Inside the Gates

Cultivating Cognitive Security to Defend the Homeland

Col Dr. William "Ox" Hersch, USAF, Retired
Lt Col Melissa "Sharpie" McLain, USAF

Abstract

In the twenty-first century, effective security strategies demand more than sophisticated military might. Social and information technologies have transformed the character of conflict, compelling democracies to expand their defenses beyond traditional military domains. Adversaries now wield unprecedented influence over the minds of individuals, leaders, and decision-makers across the security enterprise and society at large. The Chinese Communist Party wages a comprehensive and calculated political warfare campaign, exploiting cognitive weaknesses and harnessing social media platforms to subvert democratic values and advance its strategic aims. While Beijing poses an internal threat, democracies possess the means to fortify cognitive security within their societies and security frameworks. The United States and its allies must prioritize investment in and exploitation of the unique strengths of their diverse populations, while revitalizing the bedrock principles of free speech, free markets, and inherent human rights, which face renewed assault from totalitarian regimes.

***

The digital revolution in social and information technology has triggered a profound shift in the landscape of Homeland Defense and Security, challenging traditional paradigms. Democracies must embrace a philosophy of "failing forward," addressing historical shortcomings and reimagining security strategies to navigate the competitive and conflict-ridden terrain of the twenty-first century. With the ubiquity of smart devices, rival powers now possess direct access to almost every citizen, enabling nefarious actors like the Chinese Communist Party (CCP) to marshal national resources for information warfare campaigns often conducted clandestinely. In this era of information warfare, every individual becomes a potential combatant or target, exploiting historical vulnerabilities in the American way of war and capitalizing on the openness of democratic societies. As P.W. Singer and Emerson T. Brooker put it, "These new wars are not won by missiles and bombs, but by those able to shape the story lines."[1]

[1] P.W. Singer and Emerson T. Brooker, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt Publishing Company, 2018), 21.

While maintaining high-end military capabilities remains paramount, this article argues that the transformation brought about by social and information technologies necessitates a broader perspective for deterring adversaries and safeguarding the homeland. Adversaries now wield unprecedented influence over the minds of individuals, leaders, and decision-makers within both the security enterprise and society as a whole. Democracies, recognizing their susceptibility, must take proactive measures to bolster their defenses.[2] Accordingly, the article delves into an examination of the CCP's political warfare strategy, introduces cognitive theory, draws insights from past conflicts, analyzes case studies, and proposes measures at the national, communal, and individual levels to enhance cognitive security (COGSEC).[3]

The advent of the Internet era coincided with the dissolution of the Soviet Union, a time when Francis Fukuyama famously proclaimed the triumph of democracy over rival ideologies such as fascism and communism.[4] However, early optimism, buoyed by a fervent belief in the transformative potential of technology and liberal values, failed to anticipate the ways in which authoritarian regimes would harness information technologies for their own ends. President Bill Clinton's 2000 observation likening China's initial attempts to censor the Internet to "trying to nail Jell-O to the wall" now appears naïve in hindsight.[5] Today, the People's Republic of China (PRC) not only exercises strict censorship over its domestic Internet but also exploits the openness of democratic societies' information infrastructure.

---

[2] Eric Rosenbach and Katherine Mansted, "Can Democracy Survive in the Information Age?," Technology and National Security (Harvard Kennedy School: Belfer Center for Science and International Affairs: Aspen Strategy Group, October 2018), https://www.belfercenter.org/. The Aspen Group's year-long study identified four distinct vulnerabilities that democracies face: (1) weak mechanisms for distinguishing fact from fiction; (2) long, media-driven nature of elections; (3) the tech sector's profit-oriented culture; and (4) the inability of the government to oversee and coordinate issues related to the information environment. This contrasts sharply with authoritarian regimes that have near total control over their industry and information domains.

[3] Leanne Hirshfield, "Technical Proposal: Cognitive Security and Its Mitigation: A Theoretical Framework, Supporting Neurophysiological Studies, and Interactive Deep Learning Models in Sparse and Dense Information Environments" (presentation, Boulder, University of Colorado & United States Air Force Academy, 18 August 2023).

[4] Francis Fukuyama, *The End Of History And The Last Man* (New York: Free Press, 1992). xi. For the original journal article, see "The End of History?," *National Interest* 16 (Summer 1989): 3–18.

[5] Rosenbach and Mansted, "Can Democracy Survive," 3. President Bill Clinton as quoted by Rosenbach and Mansted. For original speech, see "Remarks at the Paul H. Nitze School of Advanced International Studies." (Washington, 8 March 2000).

Beijing's infiltration is evident, signaling a pressing challenge.[6] Beijing is *inside the gates*.

Cognitive Warfare and How We Think

According to Eric Rosenbach and Katherine Mansted, cognitive warfare employs cyber tools to manipulate enemy cognitive processes, exploiting mental biases, inducing thought distortions, and influencing decision-making both at the individual and collective levels.[7] This form of warfare serves as the foundation for political warfare, encompassing activities aimed at expanding a nation's influence and legitimacy while undermining adversaries, all without resorting to conventional or nuclear conflict.[8] Political warfare encompasses a broad spectrum of tactics, including public opinion/media warfare, psychological warfare, and economic warfare, using all available resources at a nation's disposal.[9]

Cognition refers to how individuals mentally respond to stimuli, making an understanding of cognitive processes essential in comprehending cognitive warfare.[10] According to Kenneth Boulding, an individual's accumulation of knowledge and experience shapes their worldview, forming an image of the world and their role within it. This image, akin to a schema, dictates perceptions and behaviors, filters reality and influences reactions to new information.[11] Robert Jervis' *Perception*

---

[6] *See*, Larry Diamond and Orville Schell, eds., *China's Influence & American Interests: Promoting Constructive Vigilance* (Stanford, CA: Hoover Institution, 29 November 2018), https://www.hoover.org/; and Shanthi Kalathil, "The Evolution of Authoritarian Digital Influence: Grappling with the New Normal," *PRISM* 9, no.1 (2020): 32–51, https://ndupress.ndu.edu/.

[7] Bernard Claverie and Francois Du Cluzel, "'Cognitive Warfare': The Advent of the Concept of 'Cognitics' in the Field of Warfare" (NATO Collaboration Support Office, 8 April 2022), hal-03635889, HAL Open Science, 1, https://hal.science/.

[8] Seth G. Jones et al., *Competing Without Fighting: China's Strategy of Political Warfare* (Washington: Center for Strategic & International Studies, August 2023), 3, https://csis-website-prod.s3.amazonaws.com/.

[9] George Kennan, as quoted in, Kerry K. Gershanek, *Political Warfare: Strategies for Combating China's Plan to "Win without Fighting"* (Quantico, VA: Marine Corps University Press, 2020), 14, https://www.usmcu.edu/. Kennan defined *political warfare* as "the employment of all the means at a nation's command, short of war, to achieve its national objectives [that] range from . . . political alliances, economic measures . . .[to] 'black psychological warfare." A Project 2049 Institute Study describes *political warfare* as an "alternative . . . [that] seeks to influence emotions, motives, objective reasoning, and behavior of foreign governments, organizations, groups, and individuals in a manner favorable to . . . political-military-economic objectives." Gershanek, 15. The PRC refers to public/opinion media warfare, psychological warfare, and legal warfare as "The Three Warfares." Gershanek, 15. For an expanded explanation of key CCP terms related to political warfare and examples of organizations involved in political warfare, *see*, Jones et al, "Competing Without Fighting," 10, 12.

