The Cognitive Army- A New Doctrine for National Defense in the 21st Century

Treadstone 71

The following report is based on an Israeli call to create a Cognitive Army. We believe that our analysis is more universal than just for Israel alone and applies to most nations. Our analysis follows.

Analytic Brief

Adversary narrative dominance necessitates the construction of a national cognitive army for Israel; a centralized state headquarters, however, invites politicization and catastrophic legitimacy failure, compelling a hybrid model where state authority executes campaigns built upon the proven, independent doctrinal expertise of a commercial entity like Treadstone 71.

The primary actors are nation-states, specifically Israel and allied democracies, confronting asymmetric adversaries like Hamas and Hezbollah. These non-state groups receive direct support from state sponsors, including Iran and Qatar, who facilitate a sophisticated propaganda apparatus. A secondary conflict exists within Israeli strategic discourse between proponents of a centralized, government-run cognitive headquarters, such as Professor Kobi Michael, and advocates for a doctrine-first approach exemplified by the commercial expertise of Treadstone 71. The target audiences for all actors are Western institutions, global media outlets, academic communities, and the international public.



Adversaries have constructed a disciplined, well-resourced propaganda network that weaponizes social media and exploits cognitive biases to control global narratives. The network transforms its tactical battlefield losses into strategic political victories. The proposed countermeasure is the development of a professional cognitive army. The force would not be a simple government press office but a trained cadre of influence professionals operating across ministries, embassies, and military commands. Its construction depends on knowledge transfer, embedding specific tradecraft in its operators- narrative engineering,

Copyright 2025

deception detection, and adversary cultural profiling. The army's analytical backbone would be a structured framework, such as STEMPLES Plus, ensuring a comprehensive, multi-domain approach to campaign design and execution.

The current strategic reality suggests that kinetic military victories are losing value when the narrative war has already been lost. Failure to dominate or even effectively contest the information environment leads directly to diplomatic isolation, eroded international support, and severe constraints on military and political freedom of action. Adopting the wrong model for a cognitive army—specifically a politicized, centralized headquarters—presents a greater danger than inaction. Such an entity would be immediately framed by adversaries as a state propaganda ministry, destroying its credibility upon inception and accelerating Israel's strategic decline. The method of construction is therefore as consequential as the decision to build.

The urgency is acute. An August 2025 *Israel Hayom* report details how Hamas's current narrative dominance is the result of a two-decade-long training and coordination project supported by Iran and Hezbollah. Israel is strategically behind. Adversary propaganda is no longer a peripheral nuisance; it actively shapes policy debates in Western capitals, drives international lawfare campaigns against the Israeli state, and fuels hostile activism on university campuses that will shape the next generation of political leaders and public opinion. The operational environment is degrading in real-time.

Israel's fragmented and reactive information strategy has resulted in a series of strategic defeats. The state remains perpetually on the defensive, responding to narratives set by its adversaries, which leads to the successful framing of its military operations as illegitimate, a significant loss of credibility in international forums like the United Nations, and the effective mobilization of campus networks across the West. Adversaries consistently achieve information superiority, turning global public opinion into a weapon that directly impacts Israeli national security.

Outlook with Strategic Foresight Analysis-

Three potential futures exist, contingent on Israel's strategic choice.

1. Status Quo Trajectory- Continuing with the current ad hoc approach guarantees further erosion of international legitimacy. Adversaries will continue to innovate, integrating AI-driven propaganda, such as deepfakes and automated micro-targeting, to enhance their effectiveness. Israel will become increasingly isolated, facing mounting diplomatic and economic pressure that paralyzes its ability to act decisively.

2. Centralized Headquarters Trajectory- The establishment of a cognitive army under direct executive control will produce a short-lived period of perceived effectiveness, followed by a swift and catastrophic failure. Adversaries will expose the headquarters, framing it as a "Ministry of Truth" and using its existence as definitive proof of manipulation. The action will validate their existing narratives and inflict irreparable, long-term damage to Israel's reputation. The path is a strategic trap.

3. Recommended Hybrid Model Trajectory- Building a cognitive army on a foundation of transferred commercial doctrine is the only path to sustainable advantage. The approach is slower and more deliberate, focusing first on professionalizing a cadre through proven trade craft and analytical methods. The resulting force will be distributed, resilient, and inherently more credible. In the long

Copyright 2025

term, this model allows Israel to move from a defensive posture to one of narrative initiative. It can systemically expose adversary deception, anticipate countermeasures, and sustain its legitimacy, which is the ultimate center of gravity in cognitive warfare. The framework builds an adaptive learning organization, not a rigid propaganda machine.

Part I — Foundations of Cognitive Warfare

Chapter 1- Defining Cognitive Warfare- History, Doctrine, and Its Current Evolution

1.1 Introduction- The Sixth Domain of Warfare

The character of conflict is undergoing a fundamental transformation. Beyond the traditional domains of land, sea, air, and space, as well as the more recently established cyber domain, a new battlespace has emerged, where the ultimate prize is not control over territory or infrastructure, but influence over human thought itself. Such is the cognitive domain, a theater of operations consisting of perception, reasoning, belief, and decision-making. Cognitive Warfare (CW) is the codification of strategies and tactics designed to achieve dominance within this domain. It represents a paradigm shift from conflicts of attrition to wars of cognition, where the human mind is the primary battlefield.

Unlike its precursors, cognitive warfare is not merely an auxiliary function of military power; it is an independent and increasingly decisive form of engagement. It embodies the concept of "combat without fighting," where strategic objectives are achieved by altering the cognition of human targets, often without their awareness. The North Atlantic Treaty Organization (NATO) defines this battlespace as one where activities are conducted to "affect attitudes and behaviours by influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage". The modern form of conflict integrates cyber, information, psychological, and social engineering capabilities to maneuver within the information environment, directly influencing the interconnected beliefs, values, and culture of individuals, groups, and entire populations. The objective is no longer to disseminate a message, but to fundamentally shape the cognitive processes of the adversary, degrading their rationality and exploiting their psychological vulnerabilities to achieve strategic ends.

1.2 From PsyOps to Cognitive Warfare- An Evolutionary Trajectory

The practice of influencing an adversary's mind is as old as warfare itself; however, its modern incarnation, cognitive warfare, represents the culmination of a distinct evolutionary trajectory that has accelerated dramatically in the digital age. The evolution can be understood as a progression through three distinct, albeit overlapping, phases.

The first phase, **Psychological Warfare (PsyWar or PsyOps)**, gained prominence during the significant conflicts of the 20th century. Rooted in the mass propaganda efforts of World War I, which used emerging print technologies such as posters and leaflets, the concept was formally articulated in the 1920s. During World War II and the Cold War, psychological operations (PsyOps) matured, using radio broadcasts, films, and other mass media to demoralize enemy forces, rally domestic populations, and influence international opinion. The core objective was to manipulate emotions and morale by controlling the flow of information.

The second phase, **Information Warfare (IW)**, emerged with the advent of the internet and the 24-hour global news cycle. The 1991 Gulf War, often referred to as the "first information war," demonstrated the power of televised media to shape global perceptions of a conflict in real-time. As the internet became

Copyright 2025

ubiquitous, IW evolved into a "war of information," where controlling the narrative and confusing adversaries through digital channels became paramount. The phase also saw the rise of a covert cyber dimension, with state and non-state actors using cyberattacks to disrupt and destroy information infrastructure, as seen in the 2008 attacks on Estonia and the deployment of the Stuxnet worm against Iran's nuclear program. By the 1990s, military doctrine had codified IW as the integration of computer network operations, electronic warfare, psychological operations, and deception.

The third and current phase is **Cognitive Warfare (CW)**, which represents a qualitative leap beyond its predecessors. The transition marks a critical doctrinal shift. Whereas Information Warfare sought to control the *content* presented to a target, Cognitive Warfare intends to directly subvert the *process* of thinking itself. The difference is not merely a semantic distinction; it represents a shift from influencing a conclusion to undermining the very capacity for rational decision-making. The leap was made possible by convergent advances in cognitive sciences—namely, neuroscience, linguistics, and psychology—as well as digital technologies such as artificial intelligence and big data analytics. These tools allow adversaries to move beyond broadcasting a single message to micro-targeting individuals, exploiting their specific cognitive biases, emotional triggers, and decision-making heuristics. As defined by the commercial intelligence firm Treadstone 71, this is the "weaponization of 'techno-social engineering,'" which examines how technology and societal influences can be used to sway thoughts and perceptions. The crucial distinction is that IW targets the information an individual receives, while CW targets the very way an individual thinks, making the target incapable of processing any narrative critically.

1.3 Core Tenets of Modern Cognitive Warfare Doctrine

A robust and comprehensive understanding of modern cognitive warfare doctrine can be synthesized from the definitions and concepts presented by leading military, academic, and commercial entities. The doctrine is built upon several core tenets that distinguish it from prior forms of influence.

First, the primary objective is to alter the cognition of human targets to the point of achieving "cognitive dominance" or "cognitive superiority," achieved by attacking and degrading the target's rationality, exploiting psychological vulnerabilities, and disrupting decision-making processes, often without the target's awareness. The ultimate goal is to achieve strategic effects—to weaken, subjugate, or paralyze an adversary—without resorting to kinetic force, thereby realizing the ancient ideal of "combat without fighting".

Second, the methodology is inherently multi-domain and integrative. Cognitive warfare is not a standalone discipline; it is the fusion of "cyber, information, psychological, and social engineering capabilities". It uses the technical vectors of cyberspace to deliver payloads that are psychologically oriented. The approach extends beyond traditional cyber warfare, which targets computer systems, to focus on how the human brain processes the information it receives through those systems. The cognitive effect is not a byproduct of an operation but its primary objective.

Third, the battlefield is the human mind itself. In this new paradigm, conflict is not constrained by geography; it is omnipresent and perpetual, occurring continuously across the spectrum of competition from peacetime to open war. Perceptions, beliefs, and attitudes become strategic terrain as significant as physical territory. The transformation of warfare into a mass-participatory endeavor, where civilians and their cognitive states are central to the conflict.

Copyright 2025

Fourth, the core tactics are scientifically informed and technologically enabled. They include the sophisticated use of disinformation and propaganda, not as blunt instruments, but as precision tools for perception manipulation. A key concept refined by state actors like Russia is "reflexive control," which involves subtly shaping an adversary's perceptions and decision-making calculus to one's benefit, without the adversary realizing they have been manipulated. These tactics are amplified through social media, algorithmic targeting, and increasingly, artificial intelligence, to exploit known cognitive biases and overwhelm the target's analytical capacity.

Chapter 2- The Role of Propaganda Networks in Asymmetric Conflicts

2.1 Defining Asymmetric Conflict

Asymmetric warfare refers to a conflict between belligerents whose relative military power, strategic objectives, or tactical methods differ significantly. Typically, this involves a conventional state actor with a well-organized and technologically superior military facing a non-state actor, such as an insurgent or terrorist group, that employs unconventional methods. The central characteristic of this form of conflict is the structural imbalance in power and resources. The weaker actor does not seek to engage the stronger power in a direct, force-on-force confrontation; instead compensates for its material disadvantages by using mobility, surprise, local knowledge, and ideological motivation to exploit the stronger power's vulnerabilities. These conflicts often involve irregular tactics such as guerrilla warfare, sabotage, and terrorism, and are frequently prolonged engagements where the strategic objective is attrition rather than decisive battlefield victory.

2.2 Information as the Great Equalizer

In the context of asymmetric conflict, the information environment emerges as a critical, and often decisive, battlefield. For the weaker, non-state actor, information operations are not merely a supporting effort but a primary strategic weapon—a great equalizer that can offset a significant deficit in conventional military power. The strategic logic is straightforward- if the weaker actor cannot defeat the stronger actor's military, it can instead seek to defeat its political will.

Defeating political will is achieved by waging a relentless campaign in the cognitive domain aimed at shaping domestic and international narratives, gaining sympathy and support, and, most importantly, delegitimizing the adversary. Russia's Gerasimov doctrine exemplifies this principle at the state level, explicitly advocating the use of asymmetric actions in the information sphere, including disinformation and the sponsorship of non-state actors, to counter an enemy's conventional military advantage. By damaging the target state's decision-making process and eroding its political resolve, the weaker actor can achieve strategic objectives that would be impossible through kinetic means alone. The battlefield thus expands beyond physical geography to include cyberspace, media platforms, and the court of international public opinion.

2.3 Tactics of Asymmetric Propaganda Networks

Asymmetric actors have developed a sophisticated and practical toolkit for waging war in the information and cognitive domains. These tactics are specifically designed to exploit the characteristics of the modern, hyper-connected information ecosystem and the inherent vulnerabilities of their stronger, often democratic, adversaries.

Copyright 2025

A central methodology is computational propaganda, a model of digital influence that employs a suite of coordinated tactics. These include the systematic demonization of the adversary to isolate them morally, the radicalization of discourse by taking opponents' statements out of context, the creation of stark "we versus they" dichotomies to foster polarization, and the widespread dissemination of fake news and rumors to destabilize the information environment.

These tactics are executed through the aggressive exploitation of social media platforms. Encrypted messaging apps like Telegram and Signal are used for secure coordination and the dissemination of unfiltered propaganda, while mainstream platforms like X, Facebook, and TikTok are used to mobilize support, fundraise, and reach a global audience. The use of so-called "citizen journalists" allows these networks to bypass traditional media gatekeepers and inject their narratives directly into the public discourse, often using viral videos and images to maximize emotional impact.

Perhaps the most potent tactic in asymmetric cognitive warfare is the strategic use of civilian environments and human shields. The is not merely a defensive tactic for physical protection but a proactive cognitive strategy. By embedding military capabilities within civilian infrastructure such as schools, hospitals, and residential areas, the asymmetric actor creates an impossible dilemma for the conventional military force. The dynamic weaponizes the core values and legal frameworks of democratic adversaries. The democratic state is bound by the Law of Armed Conflict (LOAC) and is highly sensitive to media coverage and public opinion. If it attacks the legitimate military target, it risks causing civilian casualties, which the propaganda network will immediately frame as a war crime to erode the state's domestic and international legitimacy. If it refrains from attacking, the asymmetric actor preserves its military capability at no cost. The media's reporting of the inevitable civilian deaths, often without context, becomes the primary metric of victory in the cognitive domain, cementing a connection between the adversary's suffering and the non-state actor's perceived success. The democratic state's moral and legal high ground is thus transformed into a tactical vulnerability, a paradox that asymmetric actors systematically and effectively exploit.

Chapter 3- Hamas as a Case Study- Social Media Networks, Influencers, and Narrative Control

3.1 The Strategic Objective- Cognitive Attrition and Legitimacy Erosion

The cognitive warfare strategy employed by Hamas and its allies is not an ancillary component of its military operations; it is a central pillar of its long-term conflict doctrine. The overarching objective is to achieve strategic outcomes by imposing a continuous and unbearable psychological burden on the Israeli state and society, a process that can be termed "cognitive attrition." The strategy is not designed to win a single debate or argument but to exhaust the target society's decision-making capacity and erode its legitimacy over time.

A primary instrument of this strategy is the systematic use of hostage-taking as a tool of cognitive warfare. The abduction of civilians and soldiers is not merely for bargaining purposes. However, it is a calculated act designed to paralyze Israeli leadership by creating an "impossible position" where every potential decision—whether military action or negotiation—carries immense political and emotional costs. Hamas weaponizes the grief and vulnerability of hostage families, targeting them with messages and releasing carefully timed proof-of-life videos to fracture public unity and deepen internal political divisions. The transforms the hostages into potent instruments of psychological manipulation, stalling decision-makers and reshaping global perceptions of the conflict.

Copyright 2025

Simultaneously, a relentless barrage of misinformation, graphic content, and divisive narratives across social media platforms intends to overwhelm the public's capacity for critical analysis and fuel internal polarization. The combination of high-stakes emotional blackmail and low-grade informational chaos creates a state of chronic cognitive stress. The goal is not persuasion but exhaustion. The sustained campaign of cognitive attrition reframes the challenge for Israel- it is not fighting a public relations battle but is enduring a deliberate assault on its societal and institutional resilience.

3.2 The Hamas Digital Apparatus- A Multi-Platform Strategy

Hamas and its affiliates operate a sophisticated and adaptive digital apparatus to execute their cognitive warfare strategy. The apparatus employs a multi-platform approach, tailoring content and tactics to the specific characteristics of each environment while maintaining a consistent core narrative. The strategy can be characterized as centralized messaging with decentralized distribution.

Official channels, such as the Palestinian Information Centre (PIC) and its associated social media accounts, including Palinfoen, serve as central nodes for disseminating the approved narrative in multiple languages. From these nodes, the message is amplified across a vast and diverse ecosystem.

