GEOPOLITICS AND INTERNATIONAL SECURITY PROGRAM JAN 2026

BEYOND THE KINETIC

Deconstructing Warfare in the Socio-Technical-Cognitive Battlespace

Lt Gen D S Hooda (retd)
Lt Col Pavithran Rajan (retd)

CSDR
COUNCIL FOR STRATEGIC AND DEFENSE RESEARCH

Recommended citation:
Hooda, D S, and Pavithran Rajan (2026). Beyond the Kinetic: Deconstructing Warfare in the Socio-Technical-Cognitive Battlespace. New Delhi: Council for Strategic and Defense Research.

The Council for Strategic and Defense Research (CSDR) does not take institutional positions on any issue.

C-21, 3rd Floor, Qutub Institutional Area, New Delhi, India - 110016.
Phone: 011-43104566 | Email: office@csdronline.com | Web: www.csdronline.com | Twitter:@CSDR_India

ABOUT THIS REPORT

Modern warfare is undergoing metamorphic changes. One such transition is the move beyond the kinetic-centric battlefield to a more integrated Socio-Technical-Cognitive Battlespace (STCB). This report introduces the STCB as a comprehensive framework that can help explain and prepare for the intricate, recursive, and interconnected nature of the social, technological, and cognitive domains in contemporary conflict.

As evident from the ongoing Russia-Ukraine war, this emergent battlespace is not merely an adjunct to traditional military operations but is increasingly the decisive theatre where strategic outcomes are determined. The report explores the complexities inherent in modern operations, where perceived success and strategic victory are increasingly disentangled from purely kinetic achievements. The central argument the authors posit is that ascendancy and strategic advantage in the 21st century hinge not on mere possession of military might, but on adept navigation, influence, and, ultimately, mastery of the STCB's intricate, interwoven layers.

The report also identifies shortcomings of conventional strategic doctrines, including Multi-Domain Operations (MDO), Hybrid Warfare, and China's "Three Warfares," arguing that, while valuable, they fail to encapsulate the fused, holistic essence of the STCB fully. Furthermore, it delves into the ethical questions raised by STCB warfare, particularly the systemic challenges of mass manipulation, algorithmic disinformation, exploitation of cognitive biases, and the erosion of the distinction between combatants and non-combatants.

Finally, the report outlines future trends, highlighting the transformative role of artificial intelligence (AI), weaponization of social media ecosystems, potential for large-scale, automated cognitive manipulation, and the speculative horizon of neuro-warfare. The authors offer actionable policy recommendations for governments, international organisations, and civil society to navigate and mitigate the risks of the new battlespace.

ABOUT CSDR'S GEOPOLITICS AND INTERNATIONAL SECURITY PROGRAM

The Geopolitics and International Security Program explores and analyzes India's foreign policy decisions by conducting in-depth research and analysis. The program monitors India's engagement with a rising China and the evolving dynamics in regions like the Himalayas and South Asia. It also studies the complex geopolitics involving great powers and its impact on India's strategic interests.

ABOUT COUNCIL FOR STRATEGIC AND DEFENSE RESEARCH

Founded in January 2020 by Lt. Gen. D.S. Hooda (Retd.) and Dr. Happymon Jacob, CSDR is an innovative think tank and consultancy specializing in foreign policy, geopolitical risk, connectivity, and critical areas of defense and aerospace. With a focus on the Indian subcontinent, Eurasia, and the Indo-Pacific, CSDR is committed to generating strategic insights that drive meaningful change. Read more at www.csdronline.com

AUTHOR

Lt Gen D S Hooda (retd) - Co-Founder, CSDR
Lt Col Pavithran Rajan (retd) - Advisor, Centre for National Security Studies, Ramaiah University of Applied Sciences

RESEARCH SUPPORT

Hely Desai - Research Associate, CSDR
Gaurav Saini - Cofounder, CSDR

Introduction

On February 24, 2022, as Russian warships approached Snake Island, Ukrainian border guards received a radio demand to surrender.[2] Their response—"Russian warship, go fuck yourself"—became instantly viral, generating 3.2 million Twitter mentions within 48 hours and spawning commemorative stamps, songs, and street art across allied nations.[3] This phrase accomplished what traditional military press releases could not: it crystallized Ukrainian defiance, humanized the defenders, and created a moral narrative that shaped Western aid decisions worth billions. Notably, the guards survived, were captured, and later exchanged, yet the "martyrdom" narrative's strategic effect persisted despite factual correction.[4]

Ukrainian stamp commemorating the heroes of Snake Island. Photograph: Mykhailo Polenok/Alamy

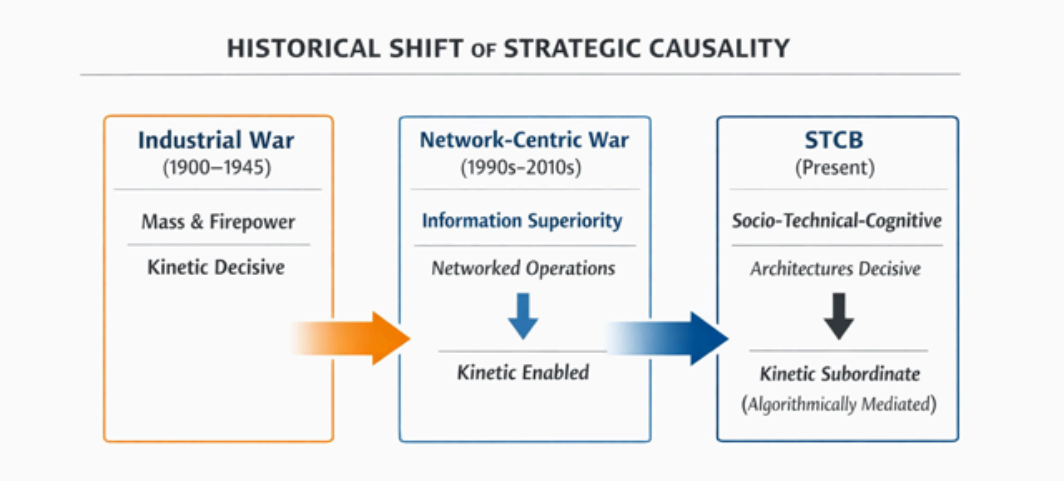
This incident encapsulates the Socio-Technical-Cognitive Battlespace: a kinetic confrontation was transformed via digital platforms into a global rallying cry that reshaped perception of Ukrainian resolve, directly influencing international assistance. The "truth" of their fate proved strategically irrelevant compared to the narrative's power. Between 2014 and 2024, documented state-sponsored disinformation campaigns increased by 750%, according to the Oxford Internet Institute's Computational Propaganda Research Project, while defense spending on cyber and information operations grew by only 43% during the same period, according to IISS Military Balance data.[5] This gap between threat expansion and defensive investment reveals a dangerous strategic blindness.

Traditional thinking about warfare has remained grounded in the physical realm—a contest of mass and energy confined to defined battlefields and timelines. Current writing on warfare's changing character emphasizes information, cyberspace, and autonomous systems, yet conventional analysis still treats hard military power as the most important variable.[6] This assumption that contemporary battlefields are restricted to geographically defined areas where kinetic exchanges occur is increasingly untenable.[7] The rapid advance of digital technologies, deeply ingrained in modern life, is having a decisive effect on the conduct of warfare. Interactions across social, technical, and cognitive domains, mediated by an algorithmic substrate—the underlying layer of codes, data, and platform governance that selects, ranks, routes, and optimizes information flows—now constitute a new battlespace as consequential as any physical terrain.[8]

This Socio-Technical-Cognitive Battlespace forces fundamental reconceptualization of warfare. From the European security theater to the Middle East and South China Sea, boundaries separating war from peace have eroded as contestation extends continuously into non-kinetic domains. The distinction between combatants and non-combatants becomes increasingly difficult to sustain amid vast networks of interconnected individuals.[9] Victory no longer requires physical destruction but instead demands systematic reshaping of how adversaries perceive reality.[10] In these modern conflicts, war transcends being a violent episode occurring within societies—it becomes a persistent condition operating through society's cognitive and social structures themselves.

The STCB framework provides an analytical tool for navigating this transformed strategic environment. It moves beyond limited, siloed perspectives on "information warfare" or "cyber warfare" to offer a holistic model that recognizes that cyber-attacks are incompletely understood without examining the social vulnerabilities they exploit and the cognitive effects they are designed to produce. Strategic success and national resilience increasingly depend on the capacity to comprehend, adapt to, and leverage the intricate dynamics binding social cohesion, technical infrastructure, and cognitive influence into an integrated whole. This report deconstructs the three core domains of the STCB, analyzes their recursive interactions through detailed examination of the Russia-Ukraine War, explores doctrinal underpinnings of the framework, confronts ethical implications, addresses critiques, projects future evolution, and concludes with policy recommendations for navigating this new battlespace.

> The assumption that contemporary battlefields are restricted to geographically defined areas where kinetic exchanges occur is increasingly untenable. The rapid advance of digital technologies, deeply ingrained in modern life, is having a decisive effect on the conduct of warfare. Interactions across social, technical, and cognitive domains, mediated by an algorithmic substrate—the underlying layer of codes, data, and platform governance that selects, ranks, routes, and optimizes information flows—now constitute a new battlespace as consequential as any physical terrain.



The Socio-Technical-Cognitive Battlespace (STCB): A New Paradigm

The STCB framework assumes that modern conflict extends beyond the conventional kinetic domain. It unfolds within an interconnected, complex adaptive system where social, technological, and cognitive factors are inextricably intertwined. While the impact of these domains has been studied in the past, they have been considered only as supporting elements to the traditional physical domains of land, sea, air, and the more recent additions of space and cyber. The STCB framework places these domains at the centre of its analysis. Further, the framework does not distinguish between kinetic and non-kinetic conflicts, an analytically convenient distinction. For these reasons, a clear visualisation of the constituents of STCB and the dynamic interplay between these constituents and the kinetic element of conflict should be an essential part of strategic planning.

The Social Domain: The Foundation and Target of Conflict

In modern warfare, societies themselves have become battlefields. The social domain encompasses the deep structures that bind populations together - shared identities, trust networks, collective narratives, and the fault lines that can fracture them. Adversaries now invest equal resources in mapping social vulnerabilities as they do in traditional intelligence on military capabilities.[11] This is because the social domain is both a nation's greatest strategic asset and its most acute vulnerability. A cohesive society can absorb devastating kinetic strikes and maintain political will indefinitely, while a fractured society may collapse from within before conventional warfare begins. Therefore, understanding this domain is not supplementary to military strategy; rather, it determines whether kinetic operations will succeed or fail, whether alliances hold or fracture, and whether victory is even recognizable when achieved.

- **Cultural Narratives and Historical Memory:** These are the dominant stories, myths, and belief systems that shape a country's collective identity and understanding of the world. For instance, Russia has used narratives of historical unity with its Soviet Era geographies and grievances over NATO expansion to justify its invasion of Ukraine.[12] Similarly, the siege mentality of the Israeli society and the traumatic collective memory of the Holocaust are perhaps the biggest obstacles to a peaceful resolution of the Palestine issue.[13] These narratives tap into deep-seated elements of national identity.

- **Social Networks and Trust:** This subcomponent encompasses the intricate web of relationships between individuals and groups, existing both online and offline. The theory of "strength of weak ties" advocated by sociologist Mark Granovetter explains how information, as well as disinformation, can rapidly bridge disparate clusters within a society.[14] Social media platforms have weaponised this dynamic, becoming critical conduits for the viral spread of content. The level of social trust, both interpersonal and institutional, is a key indicator of a society's resilience to manipulative campaigns.

- **Public Opinion and Political Will:** This refers to the collective attitudes and beliefs held by a population regarding specific issues, which directly influence political decision-making and a nation's ability to sustain a conflict. The shaping of public opinion through both overt and covert means is a primary objective of the STCB. It is the modern strategic objective analogous to breaking an army's morale in traditional warfare.

- **Identity, Group Dynamics, and Societal Fault Lines:** Drawing on Henri Tajfel and John Turner's Social Identity Theory (1979), this element focuses on the profound sense of belonging and shared identity that binds individuals within groups and influences their behaviour and attitudes.[15] STCB operations aim to exploit pre-existing societal fault lines, divisions based on ethnicity, religion, language, class, or political affiliation. By amplifying grievances and creating "in-group" vs. "out-group" dynamics, an adversary can fray a nation's social fabric from within, inducing paralysis or civil strife.[16]

- **Governance and Institutional Legitimacy:** The perceived effectiveness and legitimacy of governmental and social institutions profoundly influence social stability and resilience. A population that harbours a high degree of trust in its government, judiciary, and media is demonstrably more resistant to disinformation and conspiracy theories.[17] Conversely, eroding this trust is a key objective for an attacker.