[10] Josh Baughman, "How China Wins the Cognitive Domain," China Aerospace Studies Institute, January 2023, 1, https://www.airuniversity.af.edu/.

[11] Kenneth Boulding, *The Image: Knowledge in Life and Society*, 11th ed. (Ann Arbor: University of Michigan Press, 1977); and Boulding, *The Image*.

and Misperception in International Politics demonstrates how perceptions, including self-image and historical interpretations, give rise to biases that impact political decision making.[12] Cognitive warfare exploits these biases to achieve desired effects and reshapes the individuals' underlying images to manipulate their perceptions.

Groups that "share the same image of the world" are typically "exposed to much the same set of messages in building up images."[13] A shared image is like an anchor that grounds people to fundamental assumptions and values. If an adversary understands targets' anchors and cognitive vulnerabilities, it can exploit emotionally charged predispositions and hack individuals and groups.[14]

In psychology, the anchoring effect occurs when individuals rely on a specific value as a reference point when estimating an unknown quantity.[15] These anchors subsequently influence choices, perspectives, and behaviors. Anchoring can occur rapidly or gradually over time, as individuals accumulate images and information, often without awareness of the anchoring process. Beijing's efforts seek to destabilize free societies by undermining the anchoring narratives of democracy and imposing its own image.

---

[12] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976). 68, 172, 181–87. Jervis elucidates the concept of "Excessive and Premature Cognitive Closure," where "actors are more apt to err on the side of being too wedded to an established view and too quick to reject discrepant information," thus 'closing' an Image off. 188. Leaders establish a "dominant percept," from an accumulation of experiences or by drawing analogies and lessons from history (which themselves can be skewed by bias) and then drive agendas and policies consistent with those percepts. For in-depth analysis of the role historical analogies play in influencing wartime decision making, *see*, Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decision of 1965* (Princeton, NJ: Princeton University Press, 1992).

[13] Boulding, *The Image*. 14.

[14] Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security" (testimony, RAND Corporation, presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity on 27 April 2017), 2–3, https://www.rand.org/. In Waltzman's testimony before the Armed Services Subcommittee on Cybersecurity, he cited an example from India, where a riot requiring 13,000 Indian troops to quell broke out as the result of a fake video circulated online. The Hindus and Muslims involved were already emotionally charged and inclined toward particular perspectives, rendering them susceptible to manipulation.

[15] Daniel Kahneman, *Thinking Fast and Slow* (New York, New York: Farrar, Straus and Giroux, 2013), 119. Kahneman describes the "anchoring effect" as one of "the most reliable and robust results of experimental psychology."

Beijing's War

The CCP's extensive political warfare against the United States and its allies has been extensively documented.[16] The PRC wages a widespread campaign aimed at surveilling, harassing, and coercing residents of not only the United States but also other nations. Since 2014, it has been reported that the PRC has hacked and stolen data from approximately 80 percent of Americans.[17] Influence operations play a central role in Beijing's strategy, as highlighted by security expert Michael Pillsbury's exposition of the "Hundred-Year Marathon" strategy, which aims to realize the "China Dream" by 2049, reshaping the international order according to traditional Chinese ideals.[18]

In 2014, leading CCP theorist Zeng Huafeng outlined the concept of "brain control in cognitive space," emphasizing its importance in "future wars," where nations must leverage various informational channels—including propaganda media, national languages, and cultural products—as weapons to infiltrate, influence, and potentially dominate public cognition, emotions, and consciousness, particularly among both the general populace and national leadership.[19] President Xi Jinping has further asserted that the Chinese socioeconomic model presents a novel option for global modernization.[20]

The narratives propagated by the CCP encompass several key themes:

1. The portrayal of Beijing's strategy, policies, and intentions in a positive light.

---

[16] For analysis on PRC Political Warfare campaigns against Thailand and Taiwan, *see* Gershanek, *Political Warfare*, chapters 5–8. For analysis of what Taiwan terms *sharp power* influence and information operations, *see*, Ko Shu Ling, "Taiwan on the Frontline of China's Information Operations," *Power 3.0* (blog), 12 September 2023, https://www.power3point0.org/; and Russell Hsiao, "Political Warfare Alert: The PRC's Evolving Information Operations Targeting Provincial and Local Media Intermediaries," *Global Taiwan Brief* 8, no.1 (11 January 2023), https://globaltaiwan.org/. For a contemporary report on the Chinese Communist Party's influence operations against the United States and its allies, *see*, Jones et al., "Competing Without Fighting."

[17] Jones et al., "Competing Without Fighting," 30, XI.

[18] Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt and Company, 2022), 28. *The China Dream*, published in 2009, was written by People's Liberation Army (PLA) Colonel Liu Mingfu when he was a professor at China's National Defense University. The book is a bestseller in China and "featured in all the 'recommended reading' section[s] of all state-controlled bookstores." 29. The book is not fully translated into English and describes how China will surpass and then replace the United States.

[19] Huang Kunlun, "Seize the Brain Power of Future Wars: PLA Daily Journalist Huang Kunlun Interview with Professor Zeng Huafeng, Dean of the School of Humanities and Social Sciences, National University of Defense Technology," *PLA Daily*, 16 June 2014, http://www.81.cn/. At the time of the interview, Zeng Huafeng was dean of the School of Humanities and Social Sciences, National University of Defense Technology, headquartered in Kaifu, Changsha, Hunan China.

[20] As quoted by Yuri Momoi, "Xi's Speech Hints at Ambition to Surpass Mao: Chinese Leader Suggests Direct Ideological Descent from Marx," *Nikkei Asia*, 18 October 2022, https://asia.nikkei.com/.

2. Characterizations of the CCP's governance model as superior, emphasizing collectivism over individualism.
3. Depiction of Western nations as imperialistic and colonial powers, often accused of hypocrisy, racism, and sexism. Notably, the CCP's news agency released "Ameri-cracy" in 2022, a viral video critiquing the United States for election fraud, human rights violations, and attempts at global domination, set to a children's song.[21]
4. Promotion of "One China" themes that assert territorial claims over Taiwan and delegitimize ethnic minorities such as Tibetans, Uighurs, Mongols, and others.

The PRC has a history of employing cognitive warfare to further its strategic objectives. During China's Warring States period (475–221 BCE), a strategic landscape emerged marked by prolonged and deceptive competition. Competitors sought to undermine hegemonic powers by fostering complacency and discord, resorting to military action only when the "emperor was too weak to resist."[22] Drawing inspiration from this historical context, Beijing's "Hundred-Year Marathon" strategy is informed by insights gleaned from the *Stratagems of the Warring States*,[23] a compilation of lessons that articulate nine fundamental principles.[24]

[21] Jones et al., "Competing Without Fighting," 45–46.

[22] Pillsbury, *The Hundred-Year Marathon*, 38–45. Pilsbury is currently the director of the Center for Chinese Strategy at the Hudson Institute. His book details decades of his analysis of original Chinese documents and personal account from his time in China as an academic and as a security professional. He served in senior positions in the Department of Defense and for multiple presidential administration as a China expert. This work affords not only detailed insight into the PRC's historic and contemporary strategy (and the deep connection between the two), but his generational perspective on Beijing's ambition and the means and ways by which they are achieving it illuminates how he and the Western security enterprise were slow to recognize the CCP's true aims

[23] Pillsbury, *The Hundred-Year Marathon*, 27–29.