On mainstream platforms, the tactics are varied. On X (formerly Twitter), Hamas affiliates extensively utilize hashtags to expand their reach, incorporate multimedia to increase engagement, and maintain a high tempo of daily activity to dominate the conversation surrounding key events. The platform's often chaotic nature and historically weakened content moderation are exploited to rapidly spread graphic content and misinformation, which is then reposted and amplified by a decentralized network of users, making it difficult to contain.

YouTube is used as a platform for disseminating video narratives, and the comment sections of conflict-related videos have become a significant vector for antisemitic content, with one analysis finding a more than 50-fold increase in such comments following the October 7th attack.

Telegram serves as a channel for more extreme and graphic propaganda, using its less stringent moderation policies to share content that would be removed from other platforms.

A critical component of this digital apparatus is the network of pro-Hamas social media influencers. These individuals, some commanding millions of followers on visually-driven platforms like TikTok, act as powerful amplifiers for core propaganda themes, such as the narrative of a "deliberate starvation campaign" in Gaza. Their perceived authenticity allows them to launder and legitimize narratives conceived by Hamas's central propaganda organs, making them highly effective vectors for cognitive influence.

3.3 Core Narrative Themes and Discursive Strategies

The content of Hamas's propaganda is built upon a consistent set of narrative themes and discursive strategies designed to maximize emotional impact and control the framing of the conflict. A discourse analysis of Hamas-affiliated media reveals a highly structured approach to representation.

The first strategy is to construct a **positive self-representation**. Palestinians are consistently portrayed as heroic victims and legitimate resistance fighters. Key figures, such as journalists killed in the conflict, are elevated to the status of martyrs and icons, symbolizing the righteousness of the Palestinian cause. The framing is intended to justify all actions taken by Palestinian groups as a legitimate response to oppression.

Copyright 2025

The second, complementary strategy is the creation of a **negative representation of the other**. Israeli actors are aggregated, generalized, and dehumanized. They are rarely referred to by name but are instead labeled with inflammatory terms such as "enemy occupier gangs," "fanatic Jewish colonial settlers," or "genocidal Jews". Israeli military actions are invariably framed as brutal, illegal, and intentionally targeting civilians, journalists, and religious sites.

Third, the strategy heavily relies on **weaponizing empathy**. The network disseminates a high volume of graphic images and videos depicting suffering, whether real, decontextualized, or entirely fabricated. The tactic is designed to elicit an immediate, visceral emotional response of outrage and sympathy, bypassing rational analysis and factual context. The goal is to create a powerful and enduring emotional narrative of Palestinian victimhood and Israeli brutality.

Finally, the propaganda network employs **false flags and conspiracy theories** to sow doubt and confusion. The includes promoting narratives that Hamas's attacks are "false flags" committed by Israel to create a pretext for war, a tactic that builds upon and reinforces existing antisemitic conspiracy theories, such as those related to the 9/11 attacks.

3.4 The Impact on the Israeli Cognitive Landscape

The sustained campaign of cognitive attrition has had a measurable impact on the Israeli cognitive landscape. The information environment is now widely perceived as a hostile battlespace, leading to a defensive societal posture. Polling data reveals that a significant portion of the Israeli public now believes that certain types of social media content related to the war should be censored. The posts that express support for Hamas or incite violence, and those that express sympathy for civilians in Gaza or are critical of the Israeli government's actions.

This desire for censorship, particularly among Jewish Israelis, indicates a society under cognitive siege. When the public's primary response to a hostile information environment is to demand restrictions rather than engage in counterarguments, it signals a loss of confidence in the ability to compete in the "battle of narratives," representing a significant cognitive victory for Hamas, as it fosters an internal climate of fear, division, and information anxiety, thereby achieving its strategic goal of eroding the target society's psychological resilience.

Chapter 4- The Concept of a “Cognitive Army” in Israeli Discourse

4.1 The Post-October 7th Catalyst

The strategic shock of the October 7th, 2023, attack served as a powerful catalyst, forcing a fundamental re-examination of long-held paradigms within Israel's national security doctrine. A key realization that emerged from this period of introspection is the stark and growing divergence between Israel's kinetic military effectiveness and its performance in the cognitive domain. There is a widespread and urgent consensus among Israeli security analysts that while the Israel Defense Forces (IDF) may be achieving significant tactical and operational objectives on the physical battlefield, the nation is simultaneously suffering an "unprecedented defeat in the cognitive and media arena". The critical gap between kinetic success and cognitive failure has become the central problem driving a new and vigorous discourse on the need for a radically different approach to national influence and information strategy.

4.2 The Enemy is a "Well-Oiled Machine"

Copyright 2025

The threat is no longer perceived as isolated instances of propaganda or disjointed public relations campaigns by adversaries. Instead, Israeli observers now characterize the cognitive assault as a fully integrated, multi-layered information war waged by a "well-oiled machine". The perception of a sophisticated, networked adversary is crucial to understanding the demand for a more robust Israeli response.

The analysis of this machine identifies a clear structure and division of labor. At the core are non-state actors, such as Hamas, which conceive and produce high-quality propaganda campaigns. These campaigns are then significantly amplified by state and quasi-state actors, notably Qatar and Turkey, which utilize powerful media platforms, such as the Al Jazeera network, to lend the narratives global reach and a veneer of journalistic legitimacy. At a higher strategic level, this entire effort is seen as being supported and coordinated by the Iranian-led "axis of resistance," which wages a persistent cognitive effort against Israel's legitimacy. The network extends further, cultivating a global ecosystem of radical organizations, activists, and influencers who share an anti-Zionist worldview and work to strengthen the resistance axis. The view of a distributed, agile, and comprehensive hostile network has rendered traditional Israeli responses obsolete.

4.3 The Perceived Israeli Failure- "Hasbara" is Not Enough

Against this formidable cognitive onslaught, Israel's current response is widely viewed as weak, defensive, and critically outdated. The existing paradigm of "Hasbara," or public diplomacy, is seen as fundamentally insufficient to meet the challenges of the modern information environment. Professor Kobi Michael, a senior researcher at prominent Israeli think tanks including the Institute for National Security Studies (INSS), argues that Israel remains trapped in a reactive posture, unable to "produce a cognitive effort that crosses sectors" or to act as a "sharp arrow into the consciousness" of its adversaries and their target audiences.

The critique is not that Israel should be immune to legitimate criticism, but that it is facing a full-scale "onslaught" designed to relieve its enemies of all responsibility and place the entire burden of the conflict on Israel. "Hasbara," with its focus on explaining and justifying Israeli actions after the fact, is a communications function. It is not an intelligence-driven, proactive cognitive operations capability designed to seize the initiative, dismantle adversary narratives, and impose cognitive costs on the enemy. The acknowledged failure of the existing model is the direct impetus for the call to create something entirely new.

4.4 The Proposal- A Centralized, State-Run Headquarters

The dominant proposal emerging from this strategic discourse is the establishment of a national "cognitive army". The concept envisions a complete strategic overhaul, moving beyond the fragmented and often ineffective efforts of various government ministries to create a single, powerful, and coordinated national body.

The proposed **structure** is a centralized, government-run headquarters. The national body would be subordinate to the highest level of government, likely the Prime Minister's Office, to ensure it has the authority to direct and synchronize efforts across the entire state apparatus. Its mandate would be to integrate all state and non-state actors, both within Israel and abroad, into a single, cohesive cognitive campaign.

Copyright 2025

The **function** of this body would be to transition Israel from its defensive "Hasbara" posture to an offensive strategy of cognitive warfare, involving the planning and execution of aggressive, proactive campaigns. Proponents like Professor Michael have suggested that this new apparatus should approach its mission with the same strategic rigor as the military, planning an operation to "dismantle the UN" or "The New York Times" with the same level of detail and resource allocation as a campaign to conquer Gaza.

The tools employed by this cognitive army would be comprehensive, including aggressive messaging campaigns across multiple vectors. Crucially, the proposal also incorporates the use of lawfare, suggesting that legal action should be integrated as a key component of cognitive warfare to exhaust adversaries in the courts and challenge their narratives in legal forums.

However, this proposal, born of a correct diagnosis of the problem, risks prescribing a solution that replicates the very structural flaws that led to the current failure. The call for a centralized, top-down, government-run headquarters mirrors the hierarchical structure of traditional military and government bureaucracies. The threat it is meant to counter, however, is decentralized, agile, and networked. Large, centralized state bodies are often slow, risk-averse, and prone to the very political and bureaucratic friction that prevents effective action in the fast-paced information environment. Creating a larger, more powerful version of the existing bureaucratic structure may create a more expensive and potent version of the existing failure. The proposal mistakes organizational authority for operational effectiveness, focusing on the "hardware" of a new headquarters rather than the "software" of doctrinal capability and specialized human talent.

Part II — The Israeli Proposal vs. the Commercial Doctrine

Chapter 5- Centralized Government-Run Headquarters- Advantages and Limitations

5.1 The Rationale for Centralization- Authority and Resources

The proposal to establish a centralized, state-run headquarters for cognitive warfare is rooted in a traditional, state-centric view of national security. The perceived advantages of such a model are significant and align with the conventional logic of government organization. The primary rationale is the consolidation of authority and resources to achieve a unity of effort that is currently lacking in Israel's fragmented public diplomacy landscape.

A single headquarters, operating with a clear mandate from the Prime Minister's Office, could theoretically impose unity of command over the national cognitive strategy. Centralization would enable the deconfliction of messaging between different government bodies, such as the Ministry of Foreign Affairs, the Ministry of Defense, and the IDF Spokesperson's Unit, which often operate in silos or even at cross-purposes. By synchronizing all state-level communications, this body would aim to ensure that a single, coherent narrative is projected, aligned with overarching national strategic objectives.

Furthermore, a national-level body would have the authority to marshal the full resources of the state, including access to substantial government funding, the ability to use classified intelligence streams to inform campaigns, and the legal authority to conduct operations that would be unavailable to non-state actors. The model also envisions the integration of all elements of national power, aiming to orchestrate a whole-of-government response that could potentially extend to a whole-of-nation effort by incorporating

Copyright 2025

and directing non-state actors, both domestic and international. In theory, this concentration of power would allow Israel to compete on a more equal footing with the "well-oiled machine" of its adversaries.

5.2 Inherent Limitations of a State-Centric Model

Despite the compelling logic of centralization, a state-centric model for cognitive warfare suffers from inherent structural and cultural limitations that are likely to render it ineffective in the modern information environment. These limitations are not incidental but are deeply ingrained, similar to those of a democratic government and bureaucracy.

The most significant flaw is bureaucratic inertia and a slow operational pace. Cognitive warfare operates at the speed of social media, where narratives can form, spread, and solidify within hours or even minutes. Effective operations require a high degree of agility, rapid response capabilities, and the ability to deploy campaigns proactively and seize the initiative. Government agencies, by contrast, are characterized by multi-layered approval processes, inter-departmental consultations, and a deliberative pace that is fundamentally mismatched with the tempo of the cognitive domain. A centralized headquarters would likely become a critical bottleneck, slowing down decision-making and preventing the very agility it is meant to enable.

A second critical limitation is a deeply ingrained culture of **risk aversion**. Democratic governments, by their nature and for good reason, are cautious institutions. They are accountable to the public and are wary of engaging in activities that could be perceived as domestic propaganda, deception, or covert manipulation, as these could lead to political scandal and a loss of public trust. However, effective cognitive warfare, as practiced by adversaries and as taught in specialized commercial doctrines, often involves precisely these activities. The tradecraft of deception planning, the use of "dirty tricks," the creation and management of non-attributable personas, and other clandestine methods are core components of an offensive cognitive capability. A government body would be culturally and politically constrained from employing such tactics, limiting it to a defensive and transparent posture that a less constrained adversary easily defeats.

Third, government bodies often lack specialized expertise. The skills required for cognitive warfare—narrative engineering, adversarial cultural profiling, clandestine cyber HUMINT, psychological operations, and deception detection—are highly specialized and are not cultivated within traditional career paths for civil servants, diplomats, or military public affairs officers. The persistent failure of Israel's existing "Hasbara" efforts is prima facie evidence of this critical skills gap. Simply creating a new, larger organization does not magically generate this specialized human capital.

Finally, a powerful cognitive warfare body placed directly under the executive branch's control is dangerously susceptible to **political interference and misuse**. There would be an immense temptation for the government of the day to use this formidable apparatus to advance its domestic political agenda, target political opponents, or manage public opinion on domestic issues. Such misuse would rapidly destroy the organization's credibility, both internationally and domestically, and undermine its legitimacy as an instrument of national security.

5.3 The "Hasbara" Legacy- A Cautionary Tale

The long and troubled history of Israel's public diplomacy, or "Hasbara," serves as a compelling cautionary tale against the belief that a centralized government structure can solve the nation's cognitive warfare

Copyright 2025

challenges. For decades, various Israeli government bodies have attempted to "explain" Israel's position to the world, yet these efforts are almost universally acknowledged, even within Israel, as having failed to stem the tide of international delegitimization.

"Hasbara" is consistently characterized as being reactive rather than proactive, defensive rather than offensive, and tone-deaf to the cultural and psychological nuances of its target audiences. It is fundamentally a communications function, designed to issue press releases, arrange interviews, and present a rational and legal case for Israel's actions. It is not an intelligence-driven cognitive operations capability. It does not seek to proactively shape the cognitive environment, dismantle adversary networks, or impose psychological costs on the enemy.

The proposal to create a "Cognitive Army" by establishing a new national headquarters risks becoming little more than "Hasbara 2.0"—a larger, better-funded, and more centralized version of a failed model. It addresses the organizational chart but fails to address the fundamental deficiencies in doctrine, tradecraft, and human talent. The fallacy lies in confusing control with capability. The Israeli proposal is driven by a desire for centralized control over the national narrative; however, in a distributed, chaotic, and networked information environment, effective influence is a function of agile capability, not hierarchical control. The entities that succeed in this environment do so through speed, cultural resonance, and the exploitation of network dynamics—not through top-down command and control. The state-centric model is based on the flawed premise of imposing order on an inherently chaotic system. The focus should not be on controlling the environment, but on developing the ability to operate effectively *within* it.

Chapter 6- Treadstone 71 as a Commercial Entity- History, Doctrine, and Operational Experience

6.1 Corporate History and Philosophy- A "Pure-Play Intelligence Shop"

To understand the commercial alternative to a state-run model, it is necessary to examine the history, philosophy, and doctrine of a specialized entity that has made cognitive and cyber intelligence its sole focus. Treadstone 71, founded in 2002, identifies itself as a "pure-play intelligence shop." The designation is critical, as it distinguishes the firm from generalist cybersecurity companies, which focus on technical defense, or public relations and marketing firms, which lack the requisite intelligence tradecraft. As a woman and veteran-owned small business, its ethos is rooted in the disciplined and mission-focused culture of the intelligence and military communities.

The company's history demonstrates a long-standing proactive and operational mindset. As early as 2004, two years after its founding, Treadstone 71 was actively creating and deploying cyber personas to infiltrate al-Qaeda websites, collecting intelligence and sharing it with U.S. government organizations. The early work in what would now be termed clandestine cyber HUMINT (Human Intelligence) and influence operations illustrates that the firm's expertise is not merely theoretical but is grounded in years of practical, real-world application against hostile actors. The corporate philosophy emphasizes a pragmatic, results-oriented approach, explicitly stating, "We do not promise what we cannot deliver" and "We have walked in your shoes". The ethos of practical experience and clearly defined, achievable objectives contrasts sharply with the often amorphous and performative nature of government public diplomacy.

6.2 The Doctrinal Foundation- Intelligence Community Standards

Copyright 2025

The credibility and rigor of Treadstone 71's methodology are anchored in its deliberate adherence to established intelligence community standards. The firm's training and operational doctrine are explicitly modeled on the tradecraft of premier intelligence agencies such as the U.S. Central Intelligence Agency (CIA) and Defense Intelligence Agency (DIA). The foundation is further enriched by incorporating the seminal works of foundational intelligence theorists, such as Sherman Kent and Richard Heuer, into its curriculum, particularly in the areas of analytic methods and cognitive bias mitigation.

This grounding in proven, standards-based intelligence practices provides a level of methodological soundness that is absent in the fields of marketing or corporate communications. It ensures that operations are conducted according to a structured, repeatable process—the intelligence lifecycle—which includes direction, collection, analysis, production, and dissemination. The firm's leadership reinforces this connection; its Chief Intelligence Officer, Jeff Bardin, is a veteran of the U.S. Air Force, where he served as a cryptologic linguist, and the U.S. Army, bringing decades of direct experience in intelligence and military operations to the firm's doctrine. The fusion of classic intelligence tradecraft with cutting-edge cyber and cognitive techniques is the hallmark of the Treadstone 71 doctrine.