Exploiting Social Vulnerabilities: Russia's Operations in Ukraine

This billboard in occupied Ukraine reads: "Russians and Ukrainians are one people, one whole". Source: BBC

Russian information operations in Ukraine exploited genuine demographic and cultural divisions, though their effectiveness varied significantly by region and time period.[18] According to Ukraine's 2001 census, Crimea's population was approximately 58% ethnically Russian, 24% Ukrainian, and 12% Crimean Tatar, with Russian as the predominant language.[19] During Russia's 2014 military intervention in Crimea, a referendum conducted under occupation reported overwhelming support for annexation, though this vote was conducted without international observers and was not recognized as legitimate by the United Nations or most Western governments.[20] The peninsula's ethnic composition and historical ties to Russia provided fertile ground for Russian narratives that emphasized protecting Russian-speaking populations.[21]

However, when Russian forces entered Kharkiv oblast in 2022,[22] similar tactics failed despite the region's significant Russian-language use. While Kharkiv city had a substantial Russian-speaking population,[23] the eight years following the 2014 Donbas conflict had fundamentally shifted Ukrainian national identity.[24] Multiple polling organizations, including the Kyiv International Institute of Sociology and Rating Group Ukraine, documented dramatic increases in Ukrainian national identification across all regions between 2014 and 2022, including in traditionally Russian-speaking areas.[25] This consolidation of Ukrainian identity proved more decisive than linguistic or historical factors, demonstrating that the social domain is dynamic rather than static—shaped by events rather than predetermined by demographics alone.[26]

The Technical Domain: The Enabler and the Weapon

The technical domain encompasses the full spectrum of technological systems that enable modern conflict, from cyber capabilities and artificial intelligence to data analytics and communication networks. This domain includes not only digital infrastructure but also the software and network dependencies that underpin contemporary weapon systems. Even kinetic military hardware now falls partially within the technical domain, as modern missiles, drones, and command systems rely on software, GPS, and network integration to operate. Beyond purely military applications, the technical domain includes the information infrastructure on which societies depend, such as internet platforms, communication networks, cloud services, and the algorithms that govern information flow. These systems both enable military operations and serve as vectors for influencing populations, making them dual-use assets in the socio-technical-cognitive battlespace. Key subcomponents include:

- **Cyber and Electromagnetic Capabilities:** This includes the full spectrum of offensive and defensive cyber operations targeting enemy infrastructure, communication networks, and critical information systems.[27] It extends beyond traditional hacking to include manipulating the electromagnetic spectrum, such as jamming signals, spoofing GPS, and disrupting the flow of data that underpins modern military and civilian life.

- **Artificial Intelligence (AI) and Machine Learning (ML):** The application of AI is revolutionising the STCB. This includes the weaponisation of AI-generated content (deepfakes, synthetic text) for disinformation campaigns,[28] the use of ML for micro-targeting populations with tailored messaging,[29] and the deployment of AI in autonomous weapons systems.[30] AI can both enhance decision-making and automate manipulation at an unprecedented scale.

- **Data Analytics and Big Data:** The systematic collection, sophisticated processing, and meticulous analysis of expansive datasets (Big Data) to discern patterns, identify emerging trends, and derive actionable insights is the engine of modern cognitive operations. By analysing social media trends, consumer data, and other information, actors can map a society's vulnerabilities with startling precision.[31]

- **Communication Networks and Platforms:** This refers to the physical and digital infrastructure that enables seamless communication, most notably the internet and the global social media platforms that are built upon it. These platforms are not neutral conduits. Their very design, driven by engagement-based algorithms, can be exploited to promote polarising and emotionally charged content, making them ideal vectors for cognitive attacks.

- **Surveillance, Reconnaissance, and Sensing Technologies:** This includes sensors, both military grade and wearable; imagery from surveillance cameras, unmanned aerial vehicles (drones), and satellites; and the pervasive surveillance architecture of the digital age, where online activity, financial transactions, and location traces are continuously harvested, cross-linked, and weaponised for control and coercion. In the STCB, these tools are used not only for traditional intelligence gathering but also for narrative shaping. Real-time drone footage, for example, is not just intelligence, but content to be deployed in the cognitive domain to prove a claim or evoke an emotional response.[32]

A crucial, often understated, dimension of the technical domain is the control over the platform. To truly compete and dominate in the STCB, it is not enough to merely operate on the digital platforms of the day. Strategic advantage flows from the control and ownership of the platforms themselves. Actors who are confined to creating fake accounts, deploying botnets, and disseminating propaganda within ecosystems they do not own are engaging in tactical skirmishes on a strategic terrain defined and controlled by another.[33] They are tenants in a digital world where the landlord, the platform owner, can change the rules, cut off users, alter algorithms, and control the flow of data at will. This does not mean that non-owners are completely powerless. As the Ukrainian case study will illustrate, an agile and narratively adept actor can achieve significant success by mastering the rules of an ecosystem they do not control. They do, however, remain perpetually vulnerable to the strategic choices of the platform's ultimate owner, e.g., Elon Musk's refusal to provide Starlink coverage for operations in Crimea.[34]

> A crucial, often understated, dimension of the technical domain is the control over the platform. To truly compete and dominate in the STCB, it is not enough to merely operate on the digital platforms of the day. Strategic advantage flows from the control and ownership of the platforms themselves. Actors who are confined to creating fake accounts, deploying botnets, and disseminating propaganda within ecosystems they do not own are engaging in tactical skirmishes on a strategic terrain defined and controlled by another. They are tenants in a digital world where the landlord, the platform owner, can change the rules, cut off users, alter algorithms, and control the flow of data at will.

Starlink and the Strategic Implications of Private Infrastructure Control

The deployment of SpaceX's Starlink satellite internet system in Ukraine illustrates how privately owned technical infrastructure has become strategically decisive in modern conflict.[35] Following Russia's February 2022 invasion, Ukrainian Vice Prime Minister Mykhailo Fedorov publicly requested Starlink access, and SpaceX rapidly deployed terminals to Ukraine.[36] By mid-2023, the Ukrainian military was reported to be operating tens of thousands of Starlink terminals, which provided critical battlefield connectivity for drone operations, artillery coordination, and communications when terrestrial infrastructure was damaged or destroyed by Russian strikes.[37]

However, the private ownership of this critical infrastructure introduced unprecedented strategic complications. In October 2022, Elon Musk publicly discussed the financial burden of providing free service to Ukraine and suggested potential service limitations, sparking immediate international controversy before reversing course.[38] More significantly, Musk denied Starlink access for a planned Ukraine attack in Crimea.[39] While Musk and SpaceX later clarified that the service had never been activated over Crimea rather than being "turned off," the incident exposed how individual decisions by a private citizen could directly constrain military operations.[40]

These events demonstrated that in the socio-technical-cognitive battlespace, control over communication platforms creates decision leverage that operates outside traditional alliance structures and military chains of command. Ukrainian forces became dependent on infrastructure whose availability could be influenced by one individual's risk calculations, financial considerations, or geopolitical assessments. This dependency introduced strategic uncertainty into Ukrainian operational planning and revealed a fundamental tension in modern warfare: the most critical technical infrastructure enabling military operations may be privately owned and governed by corporate rather than state logic, creating vulnerabilities that have no clear precedent in international law or military doctrine.

The Cognitive Domain: The Ultimate Nerve Centre

This domain is the centre of gravity in 21st-century warfare. It focuses on the intricate mental processes of both individuals and groups, encompassing perception, belief, decision-making, and meaning construction. The Cognitive domain includes the mechanisms and tools that alter attention, meaning, belief, and decision, transforming social baselines into altered behaviour. It acknowledges the fundamental reality that conflicts are ultimately won or lost in people's minds. Shaping their perceptions, influencing their beliefs, and carefully guiding their decision-making processes are pivotal to achieving overarching strategic objectives. As NATO-affiliated experts have starkly put it, "the objective is to attack, exploit, degrade or even destroy how someone builds their own reality".[46] The aim is not merely to alter what people think, but to fundamentally reshape how they think, reason, and act. Key subcomponents and mechanisms include:

- **Perception and Meaning Management:** The art of shaping perceptions among targeted audiences to influence their attitudes, beliefs, and behaviours. It aligns events to strategic aims through framing and priming, agenda-setting, narrative substitution, and careful messenger selection. It is a continuous process of constructing a preferred reality.

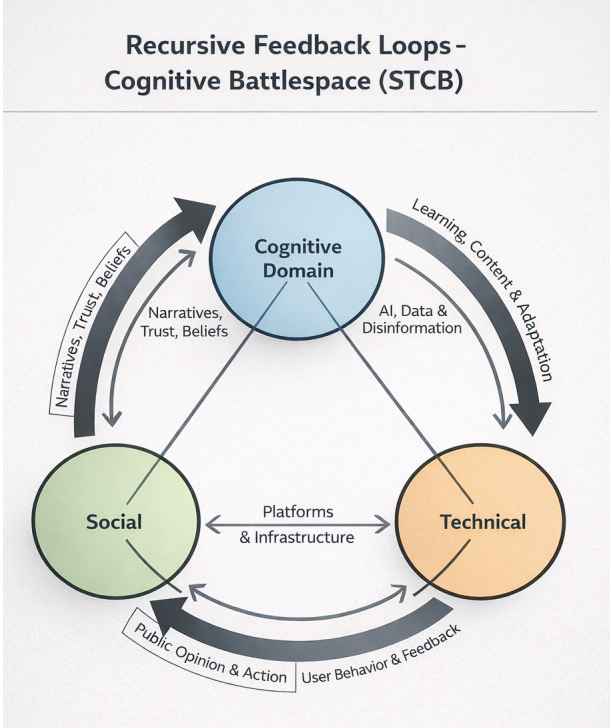
- **Targeting Cognitive Biases:** This is a sophisticated form of manipulation that weaponises the known bugs in human psychology. Drawing on the work of psychologists like Daniel Kahneman and Amos Tversky,[47]cognitive operations can be designed to exploit biases such as confirmation bias (favouring information that confirms existing beliefs), the availability heuristic (overestimating the importance of recent or dramatic information), and framing change (choices shifting if the same facts are framed as gain vs. loss).

- **Disinformation, Misinformation, and Malinformation:** While often used interchangeably, these terms have distinct meanings. Disinformation is deliberately spread false information to deceive. Misinformation is false information spread without malicious intent. Malinformation is genuine information shared out of context to cause harm. A sophisticated cognitive campaign will use all three to pollute the information environment, creating what the RAND Corporation has called "truth decay."[48]

- **The OODA Loop and Cognitive Paralysis:** A foundational concept for understanding cognitive warfare is Colonel John Boyd's OODA Loop (Observe, Orient, Decide, Act).[49] Boyd, a USAF strategist, argued that in any conflict, the side that can cycle through this decision loop faster than its opponent will gain a decisive advantage. Cognitive warfare aims to attack the adversary's OODA loop directly. By injecting disinformation and ambiguity (affecting "Observe"), exploiting cultural biases (affecting "Orient"), and inducing uncertainty (affecting "Decide"), an attacker can slow or even paralyse an opponent's decision-making process, effectively getting inside their loop.

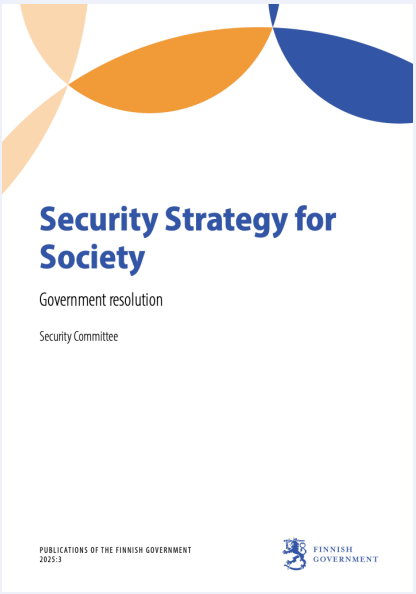
- **Psychological Operations (PSYOP):** Using the mechanisms mentioned above, PSYOPs are planned operations that convey selected information and indicators to audiences to influence their emotions, motives, and objective reasoning, ultimately affecting the behaviour of governments, organisations, groups, and individuals. Modern PSYOP is cyber-enabled, using social media and digital platforms for mass dissemination.

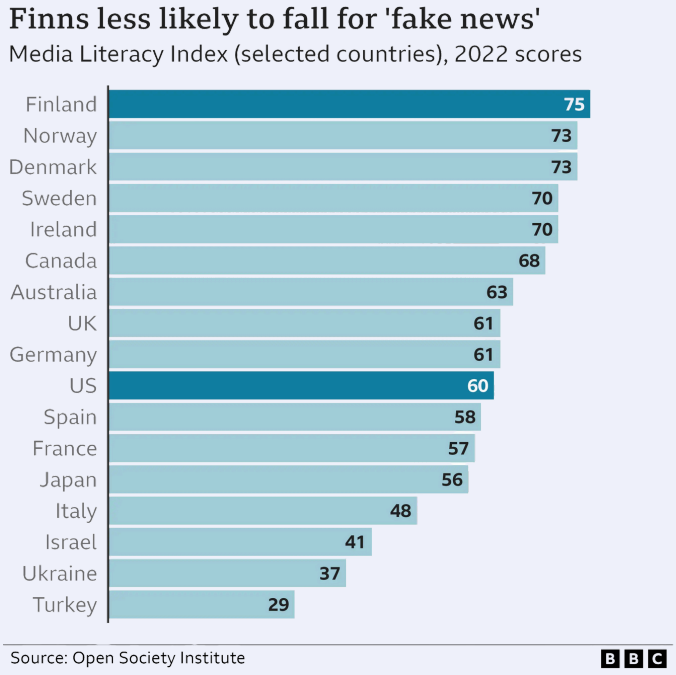
The STCB framework's true power lies in its emphasis on the recursive and dynamic interplay among these domains. Technical capabilities (platforms, data, sensing) provide reach, speed, and content; social structures (identities, networks, institutions) determine vulnerabilities and transmission paths; the cognitive domain converts both into decisions and behaviour. A successful cognitive campaign that erodes trust in a society (social) can lead to civil unrest, which could force the government to shut down social networks (technical), compounding mistrust. Effective strategies must account for these intricate, non-linear interdependencies and develop integrated approaches that address all three domains simultaneously.