[24] The Chinese concept of *shi* is about "aligning all forces" and consists of two strategic elements: "deceiving others into doing your bidding and waiting for the point of maximum opportunity to strike." Pillsbury, *The Hundred-Year Marathon*, 36, 42.

Figure 1. Stratagems of the Warring States of China. The Stratagems of the Warring States, also known as Zhan Guo Ce, is an ancient Chinese text filled with anecdotes of political manipulation and warfare during the Warring States period (fifth to third centuries BCE). It offers a fascinating glimpse into the strategies and political views of that era.

Paraphrasing one author stated from an official People's Liberation Army (PLA) publication, warfare has transcended the physical realm and increasingly revolves around mass media, making cognitive warfare the focal point where information serves as the ammunition.[25] In 2015, the PRC allocated USD 10 billion toward foreign propaganda, an amount that has certainly increased since then.[26] The PRC

[25] Lee Myung Hae, "Perspective on the Evolution Trend of Cognitive Warfare," *PLA Daily*, 29 September 2022, 2, http://www.81.cn/.

[26] Ko, "Taiwan on the Frontline."

actively conducts "a concerted information operations (IO) campaign on a global scale . . . to influence governments and voters."[27] A 2023 cyberthreat analysis identified 10 coordinated covert information operations promoting CCP narratives, with a noted acceleration in PRC efforts against the United States and its allies, exploiting "emerging conspiracy theories."[28]

The security enterprise inevitably experiences conceptual delays in adopting new technologies as it deliberates their implications. However, there comes a point when the profession can no longer ignore anomalies and must embark on the extraordinary investigations that lead to paradigm-shifting revolutions.[29] Authoritarian regimes adeptly exploit and adapt to new technologies, employing information as a potent tool in the "heart of great-power competition," while democracies often find themselves lagging behind.[30] Insights from past conflicts can guide adaptation to the evolving security landscape.

Truth emerges more readily from error than from confusion.

—Francis Bacon

Lessons from Wars Past

On 31 January 1968, North Vietnam launched the Tet Offensive, unleashing 70,000 Communist troops in a coordinated surprise attack from the 20th parallel to the southern tip of Vietnam.[31] Vietcong sappers breached the American Embassy in Saigon, and the disturbing images permeated the airwaves. Up to that point,

---

[27] Hsiao, "Political Warfare Alert," 1. "The PRC's well-documented interference in [Taiwan's] 2018 and 2020 elections underscore the growing challenge facing all democracies." *See also*, Gershanek, *Political Wafare*, 51, 138. It is estimated that the PRC spends more than USD 337 million annually on United Front Work Department (UFWD) recruiting efforts in Taiwan. The UFWD serves as an intelligence gathering and social engineering arm of the CCP that is charged with gaining influence over elite individuals and organizations outside the mainland. See: Alexander Bowe, *China's Overseas United Front Work: Background and Implications for the United States* (Washington: U.S.-China Economic and Security Review Commission, 24 August 2018), https://www.uscc.gov/.

[28] Insikt Group, *Empire Dragon Accelerates Covert Information Operations, Converges with Russian Narratives* (Somerville, MA: Recorded Future, 30 August 2023), 2, https://go.recordedfuture.com/. This study notes distinct convergence with Russian anti-Western narratives and that the CCP's information warfare efforts are becoming more coordinated and tailored, leveraging metadata and emerging AI technologies to target individuals and exploit opportunities more surreptitiously at the tactical, operational, and strategic levels.

[29] Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 3rd ed. (Chicago: Chicago University Press, 1996), 5–6.

[30] Kalathil, "The Evolution of Authoritarian Digital Influence," 33.

[31] William R. Hersch, *Images of Inherited War: Three American Presidents in Vietnam*, The Drew Papers 13 (Maxwell AFB, AL: Air University Press, 2014), 107, https://media.defense.gov/. During the first day of the Tet Offensive, Communist forces attacked most of the 44 provincial capitals, five of the major cities, 64 district capitals, and approximately 50 hamlets.

Americans had consistently ingested realistic war coverage and become accustomed to a familiar pattern. However, Tet shattered this familiarity. The years of witnessing helicopters hovering, navigating dense jungles, and encountering booby traps had ingrained in the American psyche images of a distant war and elusive enemy.[32] In stark contrast, the coverage of the Tet Offensive portrayed the North as bold and triumphant, challenging previous perceptions.[33]

Tet proved to be a resounding military setback for the North. Despite initial gains, American and South Vietnamese forces swiftly regained control of most territory, repelled subsequent offensives, and inflicted significant losses on North Vietnam and the Vietcong.[34] However, the objective reality of the situation paled in comparison to the prevailing perception. After years of conflicting messages and faltering narratives, compounded by a nation increasingly uncertain about the direction and purpose of the Vietnam War and America's role in it, President Lyndon Johnson addressed the nation, acknowledging, "There is a division in the American house now. There is a divisiveness among us . . . I cannot disregard the peril . . . With America's sons in the fields far away, with America's future under challenge at home, with our hopes and the world's hopes for peace in the balance . . . I shall not seek . . . the nomination of my party for another term as your President."[35]

The Tet-induced cognitive dissonance, while not the sole factor, played a significant role in the demise of Johnson's presidency, just as conflicting perceptions

[32] Stanley Karnow, *Vietnam: A History; The First Complete Account of Vietnam at War* (New York: Penguin Books, 1984). 523

[33] Hersch, *Images of Inherited War*. 154.

[34] George C. Herring, *America's Longest War: The United States and Vietnam, 1950-1975.*, 2d ed., America in Crisis Series (New York: Knopf, 1986). 189–92. It is estimated that between the two offensives, the United States lost 1,100 men, the South Vietnamese lost 2,300 troops, and the Vietcong and North Vietnamese suffered close to 40,000 deaths.

[35] "The President's Address to the Nation Announcing Steps to Limit the War in Vietnam and Reporting His Decision to Not Seek Reelection, March 31, 1968," LBJ Presidential Library, 31 March 1968, https://www.lbjlibrary.org/.

and shifting public opinion contributed to the war's ultimate outcome.[36] Though not initially intended, the impact of Tet on the United States was deemed favorable by the politburo's official history, acknowledging, "We had struck a decisive blow that bankrupted the 'limited war' strategy of the American imperialists."[37] The images from Tet reshaped American perceptions of the war and their government, effectively unmooring and re-anchoring them. As observed, "Tet contorted the reality of American military achievements to a false perception of North Vietnamese Victory. What mattered was not the reality of Tet but what the public perceived to be true."[38]

Despite possessing military, economic, and technological superiority, the United States encountered strategic failure in Vietnam. Similarly, more recent American efforts in Iraq and Afghanistan also fell short despite similar advantages. In 1972, President Richard Nixon contextualized the Vietnam War within the broader framework of great-power competition, remarking, "We're in a much bigger game—we're playing a Russia game, a China game, and an election game."[39] As the United States once again shifts focus toward great-power competition, it must heed the lessons learned from Vietnam, Iraq, and Afghanistan.[40]

