

DISINFORMATION
PROPAGANDA



CONSPIRACY
THEORY

War is a mind game: countering weaponised information

No. 01 January 2026

Marek Havlík, Jiří Horáček¹

Center for Advanced Studies of Brain and Consciousness, National Institute of Mental Health, Klecany, and Third Faculty of Medicine, Charles University, Prague, Czech Republic.

Cognitive warfare is rapidly becoming a central focus in discussions on the nature of modern and future conflicts. Despite the absence of a precise definition, experts from both military and academic circles agree on several fundamental aspects. At its core, the battlefield of cognitive warfare is the *human brain* and its *cognitive processes*.² The weapons deployed on this battle-

Summary

Cognitive warfare is the weaponisation of information that exploits natural cognitive vulnerabilities to disrupt, manipulate and control individuals' perceptions of reality.

NATO's current countermeasures, such as pre-bunking, strategic communications, and trust-building efforts, don't fully address the deeper psychological and cognitive vulnerabilities targeted in cognitive warfare.

In addition to common cognitive vulnerabilities like emotions, cognitive biases, and uncertainty, other critical traits are being exploited on the cognitive battlefield to manipulate and control vulnerable individuals.

¹ The work on this paper was supported by the OP JAK, MŠMT, reg. no. CZ.02.01.01/00/23_025/0008715 ("Social and Cultural Determinants of the Impact of Circulating Representations on Human Mind, and Strategies of Remediation"). This work was also supported by Ministry of Health of the Czech Republic under grant no. NU22-D-132, and Czech Science Foundation under grant no. 20-13458S. Cooperatio Neurosciences, Charles University, Third Faculty of Medicine; MEYS, LRI CZECRIN (LM2023049).

² Allied Command Transformation, "Allied Command Transformation Develops the Cognitive Warfare Concept to Combat Disinformation and Defense Against 'Cognitive Warfare'," 3 July 2024, <https://www.act.nato.int/article/cogwar-concept/>; "Protecting the Alliance Against the Threat of Cognitive Warfare," <https://www.act.nato.int/activities/cognitive-warfare/>; "Cognitive Warfare: Strengthening and Defending the Mind," 5 April 2023, <https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/>.

OUTLOOK

field are diverse and potent, including disinformation, an aggressor's propaganda, the deliberate spread of conspiracy theories, social media manipulation, micro-targeted political messaging, the strategic use of bots, and more, all part of weaponized information activities.³

NATO recognizes the serious threats posed by these tools of cognitive manipulation, as well as the aggressors' goals. These include undermining societal cohesion, weakening democratic processes, and eroding liberal values by fostering polarization and fragmentation within societies. They also seek to facilitate fringe political parties, destabilize international organizations like the EU and NATO, and steer individuals and groups into decisions that benefit the aggressor, often by influencing cognition without their awareness – a tactic known as reflexive control.⁴ On an individual level, weaponized information contributes to a decline in mental well-being, fosters frustration, and radicalizes vulnerable individuals.

However, the ultimate goal of weaponized information is to distort or even completely reshape an individual's perception of reality in alignment with the aggressor's strategic objectives. For example, the Russian Federation uses weaponized disinformation to weaken its geopolitical adversaries, sow division, and strengthen its own position on the international stage (see e.g. the methods in Figure 1). In response, NATO and its member states are actively working to enhance the cognitive security of their civilian populations and military personnel. These efforts aim to prevent foreign aggressors from achieving their strategic goals: *the disruption, manipulation, and control of individuals' perceptions of reality*.

The fight so far: how NATO combats weaponized information

Unlike authoritarian regimes, democratic states and alliances face significant disadvantages on the cognitive battlefield. Their commitment to freedom of information, diversity of opinion, and minimal censorship creates an environment that enables the easy spread of weaponized information by foreign adversaries. The rise of artificial intelligence (AI) has further amplified this challenge by enabling the creation and dissemination of tailored disinformation at an unprecedented scale and speed.

A prominent illustration of this emerging threat is the 2024 Romanian presidential election. This election was marked by widespread cyber intrusions, coordinated influence campaigns and strategic social media manipulation, which collectively targeted the integrity of the electoral process. The campaign of a pro-Russian candidate relied extensively on artificially inflated support, the employment of paid influencers, and the use of bots and disinformation networks to spread false narratives and amplify engagement. The tactics employed – such as micro-targeted political messaging, astroturfing (a deceptive tactic using a fake grassroots movement), and the creation of viral challenges – were explicitly designed to target vulnerable demographics, including young people, rural voters, and conspiracy theorists, all of whom were disillusioned with traditional political structures. The culmination of these manipulative tactics, coupled with evidence of broader foreign interference by the Russian Federation, led to the annulment of the election's first round.⁵

This unprecedented event underscores the growing power of social media in shaping electoral outcomes and highlights the ability of foreign actors to influence public opinion through digital platforms. It also emphasizes the role of the digital ecosystem in cognitive warfare, as similar strategies were employed in the 2016 U.S. Presidential Election and the Brexit referendum.⁶

Alongside other geopolitical adversaries like Iran and China, Russia has emerged as NATO's most active and primary opponent on the cognitive battlefield, employing its "Firehose of Falsehood" strategy to disseminate weaponized disinformation on a massive scale with the goal to confuse and overwhelm. Since the annexation of Crimea in 2014, NATO has observed an unprecedented increase in Russian information operations aimed at destabilizing societies and eroding trust in NATO, its allies and democratic institutions.⁷

NATO's approach to counter weaponized information is multi-faceted, as NATO's strategy for countering disinformation involves a wide range of activities and evolves on daily basis. One of the most important strategies to counter Russian disinformation is the NATO Toolbox 2021, a systematic and comprehensive package for Countering Hostile Information Activities. This document follows the strategy of "understand" and "engage" and provides member countries with resources to assess and counter information threats, including weaponized information.⁸ "Setting the Record Straight" focuses on

³ In this article, the term "weaponized information" is used as an umbrella term encompassing all hostile information operations and activities employed by foreign aggressors on the cognitive battlefield, designed to influence, alter, and control the cognition of individuals or populations over the long term. It exploits cognitive vulnerabilities and biases in a subtle way. In contrast, PSYOPS (Psychological Operations) focuses on short-term influence to achieve immediate goals such as demoralization or surrender, without seeking deeper, systematic changes in cognition.

⁴ One of the key strategic objectives of cognitive warfare is not simply to misinform, but to steer population into making decisions that serve the attacker's interests. This reflects the Soviet-born concept of reflexive control, which means influencing an opponent's perceptions, so they act in ways that benefit the initiator, often without realizing it. In modern information environments, this is done through narrative framing, selective exposure to information, and manipulating trust: Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies*, 17(2), 2024, 237-256.