Cognitive Resilience and Societal Inoculation—The Finnish Model

Finland provides a compelling case study in building structural cognitive resilience against information operations.[50] Following Russia's 2014 annexation of Crimea and documented Russian interference in European politics, Finland implemented a comprehensive national strategy recognizing that cognitive defense requires long-term societal investment rather than reactive countermeasures. The Finnish approach integrated media literacy education into the national curriculum starting in primary school, where students learn to identify manipulative techniques, verify sources, and understand how algorithms shape information exposure.[51] By 2019, according to the Open Society Institute's Media Literacy Index, Finland ranked first globally in resilience to misinformation.[52]





This educational foundation operates alongside institutional structures that reinforce cognitive resilience. Finland maintains high levels of institutional trust—Edelman's 2024 Trust Barometer ranked Finland among the top five countries for public trust in government, media, and civil society institutions, a finding that research demonstrates correlates strongly with resistance to disinformation campaigns.[53] The Finnish government's strategic communications unit, established in 2015, does not primarily focus on censorship or counter-messaging but on ensuring rapid, transparent, and consistent government communication during crises, thereby maintaining credible information channels when adversaries attempt to flood the information environment.

Finland's approach also includes regular cross-governmental exercises simulating hybrid threats, including coordinated disinformation campaigns.[54] These exercises, conducted under the "Comprehensive Security" framework, involve not only government agencies but also private-sector actors, civil society organizations, and citizens, creating a shared understanding of information threats across society. The measurable outcome of this multi-year investment emerged during the COVID-19 pandemic, when Finland experienced significantly lower rates of vaccine hesitancy and conspiracy theory adoption than most Western nations, despite being targeted by the same international disinformation networks.[55] This case demonstrates that cognitive domain defense requires treating societal resilience as strategic infrastructure—built over years through education, institutional trust-building, and practiced coordination—rather than as a tactical problem solvable through censorship or counter-propaganda alone.

The Algorithmic Substrate

Social, Technical, and Cognitive domains are not new—they have been part of warfare for centuries. The importance of morale, targeting commanders' minds, leveraging social networks, and technological advancement have consistently influenced war's outcomes.[56] However, what has fundamentally changed is the algorithmic substrate binding these domains together. This substrate—the stack of platforms, models, and control policies that determine who sees what, when, and with what credibility—now serves as a conductor, amplifier, and gatekeeper, setting the speed, reach, and trust of information flows across the STCB.

Unlike earlier information environments where human editors created and filtered narratives, today's social reality is increasingly curated by algorithms embedded in recommendation systems, search engines, and large language models.[57] These systems are not passive conduits but active shapers of perception. They amplify emotionally charged content, reward polarization, and prioritize engagement over truth. The very architecture of digital platforms structures control over what populations see, believe, and act upon. Cognitive campaigns exploiting algorithmic mediation do not simply insert messages into information streams—they weaponize the streams themselves, steering collective attention and discourse in ways that can destabilize entire societies.

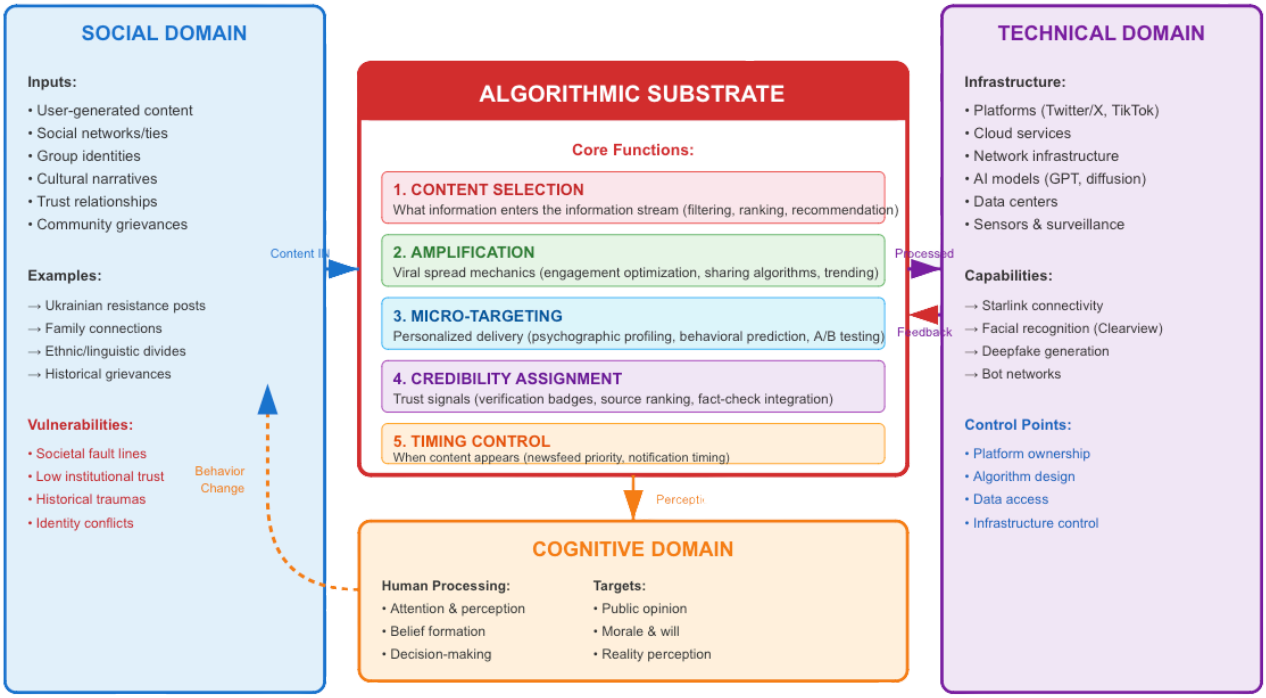
This algorithmic mediation creates new strategic imperatives around what might be called "algorithmic sovereignty." In the 21st century, a nation's strategic resilience no longer rests solely on territorial integrity or control of conventional infrastructure but increasingly on whether it controls or depends on foreign-owned digital platforms and algorithmic systems.[58] States relying on adversary-controlled or foreign-owned algorithms for critical social communication, information flows, or national security operations effectively cede elements of sovereignty.[59] The digital landlord, whether corporation or state, can recalibrate algorithms, suppress narratives, or deny access, thereby reshaping the battlespace without firing a shot. Algorithmic control thus emerges as the digital high ground of modern conflict, determining which actors define the rules of engagement in the STCB.

> Unlike earlier information environments where human editors created and filtered narratives, today's social reality is increasingly curated by algorithms embedded in recommendation systems, search engines, and large language models. These systems are not passive conduits but active shapers of perception. They amplify emotionally charged content, reward polarization, and prioritize engagement over truth. The very architecture of digital platforms structures control over what populations see, believe, and act upon.

The most disquieting frontier involves fully autonomous cognitive operations. The fusion of generative AI, big data analytics, and automated bot networks enables disinformation and influence campaigns operating continuously without direct human oversight.[60] AI systems identify societal vulnerabilities, generate tailored content, deploy it through synthetic agents, and iteratively refine campaigns based on real-time feedback, executing entire OODA loops at machine speed.

These autonomous operations would mark a categorical leap—adaptive and relentless influence at scale, operating in a domain where attribution is nearly impossible and escalation may unfold faster than human decision-makers can comprehend or control. This represents a battlespace in which human cognition is systematically manipulated by non-human actors, raising profound questions about meaningful human control over the conduct and escalation of warfare.[61]

The algorithmic substrate is not merely technical infrastructure supporting STCB operations—it is the STCB's nervous system, mediating every interaction among the three domains and determining whether cognitive effects amplify or dissipate, whether social movements coalesce or fragment, and whether technical capabilities translate into strategic advantage. Mastery of this substrate, through ownership, transparency requirements, or countervailing algorithmic defenses, has become as strategically essential as naval dominance was in previous eras. Nations that fail to recognize this reality will find themselves outmaneuvered by adversaries who understand that, in the 21st century, those who control the algorithms increasingly control the battlespace.

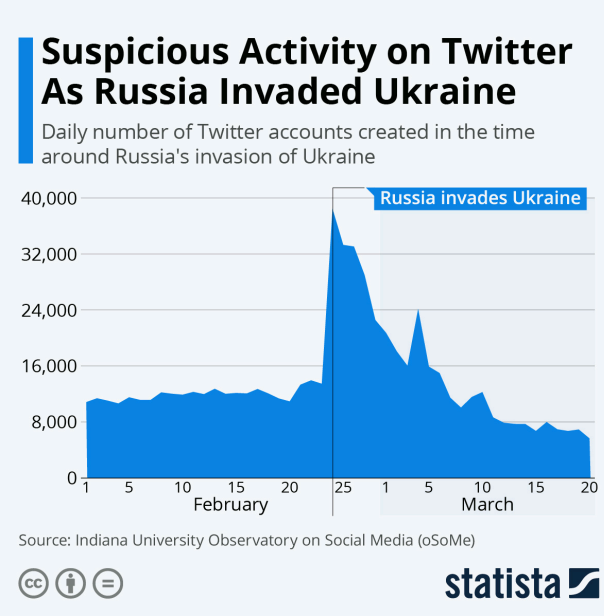


The Russia-Ukraine War: A Case Study in STCB Warfare

The 2022 Russia-Ukraine conflict provides the most compelling and contemporary illustration of the STCB in action alongside the use of force. The conflict, while brutally kinetic, was from its inception an all-encompassing war of narratives waged across digital platforms and global media.[62] While Russian armoured columns crossed the border, a parallel information war sought to justify the invasion, demoralise the Ukrainian population and military, and fracture the international coalition arrayed against it.[63] This case study dissects the STCB dynamics at play, revealing how strategic outcomes in the cognitive and social domains have, at times, been as consequential as gains on the physical battlefield.

- **Social Domain**

The 2022 kinetic invasion was not the start of the conflict, but an escalation of a long-running battle fought within the social domain. This pre-war phase was sparked by pivotal events in 2014, culminating in the Euromaidan Revolution that ousted Ukraine's democratically elected, pro-Russian president.[64] From Russia's perspective, this was an illegitimate, Western-backed "colour revolution" or coup.[65] This narrative was then relentlessly propagated to frame the new Ukrainian government as a "junta," thereby providing the justification for Russia's annexation of Crimea and its support for separatists in Donbas.[66]



Russia's strategy was heavily predicated on exploiting perceived fault lines within Ukrainian society. In the east and south—where Russian language use, Soviet-era memory, and cross-border kinship ties were strongest—parts of the population were predisposed to view Moscow favorably and Kyiv with suspicion. For years leading up to the 2022 invasion, Russian information operations had sought to amplify divisions between Russian and Ukrainian speakers, promote a narrative of a culturally and historically divided nation, and portray the post-2014 Ukrainian government as an illegitimate, "Nazi" junta oppressing a Russian-speaking minority.[67] This was a classic STCB strategy aimed at weakening the target state's social cohesion, with the hope of precipitating a political collapse that would facilitate a swift, relatively bloodless military takeover.

However, this strategy found resonance only in areas with a Russian-speaking population and was unsuccessful in areas where Ukrainian was the predominant language. Ukrainian society demonstrated profound resilience and unity. The external threat, rather than exploiting fault lines, forged a powerful, unified national identity. This process was a form of "social defence," where societal bonds and a shared sense of purpose became a strategic asset. This was bolstered by a global deluge of support orchestrated by Western media. President Volodymyr Zelensky's refusal to flee Kyiv and his constant communication with the Ukrainian people reinforced social trust and national will.[68] This demonstrates a key principle of the STCB: the social domain is not a static landscape, but a dynamic field of contention where identity and cohesion can be either destroyed or forged.

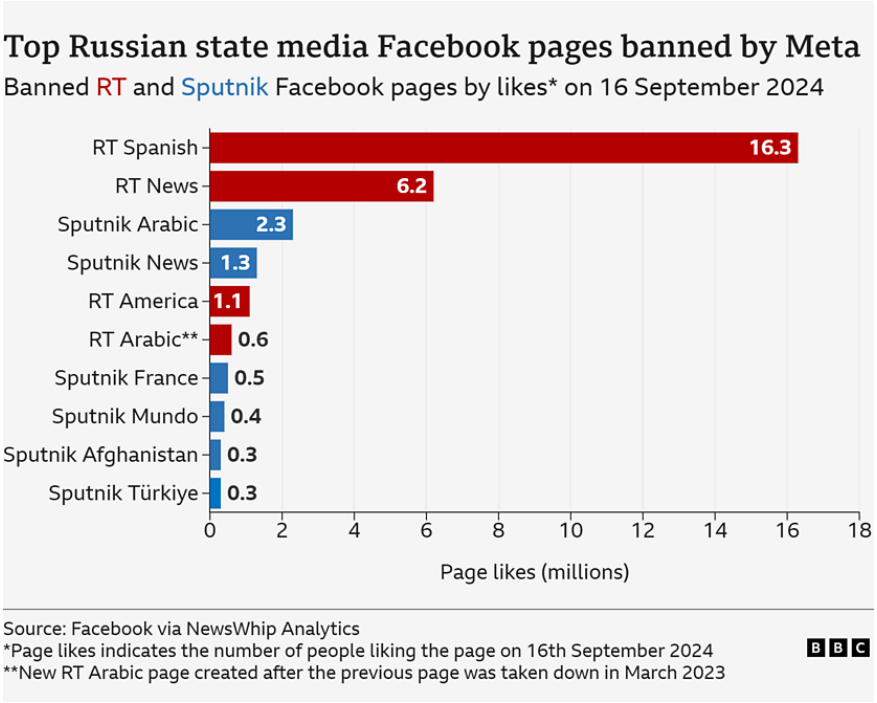
- **Technical Domain**

The war has been a showcase for the fusion of military and civilian technology. On the Russian side, the technical campaign began with cyberattacks aimed at Ukrainian government websites and critical infrastructure, intended to sow chaos and disrupt command and control. Precision-guided missiles targeted physical infrastructure, a kinetic action with direct effects in the social and cognitive domains (demoralisation and the creation of a humanitarian crisis).