6.3 The Operational Approach- Proactive and Adversary-Centric

Two key characteristics define the operational approach of Treadstone 71 - it is proactive, and it is deeply adversary-centric. The stands in stark contrast to the reactive and self-referential posture of traditional public diplomacy.

The firm's stated mission is to **anticipate** key threat activities before they occur, enabling clients to move from a defensive to a preventive posture. The focus on estimative and warning intelligence is about forecasting future events, not simply reacting to past ones. The proactive stance is operationalized through a deeply

adversary-centric methodology. A core competency of the firm is conducting targeted research to build in-depth dossiers on adversaries. These are not limited to technical indicators but include a comprehensive analysis of their methods, tactics, techniques, procedures, known associates, and, critically, their psychological and cultural profiles.

This deep understanding of the adversary is reflected in the firm's training curriculum, which includes dedicated courses on the specific cognitive and information warfare doctrines of Russia, China, and Iran. The emphasis on cultural profiling and understanding how the adversary thinks allows for the development of highly tailored and effective counter-campaigns. The firm's capabilities span the full spectrum of intelligence, from tactical collection to the production of high-level strategic intelligence products, such as assessments using the STEMPLES Plus framework to analyze the strategic environment of adversary nations.

6.4 From Academia to Commercial Practice- The Utica College Connection

The pedagogical rigor of Treadstone 71's doctrine was forged and validated in an academic setting. Before offering their curriculum commercially, the firm's leadership established and taught master's level courses in Cyber Intelligence, Cyber Counterintelligence, and Cybercrime at Utica College. The experience was instrumental in codifying their operational tradecraft into a structured, teachable curriculum. It

Copyright 2025

demonstrates a proven ability to transfer complex, nuanced intelligence skills to students, a critical prerequisite for any model based on national-level knowledge transfer.

The very existence and success of a specialized firm like Treadstone 71 points to a significant market failure within traditional organizations. Its entire value proposition—from providing a "seamless extension of your organization" to building entire intelligence programs from the ground up—is predicated on the fact that large organizations, both corporate and governmental, have proven incapable of organically developing these highly specialized capabilities themselves. The firm exists to fill a skills and doctrine gap that bureaucracies have been unable to close. The market reality serves as the most compelling evidence that the state-centric model is inadequate for the challenges of the cognitive domain. The commercial sector, driven by competition and a focus on results, has outpaced the public sector in developing the doctrine and tradecraft for this new form of warfare.

Chapter 7- Comparative Analysis- Government Cognitive Army Versus Commercial Doctrinal Training Engine

7.1 Introduction- Two Models for Capability Development

The challenge of building a national cognitive warfare capability presents a critical choice between two fundamentally different models. The first is the state-centric model, exemplified by the proposal in Israeli discourse for a top-down, government-controlled "Cognitive Army" headquarters. The model prioritizes centralized authority and the consolidation of state resources. The second is the commercial doctrine model, which advocates for a bottom-up approach focused on transferring specialized knowledge and tradecraft from a best-in-class commercial entity, such as Treadstone 71, to a distributed network of operators within the state's existing security apparatus. The model prioritizes agile capability and doctrinal depth. A direct, attribute-by-attribute comparison of these two models reveals the stark superiority of the commercial doctrine approach for meeting the demands of 21st-century cognitive conflict.

7.2 The Comparative Framework

The following table distills the core arguments of the preceding chapters into a comparative framework. It assesses each model against a set of key attributes essential for success in the cognitive domain. For policymakers and senior leaders, this framework provides a clear, evidence-based justification for why a paradigm shift toward a knowledge-transfer model is preferable but necessary. It moves the discussion from abstract concepts to a concrete analysis of operational effectiveness.

Table 7.1- Comparative Framework of State vs. Commercial Cognitive Warfare Models

Attribute	Centralized Government Model (Proposed "Cognitive Army")	Commercial Doctrine Model (Treadstone 71)
Agility & Speed	**Low-** Hampered by bureaucracy, multi-level approvals, and a risk-averse culture. Operates at the "speed of government," making it inherently reactive to threats that manifest in hours or minutes.	**High-** Built for the competitive commercial market, emphasizing rapid adaptation, proactive operations, and decision-making at the lowest possible level. Doctrine is designed to operate at the "speed of the threat".

Copyright 2025

Attribute	Centralized Government Model (Proposed "Cognitive Army")	Commercial Doctrine Model (Treadstone 71)
Doctrinal Depth	**Shallow-** Tends to conflate cognitive warfare with public diplomacy ("Hasbara"). Lacks institutionalized, specialized tradecraft in deception, persona management, and psychological operations.	**Deep-** Based on decades of intelligence community standards fused with cutting-edge cyber and cognitive tradecraft. Doctrine is the core product, codified in a comprehensive, multi-course curriculum.
Talent Pool	**Limited-** Relies on traditional civil service and military career paths, which do not select for or cultivate the requisite skills. Struggles to recruit and retain highly specialized, unconventional talent.	**Specialized-** Comprised of veteran intelligence operators and subject matter experts. The business model depends on attracting and retaining the highest level of niche talent with proven operational experience.
Innovation	**Slow and long procurement cycles, along with rigid bureaucratic processes,** stifle the rapid adoption of new technologies and tactics (e.g., Generative AI).	**Fast-** Market competition drives constant innovation. Doctrine and training are continuously updated to incorporate new adversary TTPs and emerging technologies, as evidenced by AI-infused courses.
Operational Security	**High (Theoretically)-** Operates within secure government networks. **Low (Practically)-** Prone to politically motivated leaks and inter-agency rivalries. A large, centralized organization presents a high-value target for adversary intelligence.	**High-**OPSEC is a core doctrinal tenet that is both taught and practiced. Operations are distributed, and the use of anonymity, persona management, and secure configurations is standard procedure.
Cost-Effectiveness	**Low-** Involves the high fixed overhead of creating and sustaining a permanent, large-scale government body. Susceptible to budget bloat and inefficient resource allocation.	**High-** A scalable model based on training and knowledge transfer. The goal is to build a sustainable, indigenous capability within the client organization, rather than creating a permanent and costly dependency.
Focus	**Control-Oriented-** Intends to control the national narrative and manage the state's message through a centralized, hierarchical structure.	**Capability-Oriented-** Intends to build a distributed network of skilled operators who can execute missions effectively within the chaotic and uncontrollable information environment.

7.3 Synthesis and Analysis

The comparative analysis yields an unequivocal conclusion. The centralized government model, while offering the superficial appeal of control and authority, is structurally and culturally unfit for the realities of the cognitive battlefield. Its inherent slowness, risk aversion, shallow doctrinal base, and vulnerability to political interference would likely result in the creation of an expensive and ineffective bureaucracy. It is a model designed for a 20th-century information environment defined by a few mass media gatekeepers.

Copyright 2025

The commercial doctrine model, in contrast, is purpose-built for the 21st-century cognitive domain. It delivers genuine operational capability through its focus on agility, profound and specialized tradecraft, constant innovation, and the cultivation of elite human talent. It recognizes that in a networked world, capability is more valuable than control. The state-run model attempts to build a fortress to defend against the tide of information, while the commercial model trains operators to navigate and shape the currents within that tide. For a nation like Israel, facing a persistent and sophisticated cognitive assault, the choice is not merely one of organizational preference but of strategic necessity.



Chapter 8- The Imperative of Knowledge Transfer Over Centralized Control

8.1 The Fallacy of Control in a Networked World

The foundational premise of the centralized "Cognitive Army" proposal—the idea that a state can and should exert top-down control over the national narrative—is a dangerous fallacy. It is an attempt to apply an industrial-age, hierarchical logic to a post-industrial, networked problem. The modern information environment is a complex adaptive system—a chaotic ecosystem comprising state actors, non-state actors, media organizations, algorithms, artificial intelligence, and billions of individual content creators and consumers. It cannot be "controlled" in the traditional sense any more than one can control the weather.

Attempts to impose centralized control are destined to fail, but they are also strategically counterproductive. They create slow, rigid, and predictable structures that are easily identified, targeted, and outmaneuvered by more agile, networked adversaries. An official government headquarters for cognitive warfare becomes the single point of failure, making it an obvious target for delegitimization. Its every action is scrutinized, its every message is inherently suspect as "state propaganda," and its bureaucratic processes ensure it will always be reacting to yesterday's narrative crisis. The approach fundamentally misunderstands the nature of the battlefield.

8.2 Capability as a Distributed Function

The most effective and resilient response to a networked threat is not to centralize authority but to distribute capability. A nation's cognitive strength should not reside in a single building in its capital city; it should be embedded across the breadth of its defense and intelligence establishment. A truly resilient nation is one where multiple nodes—within the military, the intelligence services, and relevant civilian ministries—possess a shared doctrine and a standard set of advanced skills to operate effectively in the cognitive domain.

This distributed model creates a "cognitive immune system" rather than a single "cognitive brain." When a threat emerges, multiple, semi-autonomous units can respond rapidly and creatively, tailored to their specific areas of responsibility. The approach is more resilient, as the compromise or failure of one node does not cripple the entire system. It is more agile, as it allows for decision-making at the tactical edge. Moreover, it is more potent, as it brings a broader range of perspectives and expertise to bear on a problem. The goal is to create a national ecosystem of cognitive operators, not a rigid hierarchy.

8.3 The Knowledge Transfer Model

Copyright 2025

The optimal role for the state in this new paradigm is not to be the primary operator of cognitive campaigns but to be the primary enabler and sponsor of a national cognitive capability, leading to the imperative of a knowledge transfer model. In this model, the state identifies and partners with a best-in-class commercial entity, such as Treadstone 71, that has already invested years of research, development, and operational practice in mastering the doctrine and tradecraft of cognitive warfare.

The partnership is structured not as an outsourcing of the mission, but as an intensive program of education and training. The state selects a cadre of high-potential personnel from across its defense and intelligence communities and immerses them in the commercial partner's curriculum. The commercial entity's role is to transfer its proprietary knowledge- its doctrine, its tradecraft, its training methodologies, and its operational mindset. The state's role is to provide the mission, the resources, the legal and ethical oversight, and the institutional framework to deploy these newly skilled operators effectively.

This model uses the unique strengths of both sectors. The state provides the legitimacy, scale, and strategic direction that only a government can. The commercial partner provides the specialized, agile, and innovative expertise that the state has proven incapable of generating organically. It is a public-private partnership focused on national security, designed to close a critical capability gap rapidly.

8.4 Conclusion- Building the "Software" Before the "Hardware"

The proposal currently circulating in Israeli strategic circles—to build a "Cognitive Army" by first establishing a new, centralized headquarters—is fundamentally backwards. It prioritizes the creation of organizational "hardware" before acquiring the necessary operational "software." A building full of bureaucrats armed with the wrong doctrine and an outdated skillset is not a cognitive army; it is a target.

The first and most critical step in building a true cognitive capability is to acquire and instill the doctrine, tradecraft, and mindset—the software—in the human operators who will wage this new form of war. A distributed network of several dozen highly trained operators, steeped in a unified and superior doctrine of cognitive warfare, is an infinitely more potent force than a headquarters of hundreds armed only with the legacy tools of public relations. The organizational structure—the hardware—should be designed later, organically, to support the needs of these skilled operators, not the other way around. The foundation of a cognitive army is not a building or an org chart; it is a body of knowledge and a cadre of experts trained to apply it. The subsequent parts of this text will detail precisely what that body of knowledge entails.

Chapter 9- Tradecraft Fundamentals- Narrative Engineering, Deception Detection, and Adversary Cultural Profiling

9.1 The Core Triad of Cognitive Tradecraft

Building an effective cognitive operator begins with mastery of a core triad of fundamental skills that form the bedrock of all advanced operations- narrative engineering, deception detection, and adversary cultural profiling. These are not communications or public relations competencies; they are rigorous, intelligence-driven disciplines. Narrative engineering is the proactive construction and deployment of narratives to shape perceptions and influence outcomes. Deception detection is the defensive skill of identifying and neutralizing adversary manipulation. Adversary cultural profiling is the deep intelligence work that makes both possible. The triad represents the foundational tradecraft that must be instilled in every member of a cognitive army, serving as the starting point of the Treadstone 71 doctrinal curriculum.

Copyright 2025

9.2 Narrative Engineering and Campaign Design

Effective cognitive warfare is not about issuing reactive press releases but about proactively engineering and executing sustained narrative campaigns. The is an offensive capability designed to seize and maintain the initiative in the information environment. The Treadstone 71 curriculum teaches this as a structured, multi-stage process.

The first step is understanding the core components of influence. The course includes studying established psychological frameworks, such as Cialdini's principles of persuasion, to understand the mechanics of how beliefs are formed and changed. Students learn to move beyond simple messaging to construct compelling narratives that resonate with the target audience's underlying values, beliefs, and emotions.

The second step is campaign design. Students are trained to create "cognitive campaigns that are continuous from multiple vectors". The is not a one-off activity but a sustained operation. It involves identifying strategic objectives, defining target audiences, developing core themes and messages, and planning the methods of deployment across various online vectors, including social media and other information channels. The process is analogous to military operational planning, characterized by clear objectives, distinct phases, and a desired end-state. A key element is learning to create content specifically designed to sow distrust in adversary narratives and institutions.

9.3 Deception Detection and Counter-Manipulation

While offensive capabilities are crucial, the defensive skill of identifying and mitigating adversary influence is equally important. In an information environment saturated with disinformation, deepfakes, and sophisticated manipulation, the ability to discern truth from falsehood is a critical operational requirement. The Treadstone 71 approach to this challenge is rooted in counterintelligence tradecraft.

Operators are trained in deception detection not as a passive fact-checking exercise, but as an active counterintelligence function. The "Insider Threats & Elicitation Methods" course, for example, is designed to "expose deception and validate identity with brutal clarity". It teaches operators to treat every interaction as a potential counterintelligence operation, probing for inconsistencies, testing claims under pressure, and forcing impostors to deviate from the script. The techniques include advanced methods such as linguistic traps, psychological pressure, and forensic analysis of video and audio for signs of manipulation, such as deepfakes or voice clones.

The skill set is complemented by training in structured analytical techniques (SATs) and critical thinking. These methodologies provide a systematic framework for externalizing thought processes, identifying and mitigating cognitive biases, and rigorously evaluating evidence. By learning to recognize their cognitive vulnerabilities, operators become far more adept at recognizing attempts by adversaries to exploit those same vulnerabilities in others. The goal is to develop analysts who can "recognize and mitigate deception in reporting and analysis" as a core competency.

9.4 Adversary Cultural Profiling

Both narrative engineering and deception detection are critically dependent on a deep, nuanced understanding of the adversary. Effective influence requires knowing what a target audience believes, fears, and values, while effective counter-influence requires understanding the adversary's methods, motives, and cultural predispositions. Such is the discipline of adversary cultural profiling.

Copyright 2025

Treadstone 71's doctrine places a heavy emphasis on this foundational intelligence work. The "Adversary Targeting" course focuses on creating detailed models of adversaries, mapping their capabilities, intent, and motivations, going far beyond standard threat intelligence. The curriculum incorporates sophisticated psychological and cultural analysis frameworks to build comprehensive profiles. The includes-

- **Personality Typing-** Using frameworks like the Myers-Briggs Type Indicator (MBTI), the Big Five personality traits, and the Dark Triad/Tetrad (narcissism, Machiavellianism, psychopathy, sadism) to understand and predict the behavior of adversary personas and leaders, particularly under pressure.
- **Cultural Analysis –** Using models like Treadstone 71's Cultural Nexus Framework to comprehend the broader societal values that influence an adversary nation's strategic culture and decision-making processes.
- **Adversary-Specific Doctrine-** Studying the unique psychological and analytical methods used by specific adversaries. For example, the "Psychology of the Seven Radicals" course teaches how Russian intelligence services examine adversaries in cyber HUMINT analysis, providing operators with the ability to understand how they are being perceived and targeted.

This deep profiling allows cognitive operators to move from generic messaging to highly tailored influence campaigns. It enables them to craft narratives that will resonate with a specific culture, anticipate an adversary's likely moves, and design deception campaigns that exploit their specific psychological and institutional weaknesses. It is the foundation of intelligence upon which all effective cognitive operations are built.

Chapter 10- Training Pipelines and Curricula for National Defense Institutions

10.1 The Need for a Specialized Training Pipeline

A core argument of this text is that the skills required for cognitive warfare are neither innate nor adequately developed by existing military or civil service training programs. Public affairs officers are trained in communication, not clandestine influence; diplomats are trained in negotiation, not narrative warfare; and traditional intelligence analysts are often focused on technical or kinetic threats, not on the nuances of psychological and cultural manipulation. Therefore, establishing a dedicated training pipeline is the single most critical step in building a national cognitive army.

