspora networks;
- digital influencers;
- state-affiliated media systems;
- commercial information infrastructures;
- and cross-border online communities.

This trans-domain circulation produces ricochet effects between digital and physical environments. Online narratives influence offline political behaviour, while physical events are rapidly reintegrated into digital amplification cycles. During the COVID-19 pandemic, for example, public health decisions, protest movements, conspiracy narratives, institutional trust, and geopolitical competition became deeply intertwined across multiple information layers simultaneously.

Taken together, speed, scale, and scope generate a structurally asymmetric environment. Attackers benefit from low-cost experimentation, rapid iteration, and ambiguity, while defenders remain constrained by verification requirements, legal standards, coalition coordination, and democratic accountability mechanisms.

Attribution, deniability, and the politics of proof

One of the defining characteristics of contemporary CogWar environments is the growing difficulty of attribution under conditions of information complexity and transnational connectivity. Attribution is not merely a technical process of identifying origin points or digital signatures; it is fundamentally political and strategic.

Open societies typically require high evidentiary thresholds before publicly attributing hostile influence activities to state or non-state actors. Democratic institutions must consider legal standards, diplomatic consequences, coalition

coordination, intelligence protection, and public legitimacy before formal attribution occurs. Adversaries exploit this asymmetry through operational architectures specifically designed to complicate proof and delay response.

Contemporary influence ecosystems frequently rely on:

- proxy actors;
- front organisations;
- third-country digital infrastructure;
- commercial intermediaries;
- unofficial online communities;
- and coordinated but loosely networked amplification channels.

The objective is not necessarily perfect concealment, but sufficient ambiguity to slow institutional orientation and complicate proportional response.

Russian electoral interference campaigns and coordinated online influence operations offer particularly illustrative examples. In many cases, attribution emerged incrementally through the aggregation of intelligence indicators, forensic analysis, investigative journalism, and platform disclosures rather than through immediately observable evidence. During this interval, uncertainty itself functioned as a strategic resource, generating hesitation, polarisation, and interpretive contestation.

Similarly, the increasing availability of synthetic media technologies introduces new attribution challenges. Deepfake videos, AI-generated audio, manipulated imagery, and synthetic identity systems reduce confidence in evidentiary authenticity while increasing verification burdens on institutions and media organisations (Chesney and Citron 2019). Even poorly executed synthetic content may achieve strategic effect if circulated rapidly enough to shape initial public interpretation before debunking occurs.

Under such conditions, the politics of proof become central to strategic competition. Defenders must simultaneously:

- preserve evidentiary credibility;
- avoid premature attribution;
- maintain coalition coherence;
- and respond quickly enough to prevent interpretive destabilisation.

This tension produces a persistent decisional dilemma in open societies: institutional legitimacy requires procedural caution, yet excessive caution increases operational latency and widens attacker payoff windows.

For this reason, contemporary cognitive defence increasingly depends on coalition-based attribution mechanisms and tactic-level transparency. Publicly exposing operational techniques, amplification methods, and influence architectures may, in some cases, prove strategically more effective than waiting for definitive actor attribution. The objective becomes reducing ambiguity sufficiently to preserve orientation and resilience, even when perfect certainty remains unattainable.

Small-state constraints, allied leverage

The techno-operational environment of CogWar creates particular challenges for small and mid-sized states. Unlike major powers, smaller states frequently operate

with:

- limited specialised personnel;
- reduced technological infrastructure;
- slower procurement cycles;
- narrower intelligence capabilities;
- and limited leverage over global digital platforms.

These constraints increase dependence on external information infrastructures and allied coordination mechanisms. Smaller states may struggle to independently monitor large-scale information ecosystems, rapidly attribute complex operations, or sustain continuous strategic communication efforts across multiple domains simultaneously.

At the same time, small-state vulnerabilities are not purely technical. Cognitive operations targeting smaller states may achieve disproportionate strategic effects because institutional ecosystems are often more compressed and socially interconnected. Limited redundancy across media, political, or administrative systems can increase susceptibility to cascading trust erosion and institutional fragmentation.