On the Ukrainian side, the technical response was innovative and adaptive. The government's rapid transition of data to the cloud protected its digital infrastructure.[69] Perhaps most critically, the deployment of SpaceX's Starlink satellite internet service provided resilient communications, neutralising Russian attempts to isolate the battlefield and allowing Ukraine to maintain its connection to its own population and the outside world.[70]This single technical element had massive strategic implications in the cognitive domain, enabling Ukraine to continue its information campaign.

US companies exploited their platform control. Facebook and YouTube blocked Russian state media from their platforms, while Twitter labelled and reduced the visibility of links to Russian state media. In a temporary change to its hate speech policy, Facebook and Instagram users in some countries were allowed to call for violence and death against Russian soldiers and leaders.[71] These actions raised the cost and slowed the spread of Russian state narratives.

Furthermore, the war has seen the democratisation of Intelligence, Surveillance, and Reconnaissance (ISR). Commercial satellite imagery from companies like Maxar and Planet Labs provided open-source intelligence (OSINT) analysts and journalists with near-real-time data on Russian troop movements, effectively countering Russia's official denials and shaping the global narrative.[72] Drones became ubiquitous and were used not only for kinetic strikes but also as propaganda tools. A video of a Ukrainian drone destroying a Russian tank, set to music and shared on Telegram and Twitter, is a perfect STCB artifact: a technical system used to achieve a kinetic effect, with its output deployed as content to influence the cognitive domain.[73]



- **Cognitive Domain**

This has been the decisive domain of the conflict. Russia's primary cognitive objective was to frame the invasion as a limited "special military operation" to "denazify" Ukraine and prevent a genocide of the Russian-speaking population.[74] This narrative was aimed at multiple audiences: the domestic Russian

population to secure support for the war; the Ukrainian population to encourage capitulation; and international audiences to create ambiguity and justify the invasion.

Russia's technical apparatus, including state-controlled media such as RT and Sputnik, and vast networks of social media bots, were mobilised to push these narratives.[75] A key Russian doctrine at play here is "reflexive control," a concept from the Soviet era of conveying specific information to a target to induce a predetermined decision.[76] By framing NATO as the aggressor, Russia hoped the West would hesitate in its response.

> Russia's technical apparatus, including state-controlled media such as RT and Sputnik, and vast networks of social media bots, were mobilised to push these narratives. A key Russian doctrine at play here is "reflexive control," a concept from the Soviet era of conveying specific information to a target to induce a predetermined decision. By framing NATO as the aggressor, Russia hoped the West would hesitate in its response.

Ukraine, however, with NATO's support, mounted a masterful cognitive defence that quickly morphed into a cognitive offensive. President Zelensky, a former actor, understood the power of performance and narrative. His simple, self-shot videos from the streets of Kyiv directly countered the Russian narrative that he had fled, projecting an image of defiant leadership and courage. The Ukrainian government and its supporters crafted and disseminated a series of powerful, resonant counter-narratives:

- **David vs. Goliath**: Ukraine was framed as a small, democratic nation bravely resisting a brutal, authoritarian giant. This narrative tapped into universal archetypes and resonated powerfully with Western audiences.[77]

- **Heroic Myths**: Stories like that of the "Ghost of Kyiv" (a mythical flying ace)[78] and the defiant soldiers of Snake Island ("Russian warship, go fuck yourself") became viral symbols of Ukrainian resistance.[79]Whether factually accurate or not, it was secondary to their cognitive effect, which built morale and created a global sense of solidarity.

- **Documenting War Crimes**: Ukraine used social media to disseminate real-time evidence of alleged Russian atrocities, such as the Bucha massacre.[80] This cognitive campaign aimed to evoke moral outrage in international audiences, thereby increasing political pressure on Western governments to provide more aid.

- **Demoralising the Opposition Society**: In March 2022, Ukraine's defense ministry began using US firm Clearview's facial-recognition tool to match images of dead or captured Russian soldiers to billions of scraped photos from social networks.[81] These were then put on a website and a channel on Telegram to allow Russian citizens to find the fate of their relatives who were sent to the war.[82] The aim was to undermine support for the war among Russian citizens.

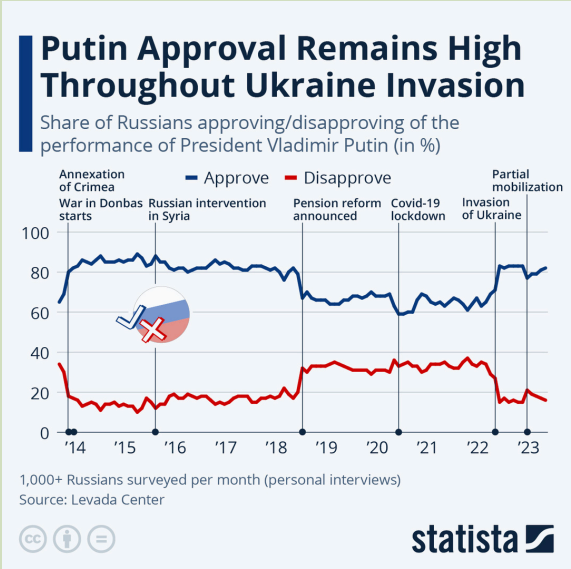
This intense clash of narratives demonstrates that in the STCB, the most resonant story often outweighs battlefield realities. Ukraine achieved narrative dominance early in the conflict, which was instrumental in galvanising unprecedented international military and financial support that has allowed it to continue its defence.

Looking from the perspective of a conventional force balance, Ukraine was expected to fold in a matter of weeks. Indeed, as a lesser military power that has lost strategic territory, Ukraine would likely have sued for peace long before now. However, its mastery of the social and cognitive domains, both within its own population and across the West, along with US and NATO support, is what continues to shore up its warfighting effort.

On 27 February, Ukraine called the "Ghost of Kyiv" an "angel" for downing 10 Russian planes. Source: BBC

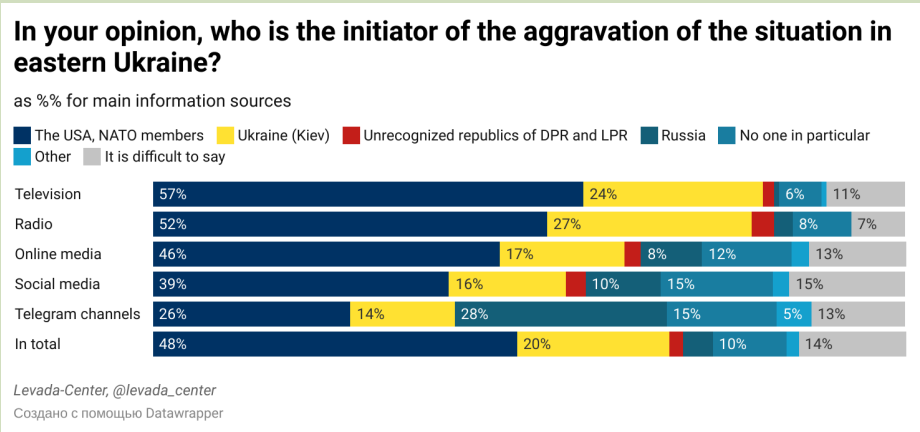
Russian Cognitive Operations: Domestic and International Successes

While Western analysis often emphasizes Ukrainian cognitive dominance during the 2022 invasion,[83] Russian information operations achieved significant success within specific audiences, particularly domestically and across parts of the Global South.[84] Within Russia, the Levada Center—an independent polling organization—consistently recorded approval ratings for the "special military operation" exceeding 70% throughout 2022 and 2023,[85] despite Russia suffering an estimated 315,000 casualties by late 2024 according to U.S. intelligence assessments.[86] This sustained domestic support occurred even as Russian forces retreated from Kyiv, abandoned Kharkiv oblast, and withdrew from Kherson city. The Kremlin's narrative framing—that Russia faced an existential struggle against NATO expansion rather than a war of territorial conquest against Ukraine—appears to have resonated sufficiently to maintain social cohesion despite mounting costs.



The "denazification" narrative, while rejected in Western media environments, gained substantial traction within Russia itself.[87] Levada polling in April 2022 indicated that 53% of Russians believed Ukraine was controlled by Nazis or fascists, rising to 62% by September 2022 despite extensive international debunking efforts. This demonstrates how information environments operate as separate ecosystems: narratives that fail completely in one context can achieve strategic effects in another, particularly when reinforced by state media monopolies and restrictions on alternative information sources.

Internationally, Russian messaging achieved partial success in fragmenting the global consensus against the invasion. United Nations General Assembly votes illustrate this erosion: the March 2022 resolution condemning Russian aggression received 141 votes in favor, with 35 abstentions and 5 against.[88] By the time of the February 2023 resolution on withdrawal, while 141 countries again voted in favor, the abstention bloc had grown more vocal, and several African and Asian nations explicitly framed their positions in terms of opposition to Western "double standards" regarding Iraq, Libya, and Palestine.[89] Russian diplomatic messaging emphasizing Western hypocrisy and framing the conflict as a proxy war found receptive audiences in regions with historical grievances against Western intervention. While this did not translate into active support for Russia, it successfully prevented the unified international isolation that Western powers sought, particularly regarding sanctions compliance and arms supply restrictions.



Ethical Considerations in STCB Warfare

The STCB framework raises profound ethical challenges, striking at the foundation of democratic values and international law. By making the human mind the central battlefield, cognitive warfare erodes traditional ethical guardrails and creates dilemmas for which existing moral frameworks offer limited guidance.

While deception has always been part of warfare, from the Trojan Horse to Operation Fortitude's phantom armies, the scale, precision, and automation of modern cognitive manipulation constitute a categorical rather than quantitative shift. Traditional military deception targeted enemy commanders' understanding of the battlefield. Contemporary cognitive warfare systematically exploits documented vulnerabilities in human psychology across entire populations using algorithmic amplification to deliver personalized manipulative content at speeds human fact-checkers cannot match. This raises fundamental questions about cognitive liberty, the right to mental self-determination that philosophers have long considered central to human dignity. When external actors can covertly shape individuals' beliefs and behaviors through techniques operating below conscious awareness, the premise of personal autonomy becomes compromised. Unlike kinetic warfare, where physical coercion is visible, cognitive manipulation operates invisibly, leaving targets unaware that their mental autonomy has been violated.

The blurring of lines between combatants and non-combatants poses equally troubling challenges. A foundational principle of Just War Theory and International Humanitarian Law is the principle of distinction, mandating that civilians be protected from direct attack. In STCB warfare, however, civilians are not collateral damage but primary terrain and target. Cognitive campaigns explicitly target civilian populations seeking to fracture social cohesion, erode institutional trust, and reshape political will. Contemporary legal frameworks designed for kinetic warfare prove inadequate to address scaled non-physical harm. When Russian information operations in Ukraine amplified ethnic divisions and historical grievances, they attacked the social fabric without firing shots in ways traditional law cannot address. When coordinated disinformation during COVID-19 undermined vaccine confidence, causing preventable deaths, the harm was real,[98] but perpetrators remained beyond existing legal mechanisms. The principle of distinction becomes conceptually incoherent when warfare's nature makes civilian minds the battlefield itself.

> A foundational principle of Just War Theory and International Humanitarian Law is the principle of distinction, mandating that civilians be protected from direct attack. In STCB warfare, however, civilians are not collateral damage but primary terrain and target. Cognitive campaigns explicitly target civilian populations seeking to fracture social cohesion, erode institutional trust, and reshape political will. Contemporary legal frameworks designed for kinetic warfare prove inadequate to address scaled non-physical harm.

Ascertaining responsibility for cognitive warfare operations presents immense challenges. The strategic use of anonymous accounts, bot networks, and proxy actors makes tracing the origins of disinformation campaigns exceedingly difficult. Russia's Internet Research Agency operated through shell companies with contractors working from home across time zones and bot networks purchased on dark web markets, creating attribution chains so complex that definitive proof meeting legal standards becomes nearly impossible.[99] The increasing use of AI compounds this complexity. When autonomous systems create harmful narratives, who bears responsibility? The AI developer, the platform hosting the content, the deploying entity, or the training data that encodes harmful patterns? When escalation operates at machine speed with AI systems iteratively refining attacks in seconds, can humans maintain meaningful control over escalation dynamics?