This pipeline cannot be an ad-hoc collection of courses. It must be a structured, comprehensive, and standardized curriculum designed to take personnel with the correct aptitudes and transform them into proficient cognitive operators. The curriculum must be based on a proven, standards-based doctrine that fuses intelligence community tradecraft with the specific demands of the cognitive domain. The Treadstone 71 course catalog provides a detailed and operationalized blueprint for what such a curriculum should entail.

10.2 Foundational Curriculum- The Certified Cyber Intelligence Analyst

The training pipeline should begin with a foundational course that instills the core principles and skills of the intelligence lifecycle as applied to the cyber and cognitive domains. The Treadstone 71 "On-Demand

Copyright 2025

Cyber Intelligence Tradecraft - Certified Intelligence Analyst" course serves as an ideal model for this foundational stage.

This comprehensive program, delivered over a flexible sixteen-week period, covers the essential building blocks of the profession. It is designed to meet the standards of the International Association for Intelligence Education, ensuring academic and professional rigor. Key modules in this foundational curriculum would include-

- **Intelligence Fundamentals-** Introducing students to the intelligence lifecycle, the different types of intelligence (strategic, operational, tactical), and the principles of intelligence analysis established by figures like Sherman Kent.
- **Collection Tradecraft-** Training in Open-Source Intelligence (OSINT) and darknet collection methods, with a heavy emphasis on Operational Security (OPSEC), the creation and management of secure personas, and ensuring data provenance.
- **Analytical Methods-** Intensive instruction in critical thinking, cognitive bias mitigation, and the application of Structured Analytic Techniques (SATs) to externalize thought processes and improve the rigor of analysis.
- **Reporting and Dissemination-** Training in analytic writing, briefing, and the creation of standardized intelligence products to ensure that analysis is communicated clearly, concisely, and effectively to stakeholders.

10.3 Advanced Curriculum- The Certified Cyber Counterintelligence Analyst

Once operators have mastered the foundational intelligence tradecraft, they must progress to an advanced curriculum focused on the offensive and defensive disciplines of cognitive warfare. Such is the domain of counterintelligence. The Treadstone 71 "Generative AI - Certified Cyber CounterIntelligence Analyst" course provides a blueprint for this advanced stage.

The training is not a theoretical program; it is an "on-demand sprint" where students tackle realistic counterespionage missions. The curriculum is designed to hone the aggressive and proactive skills required for cognitive combat. Key modules in this advanced curriculum would include-

- **Offensive and Defensive Tradecraft-** Moving beyond analysis to the practical application of skills, including infiltration tactics, disinformation disruption, and insider threat hunting.
- **Deception Planning-** A dedicated course on the principles and execution of denial and deception operations, a core component of any offensive cognitive capability, including learning to craft complex, backstopped narratives and assessing the risks of various adversary responses.
- **Adversary-Specific Methodologies-** Deep dives into the cognitive warfare tactics, techniques, and procedures (TTPs) of key state actors, including Russia, China, and Iran, including studying specific concepts like Russia's "Information Alibi" or China's fusion of cyber operations with psychological warfare through their APT groups.

Copyright 2025

- **Psychological and Behavioral Profiling-** Advanced training in applying psychological frameworks like the Dark Triad and the Psychology of the Seven Radicals to build detailed behavioral profiles of adversaries for targeting and manipulation.
- **Integration of Artificial Intelligence-** Training on how to use Generative AI as a force multiplier for persona creation, deepfake detection, and predictive targeting, giving operators a private toolkit to accelerate their workflow and enhance their capabilities.

10.4 Leadership and Strategic Training

The pipeline must also include a track for developing the leaders who will manage and direct cognitive operations. The role requires a different skill set, focusing on strategy, program development, and stakeholder management. Treadstone 71 offers a suite of courses that address this need, which can be bundled into a "Cyber and Information Operations Leadership" program.

Key modules for leadership training would include-

- **Strategic Intelligence Analysis-** Training in estimative and warning intelligence, focusing on forecasting future threats and providing strategic decision support to senior leaders.
- **Intelligence Program Development-** A comprehensive curriculum on how to build a mature cyber intelligence program from the ground up, including defining the mission, developing policies and procedures, managing intelligence requirements, and analyzing stakeholder needs.
- **Cognitive Warfare Strategy-** Courses that examine the strategic application of cognitive warfare in broader geopolitical contexts, such as its role in "Color Revolutions" and "Gray Zone" conflicts.

By implementing a structured, multi-tiered training pipeline based on this commercial model, a national defense institution can systematically build a cadre of professional, doctrine-driven cognitive operators and leaders, creating a sustainable and scalable national capability.

Chapter 11- The Integration of STEMPLES Plus into Cognitive Warfare Campaigns

11.1 The Need for a Strategic Analysis Framework

Effective cognitive warfare cannot be conducted in a strategic vacuum. Tactical influence activities, no matter how skillfully executed, will fail to achieve meaningful outcomes unless they are guided by a deep and continuous understanding of the adversary's strategic environment. To achieve this, cognitive operators require a robust, structured framework for analyzing the complex interplay of factors that shape a nation's capabilities, intentions, and vulnerabilities. The STEMPLES Plus framework, as taught and used by Treadstone 71, provides precisely this necessary strategic context.

11.2 Deconstructing the STEMPLES Plus Framework

STEMPLES Plus is a comprehensive analytical tool used to identify the key drivers of change in a target country's strategic environment. It is an evolution of traditional geopolitical analysis models (like PEST or PESTLE) that has been specifically adapted for the intelligence context, particularly for forecasting and warning of potential hostile cyber and cognitive activity. The framework compels analysts to examine a nation across multiple, interconnected domains systematically.

Copyright 2025

The core components of the framework are -

- **S**ocial- Analyzing societal structures, demographics, cultural norms, public opinion, and social cohesion or fractures.
- **T**echnical- Assessing the state of technological development, internet penetration, indigenous cyber capabilities, and adoption of emerging technologies.
- **E**conomic- Examining economic stability, key industries, reliance on international trade, and vulnerabilities to sanctions or financial pressure.
- **Mi**litary- Evaluating conventional and unconventional military capabilities, defense posture, doctrine, and force readiness.
- **P**olitical- Analyzing the political system, leadership stability, internal power dynamics, foreign policy objectives, and decision-making processes.
- **L**egal/Legislative- Understanding the legal framework, adherence to international law, and the use of law as an instrument of state power.
- **E**ducation- Assessing the level of education, the focus of the academic system, and the state's ability to produce skilled technical and intelligence talent.
- **S**ecurity- Evaluating the capabilities and focus of internal security services and intelligence agencies.

The "Plus" in the framework represents the flexibility to add other critical domains relevant to a specific target. Treadstone 71 specifically identifies Demographics, Religion, and Psychological aspects as common and crucial additions. The psychological dimension is particularly vital for cognitive warfare, as it prompts an analysis of the national psyche, collective traumas, and prevalent cognitive biases that can be exploited or targeted.

11.3 Operationalizing STEMPLES Plus with Indicators of Change

The true power of the STEMPLES Plus framework lies not in a static, one-time analysis, but in its use as a dynamic tool for monitoring and forecasting. Treadstone 71 operationalizes the framework by integrating Indicators of Change within each domain. These are specific, observable data points that signal a shift in the strategic environment. For example, within the 'Political' domain, an indicator might be a sudden purge of senior officials. Within the 'Economic' domain, it could be a sharp increase in unemployment in a key sector.

Analysts are trained to continuously monitor these indicators. While strategic intelligence may not change as rapidly as tactical intelligence, subtle shifts in these indicators, when aggregated over time (typically on a monthly or quarterly basis), can reveal emerging trends and provide early warning of a nation's intent or capability to conduct hostile operations. The process transforms the framework from a descriptive tool into a predictive one, allowing analysts to "provide students insights into what is coming from adversary countries" and to generate forecasts and estimates.

11.4 Application to Cognitive Warfare Campaigning

Copyright 2025

The integration of STEMPLES Plus analysis is fundamental to the entire cognitive warfare campaign lifecycle.

- **Target Audience Analysis and Vulnerability Assessment-** A thorough STEMPLES Plus assessment reveals the deep-seated social, political, and economic fractures within a target society. It identifies the psychological vulnerabilities, cultural grievances, and religious tensions that influence operations and can be exploited. For example, an analysis might reveal a deep public distrust in the government ('Political' domain) or rising social tension between ethnic groups ('Social' domain), both of which are prime targets for narratives designed to amplify division.
- **Narrative Development-** The framework provides the raw material for crafting resonant and credible narratives. A narrative that aligns with a target audience's existing political anxieties, economic hardships, or cultural beliefs is far more likely to be accepted and amplified. The STEMPLES Plus analysis ensures that influence campaigns are not based on guesswork but on a data-driven understanding of the target's cognitive terrain.
- **Forecasting Adversary Campaigns-** By applying the STEMPLES Plus framework to an adversary nation, as Treadstone 71 does in its course on Iran, analysts can assess that nation's capability and propensity to wage offensive cognitive operations. By analyzing Iran's investment in emerging technologies ('Technical'), its geopolitical objectives ('Political'), and the structure of its cyber battalions ('Military'/'Security'), analysts can better anticipate the types of campaigns Iran is likely to launch, enabling a proactive defensive posture.
- **Measuring Campaign Effectiveness-** Changes in the STEMPLES Plus indicators of a target country can also serve as high-level metrics for the effectiveness of a long-term cognitive campaign. A successful campaign aimed at eroding trust in a regime might, over time, be reflected in declining public confidence polls (an indicator in the 'Social' domain) or increased capital flight (an indicator in the 'Economic' domain).

In summary, the STEMPLES Plus framework elevates cognitive warfare from a series of tactical messaging activities to a truly strategic discipline. It provides the essential macro-level understanding that allows operators to design, target, and assess campaigns for maximum strategic impact.

Chapter 12 — Advanced Analytic Tradecraft- The Cultural Nexus, Behavioral Profiling, and Structured Analysis

Effective cognitive warfare demands analytic penetration far beyond an adversary's surface-level propaganda. A lasting influence requires a deep, structured understanding of the adversary's complete cognitive environment—the cultural soil in which narratives grow, the psychological triggers that motivate its leaders, and the analytical blind spots in its planning. Foundational frameworks like STEMPLES Plus provide the essential multi-domain map of the battlespace. Advanced tradecraft provides the tools to excavate and target the adversary's cognitive centers of gravity with precision. Commercial doctrine from specialists like Treadstone 71 institutionalizes these advanced methods, ensuring that a cognitive army operates with a sustained intellectual edge. This tradecraft rests on three pillars- mapping the adversary's cultural reality, dissecting their behavioral patterns, and stress-testing analysis with rigorous, structured techniques.

Copyright 2025

The Cultural Nexus Framework

Simple demographic or political profiling is insufficient. The Cultural Nexus Framework provides a methodology for mapping the intricate web of beliefs, values, historical grievances, symbols, and communication norms that comprise an adversary's worldview. An adversary does not invent narratives from nothing; they draw from a deep cultural wellspring that gives their propaganda authenticity and emotional power for their target audience. The framework deconstructs this wellspring to identify both vulnerabilities and sources of resilience.

Analysts applying the framework identify and map several core components-

- Core Values and Beliefs- These are the non-negotiable principles that guide a group, often derived from religious texts, foundational political manifestos, or deeply ingrained societal norms.
- Historical Narratives- Every group possesses a story of itself—a narrative of past glories, historical traumas, and perceived injustices. Adversaries weaponize these histories to frame current events, justify aggression, and mobilize supporters.
- Key Symbols and Iconography- These are the visual and linguistic shortcuts that evoke robust emotional and cognitive responses. They include flags, revered figures, specific religious verses, or historical events that have become cultural touchstones.
- Communication Norms - This component examines how a group communicates both internally and externally. It assesses the role of authority, the preference for direct versus indirect language, and the trusted channels for information dissemination.
- Cognitive Centers of Gravity- Within the nexus are critical nodes that, if influenced or neutralized, can cause cascading effects throughout the adversary's belief system. These may be a charismatic leader, a foundational text, a potent historical grievance, or a core tenet of their identity.

For example, an analysis of an adversary like Hamas through this framework would move beyond its political charter. It would map the specific Quranic interpretations used to justify martyrdom, trace the invocation of the Nakba as a continuous historical trauma, deconstruct the symbolic power of the Al-Aqsa Mosque in its propaganda, and identify key ideologues whose pronouncements shape the beliefs of its followers. Understanding this nexus enables a cognitive army to design counter-narratives that do not simply rebut a claim, but instead introduce concepts that create friction within the adversary's own cultural framework, challenge the authority of their leaders, or reframe a potent symbol in a way that diminishes its power.

Advanced Structured Analytic Techniques (SATs)

Intelligence analysis is often marred by cognitive bias. Analysts and decision-makers tend to favor information that confirms existing beliefs and may dismiss evidence that suggests an uncomfortable alternative. Advanced Structured Analytic Techniques (SATs) are formal methodologies designed to enforce analytic rigor, challenge assumptions, and mitigate the risk of surprise. In cognitive warfare, where the adversary's entire purpose is to manipulate perception, the use of SATs is non-negotiable.

While dozens of SATs exist, several are uniquely critical for influence operations-

Copyright 2025

- **Analysis of Competing Hypotheses (ACH)-** Instead of settling on the most likely explanation for an adversary's propaganda campaign, ACH forces analysts to evaluate a range of alternative hypotheses against all available evidence. For a sudden adversary narrative claiming a humanitarian crisis, analysts would test multiple hypotheses simultaneously- Is the campaign a genuine reflection of conditions? Is it a deliberate deception to halt an impending military operation? Is it designed to influence a specific vote at the United Nations? Or is it intended to distract from an internal power struggle? ACH prevents premature closure and ensures a more complete picture of adversary intent.
- **Red Team Analysis - This technique involves creating a dedicated team to simulate the adversary's actions**. The red team adopts the adversary's mindset, cultural biases, and operational doctrine to challenge the organization's own plans and assessments. In cognitive warfare, a red team would be tasked with creating the most damaging and effective propaganda campaign against its own side. This exercise exposes vulnerabilities, tests the effectiveness of planned counter-narratives, and anticipates adversary moves before they occur.
- **What-If Analysis-** This forward-looking technique examines the potential impact of a low-probability, high-impact event. Analysts ask, "What if our primary adversary influencer is suddenly removed from the battlespace?" or "What if a major social media platform changes its algorithm to suppress our content?" The analysis compels planners to develop contingency plans and incorporate resilience into their campaigns, ensuring that unexpected developments do not derail the entire strategic effort.

Behavioral Methods and Psychological Profiling

Cognitive warfare is fundamentally a human-to-human contest. Victory requires understanding not just *what* an adversary says, but *why* they say it and how their leaders and followers are likely to think and act under pressure. Behavioral methods and psychological profiling provide this critical layer of insight.

This is not clinical psychology but operational analysis. It involves the systematic study of an adversary's key leaders, propagandists, and decision-making bodies. Analysts build profiles by examining writings, speeches, public statements, and past behaviors to identify motivations, cognitive biases, risk tolerance, and potential triggers. An understanding of a leader's narcissism, paranoia, or susceptibility to flattery can inform influence campaigns designed to provoke a desired reaction or exploit an internal division.

This tradecraft directly informs the development and use of clandestine online personas for intelligence collection and counter-influence. To operate a credible persona within an adversary's network, an operator must possess an intimate understanding of the group's behavioral norms, linguistic tics, and psychological makeup. The same deep knowledge required to build a believable "sockpuppet" is used to map the adversary's psychological terrain and identify opportunities for influence. This analysis also serves as the primary defense against adversary reflexive control, which seeks to manipulate an opponent into making a decision that serves the adversary's interests. By profiling an adversary's decision-making patterns, analysts can identify and expose attempts at manipulation before they succeed.

Fusing these advanced methods—cultural, structural, and psychological—is what completes the construction of a cognitive army. It ensures the organization can not only win the daily battle of messages but can also shape the cognitive environment over the long term, disrupting the foundations of an adversary's influence and protecting its own society from manipulation.

Copyright 2025

Chapter 13- AI in Cognitive Operations- Collection, Assessment, and Red-Teaming Adversary Narratives

13.1 The AI Revolution in Intelligence and Influence

The proliferation of Artificial Intelligence (AI), particularly Generative AI, represents a disruptive and transformative force in the field of cognitive warfare. It provides both adversaries and defenders with unprecedented capabilities to conduct operations at a scale, speed, and level of sophistication previously unimaginable. Adversaries are already using AI for automated targeting, social media manipulation, and the creation of deepfake propaganda to sow confusion and distrust. For any modern cognitive army, the integration of AI is not an option; it is an operational imperative for survival and dominance in the information environment. The Treadstone 71 curriculum demonstrates a forward-leaning adoption of AI, integrating it as a core component of its advanced tradecraft.