The three wars were marked by significant cultural, historical, and social complexities that defied mere military prowess. When viewed through the lens of a

---

[36] The Paris Peace Accords were signed under the Nixon administration in January 1973, calling for a ceasefire, withdrawal of US troops (although Nixon did promise continued support from American airpower), and for the North and South to find a peaceful resolution to the conflict. Despite the Accords, fighting continued, albeit without direct US involvement, and Saigon ultimately fell to North Vietnamese forces during the Ford administration in April 1975. For more in-depth analysis on the relationship between the media, policy, and the military during the Vietnam era, *see*: William M. Hammond, *Public Affairs: The Military and the Media, 1962*–1968 (Washington: Center of Military History, 1990), https://history.army.mil/. For further reading on the arc of the Vietnam War and US policies *see*: Karnow, *Vietnam*; George C. Herring, *America's Longest War: The United States and Vietnam, 1950–1975* (Boston: McGraw-Hill, 1996); George C. Herring, *LBJ and Vietnam: A Different Kind of War* (Austin: University of Texas Press, 1994); and Robert S. McNamara and Brian VanDeMark, *In Retrospect: The Tragedy and Lessons of Vietnam* (New York: First Vintage Books, 1996).

[37] Karnow, *Vietnam*, 523; and Merle L. Pribbenow, trans., *Victory in Vietnam: The Official History of the People's Army of Vietnam, 1954–1975; The Military History Institute of Vietnam*, Modern War Studies (Lawrence: University Press of Kansas, 2002), 223–24.

[38] Hersch, *Images of Inherited War*. 109.

[39] "Conversation Between President Nixon and His Assistant for National Security Affairs (Kissinger)," Government, Department of State: Office of the Historian, 3 April 1972, https://history.state.gov/.

[40] In 2011, the Obama administration announced the "pivot to Asia," *see*, "Barrack Obama says Asia-Pacific Is 'Top US Priority,'" *BBC News*, 17 November 2011, https://www.bbc.com/. The Biden administration's 2022 *National Security Strategy* describes the current decade as "decisive . . . for America and the world . . . [when] terms of geopolitical competition between . . . major powers will be set." *National Security Strategy* (Washington: The White House, October 2022), 6, https://www.whitehouse.gov/.

socio-technical system, war emerges as a dynamic interplay between hard systems and human elements, indivisible in their interaction. According to socio-technical systems theory, organizations consist of interconnected subsystems encompassing both social and technical dimensions, where individuals work toward common goals, adhere to established processes, use technology, and share cultural assumptions and norms. Failures within campaigns or organizations often stem from a narrow focus on isolated aspects of the system, neglecting to analyze the intricate interdependencies that exist within it.[41]

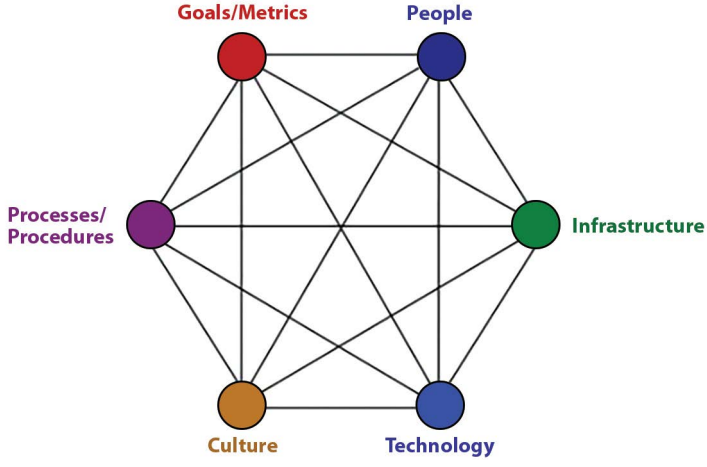

Figure 2. Socio-technical systems theory. (Source: "Socio-technical systems theory," Leeds University Business School, n.d., https://business.leeds.ac.uk/.)

Past shortcomings in warfare can be partly attributed to the security enterprise's failure to adequately consider critical cultural, social, and human subsystems. Colin Gray identifies eight characteristics of American strategic culture, including a disregard for historical context, a preference for technical solutions, a lack of appreciation for cultural nuances, and a tendency to resort to military force.[42] Gray criticizes what he terms "a cult of modernity," which often neglects the complexities of the human dimension when formulating and implementing security strategies.[43]

[41] "Socio-Technical Systems Theory," Leeds University Business School, n.d., https://business.leeds.ac.uk/.

[42] Colin S. Gray, *Explorations in Strategy* (Westport, CT: Praeger, 1996), 89–93. Gray explains that five interdependent factors of American strategic culture drive eight distinct characteristics that influence the country's way of war: the engineering style and the technical fix; impatience; indifference to cultural distinctions; a continental outlook, maritime situation, airpower preference; indifference to strategy; the resort to force, belated but massive; and the evasion of politics. Gray's elucidations are salient and offer useful insight into past wartime strategies and on America's contemporary planning, engagements, and strategic thought.

[43] Gray, *Explorations In Strategy*, 90.

Achieving growth necessitates recognizing both gaps and opportunities. Cyberspace comprises not only technology but also the individuals and processes that connect them. While technology undoubtedly plays a vital role, the human element remains indispensable.[44] The security enterprise must accelerate its adaptability or risk losing an ongoing information-cyber war that threatens "social, economic, and political cohesion."[45] Past failures should be viewed as opportunities for improvement rather than condemnations, and democracy, despite its imperfections, must not be relegated to the dustbins of history. Nonetheless, democracy faces significant threats, necessitating security strategies that can effectively counter the evolving landscape of "psychological-social-technical warfare."[46]

The manipulation of perceptions occurs on unprecedented "scales of time, space, and intentionality," constituting one of the most significant vulnerabilities we, both as individuals and as a society, confront.[47] Metadata algorithms empower the PRC to surveil, define, and manipulate targets.[48] Smart devices serve as homing beacons for cognitive "bombs" within the networked information ecosystem, pinpointing weaknesses with precision. Beijing adeptly exploits cognitive vulnerabilities, categorizing targets based on their image, and either leveraging existing anchoring narratives or subverting and reshaping them to align with Beijing's worldview. This article presents four interrelated terms encapsulated by the acronym NIRV, delineating how the PRC generates cognitive effects:

- **Nudging**—involves subtly attaching new or minor changes to already accepted narratives to steer target images toward CCP-aligned views, likened to putting kale in a child's chocolate milkshake to get them to consume vegetables.
- **Injection**—entails the rapid dissemination of flash messages, images, or narratives directly to the subconscious, often devoid of context.
- **Repetition**—refers to the frequency with which a particular narrative recurs across all mediums.
- **Volume**— encompasses the diversity of narratives directed at a target, encompassing a wide range of perspectives and themes.

---

[44] Former National Security Agency Deputy Director John Inglis testimony before Congress. *See*, "Cyber-Enabled Information Operations" (testimony, Washington, DC, Homeland Security Digital Library, Naval Postgraduate School, Center for Homeland Defense and Security, 27 April 2017), https://www.hsdl.org/

[45] Karen Guttieri, "Accelerate Change or Lose the Information War," *Æther: A Journal of Strategic Airpower & Spacepower* 1, no. 1 (Spring 2022), 91, https://www.airuniversity.af.edu/.