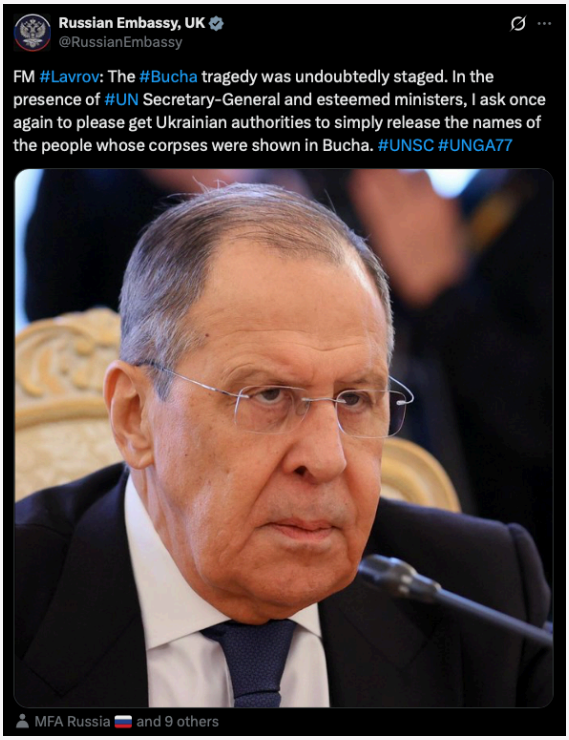
Perhaps the most profound challenge confronts democratic societies directly. How can liberal democracies founded on free speech and open debate defend themselves against cognitive attacks without adopting authoritarian adversaries' manipulative tools? Implementing robust defenses against disinformation risks veering into censorship and propaganda, undermining the values democracies seek to protect. Authoritarian regimes face no such dilemma since they already exercise comprehensive information control. China's Great Firewall and Russia's media apparatus provide substantial advantages in cognitive warfare.[100] Democratic societies attempting similar control would fundamentally compromise their character: government fact-checking risks becoming truth determination, content moderation can become opinion censorship, and strategic communication can resemble state propaganda. Yet passivity invites strategic defeat as adversaries exploit openness to destabilize democratic institutions from within.

Finland's approach suggests potential resolution through societal resilience rather than control, investing in media literacy, institutional trust, and transparent communication, empowering citizens to resist manipulation rather than preventing exposure to it.[101] Such approaches require decades of investment and cannot provide immediate defense during acute crises, but they preserve democratic character while building genuine cognitive resistance. The ethical framework for cognitive warfare remains underdeveloped precisely because the domain is new, and established traditions developed for kinetic conflict provide limited guidance. Just War Theory's principles of proportionality, necessity, and discrimination become difficult to apply when weapons are narratives, targets are minds, and harms are primarily psychological rather than physical.

“ The most profound challenge confronts democratic societies directly...Implementing robust defenses against disinformation risks veering into censorship and propaganda, undermining the values democracies seek to protect. Authoritarian regimes face no such dilemma since they already exercise comprehensive information control...Democratic societies attempting similar control would fundamentally compromise their character: government fact-checking risks becoming truth determination, content moderation can become opinion censorship, and strategic communication can resemble state propaganda.

What remains clear is that cognitive warfare cannot proceed ethically without sustained attention to the development of appropriate frameworks. Democratic societies must urgently invest in ethical guidelines, legal frameworks, and oversight mechanisms that preserve democratic values while enabling effective defense. This requires bringing together ethicists, legal scholars, technologists, and military professionals to grapple with questions lacking historical precedent. The alternative is allowing cognitive warfare to evolve unconstrained, leading toward a world where manipulation becomes normalized, truth loses meaning, and democratic deliberation becomes impossible because citizens can no longer trust their own cognitive processes.

The Bucha Massacre: Competing Narratives and Cognitive Battlespace Dynamics



The discovery of civilian casualties in Bucha following Russian withdrawal in early April 2022 became a critical inflection point, demonstrating how physical evidence, technical verification, and narrative framing intersect in the cognitive domain. On April 2-3, 2022, Ukrainian forces entering Bucha documented bodies of civilians in streets and yards, many showing signs of execution-style killings with hands bound.[90] Ukrainian authorities initially reported 458 civilian deaths, a figure later revised upward as more remains were discovered.[91]

The cognitive battle began immediately. Ukrainian President Zelensky termed the killings "genocide" within hours, while Russian officials claimed the images were staged provocations, asserting that bodies had been placed in streets only after Russian forces departed.[92] This created a binary cognitive contest: either Russian forces had committed atrocities, or Ukraine had fabricated evidence—tertiary explanations received little attention in the initial information environment.

Technical verification became decisive in this contest. Maxar Technologies released commercial satellite imagery captured between March 9-11 and March 19-21, 2022—while Russian forces controlled Bucha—showing bodies visible in streets at the same locations where they were subsequently found by Ukrainian forces.[93] The New York Times Visual Investigations team conducted detailed geolocation analysis, matching satellite imagery to ground-level videos and photographs, while Bellingcat investigators used open-source methods to corroborate timelines and locations.[94] This convergence of commercial satellite capabilities, journalistic verification, and open-source intelligence created a technical evidence base that substantially undermined Russian counter-narratives, at least within information environments where this evidence received distribution.

The cognitive effects manifested rapidly in policy outcomes. Within 72 hours of the Bucha imagery spreading globally, Germany—which had previously resisted sending heavy weapons to Ukraine—announced a reversal of its policy.[95] The European Union fast-tracked its fifth sanctions package against Russia, approved on April 8, 2022, explicitly citing Bucha in its justification.[96] Western media mentions of "genocide" in connection with Ukraine increased by approximately 2,400% in the week following April 2, according to media monitoring by Media Tenor. Public opinion polling in major European countries showed increases of 15-20 percentage points in support for stronger action against Russia.

However, the Bucha incident also demonstrated the limits of cognitive operations even when supported by substantial evidence. Despite massive international attention and documented atrocities, direct NATO military intervention remained politically untenable in Western capitals.[97] The incident shifted the threshold of acceptable military aid but did not fundamentally alter the Western calculation against direct confrontation with a nuclear-armed power. This reveals an important constraint within the STCB framework: cognitive effects, while powerful in shaping perceptions and enabling policy shifts within existing parameters, operate within structural limits imposed by material capabilities and existential risk calculations. Narrative dominance can expand the range of politically possible actions, but cannot override fundamental strategic constraints rooted in nuclear deterrence and alliance commitments. Accordingly, the STCB framework must be applied as an integrated analytic lens that takes structural constraints in view.

Future Trends in STCB Warfare

The STCB represents a dynamic battlespace where technological acceleration drives continuous transformation. Several emerging trends promise to reshape the character of cognitive warfare in the coming years, each amplifying current challenges while introducing qualitatively new threats that existing defenses are poorly equipped to address.

The proliferation of AI-powered manipulation constitutes the most immediate threat. Generative AI, including large language models and synthetic media generators, has dramatically lowered barriers to creating high-quality disinformation. What required state resources and specialized expertise five years ago can now be accomplished by individual actors with consumer hardware and publicly available tools. GPT-4 and similar models generate culturally nuanced propaganda tailored to specific audiences, create hundreds of synthetic social media personas that maintain consistent interaction patterns, and produce deepfake videos so convincing that casual viewers cannot distinguish them from authentic footage.[102] This democratization means not only major powers but also minor states, terrorist organizations, criminal enterprises, and committed individuals can conduct sophisticated influence operations.

We are heading toward environments of "zero trust" information, where seeing is no longer believing, where every piece of evidence must be suspected of being synthetic, and where the cognitive costs of verification exceed most people's available attention.[103] In such environments, truth does not disappear; rather, it becomes increasingly difficult to distinguish from sophisticated falsehood. The next evolutionary stage involves fully autonomous cognitive campaigns where AI identifies societal vulnerabilities, generates tailored content, deploys it through bot networks, measures effectiveness through real-time metrics, and iteratively refines messaging in continuous automated loops. These systems would execute complete OODA loops at machine speed, adapting faster than human analysts can track, let alone counter.

The weaponization of immersive environments represents a second major trend as social interaction migrates to augmented and virtual reality spaces. Current social media platforms mediate reality through flat screens, where users maintain awareness that they are consuming mediated content. Virtual reality technologies create immersive experiences in which the boundaries between digital content and perceived reality become phenomenologically indistinct. VR possesses unique persuasive power because it engages multiple sensory channels simultaneously and creates a sense of presence and embodiment that flat media cannot match.[104] Research demonstrates that virtual reality experiences can shape attitudes and behaviors as powerfully as real-world experiences.[105]

> "The proliferation of AI-powered manipulation constitutes the most immediate threat. Generative AI, including large language models and synthetic media generators, has dramatically lowered barriers to creating high-quality disinformation. What required state resources and specialized expertise five years ago can now be accomplished by individual actors with consumer hardware and publicly available tools...The weaponization of immersive environments represents a second major trend as social interaction migrates to augmented and virtual reality spaces.

Adversaries could create immersive propaganda experiences that feel like direct personal encounters rather than mediated messaging, leverage virtual environments to normalize extremist ideologies through gradual exposure in gamified settings, or use AI-controlled avatars to conduct targeted influence operations with persuasive power exceeding text-based social media.

If metaverse platforms develop as technology companies envision, they will create persistent shared virtual spaces where people conduct significant portions of their social and economic lives. Such environments would offer unprecedented surveillance opportunities, as every interaction and physiological response captured by VR headsets generates data streams far richer than those collected by current social media platforms. Entities controlling metaverse platforms would possess capacities to shape user experiences, manipulate social dynamics, and influence behavior through environmental design in ways that make current algorithmic curation seem crude by comparison. The concentration of such power in private corporations or adversary states raises strategic concerns that current policy frameworks do not address.

Cognitive manipulation at scale through big data convergence represents a third trend as advanced AI combines with vast repositories of personal data collected over two decades of digital surveillance capitalism. When analyzed by machine learning systems optimized for prediction and influence, detailed psychological models of entire populations enable targeting specific individuals with personalized, emotionally resonant messages designed to exploit their particular vulnerabilities and biases. This represents industrialized manipulation on a civilization scale. Where traditional propaganda relied on broad messaging, AI-enabled micro-targeting can craft millions of slightly different messages each optimized for specific recipients.[106] The effect is systematic amplification of every societal division with precision impossible in previous eras, engineering incommensurable worldviews at the population scale through weaponized personalization.

The speculative horizon points toward neuro-warfare as advances in brain-computer interfaces eventually create technologies capable of bidirectional communication between computers and neural systems. While this remains largely science fiction, research trajectories suggest technical feasibility within the coming decades. When such technologies mature, they will enable cognitive warfare of unprecedented directness, in which adversaries might compromise neural implants to induce emotions, manipulate decision-making, or monitor neural activity for intelligence purposes more revealing than any interrogation. The ethical and strategic implications demand that frameworks be developed now, before technical capability arrives, as history suggests that by the time capabilities become operational, it is too late to establish ethical constraints.

> “The speculative horizon points toward neuro-warfare as advances in brain-computer interfaces eventually create technologies capable of bidirectional communication between computers and neural systems...When such technologies mature, they will enable cognitive warfare of unprecedented directness, in which adversaries might compromise neural implants to induce emotions, manipulate decision-making, or monitor neural activity for intelligence purposes more revealing than any interrogation.

These trends share common characteristics: each represents acceleration of existing STCB dynamics rather than entirely new phenomena; each has advantages for actors willing to use them without ethical restraint; each raises questions for which existing frameworks provide inadequate guidance; and each suggests the STCB will become more rather than less central to conflict in the coming decades. The challenge for democratic societies is to develop capabilities to compete in evolving STCB environments while maintaining ethical commitments that differentiate them from authoritarian adversaries—a challenge that will define great power competition throughout the 21st century.

Policy Recommendations

The complexity and pervasiveness of STCB warfare demand coordinated action across government, military, private sector, and civil society.

For National Governments

Develop a Comprehensive National STCB Security Strategy

Governments must develop dedicated national strategies addressing Socio-Technical-Cognitive Battlespace threats as a unified challenge requiring whole-of-government coordination. These strategies should establish clear policy frameworks integrating cyber defense, information operations, social resilience, and cognitive security under a single strategic vision aligned with broader national security objectives.

A comprehensive STCB security strategy should include:

- **Threat Assessment Framework:** Systematic analysis of adversary STCB capabilities, historical patterns of cognitive operations, vulnerabilities across social, technical, and cognitive domains, and long-term threat trajectories.

- **National Objectives:** Clear articulation of defensive goals (protecting democratic institutions, social cohesion, critical information infrastructure) and, where legally and ethically appropriate, offensive capabilities for deterrence and response.

- **Resource Allocation:** Multi-year budgeting across relevant agencies, dedicated R&D funding for STCB-relevant technologies, investment in training programs for government personnel, and public media literacy initiatives.

- **Institutional Architecture:** Identification of gaps in existing arrangements and explicit mandates for integrated coordination bodies where current structures prove inadequate, serving as implementing mechanisms for the broader strategy.

Implementation: Integrated Coordination Bodies

Based on strategic requirements, governments should establish interagency coordination bodies reporting directly to national security leadership with multidisciplinary staff (intelligence analysts, social scientists, technologists, legal experts, military liaisons). These bodies coordinate implementation across departments while including private-sector advisory boards from technology companies, academic institutions, and civil society.