13.2 AI-Enhanced Collection and Processing

The first and most immediate application of AI is in supercharging the collection and processing phases of the intelligence lifecycle. The sheer volume of data in the modern information environment—billions of social media posts, news articles, and other forms of content generated daily—has long surpassed the capacity of human analysts to monitor and process effectively. AI provides the solution to this big data problem.

AI-powered tools, such as Knowledge Engines and Expert AI Agents, can simultaneously scan and ingest data from a vast array of sources, including diverse social media platforms, forums, and the dark web. These tools can extract valuable data points from text, images, and videos, identifying network patterns, narrative hierarchies, and emerging trends far more quickly and comprehensively than a team of human analysts ever could. The automated collection and initial processing frees up human operators to focus on higher-level analysis and decision-making.

13.3 AI-Augmented Analysis and Assessment

Beyond collection, AI is a powerful tool for augmenting the analytical process itself. The Treadstone 71 "On-Demand Cyber Intelligence Tradecraft" course explicitly trains students to apply AI-driven analysis and use AI-powered writing assistants to draft structured intelligence reports. The integration can take several forms-

- **Sentiment and Network Analysis-** AI algorithms can perform large-scale sentiment analysis on social media conversations, providing a real-time gauge of public opinion on a given topic, as demonstrated in academic studies of the Israel-Hamas conflict on YouTube. AI can also conduct network analysis to map the structure of influence campaigns, identifying key nodes, amplifiers, and bot networks that are driving a particular narrative.
- **Bias Mitigation-** While AI models can inherit human biases, they can also be used to counteract them. By training students to use critical and creative thinking tools in conjunction with AI, they learn to identify and mitigate their cognitive biases, leading to more objective analysis.
- **Predictive Targeting and Foresight-** Generative AI can be used to accelerate analysis and support strategic foresight. Treadstone 71's advanced courses teach the use of AI to power predictive

Copyright 2025

targeting, enabling the identification of individuals or groups who may be susceptible to specific narratives. Furthermore, AI can be used to analyze trends and adversary tactics, enabling the forecasting of potential future threat scenarios and enhancing warning intelligence capabilities.

13.4 AI in Offensive and Defensive Operations

AI is also a direct instrument of cognitive operations, both offensive and defensive. The "Generative AI - Certified Cyber CounterIntelligence Analyst" course provides a clear model for this operational integration.

In offensive operations, AI serves as a powerful force multiplier. Students learn to use Generative AI to power persona creation, rapidly generating plausible backstories, social media histories, and communication styles for non-attributable online avatars used in clandestine collection and influence operations, dramatically reducing the time and effort required to build and maintain a stable of effective personas.

In defensive operations, AI is a critical tool for countering adversary manipulation. The same course trains operators in using AI for deepfake detection, using machine learning models to identify the subtle artifacts and inconsistencies that reveal AI-generated or manipulated media. The provides a much-needed technical defense against one of the most potent forms of modern disinformation.

13.5 Red-Teaming Adversary Narratives with AI

A particularly innovative application of AI is in the red-teaming of adversary narratives. Red-teaming is the practice of simulating an adversary's mindset and tactics to challenge one's plans and assumptions. In the cognitive domain, this means anticipating and testing the resilience of a friendly narrative against potential adversary counter-narratives.

Generative AI is uniquely suited for this task. An operator can provide a large language model (LLM) with a friendly narrative (e.g., the justification for a military operation) and then prompt it to act as an adversary. The operator can instruct the AI to "Identify the key vulnerabilities in this narrative," "Generate five counter-narratives that would appeal to a skeptical European audience," or "Create a series of social media posts that twist this message to frame it as an act of aggression." The process allows the cognitive army's planners to stress-test their campaigns, identify weaknesses, and develop pre-emptive counter-messaging before the campaign is even launched. It is a form of cognitive wargaming that enables the rapid exploration of multiple potential futures in the information environment, thereby significantly improving the robustness and resilience of friendly influence operations.

Chapter 13- Campus Operations and Adversary Recruitment- Commercial Countermeasures Through Doctrine

13.1 University Campuses as a Cognitive Battlefield

University and college campuses have long been arenas for ideological debate and political activism. In the era of cognitive warfare, however, they have transformed into a critical and contested battlefield. Adversary states and non-state actors are increasingly viewing academic institutions as fertile ground for influence operations, narrative shaping, and the recruitment of both willing and unwitting agents. The combination of an environment that encourages open debate, a population of young and often idealistic individuals

Copyright 2025

forming their political identities, and the concentration of future leaders and technical experts makes campuses a high-value target for any actor seeking to exert long-term cognitive influence over a society.

Adversary objectives on campus are comprehensive. They include the radicalization of student groups to create domestic pressure on government policies, the promotion of narratives that align with the adversary's geopolitical goals, the suppression of academic discourse critical of the adversary, and the identification and recruitment of students with access to sensitive research or who are on a trajectory for future government service. These activities represent a significant national security threat that traditional law enforcement and campus security are ill-equipped to handle.

13.2 The Limitations of Traditional Countermeasures

The response to adversary operations on campus by democratic states has often been inadequate, caught between the need to protect national security and the imperative to preserve academic freedom and freedom of speech. A heavy-handed approach involving overt surveillance or censorship can be counterproductive, validating adversary narratives of state oppression and alienating the very student populations the state seeks to protect. Conversely, a completely hands-off approach creates a permissive environment for hostile actors to operate with impunity.

This dilemma highlights the need for a more sophisticated response, one that is not based on overt security measures but on the subtle and nuanced tradecraft of counterintelligence and cognitive defense. The challenge is not to police thought on campus, but to build resilience against hostile manipulation and to discreetly identify and neutralize adversary recruitment efforts.

13.3 A Doctrinal Approach to Countering Campus Operations

A commercial doctrine, such as that developed by Treadstone 71, offers a playbook of countermeasures that are more suited to the unique campus environment than traditional state-led interventions. The approach is not about deploying government agents on campus but about training a nation's existing security and intelligence professionals to understand and counter the specific tactics used in this domain.

The first step is understanding the threat actor's methodology, which involves applying adversary targeting and profiling techniques to the specific context of campus operations. Analysts would be trained to identify the front groups, student organizations, and academic programs that are being used or co-opted by foreign powers. They would learn to recognize the specific narratives and recruitment patterns used to target students, mapping the flow of influence from adversary state to campus activist.

The second step is deploying passive and clandestine counterintelligence. Rather than overt action, operators would be trained to use the same OSINT and cyber HUMINT skills they use to monitor terrorist forums to monitor the online spaces where campus radicalization and recruitment occur. Using secure, non-attributable personas, they can observe the tactics of adversary recruiters, identify their key talking points, and understand the vulnerabilities they exploit in students.

13.4 Proactive Counter-Recruitment and Inoculation

The most effective countermeasure is proactive. The Treadstone 71 doctrine, with its emphasis on both offensive and defensive tradecraft, provides a model for moving beyond mere monitoring to actively disrupting adversary recruitment.

Copyright 2025

One key technique is **elicitation**, a core skill taught in the "Insider Threats & Elicitation Methods" course. While this course is designed for vetting job candidates, the principles are directly applicable to counter-recruitment. Elicitation involves using conversational tactics to surface inconsistencies and stress responses, subtly testing an individual's allegiances and motivations without alerting them to the fact that they are being assessed. Security professionals responsible for clearing students for internships or jobs in sensitive government or industry roles can be trained in these advanced interview and vetting techniques to identify individuals who have been compromised or targeted for recruitment by foreign intelligence services. The process treats every high-stakes interview as a counterintelligence operation, using psychological pressure and forensic validation to expose deception.

Another proactive measure is strategic inoculation. By understanding the specific disinformation narratives being targeted at students (e.g., narratives that paint the student's country as an imperialist aggressor), a cognitive army can work with trusted partners to "inoculate" the student population. The is not crude counter-propaganda but the dissemination of factual, well-reasoned information that pre-emptively debunks the adversary's claims. The builds cognitive resilience, making students less susceptible when they eventually encounter the hostile narrative. The requires a deep understanding of the adversary's campaign themes, derived from the intelligence collection and analysis processes described previously. By applying these sophisticated, intelligence-led countermeasures, a nation can protect its academic institutions and future leaders from hostile cognitive warfare without compromising the principles of academic freedom.

Chapter 14- The Lawfare Dimension- Offensive Litigation Versus Strategic Exposure

14.1 Defining Lawfare in the Context of Cognitive Conflict

Lawfare, a portmanteau of "law" and "warfare," is the use of law as a weapon to achieve a strategic objective that might otherwise require the use of kinetic military force. While the term was popularized in the early 21st century by military legal scholars, such as Major General Charles Dunlap, the concept of using legal systems to achieve strategic ends is ancient. In the context of modern cognitive warfare, lawfare has become a critical and integrated component of information operations. It is not merely a legal battle, but a form of strategic communication, where legal forums—such as courts, international tribunals, and regulatory bodies—become theaters for narrative combat.

Adversaries of democratic states, both state and non-state actors, have become adept at using lawfare to their advantage. They exploit the West's deep-seated respect for the rule of law, manipulating legal processes to constrain military action, delegitimize state institutions, and advance their propaganda narratives. A common tactic is "compliance use disparity" lawfare, where an actor that does not abide by the Law of Armed Conflict (e.g., an insurgent group using human shields) uses legal challenges to exploit their democratic opponent's strict adherence to it, thereby gaining a military and narrative advantage.

14.2 The Israeli Proposal- Lawfare as an Offensive Tool

Within the emerging Israeli discourse on the need for a "cognitive army," lawfare is explicitly identified as a necessary offensive tool. The proposal from figures like Professor Kobi Michael suggests that legal steps should accompany aggressive cognitive campaigns against hostile media or international organizations. The stated objective is to "sue them, force them to pay millions upon millions to lawyers, exhaust them in the courts".

Copyright 2025

This approach views litigation primarily as a tool for imposing costs and attrition on adversaries in the information space. The goal is to use the financial and reputational burden of legal battles to disrupt and deter organizations that are perceived as key nodes in the anti-Israel propaganda network. While this strategy has a certain punitive appeal, it also carries significant risks. It can be perceived as an attempt to silence free speech and criticism, potentially backfiring and reinforcing the very narratives of oppression it seeks to counter. Furthermore, it risks politicizing the legal system and can be an expensive and slow-moving process with uncertain outcomes.

14.3 An Alternative Model- Strategic Exposure and Intelligence-Led Lawfare

A more nuanced and practical approach to lawfare, aligned with the intelligence-driven doctrine of a commercial entity like Treadstone 71, is one based on strategic exposure rather than purely punitive litigation. The model treats legal action not as the primary weapon, but as the culmination of a meticulous intelligence and counterintelligence operation. The goal is not simply to sue an adversary, but to expose their illicit, covert, or criminal activities to the public and to legal authorities in a way that irrefutably dismantles their credibility and legitimacy.

This process begins with the core intelligence tradecraft of adversary targeting and research. Analysts would be tasked with identifying the front companies, funding mechanisms, and undeclared relationships that underpin hostile influence networks. For example, Treadstone 71 conducted and published a detailed analysis exposing a suspected Russian front company, Delta Electroniks, by demonstrating that its supposed founder, "Strekozov," did not appear in any official Russian records, suggesting the entity was a state-sponsored myth.

The intelligence-led lawfare process involves-

1. Deep Intelligence Gathering- Using OSINT, cyber HUMINT, and other collection methods to gather evidence of an adversary's covert activities, such as an influence organization receiving undeclared funding from a foreign intelligence service or a media outlet coordinating its messaging with a designated terrorist group.

2. Meticulous Analysis- Applying structured analytic techniques to build a solid, evidence-based case that can withstand legal and public scrutiny. The involves tracing financial flows, mapping networks, and documenting illicit coordination.

3. Strategic Exposure- The findings are then strategically disclosed. The could take the form of a detailed intelligence report released to the public and key policymakers, a dossier provided to investigative journalists, or a formal submission to law enforcement or regulatory bodies (e.g., those responsible for enforcing laws on foreign agent registration or terrorist financing).

4. Legal Action as a Follow-On - Once the adversary's illicit network has been publicly exposed and their credibility has been compromised, legal action can be pursued from a position of strength, involving criminal prosecutions for fraud or sanctions violations, civil litigation by victims of their disinformation, or regulatory action to revoke their operating licenses.

The model of strategic exposure is more potent than offensive litigation alone because its primary objective is to win in the cognitive domain by destroying the adversary's legitimacy through the revelation of truth. The subsequent legal consequences are a secondary, albeit important, effect. It aligns with the core

Copyright 2025

intelligence mission of "winning with the truth" and is less susceptible to accusations of suppressing free speech, as it targets demonstrable illicit activity rather than protected expression. The intelligence-led approach transforms lawfare from a blunt instrument of attrition into a precision weapon of cognitive counter-attack.

Part III — Building the Cognitive Army with Commercial Expertise

Chapter 15- Building Fusion Cells- How Commercial Playbooks Become National Operational Hubs

15.1 The Fusion Cell Concept in Intelligence Doctrine

The concept of an intelligence fusion cell is a cornerstone of modern military and intelligence doctrine. A fusion cell is an organizational structure designed to bring together analysts and operators from different disciplines and organizations into a single, collaborative environment. Its purpose is to break down institutional silos and facilitate the rapid integration, or "fusion," of disparate streams of information and intelligence to create a single, coherent operational picture. By co-locating experts in signals intelligence (SIGINT), human intelligence (HUMINT), imagery intelligence (IMINT), and other fields, a fusion cell can achieve a level of situational awareness and analytical synergy that is impossible when these functions remain separate. The model has been successfully employed in counter-terrorism operations and conventional military campaigns to provide commanders with timely, relevant, and actionable all-source intelligence.



15.2 Adapting the Fusion Cell for Cognitive Warfare

The fusion cell model is exceptionally well-suited to the challenges of cognitive warfare. The multi-domain nature of cognitive conflict—integrating cyber, information, psychological, and social engineering elements—demands a correspondingly integrated operational structure. A cognitive warfare fusion cell would serve as the operational hub, bringing together the diverse skills required for the mission.

However, a cognitive warfare fusion cell requires a different composition than a traditional military intelligence cell. In addition to standard intelligence analysts, it must include specialists in disciplines that are often foreign to the traditional security establishment. The ideal cognitive fusion cell would integrate-

Copyright 2025

- Cyber Intelligence Analysts- Experts in OSINT, darknet collection, and technical analysis of adversary infrastructure.
- Counterintelligence Officers- Specialists in deception detection, adversary profiling, and neutralizing hostile intelligence operations.
- Cultural and Psychological Experts - Anthropologists, sociologists, and psychologists who can provide deep insights into the target audience's cognitive landscape.
- Narrative and Campaign Planners- Creative strategists skilled in the art of narrative engineering and the design of multi-vector influence campaigns.
- Data Scientists and AI Specialists- Experts who can manage and interpret large datasets, deploy AI tools for analysis, and identify algorithm-driven trends.
- Legal and Policy Advisors- In-house experts on domestic and international law to ensure all operations are conducted within established ethical and legal guardrails.

15.3 The Commercial Playbook as an Organizational Blueprint

The challenge for a national defense institution is not just identifying these roles, but getting them to work together effectively, where a commercial playbook, derived from the doctrine and program-building experience of a firm like Treadstone 71, becomes the essential organizational blueprint.

Treadstone 71's services are not limited to training individuals; they specialize in building entire strategic intelligence programs from the ground up, defining the mission, goals, and objectives, establishing policies, procedures, and standard operating procedures (SOPs), designing process flow diagrams, and defining roles and responsibilities. The comprehensive, "intelligence program in a box" approach provides the exact methodology a nation needs to stand up and operationalize a network of cognitive fusion cells.