However, alliance integration also creates strategic opportunities. NATO and European Union structures provide forms of interpretive interoperability, shared situational awareness, joint attribution capacity, and coordinated strategic signalling that smaller states would struggle to sustain independently. In this sense, coalition integration functions not merely as military reinforcement, but as cognitive and institutional amplification.

The challenge lies in balancing coalition coordination with national political legitimacy and decision autonomy. Effective cognitive defence, therefore, depends less on information centralisation than on interoperable orientation mechanisms capable of preserving shared understanding across allied systems while respecting national institutional frameworks.

This suggests that the strategic value of alliances in the cognitive domain increasingly resides in:

- shared interpretive frameworks;
- coordinated transparency;
- joint exercises;
- common indicators and warning mechanisms;
- and rapid institutional communication channels.

Such structures reduce fragmentation and improve collective orientation without requiring uniform political responses.

Implications for planning horizons

The accelerated and uncertain nature of contemporary CogWar environments places significant pressure on traditional strategic planning models. Linear forecasting assumptions become increasingly fragile under conditions characterised by rapid technological adaptation, information volatility, and nonlinear escalation

dynamics. Under VUCA/BANI conditions, effective planning therefore depends less on predictive precision than on anticipatory adaptability (Bennett and Lemoine 2014; Cascio 2020). The operational objective is not to forecast specific events accurately, but to reduce strategic surprise while preserving decision optionality and institutional coherence under uncertainty.

A Futures Studies perspective becomes particularly relevant in this context because it shifts attention from deterministic prediction toward structured anticipation, horizon scanning, and scenario-oriented orientation mechanisms (Schoemaker 1995). In practical terms, this implies integrating lightweight anticipatory routines into institutional decision cycles rather than treating foresight as a separate specialised activity.

Three nested planning horizons become particularly useful.

The first is the immediate operational horizon, focused on rapid situational awareness, interpretive stabilisation, and short-cycle institutional coordination during unfolding information events. Here, tempo and decisional clarity are decisive.

The second is the medium-term adaptive horizon, concerned with recurring patterns, evolving tactics, institutional vulnerabilities, and alliance coordination mechanisms. At this level, organisations seek to identify trends, recurring seams, and emerging operational methods.

The third is the long-range strategic horizon, where the focus shifts toward technological evolution, changes in media ecosystems, societal resilience, geopolitical shifts, and structural transformations in the information environment itself.

Importantly, these horizons must remain interconnected. Institutions unable to connect long-range anticipation with operational decision cycles risk producing strategically irrelevant foresight disconnected from actionable orientation. Conversely, institutions focused exclusively on immediate response may gradually lose the ability to interpret structural transformations shaping future cognitive competition.

This reinforces a central argument of the article: effective cognitive defence depends less on technological sophistication alone than on institutional capacity to sustain coherent orientation across time under conditions of persistent uncertainty.

What to measure: toward an operational evaluation framework

One of the persistent difficulties in the cognitive domain concerns evaluation. Traditional military metrics – territory seized, forces destroyed, kinetic effects generated – translate imperfectly into environments where strategic outcomes frequently concern orientation, legitimacy, and decision quality rather than physical destruction.

For this reason, assessment frameworks in CogWar environments should prioritise operational and institutional indicators rather than purely information outputs such as message volume or content removal statistics.

Several dimensions become particularly relevant.

First, decision latency: the interval between detection, orientation, and coordinated

institutional response. Reducing latency without undermining legitimacy becomes a central strategic objective.
Second, recovery time: the ability of institutions and publics to restore operational coherence following information disruption or accelerated narrative surges.
Third, cohesion and trust indicators: measures associated with institutional credibility, cross-group bridging, and the persistence of shared orientation mechanisms under stress.
Fourth, norm compliance: whether responses remain proportionate, lawful, transparent, and democratically legitimate over time.

These indicators are necessarily imperfect. Cognitive competition unfolds through diffuse, cumulative, and nonlinear effects that resist precise quantification. Nevertheless, such measures provide more strategically meaningful orientation than simplistic metrics centred exclusively on visibility, engagement, or content suppression. Importantly, the purpose of evaluation in the cognitive domain should not be to produce illusions of certainty, but to improve institutional learning and adaptive capacity over time.