⁵ Georgiana Camelia Stănescu, "Fake News, Bots, and Influencers: The Impact of Social Media on Romania's 2024 Elections," *Social Sciences and Education Research Review*, Volume 11, Issue 2/2024, 361-366.

⁶ Hunk Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," *Working Paper 23089*, National Bureau of Economic Research, 2017, <https://doi.org/10.3386/w23089>.

⁷ Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model," *Perspectives*, RAND Corporation, https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.

⁸ "NATO and Countering Disinformation – The Need For a More Proactive Approach From the Member States," GLOBSEC, 16 May 2022, <https://www.globsec.org/sites/default/files/2022-05/NATO-and-Countering-Disinformation-ver1-spreads.pdf>.

debunking Russian disinformation and the dissemination of accurate information in multiple languages, including Russian (e.g. see Figure 1).⁹ However, the debunking is often ineffective. Therefore, NATO is also focusing on pre-bunking. This strategy of inoculation is a proactive approach to ward against future disinformation with the goal of taking away their traction before they even appear in the information space.¹⁰

To complement these efforts, the NATO Strategic Communications Centre of Excellence (NATO StratCom COE) plays a pivotal role. Founded in 2014, it serves as a crucial hub for research, analysis, and practical solutions aimed at enhancing NATO's strategic communications capabilities. This includes efforts to counter disinformation and hostile information operations, as well as developing strategies, tactics, methodologies, and techniques to predict and counter such type of warfare.¹¹

In addition, NATO invests significantly in building trust by openly sharing information as a means of actively fostering trust among allies and the public, which is essential for countering weaponized information. NATO transparently and consistently shares detailed information about its activities and plans. This includes publishing schedules for NATO and Allied military exercises well in advance. The organization's commitment to accountability is further demonstrated through the annual release of civilian and military budget totals, along with other financial data.¹² Cooperation with international organizations, such as the EU and the UN, is also a key element of NATO's strategy. These partnerships enable the exchange of information, best practices, and innovative approaches to combating disinformation.¹³ The Alliance actively communicates with the public through diverse channels, including social media, media outreach, and its official NATO website. It places a strong emphasis on the value of free and independent media, which empowers journalists to pose critical questions and thoroughly verify their sources.¹⁴ NATO actively collaborates with free and independent media as this strategy builds trust of the public and builds additional resilience against weaponized information with accurate information.¹⁵

As concerns research, NATO provides grants to non-governmental organizations, universities, and other research institutions to support and fund projects specifically targeting disinformation, cognitive threats, and

information warfare.¹⁶ This is necessary given the unprecedented technological development of artificial intelligence (AI). Deepfakes and other AI-driven information threats in the hands of foreign aggressors pose one of the gravest challenges for NATO and its efforts on the cognitive battlefield.¹⁷ This new tool in the hands of foreign aggressors presents a significant challenge for NATO and underscores the need for new strategies to mitigate such threats to human cognition.

In July 2024, NATO unveiled its AI strategy, emphasizing the urgency of addressing the growing risks of AI-driven disinformation and information operations while accelerating the safe and responsible integration of AI technologies across the Alliance. The strategy also highlights the challenges posed by the lack of proper data and governance standards in combating the spread of disinformation.¹⁸ Future solutions to mitigate the dangers of AI-driven disinformation may rely on a three-pillar approach that combines technological, regulatory, and educational efforts.¹⁹ Defensive AI and machine learning will play a crucial role in combating AI-weaponized information by detecting, flagging, and classifying false information across platforms with real-time alerts. National laws will emphasize transparency and accountability in AI, but must also evolve to address issues such as liability and enforceable penalties. Media literacy and critical thinking education should be integrated into school curricula from a young age to teach students how to evaluate sources, identify disinformation, and safeguard their cognition from manipulation.²⁰

While the dangers and stakes are known and efforts are being deployed, NATO and Western democracies have yet to prepare a coherent, comprehensive and coordinated response to counter weaponized Russian information.²¹ Without a concept of cognitive deterrence or any possibility of open cognitive retaliation against cognitive aggressors, the only viable option for democratic nations and alliances is to focus on protective measures and securing cognitive resources. However, NATO strategies to face weaponized information lack an essential element: *the cognitive pillar*, which is an essential component that cannot be overlooked when addressing the cognitive battlefield. The prospect of AI-driven disinformation generating thousands of false narratives on a daily basis to overwhelm the media ecosystem is alarming in itself, but even more con-

⁹ "NATO and Countering Disinformation," GLOBSEC.

¹⁰ NATO, "NATO's Approach to Counter Information Threats," 3 February 2025, https://www.nato.int/cps/en/natohq/topics_219728.htm; Sander Van der Linden, *Foolproof: Why Misinformation Infects Our Minds And How To Build Immunity*, W. W. Norton & Company, 2024.

¹¹ Allied Command Transformation, "NATO Centres of Excellence – NATO Strategic Communications Centre of Excellence," 24 July 2023, <https://www.act.nato.int/article/nato-stratcom-coe/>.

¹² NATO, "Transparency and Accountability," 20 December 2024, https://www.nato.int/cps/en/natohq/topics_111582.htm.

¹³ NATO, "Relations With the United Nations," 25 July 2023, https://www.nato.int/cps/en/natohq/topics_50321.htm.

¹⁴ NATO, "NATO's Approach To Counter Information Threats," NATO website, updated 3 February 2025, <https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats>; NATO, "Countering Hybrid Threats," NATO website, updated 7 May 2024, <https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats>.

¹⁵ NATO, "NATO Exercises," 27 July 2023, https://www.nato.int/cps/en/natohq/topics_49285.htm.

¹⁶ Research Connect, "NATO Public Diplomacy Division Co-Sponsorship Grants Call for Applications Increasing Societal Resilience," <https://www.myresearchconnect.com/nato-public-diplomacy-division-co-sponsorship-grants-call-for-applications-increasing-societal-resilience/>.

¹⁷ Patrick Samaha, "Weaponized AI: The New Frontline In Global Disinformation Warfare," NATO Association of Canada, 24 June 2025, <https://natoassociation.ca/weaponized-ai-the-new-frontline-in-global-disinformation-warfare/>.

¹⁸ NATO, "Summary of NATO's Revised Artificial Intelligence (AI) Strategy," 10 July 2024, https://www.nato.int/cps/en/natohq/official_texts_227237.htm.

¹⁹ Ann M. Fitz-Gerald and Halyna Padalko, "The Need for a Strategic Approach to Disinformation and AI-Driven Threats," 25 July 2024, <https://www.rusi.org/explore-our-research/publications/commentary/need-strategic-approach-disinformation-and-ai-driven-threats>.

²⁰ Fitz-Gerald and Padalko, "The Need For a Strategic Approach to Disinformation and AI-Driven Threats."

²¹ GLOBSEC, "NATO and Countering Disinformation."

cerning is the likelihood that AI will increasingly exploit natural cognitive vulnerabilities, crafting disinformation specifically tailored to manipulate and alter individuals' perception of reality.