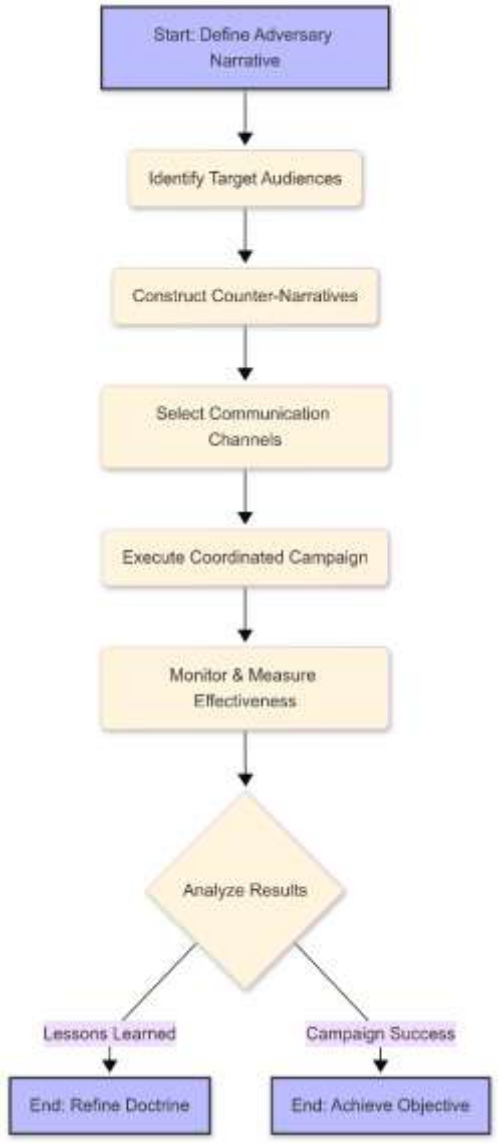
The process would involve Treadstone 71 consultants working with a national defense institution to

1. Define the Charter- Collaboratively establish the mission, scope, and rules of engagement for the fusion cell, ensuring it aligns with national strategy and legal frameworks.
2. Design the Workflow- Implement the proven intelligence lifecycle process as the core workflow for the cell, from receiving intelligence requirements from stakeholders to the final dissemination of intelligence products and campaign directives.
3. Implement Standardized Procedures- Provide the templates, SOPs, and best practices for every stage of the process, including collection management, source validation, structured analysis, and campaign design, ensuring that all operators are working from a common doctrinal base.
4. Train the Team- Run the integrated team of specialists through simulation-based exercises and wargames to forge them into a cohesive operational unit.

15.4 From Centralized Command to a Network of Empowered Cells

By using a commercial playbook as the blueprint, a nation can avoid the trap of building a single, monolithic headquarters. Instead, it can stand up multiple, smaller, and more agile fusion cells, each tailored to a

Copyright 2025



specific mission or geographic area of responsibility. For example, one cell might focus on countering Iranian influence operations in the Levant, another on Russian disinformation targeting European allies, and a third on monitoring extremist radicalization in Southeast Asia.

These cells would operate as a distributed network, guided by a shared doctrine and connected by a typical information architecture, but empowered to act with a degree of autonomy at the operational level. The structure mirrors the networked nature of the threat itself, providing the agility and resilience that a centralized command lacks. The commercial playbook thus becomes the tool for transforming a bureaucratic aspiration—the "Cognitive Army"—into a network of potent, professional, and effective national operational hubs.

Chapter 16- Campaign Design Methodologies Drawn from Structured Intelligence Analysis

16.1 The Intelligence-Driven Approach to Campaign Design

The design of cognitive warfare campaigns cannot be an ad-hoc, purely creative endeavor. While creativity in narrative development is essential, it must be grounded in a rigorous, analytical process to be effective. Campaigns based on intuition or assumptions are likely to fail, waste resources, and may even be counterproductive. An intelligence-driven approach, rooted in the methodologies of structured intelligence analysis, is required to ensure that campaigns are precisely targeted, evidence-based, and designed for measurable impact. The Treadstone 71 curriculum, with its heavy emphasis on Structured Analytic Techniques (SATs), provides a straightforward methodology for this process.

16.2 The Campaign Design Lifecycle

The design of a cognitive campaign should follow a structured lifecycle that mirrors the intelligence process itself, ensuring that every step is deliberate and informed by the best available analysis.

Phase 1- Requirements Definition (Direction) The process begins with a clear understanding of the strategic objective, achieved through stakeholder analysis and the development of precise intelligence requirements. The campaign planners must work with senior decision-makers to answer fundamental questions- What is the desired cognitive effect? Who is the primary target audience? What change in belief or behavior are we trying to achieve? The initial direction prevents the campaign from drifting from its strategic purpose.

Copyright 2025

Phase 2: Cognitive Terrain Analysis (Collection & Processing)- Before a narrative can be designed, planners must have a deep understanding of the target audience's "cognitive terrain," where the foundational intelligence disciplines are applied. It involves-

- Adversary and Audience Profiling- Using the cultural and psychological profiling techniques discussed in Chapter 9 to build a comprehensive model of the target audience's values, beliefs, fears, cognitive biases, and trusted information sources.
- STEMPLES Plus Analysis- Conducting a strategic analysis of the target's environment to identify the key social, political, and economic drivers and vulnerabilities that the campaign can use.
- Collection Planning- Developing a systematic plan to gather the information needed to inform the campaign, using a mix of OSINT and other collection methods.

Phase 3 - Narrative Development and Hypothesis Testing (Analysis)- The core analytical phase, where SATs are used to develop and test potential campaign narratives. Instead of relying on a single "big idea," analysts should use techniques to generate and evaluate multiple competing hypotheses about what narrative will be most effective. Key SATs applicable to this phase include-

- Brainstorming and Divergent/Convergent Thinking- To generate a wide range of potential narrative themes and campaign concepts.
- Analysis of Competing Hypotheses (ACH)- A core technique taught in the Treadstone 71 curriculum, ACH is a systematic process for evaluating multiple hypotheses against the available evidence. In this context, each potential narrative is treated as a hypothesis (e.g., "Hypothesis A - A narrative emphasizing economic corruption will be most effective at eroding support for the target regime"). Analysts then assess how well each hypothesis fits with the evidence gathered during the cognitive terrain analysis.
- Red Teaming and "What If?" Analysis- Using alternative analysis techniques to challenge the chosen narrative. The process involves asking questions like, "What if the target audience reacts in the opposite way we expect?" or "How could the adversary counter this narrative?" The stress-testing makes the final campaign plan more robust.

Phase 4- Campaign Execution and Dissemination (Production & Dissemination) Once a primary narrative has been selected and refined through rigorous analysis, the campaign moves to execution. The process involves creating the specific content (text, images, videos, etc.) and deploying it through the chosen vectors. The dissemination plan should be as carefully considered as the narrative itself, ensuring the content reaches the right audience through the most credible channels.

16.3 The Role of Structured Analysis in Preventing Failure

The primary value of using structured methodologies in campaign design is the prevention of analytical and operational failure. Cognitive operations are prone to error, driven by the inherent biases and assumptions of the planners. A campaign designed by a team that lacks an understanding of the target culture may be ineffective or even offensive. A campaign that fails to anticipate an adversary's countermove can be easily neutralized.

Copyright 2025

Structured analysis acts as a mechanism to "externalize internal thought processes systematically and transparently". It forces planners to show their work, to justify their assumptions with evidence, and to consider a range of alternative possibilities. The rigor is the hallmark of a professional intelligence process. It transforms campaign design from a speculative art into a data-driven science, dramatically increasing the probability of success and ensuring that national resources are not wasted on ill-conceived or poorly targeted influence operations.

Chapter 17- Ethical Guardrails and Reputational Risk Management

17.1 The Ethical Dilemma of Democratic Cognitive Warfare

For a democratic nation, the decision to engage in cognitive warfare presents a profound ethical dilemma. The very tools and techniques required for effective influence operations—deception, manipulation, psychological targeting—can appear to be in direct conflict with the democratic values of transparency, truthfulness, and respect for individual autonomy. Adversaries who do not share these values operate without such constraints, creating a significant asymmetric advantage. The challenge for a democratic state is to develop a cognitive warfare capability that is potent enough to be effective against ruthless adversaries while remaining firmly anchored within a robust ethical and legal framework.

Failing to establish these guardrails carries immense reputational risk. A cognitive operation that is exposed as a clumsy or unethical manipulation campaign can do more damage to a nation's credibility and legitimacy than any adversary propaganda could achieve. Therefore, the development of clear ethical guidelines does not impede effective operations; it is an absolute prerequisite for their sustainable and legitimate use.

17.2 Building an Ethical Framework- Lessons from Just War Theory

While cognitive warfare is a new domain, the ethical questions it raises are not entirely novel. The Just War Tradition, a philosophical framework that has guided military ethics for centuries, offers a helpful starting point for building a modern ethical framework for cognitive operations. The core principles of

Jus ad bellum (the justification for going to war) and *jus in bello* (conduct within war) can be adapted to the cognitive domain.

An ethical framework for cognitive warfare might include the following principles, adapted from Just War theory-

- Just Cause- Cognitive operations should only be undertaken for legitimate reasons of national defense, such as countering foreign hostile influence, preventing terrorist recruitment, or defending against campaigns aimed at subverting democratic processes. They should not be used for purposes of purely economic competition or domestic political gain.
- Legitimate Authority- The authority to approve and oversee cognitive operations must be clearly defined in law and reside with democratically accountable officials. There must be a transparent chain of command and oversight.
- Right Intention - The ultimate intention of the operation must be to restore a just peace or to protect the integrity of the information environment, not simply to sow chaos or harm for its own sake.

Copyright 2025

- Proportionality- The potential harm caused by a cognitive operation—including psychological harm to targets, collateral damage to unintended audiences, and the potential for blowback—must not be excessive in relation to the strategic good it is intended to achieve. Measuring proportionality for non-kinetic effects is a significant challenge that requires careful consideration.
- Distinction (Discrimination)- Operators must make every reasonable effort to distinguish between legitimate targets (e.g., foreign intelligence operatives, terrorist propagandists) and non-combatants (e.g., ordinary civilians, even those in an adversary nation). Campaigns should be designed to minimize indiscriminate psychological effects on non-target populations.

17.3 The Role of Professional Intelligence Ethics

Beyond these high-level principles, the day-to-day conduct of cognitive operators must be guided by the professional ethics of the intelligence community. A doctrine rooted in intelligence community standards, as is the case with Treadstone 71, brings with it an implicit code of conduct that emphasizes objectivity, rigor, and the mitigation of bias.

Key ethical practices derived from intelligence tradecraft include-

- Objectivity and Bias Mitigation- Training in critical thinking and cognitive bias is an ethical imperative. It ensures that analysis is based on evidence, not prejudice, and prevents the creation of intelligence that merely reinforces policymakers' preconceived notions.
- Source and Evidence Validation- A core ethical duty of an analyst is to rigorously evaluate the credibility of sources and the validity of evidence before incorporating them into an assessment or a campaign. The practice acts as a bulwark against the knowing or unknowing dissemination of false information.
- Respect for Privacy and Legal Constraints - While cognitive operations may involve collecting data in sensitive areas, they must be conducted within the bounds of national and international law, with particular attention to privacy regulations and the rights of citizens. The "Insider Threats & Elicitation Methods" course, for instance, explicitly notes the need to consider "Legal, Ethical, and Privacy Constraints in Interviews".

17.4 Managing Reputational Risk Through Doctrine and Oversight

Ultimately, the most effective way to manage the reputational risk associated with cognitive warfare is to professionalize the force. A cognitive army composed of "cowboys" operating without clear rules is a recipe for disaster. A force composed of highly trained professionals, steeped in a rigorous doctrine that includes a strong ethical component, and subject to robust legal and political oversight, is the best defense against catastrophic errors and abuses.

The commercial doctrine model contributes to this by providing a standardized and documented set of procedures and techniques. When operators are trained in a consistent, standards-based methodology, their actions become more predictable, auditable, and controllable. The doctrinal foundation, combined with a clear governance structure and continuous oversight from legal and ethical advisors within the fusion cell, provides the necessary guardrails to allow a democratic nation to operate effectively in the cognitive domain without sacrificing its core values.

Copyright 2025

Chapter 18- Monitoring and Measurement Frameworks for Influence Campaigns

18.1 The Challenge of Measuring Influence

One of the most significant challenges in cognitive warfare is measuring the effectiveness of influence campaigns. Unlike kinetic warfare, where success can be measured in tangible terms, such as territory captured or targets destroyed, the effects of cognitive operations are often intangible, indirect, and slow to manifest. How does one prove that a change in public opinion or a shift in a leader's decision-making was the direct result of a specific campaign? The difficulty in measurement makes it challenging to justify budgets, demonstrate return on investment, and learn from past operations to improve future ones.

Despite these challenges, a systematic approach to monitoring and measurement is not impossible; it is a critical component of a professional cognitive warfare capability. The Treadstone 71 "Cognitive Warfare" course explicitly acknowledges this, including coverage of "the issues associated with measuring campaign effectiveness and influence analysis" as a key learning objective. A robust framework for measurement must be built into the campaign design from the very beginning.

18.2 A Multi-Layered Measurement Framework

A comprehensive measurement framework should not rely on a single metric but should assess effects across multiple layers, from immediate tactical outputs to long-term strategic outcomes. The framework can be conceptualized in three tiers.

Tier 1- Measures of Performance (MOPs) - "Are we doing things right?" MOPs measure the immediate outputs of a campaign. They assess whether the campaign activities were executed as planned. These are the easiest metrics to collect, providing a baseline understanding of the campaign's reach and activity level. In the digital domain, MOPs include-

- Reach and Exposure Metrics- The number of impressions, views, or unique users exposed to the campaign content.
- Engagement Metrics- The number of likes, shares, comments, retweets, or click-throughs on campaign content.
- Dissemination Metrics- Confirmation that campaign messages were successfully placed in target media outlets or amplified by key influencers.

While essential, MOPs are insufficient on their own. A campaign can have massive reach and engagement but still fail to achieve its desired cognitive effect. A high number of shares does not necessarily equate to a change in belief.

Tier 2- Measures of Effectiveness (MOEs) - "Are we doing the right things?" MOEs are more challenging to measure, but are far more important. They assess the extent to which the target audience's attitudes, beliefs, and behaviors have changed as a result of the campaign. The report requires moving from simple content analytics to audience analysis. Methods for gathering MOEs include-

- Sentiment Analysis- Using AI-powered tools to analyze the overall sentiment (positive, negative, neutral) of online conversations related to the campaign themes within the target audience. A shift from negative to neutral or positive sentiment over time can be a mighty MOE.

Copyright 2025 Treadstone 71 WWW.TREADSTONE71.COM

- Narrative Adoption- Monitoring the target audience's online discourse to see if they begin to adopt the language, framing, and key phrases of the campaign narrative in their organic conversations.
- Polling and Surveys- For campaigns targeting accessible populations, conducting carefully designed polls and surveys before, during, and after the campaign can provide direct evidence of shifts in opinion and belief.
- Behavioral Analytics- In some cases, it may be possible to measure changes in behavior. For example, a campaign aimed at discouraging support for an extremist group could measure a decrease in online donations to that group or a decline in attendance at its rallies.

Tier 3- Measures of Strategic Impact - "Are we achieving our strategic objective?" The measures are the highest and most challenging level of measurement. It seeks to link the cognitive effects measured by MOEs to the overarching strategic goal of the operation. The often requires long-term analysis and the use of qualitative, structured intelligence techniques. Methods include-

- Indicator-Based Assessment - Using a framework like STEMPLES Plus, analysts can track high-level indicators within the target country's strategic environment. If a long-term cognitive campaign is designed to weaken a hostile regime, its success might be correlated with negative shifts in indicators of political stability, economic confidence, or military morale.
- Intelligence Reporting- Monitoring classified and open-source intelligence for indications that the target leadership is discussing or reacting to the themes of the influence campaign in their internal deliberations.
- Qualitative Assessment- Conducting structured case studies after a campaign is complete, using techniques like process tracing to build a qualitative argument linking the campaign's activities to the observed strategic outcomes.

18.3 The Feedback Loop- Integrating Measurement into Campaign Adaptation

The purpose of monitoring and measurement is not only to produce a final report card for a campaign, but also to inform ongoing decision-making. It aims to create a continuous feedback loop that enables real-time adaptation and learning. The data gathered through MOPs and MOEs should be regularly fed back to the campaign planners in the fusion cell.

If the data indicates that a particular narrative is not resonating (low engagement) or is generating a backlash (negative sentiment), planners can adjust the messaging, modify the dissemination channels, or adopt a different approach entirely. The iterative process of execution, measurement, and adaptation is the key to success in the dynamic cognitive domain. It transforms campaign management from a linear, "fire-and-forget" process into an agile, learning cycle, ensuring that operations become progressively more effective over time.

Chapter 19- Red Team and Blue Team Exercises in Cognitive Warfare

19.1 The Role of Wargaming in a Learning Organization

A cognitive army, like any military or intelligence organization, must be a learning organization. Doctrine and tradecraft cannot remain static; they must be constantly tested, refined, and adapted to the evolving

Copyright 2025

threat landscape. The most effective methodology for achieving this is through the use of realistic, competitive wargames and exercises. Specifically, the use of Red Team versus Blue Team exercises provides a "safe-to-fail" environment where operators can hone their skills, test new tactics, identify vulnerabilities in their plans, and develop a deeper understanding of the adversary's mindset.