Bridge to Section 4
This section has examined how accelerated technological environments, attribution complexity, and transnational information ecosystems reshape the operational conditions of contemporary cognitive competition. The analysis suggests that the decisive challenge for open societies lies not merely in information management, but in sustaining lawful speed, institutional coherence, and anticipatory orientation under persistent uncertainty.
The final section, therefore, shifts from operational environment analysis toward doctrinal implications. Specifically, it develops design principles for cognitive defence in open societies centred on legitimacy, anticipation, procedural coherence, and coalition interoperability as foundations for long-range strategic adaptation.

From Method to Doctrine: Design Principles for Cognitive Defence in Open Societies

The preceding sections established cognition as a strategic centre of gravity in open societies and identified time, ambiguity, attribution, and decision quality as decisive variables in sub-threshold competition. The remaining challenge is doctrinal: how can defence institutions translate these insights into a sustainable cognitive defence posture without undermining the democratic foundations they are tasked to protect? This section, therefore, moves from analytical method to doctrinal design. It does not propose an operational playbook or a centralised model of narrative control. Instead, it articulates principles that can guide doctrine, education, planning, and institutional adaptation in NATO and EU-oriented open societies. The aim is to define the trade-offs that cognitive defence must manage if it is to remain strategically effective, legally bounded, and politically legitimate.

Tempo versus Legitimacy

Cognitive competition rewards speed. Early framing advantages can shape public interpretation before institutional verification, legal assessment, or coalition coordination are complete. In accelerated information environments, delayed orientation can become a strategic vulnerability: institutions may be factually correct but operationally late.

Yet in open societies, speed cannot be pursued at the expense of legitimacy. Cognitive defence measures perceived as opaque, disproportionate, politically instrumentalised, or procedurally irregular may produce short-term tactical gains while eroding public trust. This is a central doctrinal tension: democratic institutions must become faster without becoming arbitrary.

The relevant objective is therefore not maximum speed, but lawful speed. This means pre-defining authorities, thresholds, communication routines, evidentiary standards, and escalation pathways before crisis conditions emerge. Institutional tempo should arise from prior alignment and rehearsed procedures, not improvised exceptionalism.

In practical doctrinal terms, this implies:

- clear mandates for monitoring, assessment, and response;
- pre-agreed thresholds for escalation;
- rapid but reviewable decision processes;
- communication protocols that distinguish confirmed facts from assessed probabilities;
- and mechanisms for correction when initial assessments change.

Lawful speed protects both effectiveness and legitimacy. It shortens the attacker's payoff window while preserving the procedural credibility on which democratic resilience depends.

Anticipation versus Democratic Accountability

Strategic anticipation is indispensable in the cognitive domain. Because influence operations often unfold gradually through pre-positioned narratives, trust erosion, and repeated probing, institutions cannot rely solely on reactive crisis response. They need horizon scanning, scenario thinking, and early-warning indicators capable of identifying emerging vulnerabilities before they become acute.

However, anticipation carries its own democratic risks. Foresight mechanisms can drift toward technocratic control if they are used to pre-empt public debate, classify dissent as threat activity, or insulate security assessments from scrutiny. In open societies, the purpose of anticipation cannot be narrative management or political pre-emption. It must be orientation: improving preparedness while preserving pluralism and contestation.

The doctrinal distinction is essential. Cognitive defence should not seek to determine what citizens ought to believe. It should seek to improve institutional capacity to

detect hostile manipulation, understand evolving threat patterns, and respond proportionately when adversarial activity targets decision quality, public trust, or institutional legitimacy.

Accordingly, anticipatory practices should be:
- explicitly bounded in scope;
- separated from partisan political interests;
- subject to legal and institutional oversight;
- periodically reviewed;
- and open to correction when assumptions prove wrong.