The cognitive pillar: bringing cognition to the cognitive battlefield

While NATO, particularly through its Allied Command Transformation (ACT), has made significant progress in addressing the strategic importance of the cognitive domain, the deeper mechanisms of human cognition remain a complex challenge.²² Although NATO's defensive strategies have advanced, they are still in the early stages of fully addressing these intricate cognitive processes.

Natural cognitive vulnerabilities

The human brain and overall cognition are highly susceptible to being hacked due to numerous cognitive vulnerabilities. Many of these vulnerabilities stem from unconscious brain processes, far away from our conscious awareness and beyond the control of our conscious will. Other vulnerabilities are natural byproducts of the brain's evolutionary design, which prioritizes survival and immediate reactions over digital literacy and emotional detachment from information. Moreover, even our consciousness lacks the ability to control the brain's perceptual pathways and determine its perceptual stimulation. In other words, there are no will-activated filters to block external stimuli, leaving individuals with a limited capacity to filter incoming information or even dictate the brain's immediate reactions. Emotional triggers are one of the best examples of such immediate brain reactions. Fear, anger, and even hope can be used to bypass rational thinking, making people more receptive to disinformation and its goal.²³ It can also provoke anger by presenting information that is perceived as unfair, unjust, or offensive, and exploit desire for hope by offering simple solutions to complex problems or promising positive outcomes in unlikely scenarios.²⁴

Emotions are not the only vulnerabilities that bypass rational thinking. Cognitive biases, the systematic errors in rational thinking, are also cognitive vulnerabilities. People

naturally seek out and agree with information that aligns with their pre-existing beliefs while neglecting or dismissing information that contradicts them (Confirmation Bias). People believe and give credibility to specific information just because many other people believe it (Bandwagon Effect). People rely heavily on the first piece of information they receive on a topic, even if it is false, inaccurate or misleading (Anchoring Bias) and believe more in information they encounter repeatedly (Familiarity Bias).

Also, brains love to explain. It is natural for them to create links between external stimuli, internal world and individual behaviour. Studies on patients with "split brain" have shown that the left hemisphere plays an essential role in interpreting and explaining human behaviour. The left side of the brain systematically constructs causal chains of explanations to better understand the world to ensure a sense of coherence by continuously linking new information with past experiences.²⁵ Its natural tendency is to constantly form causal connections between events, without much consideration whether their conclusions are truthful or entirely fabricated.

Another inherent characteristic of the brain is its preference for homeostasis, or the maintenance of stability. The brain aims to increase its chances of survival by predicting future events as accurately as possible to improve its odds. Therefore, it prefers a stable environment where unpredictable changes do not occur on a daily basis. Surprises and unexpected events pose challenges, as they do not align with the brain's expectations, leading to increased stress and cognitive load. Disinformation often exploits such unpredictability – especially during global events such as pandemics or terrorist threats – creating climate of fear, anxiety and uncertainty.²⁶ During these "surprise" moments, the brain's vulnerability to disinformation increases, especially when such messages promise safety and security, as it attempts to adjust to changes as quickly as possible even at the cost of false or misleading explanation.²⁷

These natural characteristics of the brain and human consciousness can serve as gateways for cognitive hacking that cannot be closed. However, successful cognitive hacking is not guaranteed solely by exploitation of these vulnerabilities. While a future comprehensive NATO strategy of cognitive defence should consider these, it has to consider others as well. To raise primary defences against weaponized information and cognitive hacking, strategy must consider cognitive predispositions to cognitive hacking and not so well-known cognitive vulnerabilities that can be targeted by AI-tailored disinformation.

²² Allied Command Transformation, "Allied Command Transformation Develops The Cognitive Warfare Concept."

²³ Brian E. Weeks, "Emotions, Partisanship, and Misperceptions: How Anger and Anxiety Moderate the Effect of Partisan Bias on Susceptibility to Political Misinformation," *Journal of Communication*, 65(4), 699-719. <https://doi.org/10.1111/jcom.12164>; William J. Brady, Julian A. Wills, John T. Jost and Jay J. Van Bavel, "Emotion Shapes the Diffusion of Moralized Content in Social Networks," *Proceedings of the National Academy of Sciences of the United States of America*, 114(28), 7313-7318, 2017, <https://doi.org/10.1073/pnas.1618923114>; Cameron Martel, Gordon Pennycook, and David G. Rand, "Reliance on Emotion Promotes Belief in Fake News," *Cognitive Research: Principles and Implications*, 5, 47, 2020, <https://doi.org/10.1186/s41235-020-00252-3>.

²⁴ Shalini Munusamy et al., "Psychological Factors Contributing to the Creation and Dissemination of Fake News Among Social Media Users: A Systematic Review," *National Library of Medicine*, <https://pmc.ncbi.nlm.nih.gov/articles/PMC11575416/>.

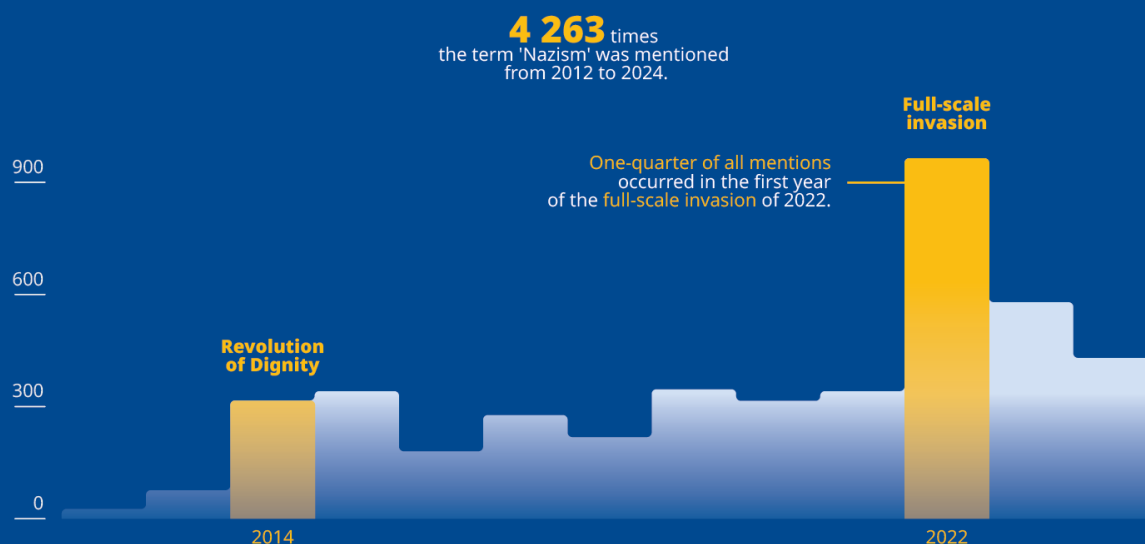
²⁵ Michael S. Gazzaniga, *The Social Brain: Discovering the Networks of the Mind*, Basic Books, November 1985.

