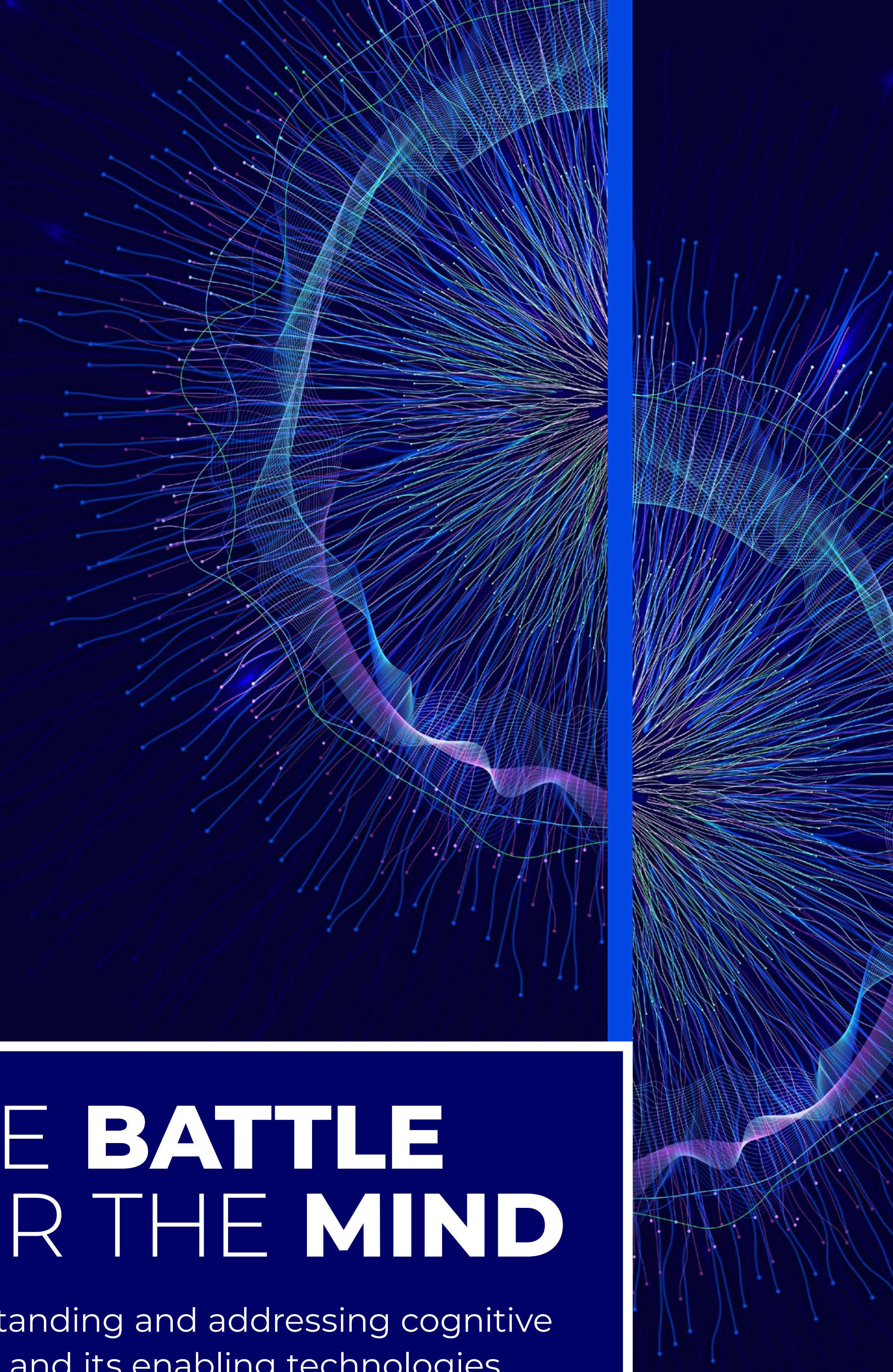
UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE



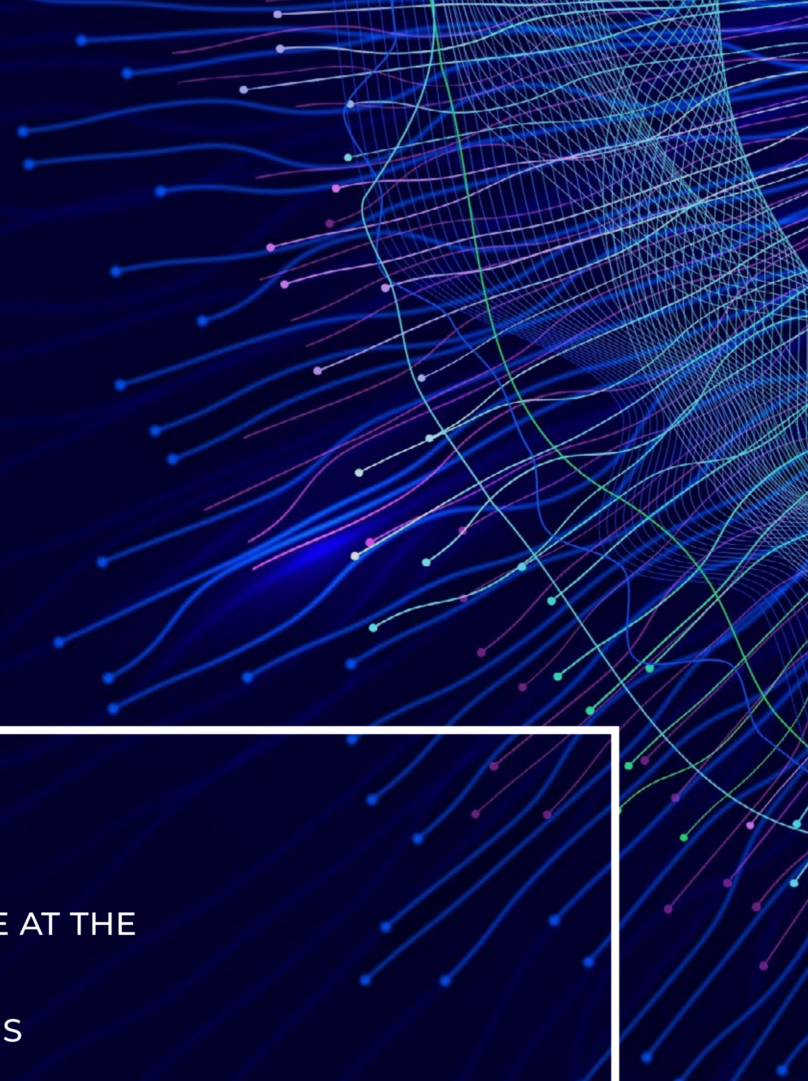
APRIL 2024

THE **BATTLE** FOR THE **MIND**

Understanding and addressing cognitive warfare and its enabling technologies

Written by:
Irene Pujol Chica & Quynh Dinh Da Xuan

TABLE OF CONTENTS



ACKNOWLEDGMENTS

This policy paper was produced under the guidance and supervision of Irene Blázquez Navarro and Carlos Luca de Tena. Their expertise and mentorship have been instrumental in shaping this work.

The paper summarizes and expands the key takeaways and recommendations from a roundtable discussion on cognitive warfare held during the latest Munich Security Conference. Special thanks are extended to Benedikt Franke, Maximilian Lister and Joana Caripidis for affording the opportunity and continuous support in the fruition of this endeavor.

Equal gratitude is extended to all the participants of the discussion for their valuable insights, thought-provoking contributions, and thorough review of the final paper.

Lastly, appreciation is extended to all those who have directly or indirectly contributed to this work, whether in the organization of the roundtable discussion, through feedback, or help with operations. Their support has been immensely appreciated and has undoubtedly enriched the outcome of this policy paper.

DISCUSSING COGNITIVE WARFARE AT THE MUNICH SECURITY CONFERENCE

On February 16, the IE Center for the Governance of Change hosted a roundtable discussion on cognitive warfare during the Munich Security Conference. 18 technology and defense leaders from government, industry, and academia discussed how the mind is becoming one of the primary battlegrounds of the 21st century as revisionist actors seek to manipulate individual and group cognition with the goal of destabilizing liberal democracies from within. Participants concurred on the need for a deeper understanding of the mechanisms and implications of cognitive warfare and emphasized the importance of better preparing citizens and legislators to confront looming threats. They also stressed how the same knowledge and technologies that enable cognitive warfare have the potential to protect our democracies from it.

Hosts:

- **Manuel Muñiz,** Provost, IE University and Chair, Center for the Governance of Change
- **Irene Blázquez**, Director, Center for the Governance of Change
- **Irene Pujol**, Project Coordinator, Center for the Governance of Change

Participants (in alphabetical order):