[46] Claverie and Du Cluzel, "Cognitive Warfare," 2-1.

[47] Waltzman, "The Weaponization of Information," 1.

[48] Kalathil, "The Evolution of Authoritarian Digital Influence," 35–37.

Case Studies

The PRC leverages Hollywood and social media platforms to exert influence over American populations. *Access* in this context refers to the capability to deploy effects into a specified operational domain with adequate freedom of action to achieve the intended objectives.

It's Just a Panda

In their 2023 Kenney Paper, *Mapping Chinese Influence in Hollywood*, Morgan A. Martin and Clinton J. Williamson provide insights into PRC objectives, investment partnerships between the PRC and US film companies, and outline PRC-approved movie narratives.[49] The evolution of narratives within the *Kung Fu Panda* franchise across its three films released between 2008 and 2016 is notable. Initially, the storyline followed the protagonist, Po, on his hero's journey as he triumphed over his adversary, echoing classic Western individualistic themes. Chinese elites questioned why the film was solely an American production and invited DreamWorks staff to visit pandas in mainland China.

Subsequent sequels witnessed a shift in scenery from a blend of Japanese, Chinese, and Korean backgrounds to predominantly Chinese imagery, with Po adopting more traditional Chinese attributes. Notably, DreamWorks and China Film Production Group collaborated on *Kung Fu Panda 3*, wherein Po's success depended on countering the potent *chi* of a long-deceased villain and rallying the townspeople (the collective) to save China. The seemingly harmless collaboration aimed to eliminate unfavorable narratives and suggest pro-China alterations.

These changes, which may seem inconsequential individually, collectively established numerous anchors in narratives and images. While some may dismiss the film as mere entertainment featuring a cartoon panda, the PRC's stratagems, inducing complacency and employing *shi* (aligning all forces and deception), remain applicable. It is crucial to recognize that youths and young adults, being particularly susceptible to significant self-image influences, constitute the primary target audience for most such coproduced films.[50] Notably, *Kung Fu Panda 4* released in 2024.

[49] Morgan A. Martin and Clinton J. Williamson, *Mapping Chinese Influence in Hollywood*, Kenney Papers on Indo-Pacific Security Studies 4 (Maxwell AFB, AL: Air University Press, January 2023), 39–40, https://www.airuniversity.af.edu/.

[50] Martin and Williamson, *Mapping Chinese Influence in Hollywood*, 26, 81.

The Guest Becomes the Owner[51]

Smart devices have expanded users' access to the world and vice versa. However, this interconnectedness has also led to information overload, creating ripe opportunities for exploitation. Users often find themselves inundated with torrents of information, compelling them to rely on biases, analogies, and emotions when making decision, and rendering them more susceptible to influence.[52] In the emerging "attention economy," truth takes a backseat to capturing interest.[53] Algorithms meticulously curate personalized feeds, frequently featuring emotionally charged content that amplifies the NIRV effects. Despite the dubious reliability of social media, these platforms continue to rank among the top sources of news for many individuals.[54]

The popularity of social media can largely be attributed to its personalized nature. Users either select interest groups themselves or have them suggested based on algorithms that gather demographic data to construct tailored interest ecosystems.[55]

The PRC employs over one million individuals in the online censorship sector, while more than 730,000 American computers have been compromised, allowing PRC hackers to transform them into "slaves."[56] PRC operatives engage in trolling, amplification, and dissemination of discord and disinformation across social platforms to achieve strategic objectives.[57] For instance, the PRC-based information operations group Empire Dragon targeted American and Taiwanese populations with more than 1,800 posts disparaging democratic elections, democracy itself, House Speaker Nancy Pelosi, her family, and Taiwanese President Tsai Ing-wen during Pelosi's visit to Taiwan in 2022.[58]

ByteDance, the parent company of *TikTok*, is owned by the PRC, exerting significant influence over Chinese domestic opinion and conducting surveillance on citizens through a suite of mobile entertainment and e-commerce applications.[59] Despite being perceived as innocuous entertainment, *TikTok* boasts 150 million

---

[51] Proverb from the Thirty-Six Stratagems, as quoted by Pillsbury, *The Hundred-Year Marathon*, 177.

[52] W.R. Proctor and T. Van Zandt, "Attention and the Assessment of Mental Workload," in *Human Factors in Simple and Complex Systems*, 3rd ed. (Boca Raton, FL: CRC Press, 2008).

[53] Singer and Brooker, *LikeWar*, 21–23.

[54] Ullich K.H. Ecker et al., "The Psychological Drivers of Misinformation Belief and Its Resistance to Correction," *Nature Reviews Psychology* 1 (January 2022), 16–18, https://www.nature.com/.

[55] Luke Moulton, "The Facebook Ads Targeting List: Interest, Demographics & Behaviours," *LeadSync* (blog), 8 August 2021, https://leadsync.me/.

[56] Pillsbury, *The Hundred-Year Marathon*, 149–50.

[57] Timothy Snyder, *The Road to Unfreedom: Russia, Europe, America* (New York: Crown, 2018).

[58] Insikt Group, *Empire Dragon*. Empire Dragon is "a coordinated inauthentic network with exhaustive breadth in its social media presences" with content "on over 180 platforms, blogs, forums, and websites in over 20 languages," 3.

[59] Jones et al., "Competing Without Fighting," 72.

monthly active users in the United States alone, contributing to its estimated global user base of 1.218 billion individuals, which accounts for approximately 25 percent of social media users worldwide—these figures only consider users aged 18 and above.[60] However, beneath *TikTok*'s façade of ostensibly harmless amusement lies an intelligence apparatus that systematically collects, analyzes, and furnishes copious amounts of data to the CCP. Beijing actively monitors, censors—referred to as *harmonizing* by the CCP—and exploits this data to serve its strategic interests.[61]

China's domestic counterpart to *TikTok*, *Douyin*, bears a striking resemblance in appearance but operates under a vastly different framework. On *Douyin*, user-generated content takes a backseat, replaced instead by the dissemination of science, technology, engineering, and mathematics (STEM) and other educational videos, carefully crafted to propagate approved narratives and educate China's populace. The stark contrast between ByteDance's domestic and international platforms speaks volumes about the company's objectives. Equally telling is the genesis of *TikTok*.

In 2017, ByteDance made headlines with its acquisition of *Musical.ly*, a US-owned karaoke application centered on user-generated content, for a staggering USD 1 billion. By merging the data-collection infrastructure of *Musical.ly* with that of *Douyin*, ByteDance birthed *TikTok*.[62]

In 2022, the US Department of Defense passed the No TikTok on Government Devices Act, two years after it was initially proposed by then-President Donald Trump.[63] While the bill provides scant context for the ban, media coverage highlighted *TikTok*'s use of location tracking and data collection, particularly against *Forbes* journalists probing the app's ties to the PRC.[64] Notably, a recent poll revealed that 32 percent of individuals aged 18-29 in the United States regularly consume "news" from *TikTok* (see fig. 3).[65] Additionally, ByteDance owns *Jinri Toutiao*, an exclusively domestic news application that delivers curated news content to Chinese citizens.[66] With ByteDance controlling the algorithms that govern content cura-

[60] Brian Dean, "Tik Tok Statistics You Need to Know in 2024," *Back Linko*, 12 December 2023, https://backlinko.com/.