²⁶ Achim Peters et al., "Uncertainty And Stress: Why it Causes Diseases And How It Is Mastered by the Brain," *Progress in Neurobiology*, 156, 164-188, <https://pubmed.ncbi.nlm.nih.gov/28576664/>; Peter McEvoy and Alison E. J. Mahoney, "To Be Sure, To Be Sure: Intolerance of Uncertainty Mediates Symptoms of Various Anxiety Disorders and Depression," *Behavior Therapy*, 43(3), 533-545, <https://pubmed.ncbi.nlm.nih.gov/22697442/>.

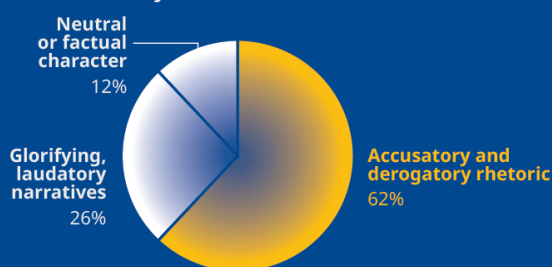
²⁷ Kelly M Greenhill and Ben Oppenheim, "Rumor Has It: The Adoption of Unverified Information in Conflict Zones," *International Studies Quarterly*, Volume 61, Issue 3, September 2017, Pages 660-676; Michael Golebiewski, danah boyd, "Data Voids: Where Missing Data Can Easily Be Exploited," *Data & Society*, 2019.

RUSSIAN NARRATIVES ON UKRAINE

News Dynamics with the Mention of the Word 'Nazism'



Distribution of Mentions by Connotation



Key Patriotic Narratives of Russia

Russia is saving Ukraine from **Nazism** by liberating oppressed Ukrainians

39%

Russia defends historical truth about WWII and won't allow it to be rewritten

17%

Russians preserve sacred memory of **Nazism's** victims

16%

The USSR single-handedly resisted **Nazism** and liberated Europe

13%

Russia actively combats **Nazi movements** inside the country

8%

Russia acknowledges allies' contribution to the common victory over **Nazism**

5%

Russia defends its borders from Ukrainian **Nazi incursions**

2%

Key Anti-Ukrainian Narratives from Russia

Ukrainian **Nazis** brutally treat civilians

29%

Ukrainians rewrite history and invent dissent

17%

Ukraine is ruled by a **Nazi regime**

14%

Nazi actions are a common phenomenon in modern Ukraine

14%

The Ukrainian government pleases **neo-Nazi groups**

9%

Ukrainians collaborated with **Nazis** during World War II

8%

Ukrainian opposition openly supports **Nazis**

5%

Ukrainian oligarchs use **neo-Nazis** as private armies

2%

Ukrainian Nazis are worse than Third Reich soldiers

1%

Sensible Ukrainians do not want to live under **Nazi rule**

1%

Figure 1. Russian narratives on Ukraine
Data: Babyn Yar Holocaust Memorial Center, 2025

Ideal cognitive targets

While the aforementioned vulnerabilities are inherent to all human brains, the following vulnerabilities are unique to certain individuals. These include specific cognitive traits and needs that make individuals particularly susceptible to foreign weaponized information. See Table 1 for an overview.

Cognitive rigidity

For a foreign cognitive aggressor, the most ideal targets are individuals with high levels of cognitive rigidity. Cognitive rigidity, also known as cognitive inflexibility, refers to the difficulty in adapting to new or changing environments and switching between different modes of thinking. These individuals hold an unwavering certainty in their beliefs, making them highly resistant to change and less likely to accept alternative perspectives.²⁸

People vary in their levels of cognitive rigidity, but it is especially prevalent among extremists, both on the political left and right, as well as those inclined toward nationalism, authoritarianism, and religious conservatism. These individuals often struggle to process socio-political arguments, tolerate ambiguity, or consider alternative explanations. Cognitive rigidity is also closely associated with right-wing

authoritarianism, conspiracy theory belief, dogmatism, and a black-and-white view of the world.²⁹

A more alarming aspect of cognitive rigidity is its link to extremism, support for violence, and a readiness to die for ideologies or one’s group.³⁰ Once individuals with high cognitive rigidity adopt the aggressor’s worldview, shifting their perceptions becomes exceedingly difficult. They not only fall victim to cognitive manipulation but also become valuable assets for the aggressor.

In this context, weaponized information often takes the form of a carefully constructed narrative, which is essential for the aggressor and its actions. A narrative is one of the three key pillars of radicalization, designed to instil fear, evoke righteous anger that leads to action, build confidence in decision-making, and define worthy goals and actions to pursue.³¹ By offering simple, black-and-white solutions, the narrative assigns blame and responsibility for perceived conflicts, outlines preferred courses of action, and provides a moral high ground not only for the aggressor, but also for individual extremist activities.³² Narratives are particularly dangerous as they can create an environment that legitimizes violence and extremism, offering individuals a pathway to glory and in-group appreciation.³³

When an aggressor successfully applies such a narrative, for example, a narrative of victimhood or Russophobia, the aggressor can hijack the cognition and actions of vulnerable individuals with cognitive rigidity. These individ-

Table 1:

Cognitive Trait	Manifestation	Vulnerability
Cognitive Rigidity	Resistance to ambiguity, difficulty updating beliefs	Prone to belief persistence, less receptive to corrective information
Need for Uniqueness	Preference for distinctiveness, aversion to conformity	Drawn to fringe theories, “hidden truth” narratives
Need for Self-Significance	Motivated by status, meaning, or recognition	Susceptible to identity-enhancing propaganda or hero/victim frames
Need for Cognitive Closure	Urge for certainty, discomfort with ambiguity	Attracted to simple, absolute narratives and rapid judgments

This table synthesizes a set of cognitive traits that we linked to heightened vulnerability to weaponized information of cognitive warfare. For each trait, we identify the primary manifestation and vulnerability. Recommendations are as follow.

- 1) *Cognitive Rigidity:* Use stepwise reframing and affirmation priming to avoid triggering defensiveness; expose contradictions gradually.
- 2) *Need for Uniqueness:* Present truth-aligned content as rare knowledge or elite insight, appeal to autonomy and critical thinking.
- 3) *Need for Self-Significance:* Reframe counter-narratives to provide alternative ways to feel impactful (e.g. “defenders of truth”, “protectors of community”).
- 4) *Need for Cognitive Closure:* Offer structured, simplified narratives that still align with factual content; avoid excessive ambiguity in messaging.

²⁸ Helena García-Mieres et al., “Placing Cognitive Rigidity In Interpersonal Context In Psychosis: Relationship With Low Cognitive Reserve and High Self-Certainty,” *Frontiers in Psychiatry*, 11, November 2020, <https://pubmed.ncbi.nlm.nih.gov/33324260/>.