Core functions of these bodies could include continuous vulnerability assessment across STCB domains; early warning systems detecting coordinated inauthentic behavior and narrative manipulation; crisis coordination; R&D oversight; and liaison with allied organizations. Critically, these bodies must map national exposure to foreign-controlled social media and data infrastructures, and advise on investment screening, merger control, and national security reviews of foreign platform operations.

Finland's Comprehensive Security Model (post-2014) provides precedent, coordinating government, private sector, and civil society to achieve a first-place global ranking in resilience to misinformation. The primary risk—politicization or domestic surveillance mission creep—requires transparent charters limiting scope to foreign-origin threats, independent civil liberties oversight with quarterly public reporting, and sunset provisions requiring parliamentary reauthorization every five years.

From Algorithmic Transparency to Jurisdictional Control

Algorithmic Transparency Requirements should differentiate between domestically controlled and foreign-adversary-controlled platforms, imposing higher obligations and potential structural remedies, such as forced divestiture or operational separation, on the latter. In addition to quarterly disclosure of amplification parameters and incident reporting, platforms above a defined user threshold that are controlled by entities in designated adversary jurisdictions should be required to:

- Establish legally distinct, domestically incorporated entities with independent boards and technical autonomy over national operations, including full control of recommendation algorithms and moderation policies for domestic users.

- Prohibit operational relationships that give foreign parents influence over domestic content curation, data access, or code updates, subject to independent security audits.

Regulators should explicitly acknowledge that deep corporate pockets and established lobbying channels will be mobilised against such reforms, and design transparency rules for lobbying and public-consultation processes to mitigate regulatory capture.

Implementation spanning three to five years would achieve legislation and stakeholder consultation in years one and two, compliance audits and researcher onboarding in year three, and enforcement actions with framework refinement in years four and five. A regulatory agency with two to three hundred specialized staff and an annual budget of one hundred fifty to two hundred million dollars remains modest compared to the FDA's eighteen thousand employees overseeing food and drug safety. The EU Digital Services Act demonstrates that major jurisdictions can successfully impose transparency requirements despite industry resistance, though early implementation reveals compliance challenges requiring iterative refinement. Industry will resist citing trade-secret exposure, while technical complexity in defining algorithms and international coordination needs pose implementation challenges. Mitigation requires a phased implementation, industry consultation, verified trade secret protections by an independent auditor, and OECD coordination for international harmonization.

Map and Mitigate Critical Algorithmic Dependencies

Governments must systematically identify dependencies on foreign-owned platforms across critical national functions, including government communications, emergency services coordination, financial system infrastructure, and defense supply chain management. This mapping should produce publicly available vulnerability assessments that include:

- Concentration metrics for reliance on specific foreign platforms in strategic sectors (elections, defence industry, energy, finance).

- Scenario analyses of hostile platform behaviour, algorithmic throttling, selective outages, and preferential amplification of adversary narratives as tools of cyber-enabled economic coercion.

- Roadmaps for diversifying these dependencies via interoperable domestic platforms, public-service information channels, and legal requirements that critical government and financial communications do not rely on a single foreign-controlled platform.

For Military and Intelligence Organizations

Integrate Cognitive Effects Cells into Operational Planning

Military organizations must institutionalize STCB analysis by creating Cognitive Effects Cells at Combatant Command levels, staffing them with social scientists, data analysts, information operations specialists, regional cultural experts, and military planners serving liaison functions. These cells must be co-located with operations planning staff and embedded in planning cycles from inception rather than consulted as afterthoughts.

During pre-operation phases, these cells should assess anticipated cognitive and social effects of planned kinetic operations, identify societal vulnerabilities in areas of operations, predict adversary and neutral population responses, and recommend modifications to minimize adverse cognitive effects or maximize strategic narrative advantage. Throughout operations, cells should conduct real-time monitoring of adversary and civilian responses through social media analysis and polling, track narrative evolution, identify emerging counter-narratives, provide decision-makers with cognitive battlespace awareness analogous to traditional intelligence pictures, and coordinate with information operations and public affairs for integrated messaging. Post-operation assessments should evaluate cognitive effects equivalent to battle damage assessment and document lessons learned for institutional knowledge building.

Professional military education must integrate STCB fundamentals with all officers at Major-equivalent rank receiving forty-hour foundational courses, staff colleges dedicating twenty to thirty hours to cognitive warfare instruction, and war college exercises incorporating cognitive domain scenarios.

For Private Sector Technology Companies

Adopt Voluntary Cognitive Impact Assessment Framework

Technology companies should proactively assess STCB implications of platform design choices before implementation. A voluntary framework would apply before implementing changes to content recommendation algorithms, user interface designs that affect information consumption, content moderation systems, and features that enable social coordination. Assessment processes should begin with a vulnerability analysis, evaluating cross-border control and data-flow risks, including how foreign legal obligations on parent entities might be leveraged for covert data access or influence in crisis scenarios; proceed to an amplification assessment, evaluating polarization risks; continue to mitigation design, determining safeguards that reduce STCB risks while maintaining innovation; and conclude with a third-party review by independent auditors that provides written opinions on assessment completeness.

Quarterly aggregated transparency reports should document assessment numbers, changes delayed due to STCB concerns, and detected exploitation attempts while protecting trade secrets and demonstrating due diligence. Multi-layered incentives would drive adoption through industry-best-practice certification, government procurement preferences, regulatory preemption when self-regulation reduces the likelihood of mandates, user trust-building, and liability protection when good-faith

assessments provide legal defense. Per-company investment of five to ten million dollars annually represents 0.001 to 0.007% of revenue for large platforms, given Meta's 2023 revenue of one hundred thirty-four billion dollars[110] and Google's three hundred seven billion.[111]

Privacy Impact Assessments under GDPR demonstrate the feasibility of technology design impact frameworks, having overcome initial compliance challenges to become standard practice.[112] Enforcement without regulation remains inherently weak since voluntary regimes depend on reputation and market pressure. Mitigation requires multi-stakeholder governance, including civil society and academics, rather than industry-only control; graduated requirements with lighter assessments for smaller platforms; and a regulatory backstop that signals a credible threat if the voluntary approach fails.

For International Organizations

Initiate Development of International Norms for Cognitive Warfare

Establishing multilateral agreements defining acceptable and prohibited practices addresses the reality that current international law leaves cognitive operations in legal gray zones. UN-sponsored multilateral negotiations employing multi-stakeholder approaches, including states, tech companies, civil society, and experts, should adopt a phased approach, recognizing that binding treaties may take decades while interim norm-setting provides immediate value.

Norms on cognitive warfare should address state responsibilities when hosting or controlling major platforms, including prohibitions against using jurisdictional control over platforms to conduct covert economic coercion or destabilising cognitive operations in other states' information spaces. Core prohibitions with the highest consensus potential should ban state-sponsored campaigns deliberately spreading false medical information during public health emergencies, deepfakes of political or military leaders without clear labeling as direct attacks on command and control, and cognitive operations designed to cause physical harm by targeting critical infrastructure operators. Required practices with moderate consensus should mandate that states engage in international information campaigns to disclose state sponsorship through standards that allow audiences to evaluate credibility, and that states disclose their use of AI for influence operations, preventing fully autonomous operations without human accountability.

Enforcement mechanisms in the near term would rely on UN monitoring bodies documenting violations, creating reputational costs; medium-term graduated responses, including conditional benefits and sanction coordination; and long-term treaty frameworks with compliance verification, though realistic expectations recognize that enforcement will remain primarily reputational rather than coercive. Track 1.5 dialogues and expert working groups drafting proposed norms would occupy years one through three, UN resolutions establishing monitoring bodies years four through six, and draft treaty negotiations years seven through ten, with a realistic assessment that full processes may require fifteen to twenty years, while interim norm-setting provides immediate value.

The Chemical Weapons Convention, adopted in 1993 and ratified by 193 states parties, demonstrates that international treaties establish strong norms despite imperfect verification.[113] The Paris Call for Trust and Security in Cyberspace, launched in 2018 by 80 states and 700 organizations, offers potential for voluntary multilateral commitments.[114] Pursuing imperfect norms despite challenges serves strategic purposes by creating legitimacy for countermeasures, establishing diplomatic engagement language, and demonstrating democratic commitment to responsible behavior, in contrast to authoritarian norm violations.

Endnotes

1. Bugayova, Nataliya, and Kateryna Stepanenko. “A Primer on Russian Cognitive Warfare.” Institute for the Study of War, 30 June 2025, https://understandingwar.org/research/cognitive-warfare/a-primer-on-russian-cognitive-warfare/
2. Lendon, Brad, Tim Lister, and Josh Pennington. “Soldiers on Snake Island Reacted with Defiant Words to Threats from Russian Warship.” CNN, 25 Feb. 2022, https://edition.cnn.com/2022/02/25/europe/ukraine-russia-snake-island-attack-intl-hnk-ml
3. Harding, Luke. “‘Russian warship, go fuck yourself’: what happened next to the Ukrainians defending Snake Island?” The Guardian, 19 Nov. 2022, www.theguardian.com/world/2022/nov/19/russian-warship-go-fuck-yourself-ukraine-snake-island.
4. Chappell, Bill. “Snake Island Sailors Are Freed as Ukraine and Russia Conduct a Prisoner Exchange.” NPR, 24 Mar. 2022, www.npr.org/2022/03/24/1088593653/snake-island-sailors-freed-prisoner-swap
5. The International Institute for Strategic Studies. The Military Balance 2025. Routledge/Taylor & Francis, 2025. ISBN 9781041049678.
6. See, for example, Christopher Pickle, “The Changing Character of Cyber Warfare,” Proceedings: U.S. Naval Institute 150, no. 6 (June 2024), and Jimena Sofía Viveros Álvarez, “The Risks and Inefficacies of AI Systems in Military Targeting Support,” ICRC Humanitarian Law & Policy Blog, 4 September 2024. Both reflect a broader strand of contemporary analysis that treats cyber and AI capabilities primarily as supportive or force-multiplying tools that enhance conventional military operations, rather than as substitutes for hard military power, which remains central to battlefield outcomes.
7. Weissmann, Mikael. “Urban Warfare: Challenges of Military Operations on Tomorrow’s Battlefield.” Advanced Land Warfare: Tactics and Operations, eds. by Mikael Weissmann and Niklas Nilsson, Oxford University Press, 2023, pp. 125–152, academic.oup.com/book/45784/chapter/400599318.
8. Pastor, Álvaro. Cognitive Warfare. HAL, hal.science/hal-04420986v2/file/Cognitive_Warfare2025_07_16_2025.pdf.
9. McAloon, Abby. “Technology Shaping Modern Warfare.” Information Integrity UK, 28 Oct. 2025, www.informationintegrityuk.org/technology-shaping-modern-warfare/
10. Wasinger, Matthias. “The Highest Form of Freedom and the West’s Best Weapon to Counter Cognitive Warfare.” The Defence Horizon Journal, 20 May 2024, tdhj.org/blog/post/freedom-counter-cognitive-warfare/.
11. Nilsson, Niklas, Mikael Weissmann, and Björn Palmertz. “Hybrid Threats and the Intelligence Community: Priming for a Volatile Age.” International Journal of Intelligence and CounterIntelligence, vol. 39, no. 1, 2025, pp. 1–23, doi:10.1080/08850607.2024.2435265
12. Dickinson, Peter. “Putin Uses NATO as an Excuse for His War against Ukrainian Statehood.” Atlantic Council, February 28, 2025. https://www.atlanticcouncil.org/blogs/ukrainealert/putin-uses-nato-as-an-excuse-for-his-war-against-ukrainian-statehood/.
13. Halperin, Eran, Daniel Bar-Tal, Rafi Nets-Zehngut, and Erga Drori. “Emotions in Conflict: Correlates of Fear and Hope in the Israeli-Jewish Society.” Peace and Conflict: Journal of Peace Psychology (United Kingdom) 14, no. 3 (2008): 233–58. https://doi.org/10.1080/10781910802229157.
14. WhatIs. “What Is Weak Tie Theory? – TechTarget Definition.” Accessed September 27, 2025. https://www.techtarget.com/whatis/definition/weak-tie-theory.
15. Gans, Steven, MD Steven Gans, MD is board-certified in psychiatry, Is an Active Supervisor, teacher, and mentor at Massachusetts General Hospital Learn about our Review Board. “Social Identity Theory—Are We the Company We Keep?” Verywell Mind. Accessed September 27, 2025. https://www.verywellmind.com/social-identity-theory-7550623.
16. Rasoulikolamaki, Sahar, Surinderpal Kaur, Alena Zhdanava, and Noor Aqsa Nabila Mat Isa. “In-Group and Out-Group Identity Construction in Extremist Discourse: A Critical Multimodal Approach.” Behavioral Sciences of Terrorism and Political Aggression, vol. 17, no. 4, 2025, pp. 377-395, doi:10.1080/19434472.2023.2245011.
17. Bateman, Jon, and Dean Jackson. Countering Disinformation Effectively: An Evidence-Based Policy Guide. Carnegie Endowment for International Peace, 31 Jan. 2024, carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en.
18. Lange-Ionatamišvili, Elīna, et al. Analysis of Russia’s Information Campaign Against Ukraine. NATO Strategic Communications Centre of Excellence, Riga, 2015, stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf.
19. Ackerman, Peter, and Maciej Bartkowski. “Challenging Annexation: In Crimea, the Referendum That Wasn’t.” openDemocracy, 22 Mar. 2014, http://www.opendemocracy.net/en/civilresistance/challenging-annexation-in-crimea-referendum-that-wa/

Endnotes

20. United Nations General Assembly. “General Assembly Adopts Resolution Calling upon States Not to Recognize Changes in Status of Crimea Region.” United Nations Press, 27 Mar. 2014, www.un.org/press/en/2014/ga11493.doc.html

21. Eds. Kupiecki, Robert, Filip Bryjka, and Tomasz Chłoń. “Militarization of Information in Russian Strategic Culture.” International Disinformation: A Handbook for Analysis and Response, Brill, 2024, pp. 132–153, doi:10.1163/9789004715769_011.