[61] Singer and Brooker, *LikeWar*.

[62] Lin Pellaeon, "TikTok Vs Douyin: A Security and Privacy Analysis," *Citizen Lab*, 22 March 2021, https://citizenlab.ca/.

[63] "No TikTok on Government Devices Act," S.1143, 117th Cong. (2022), https://www.congress.gov/.

[64] Emily Baker-White, "Exclusive: TikTok Spied on Forbes Journalists," *Forbes*, 22 December 2022, https://www.forbes.com/.

[65] "The Rise of the TikTok News Anchor," *The Economist*, 25 January 2024, https://www.economist.com/.

[66] ChatGPT, "Response to 'What Services Do the Other Companies ByteDance Owns Provide?'," conversation with the authors, 6 February 2024, https://chat.openai.com.

tion for millions of Americans (see fig. 4), concerns about information manipulation and censorship loom large.

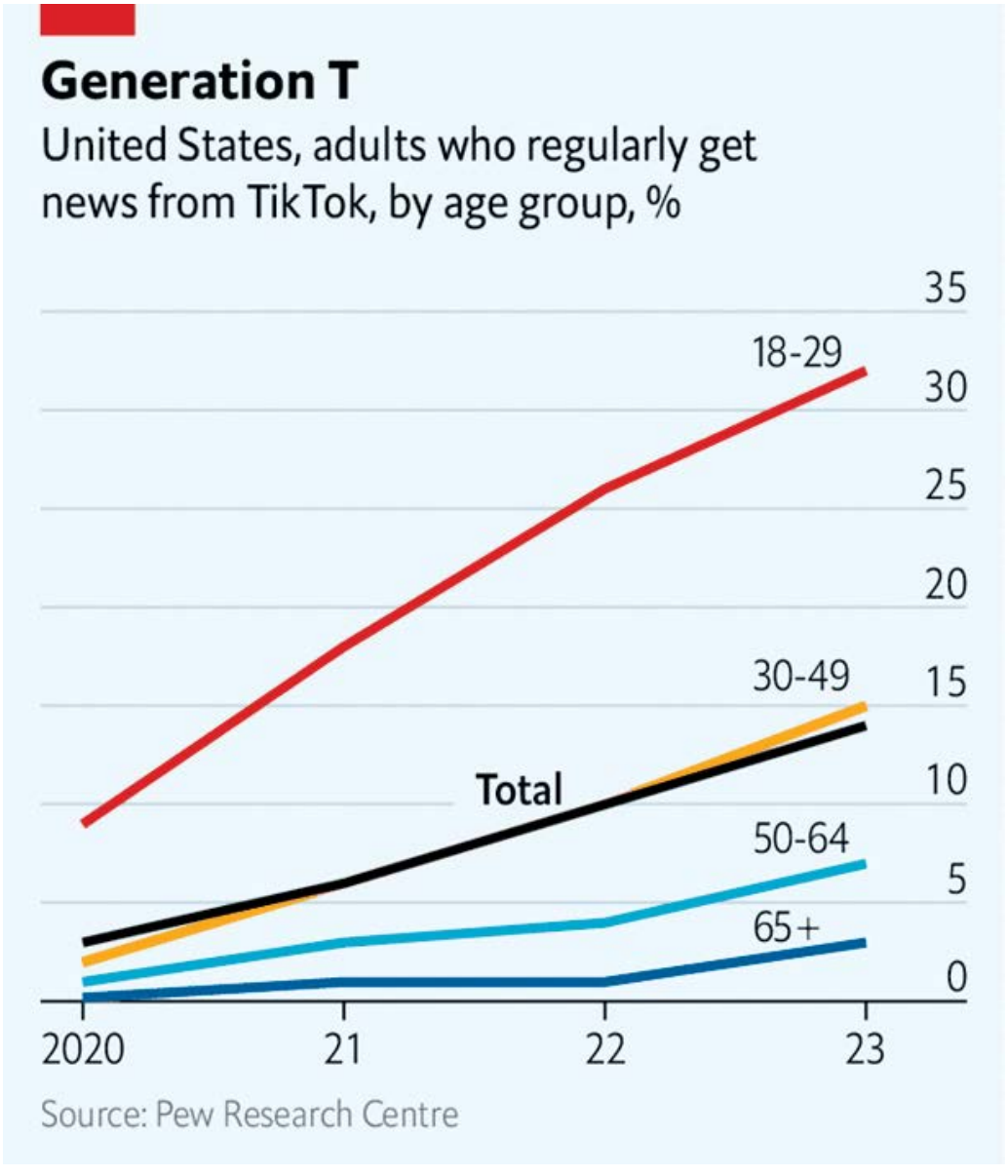

Figure 3. US consumption of TikTok "news." (Source: Pew Research Center)

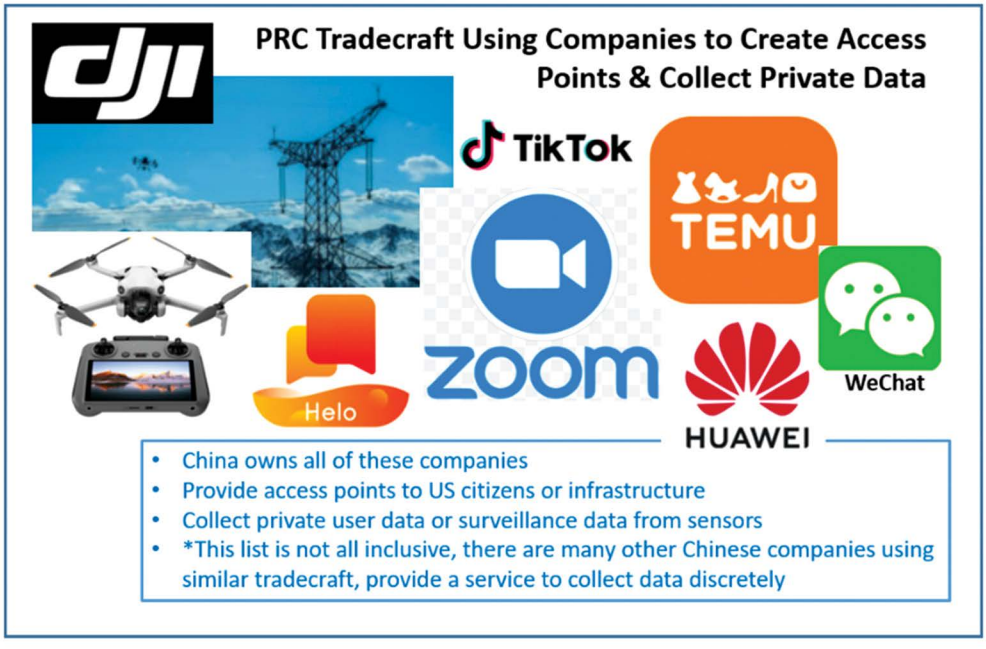

Figure 4. PRC tradecraft using companies to create access points and collect private data

Two discernible themes surface from the analysis of access points. Firstly, the PRC strategically establishes footholds within the US system, cultivates dependencies on funding, and fosters habitual relationships. Democratic institutions and free-market societies often prioritize short-term gains and only later realize they have become ensnared in a far-reaching strategic web.[67] Secondly, the CCP adeptly conceals nefarious intentions within seemingly innocuous and enticing ventures.[68] Indeed, we find ourselves embroiled in a broader geopolitical contest.