²⁹ Leor Zmigrod, “The Role of Cognitive Rigidity in Political Ideologies: Theory, Evidence, and Future Directions,” *Current Opinion in Behavioral Sciences*, 34, 34-39, <https://www.sciencedirect.com/science/article/pii/S2352154619301147>.

³⁰ Leor Zmigrod et al., “Cognitive Inflexibility Predicts Extremist Attitudes,” *Frontiers in Psychology*, 10, 2019, <https://pubmed.ncbi.nlm.nih.gov/31133930/>.

³¹ Arie Kruglanski et al., *The Three Pillars of Radicalization: Needs, Narratives, and Networks*, Oxford University Press, USA, 2019.

³² Noémie Bouhana and Per-Olof Wikström, “Theorizing Terrorism: Terrorism As Moral Action: A Scoping Study,” *Contemporary Readings in Law and Social Justice*, 2(2), 9, 2010.

³³ Arie Kruglanski et al., “The Making of Violent Extremists,” *Review of General Psychology*, 22(1), 107-120, 2018.

uals, driven by an unwavering belief in the narrative, can become assets for the aggressor simply by disseminating the disinformation created by the aggressor, or justifying the aggressor's actions. In more extreme scenarios, driven by an unwavering belief in the narrative, individuals may feel compelled to act against the out-group, often targeting their own government, media, or those with differing opinions. Their deep conviction can lead to a willingness to harm others and even to sacrifice their own lives for the cause, as they embrace violence in service of their ideology.³⁴ In this way, they contribute to the broader effort of manipulation, becoming instruments of the aggressor's strategy without fully recognizing their role in it. Thus, the manipulation of the narrative becomes a powerful tool in cognitive warfare, shaping perceptions, inciting extremist actions, and using individuals as conduits for disinformation.

Need for uniqueness

The "need for uniqueness" refers to an individual's cognitive desire to differentiate themselves from others and stand out from the crowd.³⁵ People with a heightened sense of this need often display a strong interest in rare products, exotic experiences, and unconventional beliefs, particularly conspiracy theories, which they see as rare "possessions" that reflect their originality and uniqueness. Empirical studies show that those who believe in conspiracy theories frequently feel they have access to exclusive, little-known information about global events.³⁶

In the context of cognitive warfare, an increased need for uniqueness represents a cognitive vulnerability. It not only aids in sustaining the aggressor's worldview within the individual's mind but also supports its further spread. If weaponized information successfully appeals to the narcissism of vulnerable individuals and bolsters their grandiose self-concept, the likelihood that these individuals will not only strengthen their belief in such narratives but also promote them to others increases. This allows them to project their originality by presenting unorthodox or "hidden" explanations, which showcases their uniqueness.³⁷

In doing so, the vulnerable individual becomes an asset, consciously or unconsciously, for spreading the aggressor's worldview. However, this may also lead to their social isolation, especially when their unique narratives are not accepted or significantly diverge from that of their peers. The cognitive aggressor can further exploit this by offering a sense of belonging to an alternative group or ideology,

deepening the individual's isolation from mainstream society and reinforcing radical beliefs and extremist behaviour.

Self-significance

The "need for significance" is a fundamental human desire to feel that our lives have meaning and that we are important. All people have an innate longing to feel significant, to earn respect, and to create their own identities.³⁸ Significance also encompasses other essential needs for human existence, such as competence and life purpose. People tend to lose their sense of significance during times of stress or trauma, especially when they feel marginalized or discriminated against.³⁹

When individuals lose this sense of significance, they become highly susceptible to manipulative narratives that promise to restore meaning to their lives. In the context of cognitive warfare, foreign aggressors can exploit this vulnerability by presenting themselves as the defenders of the "right" values and causes. These narratives often play on disinformation or conspiracy theories, reinforcing individuals' frustration with society and feelings of insignificance. By offering a seemingly simple solution, such as fighting for a cause portrayed as righteous, foreign aggressors give individuals a path to self-fulfilment. Often, this path involves radical or extreme actions, which the individuals begin to perceive as a way to regain their lost significance and earn recognition from others.

When the need for significance is intertwined with moral "hacking" where an aggressor manipulates an individual's moral reasoning, the potential for radicalization becomes particularly dangerous. The individual, now convinced through weaponized information that defending certain values, worldviews or an aggressor's actions is not just right but morally imperative, is particularly dangerous. At this point, such individuals are more likely to engage in extreme actions, believing these are necessary to achieve personal significance while serving a "higher" purpose.⁴⁰

Such psychological manipulation can lead to a range of dangerous behaviours, including violent protests, attacks on minority groups or refugees, or rising hostility toward one's own government and media. Such acts are justified in the minds of the manipulated individuals as both morally righteous and crucial for restoring their sense of importance and identity.⁴¹ Consequently, aggressors can transform these manipulated individuals into active participants of cognitive warfare, using their deep-seated need for

³⁴ Zmigrod et al., "Cognitive Inflexibility Predicts Extremist Attitudes."

³⁵ M. Lynn and C.R. Snyder, *Uniqueness Seeking. Handbook of Positive Psychology*, 2002, 395-410.

³⁶ Anthony Lantian et al., "I Know Things They Don't Know! The Role of Need For Uniqueness in Belief in Conspiracy Theories," *Social Psychology*, 2017, <https://psycnet.apa.org/doi/10.1027/1864-9335/a000306>.

³⁷ A. Cichocka et al., "Does Self-Love Or Self-Hate Predict Conspiracy Beliefs? Narcissism, Self-Esteem, and the Endorsement of Conspiracy Theories," *Social Psychological and Personality Science*, 7(2), 157-166, 2016, <https://psycnet.apa.org/doi/10.1177/1948550615616170>.

³⁸ Arie W. Kruglanski et al., "Frustration-Aggression Hypothesis Reconsidered: The Role of Significance Quest," *Aggressive Behavior*, National Library of Medicine, 2023, <https://pubmed.ncbi.nlm.nih.gov/37282763/>.

³⁹ Login S. George and Crystal L. Park, "Meaning in Life as Comprehension, Purpose, and Mattering: Toward Integration and New Research Questions," *Review of General Psychology*, 20(3), 2016, 205-220.

⁴⁰ Arie W. Kruglanski et al., "Fully Committed: Suicide Bombers' Motivation and the Quest for Personal Significance," *Political Psychology*, Vol. 30, n. 3, 2009, 331-357; Arie W. Kruglanski et al., "Frustration-Aggression Hypothesis Reconsidered: The Role of Significance Quest," *Aggressive Behavior*, Vol. 49, n. 5, 2023, 445-468.