This is where Futures Studies can contribute without becoming predictive or controlled. Horizon scanning, alternative scenarios, signposts, and structured uncertainty analysis help institutions think across multiple plausible futures while avoiding deterministic threat narratives. Used properly, foresight strengthens democratic accountability because it makes assumptions visible and revisable rather than hidden inside crisis improvisation.

Institutional Speed versus Procedural Safeguards

CogWar exploits seams between institutions, jurisdictions, legal regimes, and public-private systems. Fragmented mandates, unclear escalation routes, slow clearance procedures, and competing institutional vocabularies all increase decision latency. In this sense, bureaucratic friction can become an operational vulnerability.

The doctrinal temptation is to respond through centralisation: creating single authorities, emergency powers, or command structures capable of bypassing ordinary procedures. In some crisis conditions, central coordination may be necessary. Yet excessive centralisation risks weakening the very safeguards that differentiate democratic cognitive defence from authoritarian information control.

The more sustainable doctrinal answer is not to collapse procedural safeguards, but to make them interoperable under stress. Institutions should know in advance how their mandates connect, how information flows across agencies, how legal advice is obtained rapidly, how public communication is coordinated, and how private platforms, civil society actors, and allied partners are engaged.

This requires shared interpretive frameworks rather than unified command over public discourse. Defence institutions, intelligence services, regulators, public communicators, electoral authorities, public health agencies, and diplomatic actors may all perceive different parts of the same cognitive operation. Without a common vocabulary and pre-agreed coordination routines, these perceptions remain fragmented.

Doctrinal design should therefore prioritise:
- shared taxonomies of cognitive threats and influence techniques;
- inter-agency exercises;
- standing liaison mechanisms;

- pre-cleared communication templates;
- legal review pathways;
- and after-action learning processes.

Procedural safeguards should not be seen as obstacles to tempo. Properly designed, they are the conditions that allow institutions to act quickly without losing legitimacy.

Coalitional Alignment versus National Autonomy

Contemporary CogWar is rarely confined within national boundaries. Influence operations across languages, platforms, jurisdictions, diaspora networks, and alliance spaces. This makes coalition coordination increasingly important, particularly for small and mid-sized states that lack the scale, technological capacity, or platform leverage to act alone.

NATO and EU contexts offer significant advantages: shared situational awareness, common threat vocabularies, joint exercises, coordinated attribution, strategic signalling, and institutional learning across national systems. Coalitional alignment can reduce ambiguity, increase reputational costs for hostile actors, and strengthen resilience through shared indicators and comparative experience.

Yet cognitive defence cannot simply be outsourced to alliances. Political legitimacy, legal authority, public communication, and democratic accountability remain nationally anchored. Each state must retain responsibility for how it interprets threats, communicates with its citizens, and calibrates response within its constitutional and political context.

The doctrinal challenge is therefore to distinguish between shared cognition and sovereign decision. Shared cognition refers to common indicators, analytical categories, warning mechanisms, and interpretive frameworks. Sovereign decision refers to nationally accountable choices regarding attribution, legal action, public communication, diplomatic response, or operational measures.

Effective doctrine should seek interoperability of interpretation, not uniformity of response. Allies do not need to react identically to every cognitive threat. They do need to recognise comparable patterns, understand each other's thresholds, communicate rapidly, and coordinate when collective action increases legitimacy or deterrent effect.

For smaller states in particular, this distinction is crucial. Coalitions can provide scale, expertise, and credibility, but national institutions must remain the primary holders of democratic trust. The goal is not dependency, but reinforced autonomy through interoperable alignment.

Doctrinal Implication

Taken together, these four design tensions suggest that cognitive defence in open societies should be understood less as a discrete capability set than as a decision discipline. Its effectiveness depends on how institutions organise time, legitimacy, anticipation, procedure, and coalition alignment under conditions of uncertainty.