[67] Robert Spalding, *Stealth War: How China Took Over While America's Elite Slept*, 9th ed. (Seoul: Penguin Random House LLC, 2019). 27, 45.

[68] Pillsbury, *The Hundred-Year Marathon*, 45. Pillsbury correlates this strategy to the Chinese game of Wei qi, or "encirclement board," where players win by deceiving opponents into complacency.

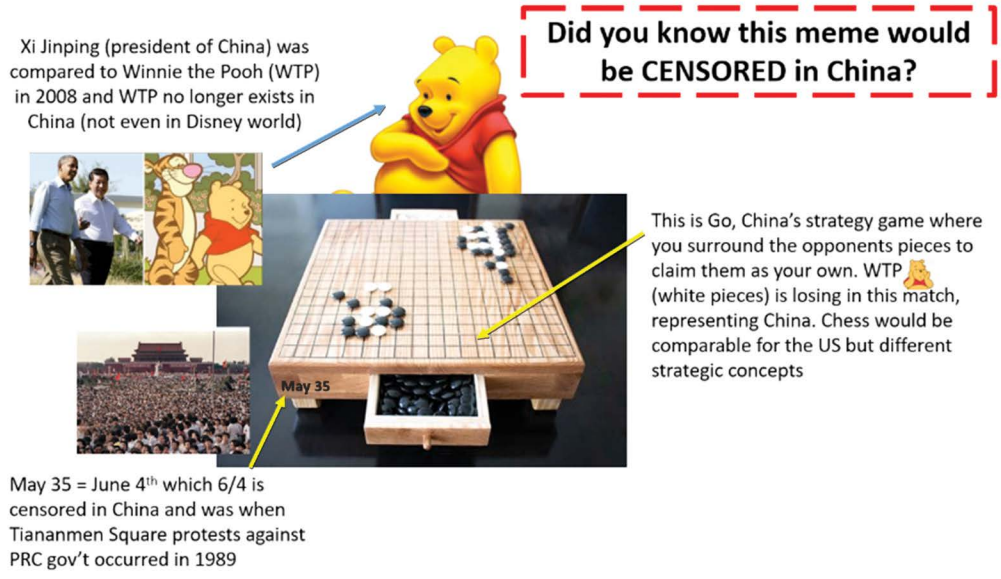

Figure 5. The new "Great Game"

Recommendations

At the national level, it is crucial to increase public awareness regarding the national security threat posed by products and services originating from the PRC. National leaders should actively disseminate the PRC's openly shared strategies concerning lawfare, media warfare, and psychological warfare to ensure a comprehensive understanding of the challenges faced.[69] Moreover, following the US Congress's passage of legislation banning *TikTok* from government devices, a national statement should have been issued to elucidate the reasons behind this decision and to empower citizens to take proactive measures to raise awareness and safeguard freedoms.

Additionally, there is a pressing need to address the significant gap between existing US data privacy legislation and the evolving threats to citizens' data security and exposure to manipulative narratives. Enhancing data privacy laws to provide more comprehensive coverage, particularly concerning metadata collection, is essential. Drawing insights from the European Union's General Data Protection

[69] Singer and Brooker, *LikeWar*. 86.

Regulation (GDPR), implemented in 2018, could inform potential US policies in this regard.[70]

Weather forecasts serve as valuable tools, prompting individuals to take precautionary measures regardless of the forecast's accuracy. Similarly, forecasting heightened adversarial information campaigns could effectively alert populations to anticipated adversarial narratives correlated with specific platforms and time horizons. By delivering forecasts akin to the air quality index, awareness of information operations could be raised, identifying groups most likely to be targeted and offering recommendations for media consumption practices (see table 1). One potential name for such an index could be the *Adversarial Influence Index* (AI2).

Table 1. Air Quality Index basics for ozone and particle pollution. (Source: "Air Quality Index (AQI) Basics," AirNow, n.d., https://www.airnow.gov/.)

Daily AQI Color	Levels of Concern	Values of Index	Description of Air Quality
Green	Good	0 to 50	Air quality is satisfactory, and air pollution poses little or no risk.
Yellow	Moderate	51 to 100	Air quality is acceptable. However, there may be a risk for some people, particularly those who are unusually sensitive to air pollution.
Orange	Unhealthy for Sensitive Groups	101 to 150	Members of sensitive groups may experience health effects. The general public is less likely to be affected.
Red	Unhealthy	151 to 200	Some members of the general public may experience health effects; members of sensitive groups may experience more serious health effects.
Purple	Very Unhealthy	201 to 300	Health alert: The risk of health effects is increased for everyone.
Maroon	Hazardous	301 and higher	Health warning of emergency conditions: everyone is more likely to be affected.

In 2024, major elections are taking place around the world, including the United States, with those in Russia and Taiwan already having taken place. Despite the conclusion of the latter two elections, the need for tailored forecasts remains relevant as future elections approach. These forecasts could be customized for specific regions, communities, and interest groups. Social media companies could play a significant role in generating these predictions through trend analysis. Subsequently, a separate entity could analyze trends across platforms to identify information operations campaigns and provide forecasts accordingly. It is worth noting that

[70] Pellaeon, "TikTok Vs Douyin."

this proposed model diverges from the existing information operations condition (INFOCON) threat level system, which primarily concentrates on providing system status updates for computer network attack defense.[71]

At the personal level, social media inundates users with vast amounts of information, often devoid of context, thereby providing adversaries with opportunities to sow and exploit internal divisions.[72] Individuals struggle to adequately process the sheer volume of media content. Compounding this challenge, social media platforms were intentionally crafted based on principles of social engineering and influence. The chart presented below illustrates the correlation between some of Robert Cialdini's seven foundational influence principles and common social media practices (see table 2).[73]

Table 2. Cialdini's seven foundational principles and common social media practices. (Source: Created using Robert Cialdini, Influence: The Psychology of Persuasion, 2nd ed. [Needham Heights, MA: Allyn and Bacon, 2001], 2–17).

Influence Principle	Definition	Media Feature Examples
Consistency	Making something familiar through repetition generates belief	Algorithm curated content generating echo chambers, auto-play based on previous video
Social Proof	Behavior is deemed correct in a given situation if we see other performing it (i.e., laughter tracks in 1990s sitcoms)	Like buttons, sharing, demonstrating behavior on video, number of views counter
Liking	People prefer to say yes to individuals they know, share similarities with, and like	Interest groups, like buttons, connection recommendations
Scarcity	Opportunities seen as more valuable when they are less available	Number of views counter, endless scrolling, 24/7 news cycle
Automaticity	Avalanche of information and choice (cognitive overload) require shortcuts to function in the modern world	Endless scrolling, billions of content generators, "short" format videos

Platforms strategically optimize design features, such as delaying the release of "likes" until a specific time, to trigger fixed-action subconscious responses. These features provide users with a series of calculated dopamine hits—a neurotransmitter associated with instant gratification.[74] Additionally, applications capitalize on

[71] "Information Operations Condition (INFOCON)," *Public Intelligence*, 25 June 2009, https://publicintelligence.net/.