⁴¹ Arie W. Kruglanski et al., "Terrorism - A (Self) Love Story: Redirecting the Significance Quest Can End Violence," *American Psychologist*, Vol. 68, n. 7, 2013, 559; Arie W. Kruglanski et al., "The Psychology of Radicalization and Deradicalization: How Significance Quest Impacts Violent Extremism," *Political Psychology* 35, 2014, 69-93. <https://onlinelibrary.wiley.com/doi/full/10.1111/pops.12163>.

significance as a weapon to drive division, conflict, and destabilization within societies.

Need for cognitive closure

As mentioned above, the brain thrives in a stable, unchanging, and easily predictable environment. Unfortunately, any disruption of this homeostasis creates ideal conditions for weaponized information to take hold. Unexpected events that cannot be predicted and easily explained disrupt the brain's ability to predict future outcomes, making it difficult to effectively prepare for unforeseen circumstances.

Examples of these situations include natural disasters such as tornadoes and floods, as well as global events like refugee crises, pandemics, economic collapses, and the outbreak of geopolitical conflicts. During these events, people are exposed to stress, fear, and, above all, *uncertainty*, as the brain is unable to predict what will happen next.⁴²

Uncertainty is a personal experience marked by a lack of confidence about future events, outcomes, or explanations.⁴³ It often comes with feelings of reduced control, anxiety, and stress.⁴⁴ This feeling arises when there is insufficient information to accurately assess a situation or predict future events. In response, individuals may experience heightened anticipatory reactions, overestimating their vulnerability and becoming hypervigilant – constantly on guard and overly sensitive to potential threats.⁴⁵ Intolerance of uncertainty can also fuel anticipatory anxiety and maladaptive coping strategies.

These maladaptive coping strategies open the door to weaponized information as the brain seeks clear and simple answers to resolve the difficult and unexpected situations.⁴⁶ This cognitive need is described as the “need for cognitive closure.” People with a high need for closure prefer structure and predictability and feel more stressed in unpredictable situations.⁴⁷ The need for cognitive closure is also tied to a desire for predictability, often satisfied by easily accessible information⁴⁸ that leads to impulsive decisions and hasty conclusions.⁴⁹ In this case, conspiracy theories and weaponized information often serve as a quick remedy for coping with uncertainty during unex-

pected global events. They provide emotionally appealing and simplified explanations to complex problems.⁵⁰ It is possible to help individuals who maladaptively manage their feelings of uncertainty and helplessness⁵¹ by offering a sense of regained control⁵² and order⁵³, which gives vulnerable people a way to make predictions in a chaotic world.

Historically, major global crises have always been accompanied by conspiracy theories⁵⁴ which help individuals cope with uncertainty by filling in the gaps in their causal explanations, often blaming secret organizations or malicious agents.⁵⁵ Today, social media amplifies the spread of these narratives. From a cognitive warfare perspective, foreign manipulators exploit the human desire to reduce uncertainty by introducing specific weaponized information aligned with their strategic goals. However, the aggressor's aim can go beyond offering a single explanation and coping with uncertainty; it is far more effective for them to continuously deepen the uncertainty of the target population, making them even more vulnerable to cognitive attacks. This tactic is known as the weaponization of global crises.

Deepening of uncertainty by weaponizing global crises

Reducing uncertainty through simplistic and manipulative narratives does not actually resolve uncertainty; instead, it intensifies it. Individuals who accept these explanations become trapped in a cycle of uncertainty, as they remain susceptible to constant threats fuelled by such manipulative narratives.

Alternatively, the aggressor's aim can go beyond offering a single explanation and coping with uncertainty; it is far more effective for them to continuously deepen the uncertainty of the target population, making them even more vulnerable to cognitive attacks. This tactic is known as the weaponization of global crises.

A clear example is the refugee crisis of 2015 and 2016. During his testimony before the House Armed Services Committee, General Philip Breedlove emphasized that

- 42 Ladislav Kesner and Jiří Horáček, “Three Challenges That The COVID19 Pandemic Represents For Psychiatry,” *British Journal of Psychiatry*, 217(3), 2020, 475-476.
- 43 Achim Peters et al., “Uncertainty and Stress: Why It Causes Diseases and How It Is Mastered By the Brain,” *Progress in Neurobiology*, 2017, 156, 164-188.
- 44 Peter McEvoy and Alison E. J. Mahoney, “To Be Sure, To Be Sure: Intolerance Of Uncertainty Mediates Symptoms of Various Anxiety Disorders and Depression,” *Behavior Therapy*, National Library of Medicine, 2012, 43(3), 533-545.
- 45 Dan W. Gruppe and Jack B. Nitschke, “Uncertainty and Anticipation in Anxiety: An Integrated Neurobiological and Psychological Perspective,” *Nature Reviews Neuroscience*, 2013, 14(7), 488-501.
- 46 Kelly M. Greenhill and Ben Oppenheim, “Rumor Has it: The Adoption of Unverified Information in Conflict Zones,” *International Studies Quarterly*, 61(3), 660-676; Michael Golebiewski, and danah boyd, “Data Voids: Where Missing Data Can Easily Be Exploited,” *Data & Society*, 2019.
- 47 Howard Berenbaum et al., “Intolerance of Uncertainty: Exploring Its Dimensionality and Associations With Need for Cognitive Closure, Psychopathology, and Personality,” *Journal of Anxiety Disorders*, 22(1), 2008, 117-125.
- 48 Arne Roets et al., “The Motivated Gatekeeper of Our Minds: New Directions in Need For Closure Theory and research,” *Advances in Experimental Social Psychology*, Vol. 52, 221-283.
- 49 Jongan Choi et al., “Need For Cognitive Closure and Information Search Strategy,” *Psychology & Marketing*, 25(11), 2008, 1027-1042.
- 50 Ibid.
- 51 Abalakina-Paap et al., “Beliefs in Conspiracies,” *Political Psychology*, 20(3), 1999, 637-647.
- 52 Jan-Willem van Prooijen and Michele Acker, “The Influence of Control on Belief in Conspiracy Theories: Conceptual and Applied Extensions,” *Applied Cognitive Psychology*, 29(5), 2015, 753-761.
- 53 Frenk Van Harreveld et al., “In Doubt and Disorderly: Ambivalence Promotes Compensatory Perceptions of Order,” *Journal of Experimental Psychology*, 143(4), 2014, 1666.
- 54 Karen M. Douglas et al., “The Psychology of Conspiracy Theories,” *Current Directions in Psychological Science*, 26(6), 2017, 538-542.
- 55 Roland Imhoff and Martin Bruder, “Speaking (un-) truth to power: Conspiracy mentality as a generalised political attitude,” *European Journal of Personality*, 28(1), 2014, 25-43.