22. Harward, Christina, Kateryna Stepanenko, Justin Young, and George Barros. “Russian Offensive Campaign Assessment, December 4, 2025.” Critical Threats, 4 Dec. 2025, www.criticalthreats.org/analysis/russian-offensive-campaign-assessment-december-4-2025

23. Higgins, Charlotte, and Artem Mazhulin. “Russian-speaking Ukrainians Want to Shed ‘Language of the Oppressor’.” The Guardian, 24 Apr. 2023, www.theguardian.com/world/2023/apr/24/russian-speaking-ukrainians-want-to-shed-language-of-the-oppressor

24. Wilson, Andrew. “Ukraine at War: Baseline Identity and Social Construction.” Nations and Nationalism, vol. 30, no. 1, 2024, pp. 8–17, doi:10.1111/nana.12986

25. Kyiv International Institute of Sociology. Indicators of National-Civic Ukrainian Identity. Press release/report, Kyiv International Institute of Sociology, 2023, www.kiis.com.ua/?lang=eng&cat=reports&id=1131&page=1

26. Chachashvili-Bolotin, Svetlana. “The Russian Invasion of Ukraine and the Strengthening of Ukrainian Identity among Former Soviet Immigrants from Ukraine: Israel as a Case Study.” Post-Soviet Affairs, vol. 40, no. 1, 2024, pp. 56–70, doi:10.1080/1060586X.2023.2277620.

27. Haig, Zsolt. “Electronic Warfare in Cyberspace.” Security and Defence, vol. 14, no. 4, 5 Jan. 2026, pp. 1–15, securityanddefence.pl/pdf-103299-36215?filename=36215.pdf.

28. Busch, Ella, and Jacob Ware. The Weaponisation of Deepfakes: Digital Deception by the Far-Right. International Centre for Counter-Terrorism (ICCT) Policy Brief, 13 Dec. 2023, icct.nl/sites/default/files/2023-12/The%20Weaponisation%20of%20Deepfakes.pdf. ; Ajayi, Oluwatomisin. AI-Powered Disinformation and Narrative Warfare: A Global Security Threat. SSRN, 19 May 2025, ssrn.com/abstract=5184687.

29. Ó Fathaigh, Ronan, Tom Dobber, Frederik Zuiderveen Borgesius, and James Shires. “Microtargeted Propaganda by Foreign Actors: An Interdisciplinary Exploration.” Maastricht Journal of European and Comparative Law, vol. 28, no. 6, Dec. 2021, pp. 856–877, doi:10.1177/1023263X211042471.

30. Blanchard, Alexander, and Laura Bruun. Autonomous Weapon Systems and AI-Enabled Decision Support Systems in Military Targeting: A Comparison and Recommended Policy Responses. Stockholm International Peace Research Institute, June 2025, doi:10.55163/YQBY3151, www.sipri.org/publications/2025/other-publications/autonomous-weapon-systems-and-ai-enabled-decision-support-systems-military-targeting-comparison-and

31. Sufi, Fahim. “Social Media Analytics on Russia–Ukraine Cyber War with Natural Language Processing: Perspectives and Challenges.” Information, vol. 14, no. 9, 31 Aug. 2023, p. 485, doi:10.3390/info14090485.

32. Maddox, J.D. “It’s Time to Think About (and Fear) Drones and Psychological Operations.” War on the Rocks, 24 July 2025, warontherocks.com/2025/07/its-time-to-think-about-and-fear-drones-and-psychological-operations/.

33. Pamment, James, Jesper Falkheimer, and Elsa Isaksson. Malign Foreign Interference and Information Influence on Video Game Platforms: Understanding the Adversarial Playbook. MPF Report Series 3/2023, Myndigheten för psykologiskt försvar (Psychological Defence Agency, Sweden), 2023, mpf.se/download/18.34f4c6361939015813e2ef/1733303782826/mpf-skriftserie-23-03-malign-foreign-interference-and-information-influence-on-video-game-platforms.pdf.

34. Brodkin, Jon. “Musk Refused Ukraine’s Request to Enable Starlink for Drone Attack [Updated].” Ars Technica, September 7, 2023. https://arstechnica.com/tech-policy/2023/09/how-am-i-in-this-war-book-details-musks-doubts-on-starlink-in-ukraine/.

35. Abels, Joscha. “Private Infrastructure in Geopolitical Conflicts: The Case of Starlink and the War in Ukraine.” European Journal of International Relations, vol. 30, no. 4, June 2024, pp. 842–866, doi:10.1177/13540661241260653.

36. “Elon Musk Says Starlink Internet Service ‘Active’ in Ukraine.” Al Jazeera, 27 Feb. 2022, www.aljazeera.com/news/2022/2/27/elon-musk-starlink-internet-service-ukraine-russian-invasion.

Endnotes

37. Roulette, Joey, Cassell Bryan-Low, and Tom Balmforth. “Musk Ordered Shutdown of Starlink Satellite Service as Ukraine Retook Territory from Russia.” Reuters, 25 July 2025, www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25
38. Exclusive: Musk’s SpaceX Says It Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick Up the Tab.” CNN, 13 Oct. 2022, amp.cnn.com/cnn/2022/10/13/politics/elon-musk-spacex-starlink-ukraine.
39. Borger, Julian. “Elon Musk Ordered Starlink to Be Turned Off during Ukraine Offensive, Book Says.” The Guardian, 7 Sept. 2023, www.theguardian.com/technology/2023/sep/07/elon-musk-ordered-starlink-turned-off-ukraine-offensive-biography
40. Darcy, Oliver. “An Explosive Elon Musk Biography Is Just Hitting Shelves. But the Book’s Acclaimed Author Is Already Walking Back a Major Claim.” CNN, 11 Sept. 2023, amp.cnn.com/cnn/2023/09/11/media/walter-isaacson-elon-musk-reliable-sources/index.html.
41. Sacks, David, and Seaton Huang. “Onshoring Semiconductor Production: National Security Versus Economic Efficiency.” Council on Foreign Relations, 17 Apr. 2024, www.cfr.org/article/onshoring-semiconductor-production-national-security-versus-economic-efficiency.
42. Zhou, Viola. “Inside TSMC’s Phoenix, Arizona Expansion Struggles.” Rest of World, 23 Apr. 2024, restofworld.org/2024/tsmc-arizona-expansion/.
43. McKinney, Jared M., and Peter Harris. Deterrence Gap: Avoiding War in the Taiwan Strait. US Army War College Press, 5 Jan. 2024, press.armywarcollege.edu/monographs/964.
44. Ramani, Vinay, Debabrata Ghosh, and ManMohan S. Sodhi. “Understanding Systemic Disruption from the COVID-19-Induced Semiconductor Shortage for the Auto Industry.” Omega, vol. 113, 29 June 2022, pp. 102720, doi:10.1016/j.omega.2022.102720. PubMed Central (PMC), pmc.ncbi.nlm.nih.gov/articles/PMC9363154/.
45. Stanford Institute for Human-Centered Artificial Intelligence. What the CHIPS and Science Act Means for Artificial Intelligence. Aug. 2022, hai.stanford.edu/sites/default/files/2022-08/HAI%20Explainer%20-%20What%20The%20CHIPS%20and%20Science%20Act%20Means%20for%20AI.pdf.
46. Claverie, Bernard, and François Du Cluzel. “‘Cognitive Warfare’: The Advent of the Concept of ‘Cognitics’ in the Field of Warfare.” In Cognitive Warfare: The Future of Cognitive Dominance, edited by Bernard Claverie, Baptiste Prébot, Norbou Buchler, and François du Cluzel. NATO Collaboration Support Office, 2022. https://hal.science/hal-03635889.
47. Bruckmaier, Georg, et al. “Tversky and Kahneman’s Cognitive Illusions: Who Can Solve Them, and Why?” Frontiers in Psychology, vol. 12, 12 Apr. 2021, doi:10.3389/fpsyg.2021.584689.
48. “Countering Truth Decay.” Accessed September 27, 2025. https://www.rand.org/research/projects/truth-decay.html.
49. DeMarco, J. William. “The Dialectic of Deception: John Boyd and the Cognitive Battlefield.” War on the Rocks, 4 Sept. 2025, warontherocks.com/2025/09/the-dialectic-of-deception-john-boyd-and-the-cognitive-battlefield/.
50. Laine, Jussi P., and Bo Petersson, editors. Resilience as Deterrence: Towards a Comprehensive Security Panorama.NATO Science for Peace and Security Series E: Human and Societal Dynamics Vol. 159, IOS Press, 2025. DiVA Portal, https://mau.diva-portal.org/smash/get/diva2:2013615/FULLTEXT01.pdf
51. Brooks, James. “Finland’s Battle Against Fake News Starts in Preschool Classrooms.” ABC News, 5 Jan. 2026, abcnews.go.com/International/wireStory/finlands-battle-fake-news-starts-preschool-classrooms-128902330.
52. Mackintosh, Eliza. Finland Is Winning the War on Fake News: What It’s Learned May Be Crucial to Western Democracy.CNN, May 2019, edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/.
53. Edelman Trust Institute. 2024 Edelman Trust Barometer: Global Report. Feb. 2024, www.edelman.com/sites/g/files/aatuss191/files/2024-02/2024%20Edelman%20Trust%20Barometer%20Global%20Report_FINAL.pdf
54. Moilanen, Panu, Miriam Hautala, and Dominic Saari. Disinformation Landscape in Finland. EU DisinfoLab, May 2023, www.disinfo.eu/wp-content/uploads/2023/05/Finland_DisinfoFactsheet.pdf
55. Ünlü, Ali, et al. “Tracing the Dynamics of Misinformation and Vaccine Stance in Finland amid COVID-19.” Information, Communication & Society, 27 Mar. 2024, pp. 1–25, doi:10.1080/1369118X.2024.2331756.
56. Culea (Șerban), Mioara. “The Role of Military Morale as an Essential Dimension of Combat Power.” Security and Defence Quarterly, vol. 47, no. 3, 2024, pp. 1–18, doi:10.35467/sdq/174832.

Endnotes

57. Muñoz, Pau, et al. “The Role of Recommendation Algorithms in the Formation of Disinformation Networks.” Information Processing & Management, vol. 62, no. 6, Nov. 2025, article 104243, Elsevier, doi:10.1016/j.ipm.2025.104243.
58. Poor Bgheshmi, Mohammad Sharif Sharifi, and Mahsa Sharajsharifi. “Managing the Crisis: AI and the Demise of National Sovereignty?”Journal of World Sociopolitical Studies, vol. 9, no. 4, Autumn 2025, pp. 853–886, doi:10.22059/wsps.2025.396021.1522.
59. Burkhardt, Fabian, and Mariëlle Wijermars. “Digital Authoritarianism and Russia’s War Against Ukraine: How Sanctions-induced Infrastructural Disruptions are Reshaping Russia’s Repressive Capacities.” SAIS Review of International Affairs, vol. 42, no. 2, 2022, pp. 21–43, doi:10.1353/sais.2022.0009.
60. Romanishyn, Alexander, Olena Malytska, and Vitaliy Goncharuk. “AI-driven Disinformation: Policy Recommendations for Democratic Resilience.” Frontiers in Artificial Intelligence, vol. 8, 31 July 2025, article 1569115, Frontiers Media S.A., doi:10.3389/frai.2025.1569115.
61. Deppe, Christoph, and Gary S. Schaal. “Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept.” Frontiers in Big Data, vol. 7, 1 Nov. 2024, article 1452129, Frontiers Media S.A., doi:10.3389/fdata.2024.1452129.
62. Zecchinon, P., and Olivier Standaert. “The War in Ukraine Through the Prism of Visual Disinformation and the Limits of Specialized Fact-Checking: A Case-Study at Le Monde.” Digital Journalism, 2024, pp. 1–19, doi:10.1080/21670811.2024.2332609.
63. Global Engagement Center. Disinformation Roulette: The Kremlin’s Year of Lies to Justify an Unjustifiable War. U.S. Department of State, 23 Feb. 2023, 2021-2025.state.gov/disarming-disinformation/disinformation-roulette-the-kremlins-year-of-lies-to-justify-an-unjustifiable-war/.
64. Krapfl, James, and Eric Kühn von Burgsdorff. “Ukraine’s Euromaidan and Revolution of Dignity, Ten Years Later.” Canadian Slavonic Papers / Revue Canadienne des Slavistes, vol. 65, no. 3–4, 2023, pp. 325–334, doi:10.1080/00085006.2023.2293420.
65. Herd, Graeme P. “Russia and Ukraine: Victory Is Not Possible; Defeat Is Not an Option.” OSCE Yearbook 2014, edited by IFSH, Nomos, 2015, pp. 199–214. IFSH, www.ifsh.de/file-CORE/documents/yearbook/english/14/Herd-en-2014_S.pdf
66. Fedchenko, Yevhen. “Kremlin Propaganda: Soviet Active Measures by Other Means.” Sõjateadlane: The Estonian Journal of Military Studies, vol. 2, 2016, pp. 140–170, www.kvak.ee/files/2021/10/Yevhen-Fedchenko_KREMLIN-PROPAGANDA-SOVIET-ACTIVE-MEASURES-BY-OTHER-MEANS.pdf
67. Jordash, Wayne, et al. Manufacturing Impunity: Russian Information Operations in Ukraine — Russia’s Use of Information Alibis and How They Materially Contribute to the Planning, Execution and Cover-Up of International Crimes. Global Rights Compliance and The Reckoning Project, May 2025, globalrightscompliance.org/wp-content/uploads/2025/05/Manufacturing-Impunity.pdf.
68. Associated Press. “Zelensky Reaffirms His Refusal to Cede Land to Russia as He Rallies European Support.” Arab News, 10 Dec. 2025.
69. White, Ryan. “How the Cloud Saved Ukraine’s Data from Russian Attacks.” C4ISRNet, June 22, 2022. https://www.c4isrnet.com/2022/06/22/how-the-cloud-saved-ukraines-data-from-russian-attacks/.
70. Jayanti, Amritha. “Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?” Belfer Center for Science and International Affairs, Harvard Kennedy School, 9 Mar. 2023, www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose
71. “Facebook Allows War Posts Urging Violence against Russian Invaders | Reuters.” Accessed September 27, 2025. https://www.reuters.com/world/europe/exclusive-facebook-instagram-temporarily-allow-calls-violence-against-russians-2022-03-10/.
72. Erwin, Sandra. “Satellite Imaging Companies Increase Profile as They Track Russia’s Invasion of Ukraine.” SpaceNews, 28 Feb. 2022.
73. Kyiv Post. “WATCH: Ukrainian Drone Destroys Russian Tank Hidden in Industrial Building.” Kyiv Post, 20 Apr. 2025, www.kyivpost.com/post/51129