- **André Loesekrug-Pietri**, Chairman, Joint European Disruptive Initiative
- **Andrew J.P. Levy**, Chief Corporate and Government Affairs Officer, Accenture
- **Anne Marie Slaughter**, Chief Executive Officer, New America
- **Arancha González Laya**, Dean of the Paris School of International Affairs (PSIA), Sciences Po; and former Minister of Foreign Affairs, European Union and Cooperation of Spain
- **Catherine Sendak**, Director of Transatlantic Defense and Security, Center for European Policy Analysis
- **Clint Watts**, General Manager of Digital Threats Analysis Center, Microsoft Corporation
- **Florence Gaub**, Director of the Research Division, NATO Defense College
- **Gabi Dreo Rodosek**, Professor for Communications System and Network Security, Bundeswehr University Munich
- **Julien Deruffe**, Political Advisor Advisor to Supreme Allied Commander Transformation, North Atlantic Treaty Organization
- **Hugo del Campo**, Senior Partner, McKinsey & Company
- **Margrethe Vestager,** Executive Vice-President for A Europe Fit for the Digital Age, European Commission
- **Marietje Schaake**, International Policy Director, Standford Cyber Policy Center
- **Shyam Saankar**, Chief Technology Officer, Palantir Technologies
- **Stephen Pomper**, Chief of Policy, International Crisis Group
- **Yasmin Green**, CEO, Jigsaw Google

SUMMARY OF RECOMMENDATIONS

Areas of Priority Action

Cultivating Awareness and Understanding of the Threats

01. Collaborate across disciplines to clearly define and understand cognitive warfare, focusing on developing the precise and specific language to describe activity in the cognitive domain.

02. Empower individuals to critically navigate the information landscape, identifying when actors are trying to manipulate them, through techniques like ‘prebunking’.

03. Increase public awareness about data privacy, encouraging caution in sharing personal information and understanding how data from different devices can be collected and exploited.

Governing Cognitive Warfare and its Enabling Technologies

04. Establish clear legal frameworks for cognitive warfare, including definitions and descriptions of its various forms and tactics.

05. Determine how existing international laws could apply to activities in the cognitive domain, including when an action can constitute a violation of international humanitarian law.

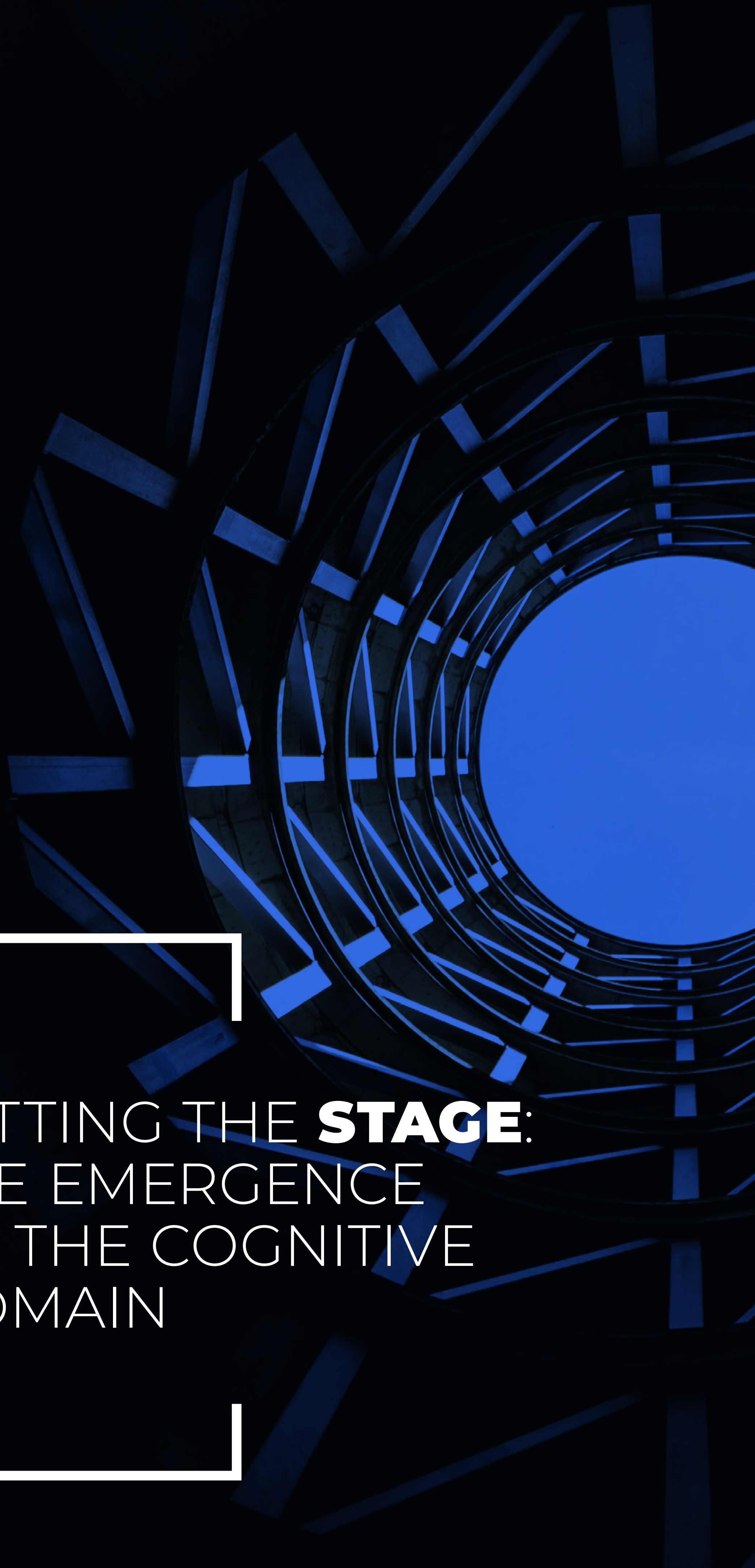
06. Develop new governance frameworks where current ones fall short, ensuring accountability and responsibility in case of breach.