Russia and the Assad regime were actively weaponizing this crisis to destabilize the European Union.⁵⁶

Russian disinformation campaigns employed three distinct narratives. The first was the “blame narrative,” which accused Europe and the U.S. of being responsible for the crisis. These campaigns claimed the EU failed to protect its citizens and was part of a conspiracy to destroy European civilization. Such narratives aimed to offer an uncertain population a clear context for the global crisis, while pointing out those responsible.⁵⁷ The second narrative was the “threat narrative,” which exploited the brain’s attention and emotions. This narrative fuelled fears about Europe’s declining security and repeatedly warned of an inevitable Islamization. These fears were amplified by fabricated stories, such as the “Lisa case,” where a thirteen-year-old girl of Russian descent was falsely reported to have been abducted and raped. Russian state media, along with politicians like Foreign Minister Sergei Lavrov, used this case to reinforce the narrative of German authorities’ failure to protect citizens from migrants. The final narrative was “security narrative.” This narrative portrayed Russia as the only credible provider of security for the European population, willing to intervene and protect Europeans from the inevitable rise in crime and unavoidable Islamization.⁵⁸

The COVID-19 pandemic became another global crisis weaponized to deepen uncertainty. Russian disinformation campaigns distorted perceptions of the virus, undermined trust in protective measures, and impeded the efforts of governments and health organizations to combat the virus effectively.⁵⁹ Weaponized information contributed to vaccine hesitancy, significantly hindering efforts to achieve the herd immunity necessary to end the pandemic.⁶⁰ Additionally, health experts were targeted and discredited, false COVID-19 cures were promoted, and the West, especially the U.S., were accused of creating and spreading the virus as a biological weapon.⁶¹ Similar to the refugee crisis, Russia used a range of weaponized information to portray

Western democracies as corrupt and incompetent,⁶² while presenting itself as a benevolent aid provider, actively blocked by EU states.⁶³

The weaponization of global crises is a powerful tool for cognitive manipulation, facilitating gradual shifts in individuals’ perception of reality. In this manipulated perception, foreign aggressors are again portrayed as benevolent aid providers, unfairly obstructed by corrupt European governments, the EU, and the U.S. These shifts in perception of reality align with the long-term strategic objectives of Russia, which seeks to weaken Western democracies and undermine international organizations like the EU and NATO.

Morality as vulnerability

From a cognitive warfare perspective, the manipulation of moral reasoning among vulnerable individuals represents a particularly dangerous tactic on the cognitive battlefield. By constructing narratives in which the aggressor is portrayed as the victim of unjust actions, foreign manipulators can not only solidify a distorted perception of reality but also instil values that vulnerable individuals feel compelled to pursue and defend.

If an aggressor successfully manipulates an individual’s sense of moral duty, the cognitive battle is effectively won. Such individuals will not only defend the aggressor’s worldview but also justify the aggressor’s actions, regardless of how extreme they may be. Driven by a sense of moral duty amplified by weaponized information, vulnerable individuals may radicalize themselves, viewing extremist actions in support of a foreign aggressor as not only pathway to self-significance and glory.⁶⁴ Furthermore, disinformation tailored to exploit moral reasoning can foster a perception of moral superiority among these individ-

⁵⁶ Hans Schoemaker, “Allegations of Russian Weaponized Migration Against the EU – With the Blackest Intention?”, *Militaire Spectator* 7/8, 2019, <https://militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/Militaire%20Spectator%207-8-2019%20Schoemaker.pdf>.

⁵⁷ Oliver Backes, Andrew Swab, “Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States,” Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2019, <https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states>.

⁵⁸ Antonio Nestoras, “How the Kremlin Is Manipulating the Refugee Crisis: Russian Disinformation As a Threat to European Security,” Institute of European Democrats, January 2019, 1-15, https://www.iedonline.eu/download/2019/IED-Research-Paper-Russia-as-a-security-provider_January2019.pdf.

⁵⁹ Wesley Moy and Kacper Gradon, “Covid-19 Effects and Russian Disinformation Campaigns,” *Homeland Security Affairs* 16(8), December 2020, https://www.researchgate.net/publication/346808562_COVID-19_Effects_and_Russian_Disinformation_Campaigns.

⁶⁰ James Hildreth and Donald Alcendor, “Targeting COVID-19 Vaccine Hesitancy In Minority Populations In The U.S.: Implications For Herd Immunity,” *Vaccines*, 9(5), May 2021, 489.

⁶¹ John Vandiver, “Poland Hit by Wave of Fake News Before Start of Major Military Exercise with U.S.,” *Stars and Stripes*, 29 May 2020.

⁶² Jonathan Bright et al., “Coronavirus Coverage By State-Backed English-Language News Sources,” Project on Computational Propaganda, Programme on Democracy and Technology, Oxford University, UK, Data Memo, 2020; Dominica Grygarová et al., “Trust In Official Information As a Key Predictor of COVID-19 Vaccine Acceptance: Evidence From a Czech Longitudinal Survey Study,” *BMC Public Health*, 25(1), February 2025, <https://pubmed.ncbi.nlm.nih.gov/40001023/>; Dominica Grygarová et al., “Beliefs In Misinformation About COVID-19 And the Russian Invasion of Ukraine Are Linked: Evidence From a Nationally Representative Survey Study,” *JMIR Infodemiology*, March 2025, <https://pubmed.ncbi.nlm.nih.gov/40063941/>.

⁶³ Juliusz Sabak, “Poland Issued No Airspace Restrictions For The Russian Humanitarian Aid Flights Headed to Italy. Coronavirus Employed by Kremlin as Means of Propaganda,” *Defence24.com*, 24 March 2020, <https://defence24.com/poland-issued-no-airspace-restrictions-for-the-russian-humanitarian-aid-flights-headed-to-italy-coronavirus-employed-by-kremlin-as-means-of-propaganda-commentary>.

⁶⁴ Arie Kruglanski, et al., “The Making Of Violent Extremists,” *Review of General Psychology*, 22(1), March 2018, 107-120.

uals,⁶⁵ further justifying extremist actions and portraying them as morally acceptable and legitimate.⁶⁶

This is especially dangerous as it not only leads individuals to accept and justify war crimes and atrocities but also encourages them to embrace extremism against their own governments and critics. They act out of a sense of moral duty, driven by righteous anger, perceived injustice, and the belief that their actions serve a higher cause.

Cognitive aggressors aim to be seen as benevolent defenders of traditional values that are being treated unfairly by corrupt foreign governments, coalitions, and international corporations. To tap into moral reasoning, the aggressor frequently employs a victim narrative, and one of the most prominent examples of this is the concept of “Russophobia” that triggers moral emotions such as sympathy, compassion, perceived injustice, and righteous anger in susceptible individuals.