This has several doctrinal implications.
First, cognitive defence should be integrated into strategic planning rather than treated as an episodic communication function. The relevant problem is not only what messages are produced, but how institutions orient themselves, decide, coordinate, and learn under information pressure.
Second, cognitive defence should privilege resilience over control. Open societies cannot and should not seek information dominance through coercive narrative management. Their comparative advantage lies in credible institutions, plural verification, lawful transparency, and adaptive learning.
Third, doctrine should define trade-offs explicitly. Speed must be balanced with legitimacy; anticipation with accountability; coordination with safeguards; coalitional alignment with national autonomy. If these tensions remain implicit, crisis conditions will force ad hoc decisions that may undermine trust.
Fourth, evaluation should focus on decision quality, latency, recovery, cohesion, and norm compliance rather than superficial visibility metrics. The success of cognitive defence is not measured by narrative victory alone, but by the sustained ability of institutions and publics to remain oriented and legitimate under pressure.
The doctrinal conclusion is therefore clear: cognitive defence ultimately concerns the disciplined organisation of democratic decision-making under persistent strategic manipulation, drawing on longstanding military experience in orientation, coordination, anticipation, and action under conditions of uncertainty.

Conclusions

This article examined how open societies can design long-range strategy in the cognitive domain under conditions of strategic uncertainty, technological acceleration, and persistent sub-threshold competition. Drawing on a conceptual-doctrinal and futures-oriented analytical framework, the analysis argued that contemporary CogWar is best understood not primarily as a struggle for narrative dominance, but as a contest over orientation, tempo, legitimacy, and decision quality across increasingly dilated socio-technical battlefields.

The analysis identified two structural paradoxes shaping the strategic environment of open societies. The openness paradox demonstrated how the same information and technological conditions that enable democratic pluralism, innovation, and participation also generate fragmentation, accelerated information volatility, and vulnerabilities exploitable through manipulation and ambiguity. The deterrence paradox showed how the long post-1945 emphasis on escalation avoidance and strategic stability unintentionally incentivised indirect and deniable forms of competition operating below the threshold of armed conflict.
Taken together, these paradoxes reposition cognition as a strategic centre of gravity. Under contemporary conditions, strategic advantage increasingly derives from the ability to preserve institutional orientation, lawful decisional tempo, coalition coherence, and public legitimacy under persistent information pressure. The

challenge is therefore not merely technological or communicational. It concerns how democratic systems organise anticipation, coordination, and strategic adaptation under uncertainty.

The article further argued that the techno-operational environment of CogWar amplifies these pressures through speed, scale, and scope. AI-assisted content generation, synthetic media, automated amplification, and transnational digital ecosystems compress verification windows, complicate attribution, and increase asymmetries between rapidly adaptive attackers and procedurally constrained defenders. In such environments, ambiguity and time themselves become operational instruments.

Against this background, the article proposed a doctrinal perspective centred on four design tensions: tempo versus legitimacy; anticipation versus democratic accountability; institutional speed versus procedural safeguards; and coalitional alignment versus national autonomy. These tensions cannot be eliminated, but they can be managed explicitly through strategic doctrine, anticipatory governance routines, and interoperable institutional frameworks capable of sustaining lawful speed and adaptive coordination under pressure.

The central implication is that cognitive defence in open societies should be understood less as a discrete operational capability than as a disciplined approach to democratic decision-making under conditions of persistent strategic manipulation. This does not imply the militarisation of democratic public space, but rather the adaptation of doctrinal disciplines long developed within military contexts – anticipation, coordination, orientation, and action under uncertainty – to the governance requirements of open societies operating in accelerated information environments.
In this sense, military institutions possess relevant experience not because democratic societies should emulate wartime command structures, but because military doctrine has historically grappled with many of the organisational problems now re-emerging in the cognitive domain: friction, ambiguity, tempo asymmetry, adversarial adaptation, coalition coordination, and decision-making under uncertainty. The contribution of military thought, therefore, lies less in securitising information space than in informing how democratic institutions can preserve coherence and legitimacy while operating under persistent cognitive pressure.

The article also suggests that effective cognitive defence depends less on information dominance than on resilience of orientation. Open societies cannot realistically eliminate ambiguity, prevent all manipulation, or control information ecosystems without undermining the very freedoms that constitute their strategic legitimacy. Their comparative advantage lies instead in the ability to sustain credible institutions, plural verification mechanisms, coalition interoperability, lawful adaptation, and public trust over long temporal horizons.