Endnotes

74. Mamedov, Intigam. “A Fragile Narrative: Transformations and Consistency in the Russian Representation of the War in Ukraine.” Media, War & Conflict, vol. 18, no. 3, 2025, pp. 383–399, doi:10.1177/17506352241264436.
75. Global Engagement Center. RT and Sputnik’s Role in Russia’s Disinformation and Propaganda Ecosystem. U.S. Department of State, 20 Jan. 2022, 2021-2025.state.gov/report-rt-and-sputniks-role-in-russias-disinformation-and-propaganda-ecosystem/.
76. “Diane Chotikul, The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study, July 1986. Unclassified. | National Security Archive.” Accessed September 27, 2025.
77. Stephan, Maria J. “It’s Time to Take Inspiration from Ukraine and Double Down on Global Democratic Solidarity.” The Horizons Project, written by Maria J. Stephan and first published on Waging Nonviolence, 9 Mar. 2022, horizonsproject.us/its-time-to-take-inspiration-from-ukraine-and-double-down-on-global-democratic-solidarity-url/.
78. Blue, Charles. “Disinformation: Misinformation’s Evil Twin.” Psychological Science Observer, Association for Psychological Science, 29 Apr. 2022, www.psychologicalscience.org/observer/disinformation-misinformation
79. Harding, Luke. “‘Russian Warship, Go Fuck Yourself’: What Happened Next to the Ukrainians Defending Snake Island?” The Guardian, 19 Nov. 2022, www.theguardian.com/world/2022/nov/19/russian-warship-go-fuck-yourself-ukraine-snake-island
80. Hamarowski, Bartosz, and Maria Lompe. “Digital Witnesses to the Crime: Visual Representation of the Bucha Massacre Across Social Media Platforms.” Media, War & Conflict, vol. 17, no. 1, 2024, SAGE Publications, https://doi.org/10.1177/17506352241243302
81. Brewster, Thomas. “Ukraine Starts Using Facial Recognition to Identify Dead Russians and Tell Their Relatives.” Forbes, 23 Mar. 2022, www.forbes.com/sites/thomasbrewster/2022/03/23/ukraine-starts-using-facial-recognition-to-identify-dead-russians-and-tell-their-relatives/
82. Bhuiyan, Johana. “Ukraine Uses Facial Recognition Software to Identify Russian Soldiers Killed in Combat.” Technology. The Guardian, March 24, 2022. https://www.theguardian.com/technology/2022/mar/24/ukraine-facial-recognition-identify-russian-soldiers.
83. Romandash, Anna. Digital Warfare and Peace: Learning from Ukraine’s Response to the Russian Invasion. Policy Brief No. 158, Toda Peace Institute, May 2023, toda.org/assets/files/resources/policy-briefs/t-pb-158_digital-warfare-and-peace_romandash.pdf.
84. Presl, Dominik. “Russia Is Winning the Global Information War.” Royal United Services Institute (RUSI), 7 May 2024, www.rusi.org/explore-our-research/publications/commentary/russia-winning-global-information-war
85. Bertelsmann Stiftung. Russia Country Report 2024. BTI Transformation Index (BTI) 2024, Bertelsmann Stiftung, 2024, www.bti-project.org/en/reports/country-report/RUS
86. Landay, Jonathan. “U.S. Intelligence Assesses Ukraine War Has Cost Russia 315,000 Casualties.” Reuters, 12 Dec. 2023, www.reuters.com/world/us-intelligence-assesses-ukraine-war-has-cost-russia-315000-casualties-source-2023-12-12/
87. Treyger, Elina, et al. The Denazify Lie: Russia’s Use of Extremist Narratives Against Ukraine. RAND Corporation, 2025, www.rand.org/content/dam/rand/pubs/research_reports/RRA3400/RRA3450-1/RAND_RRA3450-1.pdf
88. United Kingdom, Foreign, Commonwealth & Development Office, and Dame Barbara Woodward GCMG OBE. “UN General Assembly Vote on Russian Aggression Against Ukraine, 2 March 2022: UK Statement.” Gov.uk, 2 Mar. 2022, https://www.gov.uk/government/speeches/international-pressure-will-not-relent-until-every-russian-soldier-is-out-of-ukraine
89. Nadkarni, Vidya, et al. “Forum: The Russia–Ukraine War and Reactions from the Global South.” The Chinese Journal of International Politics, vol. 17, no. 4, 2024, pp. 449–489, https://doi.org/10.1093/cjip/poae021
90. Human Rights Watch. “Ukraine: Russian Forces’ Trail of Death in Bucha.” Human Rights Watch, 21 Apr. 2022, https://www.hrw.org/news/2022/04/21/ukraine-russian-forces-trail-death-bucha
91. Fredheim, Rolf, Anneli Ahonen, and James Pamment. Denying Bucha: The Kremlin’s Influence Tactics in the Aftermath of the 2022 Bucha Atrocity. Psychological Defence Research Institute Working Paper 2023:1, Lund University, Dec. 2023, https://www.psychologicaldefence.lu.se/sites/psychologicaldefence.lu.se/files/2023-12/Denying%20Bucha_0.pdf

Endnotes

92. Fredheim, Rolf, Anneli Ahonen, and James Pamment. Denying Bucha: The Kremlin's Influence Tactics in the Aftermath of the 2022 Bucha Atrocity. Psychological Defence Research Institute Working Paper 2023:1, Lund University, Dec. 2023, https://www.psychologicaldefence.lu.se/sites/psychologicaldefence.lu.se/files/2023-12/Denying%20Bucha_0.pdf
93. Doyle, Gerry. "Satellite Images Show Civilian Deaths in Ukraine Town While It Was in Russian Hands." Reuters, 5 Apr. 2022, https://www.reuters.com/world/europe/satellite-images-show-civilian-deaths-ukraine-town-while-it-was-russian-hands-2022-04-05/
94. Kramer, Andrew E. "Bodies of Civilians Lie in Streets of Bucha, Ukraine, After Russian Forces Retreat." The New York Times, 4 Apr. 2022, https://www.nytimes.com/2022/04/04/world/europe/bucha-ukraine-bodies.html
95. Arndt, Anna Clara, and Liviu Horovitz. Nuclear Rhetoric and Escalation Management in Russia's War Against Ukraine: A Chronology.Working Paper No. 03, Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, 2022, https://www.swp-berlin.org/publications/products/arbeitspapiere/Arndt-Horovitz_Working-Paper_Nuclear_rhetoric_and_escalation_management_in_Russia_s_war_against_Ukraine.pdf
96. Council of the European Union. "EU Adopts Fifth Round of Sanctions Against Russia Over Its Military Aggression Against Ukraine."Consilium, 8 Apr. 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/04/08/eu-adopts-fifth-round-of-sanctions-against-russia-over-its-military-aggression-against-ukraine/
97. Chapman, Colin. "After the Horror of Bucha, NATO Remains Unwilling to Prepare for War." Australian Institute of International Affairs – Australian Outlook, 8 Apr. 2022, https://www.internationalaffairs.org.au/australianoutlook/after-the-horror-of-bucha-nato-remains-unwilling-to-prepare-for-war/
98. Caceres, Maria Mercedes Ferreira, et al. "The Impact of Misinformation on the COVID-19 Pandemic." AIMS Public Health, vol. 9, no. 2, 12 Jan. 2022, pp. 262–277, PubMed Central, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9114791/
99. SPYSCAPE. "Inside Russia's Notorious 'Internet Research Agency' Troll Farm." SPYSCAPE, https://spyscape.com/article/inside-the-troll-factory-russias-internet-research-agency
100. Iasiello, Emilio. "Cognitive Warfare in Cyberspace: A Brief Look at China, Russia, and the United States." OODA Loop, OODAloop.com, https://oodaloop.com/analysis/decision-intelligence/cognitive-warfare-in-cyberspace-a-brief-look-at-china-russia-and-the-united-states/
101. Kivinen, Kari, and Eva-Maria Verfürth. "How Finland Is Preparing Its Citizens for a World Swamped by Fake News." D+C/Development and Cooperation, 24 June 2025.
102. Romanishyn, Alexander, et al. "AI-Driven Disinformation: Policy Recommendations for Democratic Resilience." Frontiers in Artificial Intelligence, vol. 8, 31 July 2025, Article 1569115, PubMed Central (PMC), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC12351547/
103. Kang, Hongzhaoning, et al. "Theory and Application of Zero Trust Security: A Brief Survey." Entropy, vol. 25, no. 12, 28 Nov. 2023, Article 1595, PubMed Central (PMC10742574), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10742574/
104. Chittaro, Luca, and Nicola Zangrando. "The Persuasive Power of Virtual Reality: Effects of Simulated Human Distress on Attitudes towards Fire Safety." pp. 58–69, https://doi.org/10.1007/978-3-642-13226-1_8
105. Tussyadiah, I. P., Dan Wang, T. H. Jung, and M. C. Tom Dieck. "Virtual Reality, Presence, and Attitude Change: Empirical Evidence from Tourism." Tourism Management, vol. 66, 2018, pp. 140–154, https://doi.org/10.1016/j.tourman.2017.12.003
106. Boine, Claire. "The AI Manipulation Gap." SSRN, 1 June 2021, http://dx.doi.org/10.2139/ssrn.4042321
107. Valtonen, Vesa, and Minna Branders. Tracing the Finnish Comprehensive Security Model. 2020, https://www.doria.fi/bitstream/handle/10024/186608/tracing.pdf?sequence=1
108. Kaska, K., A. M. Osula, and J. Stinissen. The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis. NATO Cooperative Cyber Defence Centre of Excellence, Oct. 2018, https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf
109. European Commission. "Digital Services Act." Shaping Europe's Digital Future, digital-strategy.ec.europa.eu/en/policies/digital-services-act.
110. Meta Platforms, Inc. "Meta Reports Fourth Quarter and Full Year 2023 Results; Initiates Quarterly Dividend." Meta Investor Relations, 1 Feb. 2024, https://investor.atmeta.com/investor-news/press-release-details/2024/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend/default.aspx

Endnotes

111. IANS. “Google Posts $307 bn Revenue in 2023, Spent Billions of Dollars to Lay People Off.” The Economic Times – HR, 31 Jan. 2024, https://hr.economictimes.indiatimes.com/news/workplace-4-0/talent-management/google-posts-307-bn-revenue-in-2023-spent-billions-of-dollars-to-lay-people-off/107285579

112. Iwaya, Leonardo Horn, Ala Sarah Alaqra, Marit Hansen, and Simone Fischer-Hübner. “Privacy Impact Assessments in the Wild: A Scoping Review.” Array, vol. 23, Sept. 2024, article 100356, ScienceDirect, https://doi.org/10.1016/j.array.2024.100356

113. Goldberg, Mark Leon. “When Treaties Work: The Chemical Weapons Convention.” Global Dispatches, 6 Jan. 2025, https://www.globaldispatches.org/p/when-treaties-work-the-chemical-weapons

114. “Paris Call for Trust and Security in Cyberspace.” Paris Peace Forum, Paris Peace Forum, 12 Nov. 2018 (launch date), https://parispeaceforum.org/initiatives/paris-call-for-trust-and-security-in-cyberspace/

C-21, 3rd Floor, Qutub Institutional Area, New Delhi, India - 110016.
Phone: 011-43104566 | Email: office@csdronline.com | Web: www.csdronline.com | Twitter:@CSDR_India