Russophobia is a central tactic in state-sponsored Russian propaganda. The global victim narrative positions Russia as the innocent target of West. Russian propagandists have frequently accused the United States of manipulating oil prices to harm Russia’s economy, which heavily depends on high oil revenues. The Panama Papers were framed as a U.S.-led conspiracy to seize offshore wealth and destabilize Russia. Tatiana Moskalkova, Russia’s Human Rights Ombudswoman, claimed that the West uses human rights issues as a form of blackmail to destabilize Russia. This narrative of victimhood is continually used to explain international isolation, falling oil prices, and sanctions as part of a Western scheme to destroy Russia. These claims help shift attention away from Russia’s actions, justify its aggression, and elicit sympathy from foreign audiences to achieve goals such as the removal of sanctions.

On an individual level, Russophobia is employed to craft narratives that depict Russians in the West as victims of discrimination, persecution, and hate crimes. Disinformation reports have claimed that Russian citizens were denied medical care in German hospitals and had their bank accounts sanctioned, and that Russian children were expelled from schools. Stories circulated about damage to cars with Russian license plates and attacks on Russian-owned property. Ukrainian refugees were often portrayed as the instigators of these acts, accused of physical violence against Russian citizens. In some cases, disinformation alleged that Ukrainian nationalists were distributing poisoned candies to Russian children in Germany and other countries.⁶⁷

Russophobia was also employed to justify Russia’s invasion of Ukraine on February 24, 2022. Russian President Vladimir Putin made the unfounded claim that Ukraine’s government had been committing genocide against the

predominantly Russian-speaking population in the Donbas region since 2014. While these assertions were widely dismissed as baseless, they represented the culmination of a long-term disinformation campaign aimed at creating a pretext for military action. Similar tactics had been used earlier to legitimize the 2014 annexation of Crimea.⁶⁸ In the lead-up to the invasion, Ukrainians were increasingly portrayed as war criminals responsible for atrocities, such as mass graves and the crucifixion of children. This narrative was reinforced by accusations of Nazism, with Russian officials calling for the “denazification” of Ukraine, referring to its government as a “Nazi/fascist junta” or as “drug addicts and neo-Nazis” under U.S. control. (See Figure 1).

Seizing moral reasoning is arguably one of the most significant objectives in cognitive warfare. When moral reasoning becomes a gateway to radicalization, narratives that legitimize violence and extremism provide individuals with a sense of moral righteousness. This serves as a critical driver for the spread of extremist ideologies, including terrorism, as individuals come to believe that acts of violence are justifiable and necessary for a higher moral cause.

Conclusion and recommendation

Cognitive warfare is no longer a distant threat. It is here, and with the advent of AI, cognitive warfare will change profoundly as AI-tailored disinformation will exploit human cognitive vulnerabilities with unprecedented precision. At this critical juncture, NATO must act decisively to integrate the cognitive pillar into its strategic framework and update its counter-disinformation toolbox to succeed on the cognitive battlefield.

The first step is to acknowledge the cognitive vulnerabilities of the human brain and the fact that it is impossible to defend every single vulnerability, especially those that are natural to the human brain such as the inability to willingly control one’s perception, emotional reactivity, the need for explanations, and brain’s desire for homeostasis. While complete protection is unattainable, NATO can focus on strategic areas, particularly by mitigating uncertainty during global crises. By anticipating the weaponized information likely to exploit such crises, NATO can proactively inoculate populations against harmful narratives. This will reduce disinformation’s ability to gain

⁶⁵ Arie Kruglanski et al., *The Three Pillars Of Radicalization: Needs, Narratives, And Networks*, Oxford University Press, USA, 2019; Doosje, B., Van den Bos, K., Loseman, A., Feddes, A. R., & Mann, L. (2012). “My In-Group Is Superior!”: Susceptibility For Radical Right-Wing Attitudes And Behaviors In Dutch Youth,” *Negotiation and Conflict Management Research*, 5(3), 2012, 253-268.

⁶⁶ Noémie Bouhana, “The Moral Ecology Of Extremism: A Systemic Perspective,” Migration and Home Affairs, European Commission, [⁶⁷ Raquel Miguel, “Russophobia And Disinformation In Germany: Weaponising The Victim Narrative,” EU Disinfo Lab, 23 VI, 2022, <https://www.disinfo.eu/publications/russophobia-and-disinformation-in-germany-weaponising-the-victim-narrative/>.](https://home-affairs.ec.europa.eu/networks/eu-knowledge-hub-prevention-radicalisation/welcome-package/learning-resources/moral-ecology-extremism-systemic-perspective_en#:~:text=Bouhana%20presents%20a%20systemic%20framework%20for%20understanding%20extremism%2C,to%20extremist%20narratives%2C%20social%20networks%2C%20and%20situational%20vulnerabilities;Noémie Bouhana and Per-Olof Wikström, “Theorizing Terrorism: Terrorism As Moral Action: A Scoping Study,” Contemporary Readings in Law and Social Justice, 2(2), 9, file:///D:/m.dimartino/Downloads/Theorizing_Terrorism_Terrorism_As_Moral_Action.pdf.</p>
</div>
<div data-bbox=)

⁶⁸ Georgii Pocheptsov, “Cognitive Attacks In Russian Hybrid Warfare,” *Information & Security* 41, 2018, 37-43, https://isij.eu/system/files/download-count/2023-01/4103_pocheptsov_cognitive_attacks.pdf.

traction and limits the exploitation of uncertainty, one of the primary cognitive predispositions for cognitive manipulation. Furthermore, NATO must address and counter the dangerous tactic of moral exploitation. This is when aggressors manipulate individuals' sense of the moral duty to radicalize and pursue extremist actions based on the distorted reality created by the aggressor. Mitigating this form of manipulation is essential to preventing vulnerable individuals from being drawn toward extremism or even domestic terrorism.

In the face of AI-driven disinformation, NATO can also explore the development of defensive AI technologies. For example, AI-powered digital personas could help reduce uncertainty among users by providing trustworthy, consistent information while conducting inoculation exercises against disinformation, and by using appropriate language and strategies when interacting with vulnera-

ble individuals, taking their cognitive susceptibilities into account (see Table 1). Such tools would not only reinforce cognitive resilience, but also empower populations to recognize and resist cognitive manipulation.

In conclusion, integrating the cognitive pillar into NATO's future strategy is essential for success on the cognitive battlefield. Proactively addressing cognitive vulnerabilities, building trust, mitigating uncertainty, and leveraging advanced technologies are essential steps for countering the immediate and long-term threats posed by AI-weaponized information. NATO's ability to adapt to these emerging challenges will determine its effectiveness in safeguarding the cognitive resources of its member populations while ensuring resilience in an era of evolving hybrid warfare.

Research Division

NATO Defense College
Via Giorgio Pelosi 1
00143 Rome – Italy

www.ndc.nato.int

Follow us on

Twitter (@NATO_DefCollege)

Facebook (NATODefenseCollege)

LinkedIn (@nato-defense-college)

The views expressed in this publication are the responsibility of the author(s) and do not necessarily reflect the opinions of the NATO Defense College, NATO, or any government or institution represented by the contributors.

The NATO Defense College applies the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