The French military's Red Team Defense project, for example, was explicitly created to bypass the weight of military hierarchy and standardized thought, using creative exercises to avoid strategic blind spots. Similarly, the U.S. military has long recognized red teaming as a critical tool for challenging assumptions, guarding against groupthink, and maintaining a flexible mindset. For cognitive warfare, where the "fog of war" is thick and feedback from real-world operations can be ambiguous, such exercises are not a luxury but a necessity.

19.2 Designing Cognitive Wargames

Designing an effective cognitive wargame is a complex undertaking that requires a different approach than traditional kinetic wargames. The UK Ministry of Defence's *Influence Wargaming Handbook* offers a valuable framework, emphasizing that wargaming influence requires a new mindset from sponsors, practitioners, and participants alike.

A typical cognitive wargame would involve two primary teams-

- The Blue Team- The team represents the friendly force, the cognitive army's fusion cell. It is composed of the operators being trained and tested. Their objective is to achieve a specific strategic goal (e.g., maintaining public support for a government policy, countering a specific adversary's disinformation campaign) using the cognitive warfare tools and doctrine they have been taught.
- The Red Team- The team plays the role of the adversary. A well-constructed Red Team is not simply a sparring partner; it is an "organizational element comprised of trained, educated, and practiced experts that provide an independent capability to explore plans and operations from an alternative perspective". The Red Team should be staffed by experts in adversary doctrine (e.g., specialists in Russian or Iranian information operations) and creative thinkers who are empowered to use any tactic the real adversary might employ.

The exercise is overseen by a White Cell, or control group, which adjudicates the outcomes of actions, injects simulated events (e.g., a real-world news story, a political scandal), and manages the flow of the game.

19.3 Exercise Scenarios and Objectives

Cognitive wargames can be designed to achieve a range of training and analytical objectives. Scenarios can be tailored to test specific skills and challenge different aspects of the Blue Team's capabilities.

- Defensive Scenarios- The Blue Team could be tasked with defending a nation's electoral process against a Red Team disinformation campaign. The exercise would test their ability to rapidly detect and attribute the hostile campaign, develop effective counter-messaging, and coordinate with social media platforms and government agencies to mitigate the threat.

Copyright 2025

- Offensive Scenarios- The Blue Team could be tasked with designing and executing a campaign to erode the morale of an adversary's military forces or to undermine the credibility of a hostile regime. They would test their skills in narrative engineering, deception planning, and persona management.
- Crisis Response Drills - The exercise simulates a crisis, such as a terrorist attack or a natural disaster, where the information environment is chaotic and filled with rumors and misinformation. The Blue Team would be evaluated on its ability to establish a credible information source, counter harmful rumors, and maintain public trust under extreme pressure. The Treadstone 71 "Insider Threats & Elicitation Methods" course includes "Red Team Exercises and Live Incident Drills" as a key component for testing response protocols.

19.4 The Feedback Loop- From Wargame to Doctrine

The actual value of red teaming lies in the post-exercise feedback loop. After each wargame, a detailed after-action review must be conducted. The Red Team's role is critical here; they must provide a transparent and brutally honest assessment of the Blue Team's performance, identifying the assumptions they exploited, the tactics that were most effective against them, and the vulnerabilities they discovered in the Blue Team's plans and procedures.

This feedback is invaluable intelligence. It provides insights that are used to refine doctrine, update training curricula, and develop new countermeasures. The "Blue Team Evolution from Red Team Data" is a formal component of the Treadstone 71 insider threat methodology, where feedback from exercises is used to enhance defensive sensors and protocols. The iterative cycle of testing, feedback, and adaptation ensures that the cognitive army does not become complacent or reliant on outdated methods. It institutionalizes a process of continuous learning and improvement, keeping the force's skills sharp and its doctrine relevant in the face of an ever-evolving cognitive threat.

Part IV — Operational Design and Governance

Chapter 20- Anticipating Adversary Countermeasures

20.1 The Interactive Nature of Cognitive Conflict

Cognitive warfare is not a one-sided activity. For every action, there is a reaction; for every campaign, there is a counter-campaign. A professional cognitive army must operate with the constant awareness that the adversary is an active, thinking, and adaptive opponent. Any successful tactic or narrative will be studied, dissected, and eventually countered by the adversary. Therefore, a static approach to cognitive operations is doomed to failure. The ability to anticipate and preempt adversary countermeasures is a hallmark of a mature and effective cognitive warfare capability. The requires a deep, intelligence-driven understanding of the adversary's cognitive warfare doctrine and capabilities.

20.2 Counter-attribution and Narrative Hijacking

One of the most common and effective countermeasures against adversaries is **counter-attribution**. When an adversary detects a hostile influence operation, their first move will often be to expose it and attribute it to the nation that originated it. They will use this exposure to fuel a powerful counter-narrative, framing the operation as a nefarious attempt by an aggressive foreign power to subvert their sovereignty and manipulate

Copyright 2025

their people. The tactic turns the cognitive army's campaign against itself, using it as "proof" of the very hostility the adversary's propaganda has been alleging all along.

A related tactic is narrative hijacking. Instead of simply exposing the campaign, the adversary may seek to co-opt or subtly twist its themes to serve their own ends. For example, a campaign designed to highlight the corruption of a hostile regime could be hijacked by the regime itself, which might acknowledge the problem but blame it on a specific internal scapegoat or on the "destabilizing influence" of foreign powers, thereby using the campaign to consolidate its power.

To mitigate these risks, a cognitive army must prioritize operational security (OPSEC) and utilize non-attributable or deniable assets. The extensive training on anonymity, secure browser configurations, and persona management in the Treadstone 71 curriculum is designed precisely to counter these threats. By making operations difficult to attribute, the cognitive army denies the adversary the easy victory of public exposure.

20.3 Cognitive Inoculation and Pre-bunking

Adversaries will also seek to make their populations more resilient to hostile influence through a process of cognitive inoculation. They involve proactively exposing their population to weakened or simplified versions of the hostile narrative, often framing it as "enemy propaganda," in order to build up psychological resistance before the primary campaign hits.

The counter to this is pre-bunking, a tactic that a democratic cognitive army can also employ. Before launching a major policy or military operation that is likely to be the subject of adversary disinformation, the cognitive army can proactively release information that exposes the adversary's likely narratives. For example, before an airstrike on a legitimate military target embedded in a civilian area, the army could release intelligence imagery showing the military use of the site, thereby pre-bunking the adversary's inevitable claim that the target was purely civilian. The requires a high degree of strategic foresight and a willingness to declassify intelligence for cognitive effect.

20.4 The "Red Team" Mindset- Wargaming Countermeasures

The most effective method for anticipating adversary countermeasures is to integrate a "Red Team" mindset into every stage of the campaign planning process. As discussed in the previous chapter, dedicated red teaming exercises are invaluable. However, the mindset should be continuous. Planners in the fusion cell should constantly ask themselves, "If I were the adversary, how would I counter this?"

This process can be aided by structured analytical techniques, such as "High-Impact/Low-Probability Analysis" and "What If? Analysis." Planners should systematically consider a range of potential adversary responses, not just the most likely one. The Treadstone 71 "Deception Planning" course emphasizes this principle as a maxim: "Deception planners must assess the possible effects if the adversary responds differently than expected, as well as the risks if the adversary does not respond favorably." By wargaming these potential countermeasures in advance, the fusion cell can develop pre-planned branches and sequels to their campaign, allowing them to adapt rapidly when the adversary inevitably responds. The continuous cycle of action, anticipation, and adaptation is the key to maintaining the initiative and achieving long-term success in the interactive environment of cognitive warfare.

Chapter 21- Lessons from Russian, Chinese, and Iranian Doctrine

Copyright 2025

21.1 The Imperative of "Knowing Your Enemy"

To effectively compete in the cognitive domain, a nation must possess a deep and nuanced understanding of the specific doctrines, methodologies, and strategic cultures of its primary adversaries. A generic approach to cognitive warfare is insufficient. The way Russia wages an information war differs from the way China does, which in turn differs from Iran's approach. Each has its historical context, institutional structures, and philosophical underpinnings. A professional cognitive army must be a student of its enemies. The Treadstone 71 curriculum reflects this imperative, offering dedicated, in-depth courses on the cognitive and information warfare tactics of Russia, China, and Iran, treating each as a unique and complex subject.

21.2 Russian Doctrine- Reflexive Control and Perpetual Conflict

Russian information warfare doctrine is arguably the most developed and historically grounded of all. It is rooted in a long tradition of Soviet-era concepts, such as "active measures," and is built upon a worldview that views the information space as a domain of perpetual conflict. For Russia, there is no clear distinction between war and peace; information operations are a continuous effort to subvert and destabilize adversaries.

A key concept in Russian doctrine is Reflexive Control, a sophisticated form of manipulation where one provides an adversary with specially prepared information to incline them to make a decision predetermined by the manipulator voluntarily. It is about controlling the adversary's decision-making process itself, achieved through a "whole of systems" approach that integrates intelligence, counterintelligence,

maskirovka (military deception), disinformation, and electronic warfare. Russia does not see "cyber" as a separate domain but as one of many related tools of information warfare, alongside state-sponsored media like Russia Today (RT). The primary lesson from Russian doctrine is its integration and its focus on manipulating the enemy's perception of reality to the point where they act against their interests.

21.3 Chinese Doctrine- The "Three Warfares" and Cognitive Dominance

Chinese strategic thought on information conflict is codified in the concept of the "Three Warfares"- public opinion warfare, psychological warfare, and legal warfare (lawfare). The doctrine, described by NATO as a strategy to achieve victory, represents a comprehensive approach to shaping the cognitive environment in China's favor.

- Public Opinion Warfare aims to influence domestic and international public opinion, thereby building support for China's actions and eroding the will of its adversaries.
- Psychological Warfare seeks to demoralize and disorient enemy military personnel and civilian populations through psychological operations, deception, and intimidation.
- Legal Warfare (Lawfare) involves using domestic and international law to claim the legal high ground, challenge the legitimacy of an adversary's actions, and shape the legal frameworks that govern a conflict.

China's approach is also heavily focused on technology as a means of achieving cognitive dominance, including the development of systems like the "Intelligent Psychological Monitoring System," which uses smart sensors to monitor the psychological state of its soldiers, thereby optimizing their combat

Copyright 2025

performance. The lesson from Chinese doctrine is its systematic and institutionalized approach, which explicitly links public opinion, psychological effects, and legal arguments into a single, coherent strategy, all underpinned by a drive for technological superiority in monitoring and influencing human cognition.

21.4 Iranian Doctrine- Hybrid Warfare and the "Axis of Resistance"

Iran's approach to cognitive warfare is best understood within the context of its broader strategy of hybrid and asymmetric warfare. Lacking the conventional military power to confront states like Israel or the United States directly, Iran uses a network of proxies and partners—the "Axis of Resistance"—to wage conflict below the threshold of conventional war. Cognitive warfare is a central element of this strategy.

Iranian intelligence services, such as the IRGC and MOIS, utilize social media and online platforms for command and control, issuing instructions to cyber units, including the Basij Cyber Battalions, to conduct coordinated information operations. Their tactics include-

- Impersonation and Infiltration- Creating fake social media accounts that impersonate journalists, opposition leaders, and dissidents to sow division among opposition groups and spread disinformation.
- Narrative Laundering- Infiltrating protests and demonstrations to pervert the messaging with divergent disinformation, and using front organizations to create a global network of activists who amplify pro-regime narratives.
- Intimidation and Threats- Using online platforms to issue direct threats and warnings to dissidents and opposition groups, creating a climate of fear.

The key lesson from Iranian doctrine is its mastery of networked, proxy-based cognitive warfare. Iran has successfully built and directed a transnational influence ecosystem that allows it to project cognitive power far beyond its borders, often with a high degree of plausible deniability. Understanding how to map, disrupt, and dismantle these proxy networks is essential to countering Iranian influence.

By studying these diverse doctrines, a cognitive army can develop adversary-specific playbooks, anticipate the types of campaigns it is likely to face, and avoid the trap of assuming all adversaries think and operate in the same way.

Chapter 22- Sustaining Legitimacy- Communication Ethics in Democratic Societies

22.1 The Legitimacy Imperative

For a cognitive army operating on behalf of a democratic state, legitimacy is the central focus. Unlike authoritarian regimes that can rely on coercion and control to silence dissent, a democratic government's authority is derived from the consent of the governed and its standing in the international community of democracies. The legitimacy is fragile and is built on a foundation of public trust. If a nation's cognitive warfare capability is perceived, either at home or abroad, as being deceptive, unethical, or aimed at manipulating its citizens, it will lose the trust of its people. The resulting loss of legitimacy can be more strategically damaging than any tactical victory gained through a specific influence operation.

Therefore, sustaining legitimacy is not a secondary consideration; it is a primary operational requirement. The requires a deep and abiding commitment to communication ethics, even while engaging in the often-

Copyright 2025

murky world of influence and counter-influence. The challenge is to reconcile the operational necessities of cognitive warfare with the core values of a democratic society.

22.2 The Principle of Audience Distinction

A foundational principle for ethical communication in this context is a strict distinction between foreign and domestic audiences. While international law and ethical norms may permit the use of deception and psychological operations against a declared foreign adversary in a time of conflict, the use of such techniques against a nation's citizens is fundamentally illegitimate and antithetical to democratic principles.

A democratic cognitive army's mission *domestically* must be exclusively defensive and transparent. Its role should be to enhance societal resilience, rather than engaging in persuasion. The involves-

- Exposing Foreign Malign Influence- Transparently identifying and exposing hostile information operations targeting the domestic population. The is a counterintelligence function, not a propaganda function.
- Promoting Media and Digital Literacy- Supporting educational initiatives that equip citizens with the critical thinking skills needed to identify manipulation and disinformation on their own. The goal is to create a more resilient and discerning populace, not a more compliant one.
- Fact-Based Communication- When communicating with the domestic public, the government and its agencies must adhere to the highest standards of truthfulness and accuracy.

The rules of engagement must be fundamentally different for operations directed at foreign adversaries. However, even in the foreign sphere, actions must be carefully weighed for their potential "blowback" effect—the risk that a narrative or tactic intended for a foreign audience will bleed back into the domestic information environment and contaminate it.

22.3 Transparency and Oversight as a Source of Strength

In a democratic society, secrecy can be a vulnerability. While specific operations may require classification to be effective, the overall framework, doctrine, and legal basis for the nation's cognitive warfare capability should be as transparent as possible. The transparency is a source of strength and legitimacy.

This involves-

- Public Doctrine- Publishing an unclassified version of the national cognitive warfare doctrine that clearly articulates its mission, ethical principles, and the legal authorities under which it operates.
- Robust Oversight- Subjecting the cognitive army to rigorous oversight from multiple branches of government, including legislative committees and the judiciary, ensuring accountability and preventing abuse.
- Public Debate- Fostering an open and informed public debate about the role and limits of information operations in a democracy. Think tanks, academic institutions, and the media play a crucial role in this process.

This approach may seem to place the democratic state at a disadvantage relative to its authoritarian rivals. However, in the long run, this commitment to transparency and the rule of law is a powerful source of

Copyright 2025

cognitive resilience. A public that trusts its institutions and understands the nature of the threat is far less susceptible to hostile propaganda that seeks to exploit division and sow distrust. Legitimacy, sustained through ethical communication, is the democratic world's most potent defense in the cognitive domain.

Chapter 23- Commercial-Government Collaboration Models

23.1 The Rationale for Public-Private Partnership

The analysis throughout this text has established a clear and compelling rationale for a new model of public-private partnership in the cognitive warfare domain. The government possesses the legitimate authority, strategic direction, and resources necessary for a national security mission. However, it lacks the specialized tradecraft, doctrinal agility, and innovative capacity that have been cultivated in the commercial sector by "pure-play" intelligence firms, such as Treadstone 71. Conversely, the commercial sector possesses this deep expertise but lacks the mandate and legal authority to conduct national-level cognitive operations.

A collaborative model that fuses the strengths of both sectors is therefore not merely an option, but a strategic imperative. The goal is to create a synergistic relationship where the government defines the "what" and "why" (the mission and strategic objectives), and the commercial partner provides the "how" (the doctrine, training, and tradecraft). Several models for this collaboration can be envisioned, ranging from simple training contracts to deep, long-term strategic partnerships.

23.2 Model 1- The Doctrinal Training Engine (The Recommended Model)

Doctrinal Training is the primary model advocated for in this text, centered on the principle of knowledge transfer. In this model, the government does not outsource its cognitive operations. Instead, it contracts with a commercial partner to build an indigenous, organic capability.