Several limitations should nevertheless be acknowledged. Given its conceptual and doctrinal orientation, the article did not seek to produce empirical causal testing, operational modelling, or quantitative measurement frameworks. The operational illustrations included throughout the analysis were intended to ground the conceptual discussion rather than function as formal comparative case studies. Future research could therefore expand this framework through empirical examination of decision latency in crisis environments, comparative analysis of national cognitive defence models, alliance interoperability mechanisms, or the development of operational indicators capable of assessing institutional resilience under information pressure.

Ultimately, the strategic challenge confronting open societies is neither purely information nor purely technological. It is epistemological and organisational. In increasingly accelerated and contested information environments, the ability of democratic systems to think, decide, coordinate, and adapt coherently under uncertainty may become one of the defining strategic variables of contemporary competition.

References

Beaufre, André. 1965. *An Introduction to Strategy, with Particular Reference to Problems of Defence, Politics, Economics, and Diplomacy in the Nuclear Age.* New York: Praeger.

Benkler, Yochai, Robert Faris, and Hal Roberts. 2018. "Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics." Edited by Oxford University Press. https://doi.org/10.1093/oso/9780190923624.001.0001.

Bennett, Nate, and G. James Lemoine. 2014. "What VUCA Really Means for You." January–February.

Cascio, W.F. 2020. "Managing a Brittle, Anxious, Nonlinear, Incomprehensible World."

Chesney, Robert, and Danielle Keats Citron. 2019. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107(6): 1753-1819.

Clausewitz, Carl von. 1976. *On War. Edited and translated by Michael Howard and Peter Paret.* Princeton, NJ: Princeton University Press.

European External Action Service. 2023. "1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence." Brussels: European External Action Service.

Freedman, Lawrence. 2013. *Strategy: A History.* Oxford: Oxford University Press.

Gray, Colin S. 2010. *The Strategy Bridge: Theory for Practice.* Oxford: Oxford University Press.

Hart, Liddell. 1967. *Strategy.* 2nd revised edition. New York: Frederick A. Praeger.

Mazarr, Michael J. 2015. *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* Carlisle, PA: U.S. Army War College Press.

Pariser, Eli. 2011. *The Filter Bubble: What the Internet Is Hiding from You.* New York: Penguin Press.

Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare.* New York: Farrar, Straus and Giroux.

Schelling, Thomas. 1966. *Arms and Influence.* New Haven, CT: Yale University Press.

Schoemaker, Paul J.H. 1995. "Scenario Planning: A Tool for Strategic Thinking." 36(2) ed.: 25–40.

Simon, Herbert A. 1971. *Designing Organizations for an Information-Rich World.* Edited by Martin Greenberger. Vols. Computers, Communications, and the Public Interest. Baltimore: Johns Hopkins University Press.

Singer, P.W., and Emerson T. Brooking. 2018. *LikeWar: The Weaponization of Social Media.* Boston: Houghton Mifflin Harcourt.

Sunstein, Cass R. 2009. *Going to Extremes: How Like Minds Unite and Divide.* Oxford: Oxford University Press.

World Health Organization. 2020. "Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation." Geneva: World Health Organization.

ACKNOWLEDGEMENTS

We would like to acknowledge the support of the Military Academy Research Centre (CINAMIL), which has been instrumental in the completion of this research.

FUNDING INFORMATION

The authors declare that no funding or financial support was received from any organisation, institution, or individual for the research, design, execution, or writing of this work.

CONFLICT OF INTEREST STATEMENT

The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

DATA AVAILABILITY STATEMENT

The data supporting this study are derived from publicly available sources and referenced within the article. No additional datasets were generated or analysed specifically for this research.

DECLARATION ON AI USE

The author confirms that AI tools, including language models such as ChatGPT, Notebooklm, and DeepL, were used solely to enhance the writing process, improve readability, and assist with grammar and formatting. All intellectual content, analysis, and critical arguments are the result of the author's original work. The AI tools were not used to generate research findings or substitute independent scholarly work.