[72] Jones et al., "Competing Without Fighting," 34.

[73] Robert Cialdini, *Influence: The Psychology of Persuasion*, 2nd ed. (Needham Heights, MA: Allyn and Bacon, 2001), 2–17.

[74] Robert Lustig, *The Hacking of the American Mind: The Science Behind the Corporate Takeover of Our Bodies and Brains*, 1st ed. (New York: Avery, 2018), 15–18.

the four stages of the habit development cycle: cue, craving, response, and reward.[75] This cycle habituates users toward behaviors that are favorable to platform providers. *You are being targeted anytime you use social media.* Designed to exploit cognitive vulnerabilities, social media is optimized for political warfare.

How to recognize if you are being targeted with disinformation? One key indicator is the emotional response elicited by the content. If a piece of content triggers a strong emotional reaction, individuals should pause and question the credibility of the content or evaluate their own response. Developing emotional intelligence (EQ) skills can enhance self-awareness, self-management, social awareness, and relationship management. By improving EQ, individuals can become more attuned to their social media habits and better regulate their responses to various types of content.[76] This heightened self-awareness facilitates improved self-management, which in turn can lead to reduced consumption of disinformation and significantly limit adversarial access.

In addition to EQ, critical thinking skills are indispensable for navigating the cognitive battlespace. Critical thinking enables users to identify logical fallacies, recognize biases (including their own), and seek out additional sources of information for verification. Digital literacy education is also crucial, as it empowers users to recognize and resist addictive design features (such as infinite scroll) and avoid harmful content. Democracies should prioritize the normalization of digital literacy as part of their K–12 curricula to ensure citizens are equipped to navigate the complexities of the digital landscape. Organizations like NATO's Strategic Communication Center of Excellence and Taiwan's counterinfluence strategy offer valuable reports and initiatives to aid in this endeavor.[77]

EQ, complemented with critical thinking and digital literacy skills, forms an indispensable toolkit for combating adversarial narratives. This multifaceted approach harnesses the adaptive and innovative potential of a democracy's diverse population, thereby capitalizing on one of its greatest strengths.

---

[75] James Clear, *Atomic Habits: Tiny Changes, Remarkable Results* (New York: Avery, 2018),15.

[76] Travis Bradberry, *Emotional Intelligence 2.0* (San Diego: TalentSmart, 2009), 23–27.

[77] James Pamment and Sara Sörensen, *Operationalising the Framework for Evaluating Capability Against Information Influence Operations: A Case Study of the Psychological Defence Agency's Courses* (Riga, Latvia: NATO STRATCOM, 16 January 2024), https://stratcomcoe.org/. For Taiwan's counterinfluence strategy, see, Ko, "Taiwan on the Frontline," 3–5.

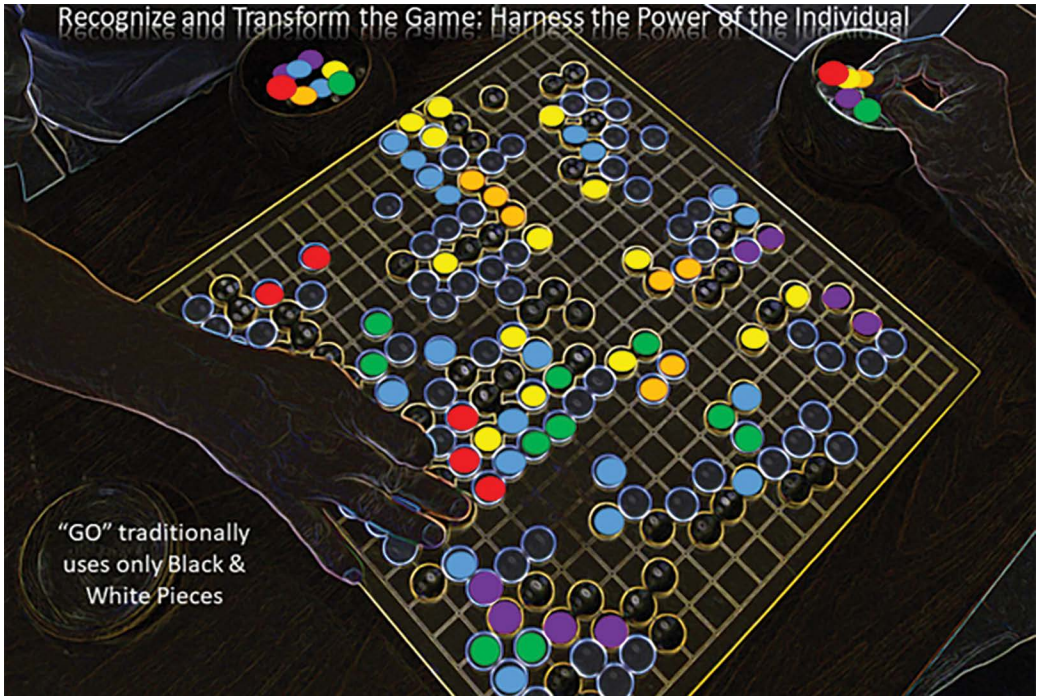

Figure 6. Democracy's version of Go. (Source: Authors' creation.)

Conclusion

The evolution of conflict demands that nations expand their focus beyond traditional military domains to safeguard their homelands. This article has provided a glimpse into essential concepts necessary for dissecting the security challenges presented by contemporary socio-technical systems. Key themes explored include political warfare, cognitive warfare, PRC anchoring narratives and stratagems, COGSEC, the image, US historical blind spots, and the NIRV acronym. Through case study analysis, we have observed the patterns of CCP access and data collection techniques aimed at propagating PRC narratives, underscoring how such access grants Beijing strategic footholds within the gates of democracy.

It is imperative for free nations to unite and implement strategies that bolster COGSEC at the national, communal, and personal levels. By safeguarding democracy's foundational image, enshrined in documents like the American Constitution and exemplified by the values upheld by democratic nations worldwide, we can fortify against external threats. As Pillsbury astutely observes, military confrontation represents only the culmination of a broader narrative. Today's

competition unfolds predominantly in the information environment—a story still in the making, where democracies undoubtedly wield significant influence. As we navigate this evolving landscape, it is clear that democracies not only have a stake but also possess the agency to shape the course of events to come.[78] ✪

Col Dr. William "Ox" Hersch, USAF, Retired

Dr. Hersch is a graduate of the School of Advanced Air and Space Studies and holds a doctorate in military strategy. He is a retired Air Force colonel and B-1 instructor weapon system officer, a veteran of Operation Enduring Freedom and Operation Iraqi Freedom, and a political-military affairs specialist. Currently, he serves as an Assistant Professor in the Department of Military and Strategic Studies, US Air Force Academy, Colorado Springs, Colorado.

Lt Col Melissa "Sharpie" McLain, USAF

Lieutenant Colonel McLain is an Institute for Future Conflict Fellow and will go on to complete her doctorate in human-agent teaming in the summer of 2024. She is a career intelligence officer with a background in B-1B missions, SIGINT analysis, and emerging technology forecasting. Currently, Sharpie serves as an instructor in the Department of Military and Strategic Studies, US Air Force Academy, Colorado Springs, Colorado.

[78] Pillsbury, *The Hundred-Year Marathon*, 195.