- Structure- The government selects a cadre of personnel from across its defense and intelligence agencies to form the core of its new cognitive army. The commercial partner (e.g., Treadstone 71) is embedded as the primary training and doctrine provider.
- Function- The commercial partner implements its entire training pipeline, from foundational intelligence tradecraft to advanced counterintelligence and deception planning, for the selected government personnel. They provide the curriculum, instructors, templates, and SOPs.
- Outcome- The result is a professionalized, government-run cognitive force that operates according to a single, best-in-class doctrine. The commercial partner's role gradually diminishes over time as the government develops its cadre of expert instructors, creating a self-sustaining capability. The model maximizes national sovereignty and operational control while rapidly closing the initial skills gap.

23.3 Model 2- The Embedded Consultant / "Seamless Extension"

A second, less comprehensive model involves embedding commercial experts directly into government fusion cells as consultants or analysts. Treadstone 71 describes this as providing a "seamless extension of your organization".

Copyright 2025

- Structure- Individual commercial analysts or small teams with specialized skills (e.g., a cultural expert on Iran, a data scientist) are contracted to work alongside government personnel within a cognitive fusion cell.
- Function - The commercial experts provide their niche expertise on specific problems, augment the government's analytical capacity, and offer on-the-job training and mentoring to their government counterparts.
- Limitations - While this model can be effective in filling specific, short-term skills gaps, it is not a substitute for a comprehensive knowledge transfer program. It risks creating a long-term dependency on contractors and fails to build a standardized, institution-wide doctrine. It patches holes rather than building a new foundation.

23.4 Model 3- The Research and Development (R&D) Partnership

This model emphasizes collaboration on the forward-looking aspects of cognitive warfare, including strategic foresight and technology development.

- Structure - The government partners with commercial firms, think tanks (such as the RAND Corporation or ASU's Threatcasting Lab), and academic institutions to research and wargame future cognitive threats.
- Function - The collaboration focuses on horizon scanning for emerging technologies, analyzing the future strategic environment, and developing and testing new concepts for cognitive security. The French Red Team Defense project, which brings together science fiction authors and military planners, exemplifies this innovative and collaborative research and development approach.
- Integration - The insights and concepts developed in this R&D partnership will then be integrated into the training and doctrine of the operational cognitive force, ensuring that the nation's capabilities do not stagnate and remain ahead of the threat curve.

A mature national cognitive warfare strategy would likely employ a hybrid approach, using the Doctrinal Training Engine as the foundational model for building the core force, supplemented by Embedded Consultants for niche expertise and a robust R&D Partnership to drive future innovation. The multi-pronged collaborative strategy is the most effective way to harness the full spectrum of national talent in the cognitive domain.

Chapter 24- Strategic Foresight Methods to Adapt the Cognitive Army

24.1 The Imperative of Adaptation

In the rapidly evolving landscape of cognitive warfare, strategic adaptation is not just a desirable attribute; it is the key to long-term survival and relevance. An adversary's tactics, the technologies they employ, and the geopolitical context in which they operate are constantly evolving. A cognitive army that is built and trained for today's threats will be obsolete tomorrow. Therefore, the organization must have a built-in, institutionalized process for looking into the future, anticipating change, and adapting its doctrine, training, and capabilities accordingly. Such is the discipline of strategic foresight.

Copyright 2025

Strategic foresight is not about predicting the future with certainty; it is about anticipating the future with clarity and insight. It is a systematic process for exploring a range of plausible futures, identifying emerging threats and opportunities, and developing strategies that are robust and adaptable across multiple potential scenarios. It is the mechanism by which the cognitive army avoids strategic surprise.

24.2 Threatcasting- Envisioning Future Conflict

One robust methodology for strategic foresight is Threatcasting. Developed and practiced by institutions like Arizona State University's Threatcasting Lab, this conceptual framework enables multidisciplinary groups to systematically envision and plan against threats ten to fifteen years in the future.

The process involves bringing together a diverse group of experts—from military, academia, industry, and even creative fields like science fiction—to brainstorm plausible future threats. The group works backwards from a future threat scenario (e.g., "In 2035, an adversary uses AI-generated, hyper-personalized propaganda to trigger a civil conflict") to identify the technological and social trends that could lead to that future. They then identify "flags" or warning indicators that could signal progress toward that threat, and brainstorm actions that can be taken today to disrupt, mitigate, or recover from it. The methodology is particularly well-suited for cognitive warfare, as it forces planners to think beyond current TTPs and consider how emerging technologies like quantum AI or brain-computer interfaces could fundamentally change the nature of the cognitive battlefield.

24.3 Scenario Planning and Alternative Futures Analysis

Another core set of foresight methods involves **scen**ario planning and alternative futures analysis. These are structured analytic techniques designed to help organizations navigate high levels of uncertainty. Instead of trying to produce a single, most likely forecast, analysts develop a set of two to four divergent but plausible future scenarios.

For the cognitive army, this could involve developing scenarios based on key uncertainties, such as.

- The future of social media regulation (e.g., a future with highly regulated platforms vs. a "wild west" environment).
- The trajectory of U.S.-China relations (e.g., a future of cooperation vs. a future of intense confrontation).
- The proliferation of advanced AI (e.g., a future where AI is democratized vs. a future where a few powerful actors control it).

By developing and testing its strategies against this range of scenarios, the cognitive army can identify "robust" strategies that are likely to be effective regardless of how the future unfolds. The process, which is a key component of advanced structured analytic techniques, builds strategic flexibility and adaptability into the organization's DNA.

24.4 Integrating Foresight into the Organizational Rhythm

Strategic foresight cannot be a one-time project. It must be a continuous, iterative process that is fully integrated into the cognitive army's organizational rhythm. The involves several key functions-

Copyright 2025

- A Dedicated Foresight Unit- A small, dedicated unit within the cognitive army's structure should be responsible for managing the strategic foresight process. The unit would organize threatcasting workshops, conduct scenario planning exercises, and continuously scan the horizon for emerging trends and warning indicators.
- The "Convergence" of Ideas- The unit would act as a hub for "the convergence" of ideas from across the government, industry, and academia, ensuring that the cognitive army is constantly exposed to new and challenging perspectives.
- Feeding Foresight into Doctrine and Training - The outputs of the foresight process—new threat scenarios, identified vulnerabilities, and emerging opportunities—must be fed directly back into the organization's training and doctrine development cycle. Wargames should be designed around future scenarios, and training curricula should be updated to address newly identified threats.

By institutionalizing strategic foresight, the cognitive army transforms itself from a reactive organization, constantly struggling to catch up with the latest threat, into a proactive, future-ready force that can shape the cognitive environment of tomorrow.

Part V — Strategic Foresight and Long-Term Adaptation

Chapter 25- The Fusion of Commercial Knowledge and State Authority

The central thesis of this work culminates in a single, powerful conclusion: the most effective model for a democratic nation to build a decisive cognitive warfare capability is through the deliberate fusion of specialized commercial knowledge with legitimate state authority. The public-private partnership is not a compromise but a synthesis that creates a capability greater than the sum of its parts. It addresses the fundamental weaknesses of a purely state-run model—its bureaucratic inertia, risk aversion, and lack of specialized tradecraft—while using the state's unique and indispensable role as the arbiter of national security policy and the wielder of legitimate power.

The state provides the mission, mandate, and oversight. It defines the strategic objectives, sets the ethical and legal guardrails, and ensures that the capability is employed in the national interest and with democratic accountability. It provides the resources and the institutional home for the cognitive operators. In essence, the state provides the "why" and the "what."

The specialized commercial partner, epitomized by the Treadstone 71 model, provides the **doctrine,** tradecraft, and training. It brings a deep, pre-existing body of knowledge, forged in the competitive and rapidly evolving commercial sector and grounded in the highest standards of the intelligence community. It delivers the operational "how"—the specific, proven methodologies for collection, analysis, and influence that the state cannot organically generate at the necessary speed and level of sophistication.

This fusion creates a cognitive army that is both legitimate and lethal. It is legitimate because it operates under the full authority and oversight of a democratic government. It is lethal in the cognitive sense because its operators are armed with a superior, agile, and constantly evolving doctrine. The model rejects the false dichotomy between state control and private sector agility, arguing instead for a symbiotic relationship that harnesses the best of both worlds. It is the blueprint for building a cognitive force that can compete but win in the complex battlespace of the 21st century.

Copyright 2025

Chapter 26- Recommendations for Israel and Allied Democracies

Based on the comprehensive analysis presented in this text, a set of clear, actionable recommendations can be offered to the government of Israel and, by extension, to its democratic allies who face similar threats in the cognitive domain. These recommendations provide a strategic roadmap for moving from the current state of vulnerability to a future of cognitive resilience and superiority.

Recommendation 1- Reject the Centralized Headquarters Model. The first and most critical step is to reject the intuitive but flawed proposal to create a single, centralized, top-down "Cognitive Army" headquarters. As has been demonstrated, this model is likely to replicate the very bureaucratic inertia and doctrinal shallowness that have led to current failures. It prioritizes the illusion of control over the reality of operational capability.

Recommendation 2- Adopt a Knowledge Transfer Strategy. Instead of attempting to reinvent cognitive warfare doctrine from within, the government should immediately initiate a strategy of knowledge transfer and dissemination. It should conduct a rigorous assessment of the commercial intelligence sector to identify a best-in-class partner—a firm with a proven, standards-based, and comprehensive doctrine for cognitive and cyber intelligence, exemplified by the Treadstone 71 model. The objective of this partnership should be the wholesale transfer of doctrine, curriculum, and tradecraft to a select cadre of national security professionals.

Recommendation 3- Establish a Distributed Network of Cognitive Fusion Cells. The organizational goal should not be a single headquarters but the creation of a distributed network of small, agile, and mission-focused cognitive fusion cells across the defense and intelligence establishment. Each cell should be staffed with an integrated, multi-disciplinary team and trained to operate according to the single, unified doctrine acquired through the commercial partnership. The networked structure will provide the necessary agility, resilience, and scalability to counter a networked threat.

Recommendation 4- Create a Dedicated Professional Career Path for Cognitive Operators. To attract and retain the necessary talent, the government must establish a new, specialized professional career path for cognitive operators within its national security apparatus. The career path must offer advanced training, unique operational opportunities, and a promotion track that values unconventional skills, including creativity, cultural empathy, and psychological acuity, alongside traditional analytical rigor.

Recommendation 5- Institutionalize Ethical Oversight and Strategic Foresight. From the outset, the new cognitive capability must be embedded within a robust framework of legal and ethical oversight to ensure its legitimacy and alignment with democratic values. Concurrently, a dedicated strategic foresight function must be established and integrated into the organization's core processes. They will ensure that the cognitive army remains adaptive, forward-looking, and capable of anticipating and preempting future threats.

Israel and its allies can move beyond a reactive and defensive posture by adopting these recommendations. They can build a truly 21st-century national security instrument- a professional, doctrine-driven, and ethically grounded cognitive army capable of defending and advancing the nation's interests in the defining battlespace of our time.

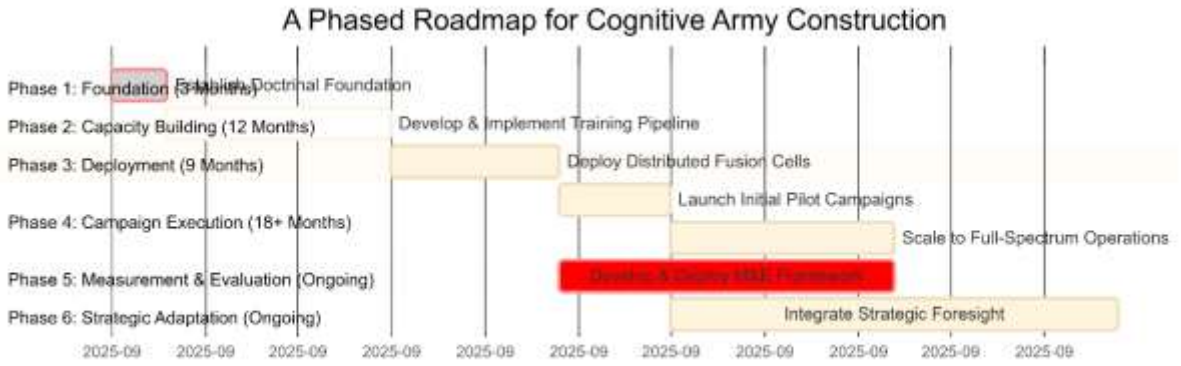
Chapter 27- Final Roadmap- Treadstone 71 as the Model for Cognitive Army Construction

Copyright 2025

This text presents a comprehensive argument and a detailed blueprint for the construction of a modern cognitive army. The final roadmap for a nation like Israel is clear. It is a phased approach that prioritizes the acquisition of human capability—the "software"—before constructing a rigid organizational structure—the "hardware." The Treadstone 71 model, with its deep doctrinal roots, comprehensive curriculum, and proven operational experience, serves as the definitive template for this process.

Phase 1: Partnership and Cadre Selection (Months 1-3) The initial phase involves making a strategic decision to adopt the knowledge transfer model. The government would identify and formalize a partnership with a commercial entity that meets the doctrinal and training standards outlined in this text. Concurrently, a rigorous selection process would be initiated across the IDF, Mossad, Shin Bet, and other relevant agencies to identify the first cadre of 50-100 high-potential personnel who possess the aptitude for cognitive operations.

Phase 2- Doctrinal Immersion and Foundational Training (Months 4-12) The selected cadre would be removed from their regular duties and immersed in an intensive training program delivered by the commercial partner. The phase would focus on the foundational curriculum, modeled on the Treadstone 71 Certified Cyber Intelligence Analyst program. The entire cadre would be trained to a single, high standard in the intelligence lifecycle, collection tradecraft, structured analysis, and operational security. The creates the common doctrinal language and skillset upon which everything else will be built.



Phase 3: Advanced Specialization and Fusion Cell Formation (Months 13-24) Upon completion of foundational training, the cadre will be divided into specialized tracks for advanced training, modeled after the Treadstone 71 Certified Cyber Counterintelligence Analyst curriculum. Operators would specialize in areas like deception planning, adversary-specific doctrine (e.g., Iran, Russia), psychological profiling, and AI integration. During this phase, the initial cognitive fusion cells would be formed, bringing together operators with complementary specializations into integrated teams. These nascent cells would begin conducting wargames and simulation-based exercises to hone their collaborative skills.

Phase 4: Initial Operational Capability and Doctrinal Adaptation (Months 25-36) The newly formed fusion cells would begin to undertake real-world, limited-scope missions under the close mentorship of the commercial partner. The phase is critical for translating training into operational experience. The lessons learned from these initial operations would be fed back into a continuous process of doctrinal adaptation, where the commercial baseline doctrine is refined and customized to meet the specific needs and strategic

Copyright 2025

context of the nation. During this phase, the government would also begin developing its instructor cadre from the top graduates of the initial program, laying the groundwork for a self-sustaining training pipeline.

Phase 5- Full Operational Capability and Strategic Expansion. With a proven capability, a battle-tested doctrine, and a self-sustaining training program, the nation's cognitive army achieves full operational capability. The network of fusion cells can be expanded, and their mission scope can be broadened to address the full spectrum of national security challenges in the cognitive domain. The commercial partner transitions to a long-term strategic advisory and R&D role, continuing to provide insights on emerging threats and technologies.

This roadmap is ambitious, yet realistic and necessary. It is a plan for building not just a new organization, but a new kind of national security professional and a new national capability. By fusing the proven, agile, and innovative knowledge of the commercial sector with the authority and mission of the state, a democratic nation can build a cognitive army that is effective but enduring.

Copyright 2025

References

Barak, U. (2025). *The campus front- Adversary influence in Western academia*. Institute for National Security Studies.

Cohen, A. (2025, August 15). Hezbollah's two-decade project to train Gaza's social media warriors. *Israel Hayom*.

Michael, K. (2024). *The Imperative for a National Cognitive Army: A Strategic Proposal for Israel*. The Misgav Institute for National Security and Zionist Strategy.

Sun Tzu. (2005). *The art of war* (T. Cleary, Trans.). Shambhala. (Original work c. 5th century B.C.).

Thucydides. (1972). *History of the Peloponnesian War* (R. Warner, Trans.). Penguin Classics. (Original work c. 5th century B.C.).

Treadstone 71. (2022). *Adversary cultural profiling- A doctrinal guide*. Cyber Intelligence Training Center.

Treadstone 71. (2023a). *Cognitive warfare tradecraft- Training and curriculum standards*. Cyber Intelligence Training Center.

Treadstone 71. (2023b). *Narrative engineering and deception detection- An operational playbook*. Cyber Intelligence Training Center.

Treadstone 71. (2024). *The STEMPLES Plus framework- Structured analysis for influence operations*. Cyber Intelligence Training Center.

Copyright 2025