Capturing the Power of Emerging Tech to Strengthen Democratic and Societal Resilience

07. Encourage cooperation among diverse stakeholders.

08. Identify vulnerabilities and flaws in our systems that need to be addressed.

09. Harness the power of emerging technologies to bolster defenses against cognitive warfare.



SETTING THE **STAGE**: THE EMERGENCE OF THE COGNITIVE DOMAIN

SETTING THE **STAGE**: THE EMERGENCE OF THE COGNITIVE DOMAIN

Operations of manipulation and deception of the mind are as old as war itself. However, for the first time in the history of human conflict, advances in cognitive science and recent developments in the digital revolution—most notably the rise of generative artificial intelligence (AI)—are enabling actors to directly influence how "an enemy community thinks, loves, or believes in".[1] This has prompted discussions in NATO and other security circles about the potential emergence of the cognitive domain as the sixth domain of warfare—after land, sea, air, outer space, and cyberspace.[2]

Recent scholarship is also beginning to emerge on the concept of 'cognitive warfare'. While still lacking a universally agreed-upon definition, the concept is being employed to refer to the set of activities that seek to shape "attitudes and behaviors by influencing, protecting, or disrupting cognition at the individual, group, or population level to gain an advantage over an adversary".[3] These activities would be part of broader hybrid warfare tactics, often conducted below the threshold of armed conflict, with objectives as diverse as thwarting specific military maneuvers to destabilizing entire societies or alliances.[4]

BOX 1. **HYBRID WARFARE**

A method of conflict characterized by the blending of conventional and unconventional instruments of power and tools of subversion. Unlike traditional warfare, which primarily relies on kinetic or lethal force, hybrid warfare involves a combination of military, economic, political, social, and informational tactics aimed at exploiting vulnerabilities in an adversary and achieving strategic objectives.

Given the novelty of the concept, the lines between cognitive warfare and other forms of hybrid warfare are often blurred (Box 1). According to subject matter expert Commander van der Klaauw, what makes cognitive warfare distinct from previous psychological operations or cyber warfare is its focus on the subconscious mind.[5]

> In fact, pundits believe that we should closely examine how neuroscience and emerging technologies may be "weaponized" to turn the mind into the main battlefield of the 21st century.[6]

Participants in the discussion agreed that actors seeking to challenge the international liberal order now have both the means and the incentives to play with our thoughts and disrupt our shared vision of reality, thereby undermining the trust and social cohesion that underpin our societies.

As the latest Munich Security Report points out, "key actors in the transatlantic community, in powerful autocracies, and in the so-called Global South have become dissatisfied with what they perceive to be an unequal distribution of the absolute benefits of the international order".[7] They will therefore use all means at their disposal to shape the future order to their advantage. This includes AI and other emerging technologies, the development and adoption of which is accelerating. Part of this stems from the geopolitical technology race between the United States and China, as both nations recognize the correlation between leadership in emerging technologies and influence over the international order.[8]

In fact, in its 2019 National Defense White Paper, the Chinese People's Liberation Army introduced the broader concept of *intelligentized warfare* (智能化战争) to refer to how AI and other emerging technologies

According to analysts, exercising “direct influence on the enemy’s cognition” is a distinctive feature of China’s *intelligentized* warfare, as the country seeks to control the fate of Taiwan, the United States and its allies without resorting to conventional warfare.[12]

could be used to achieve “mental dominance”.[9] This includes harnessing AI for increased information processing capabilities and rapid decision-making, but also wearable sensors to hone and maintain troops’ fighting spirit[10], or the use of platforms like TikTok[11] to influence public opinion, exploit user data, and shape preferences, biases, and beliefs.

According to analysts, exercising “direct influence on the enemy’s cognition” is a distinctive feature of China’s *intelligentized* warfare, as the country seeks to control the fate of Taiwan, the United States and its allies without resorting to conventional warfare.[12]

Other countries may not be as assertive as China about their intentions to disrupt group thinking for strategic purposes, but their actions speak otherwise. Russia’s Internet Research Agency’s use of bots and fake social media accounts to fuel polarization and interfere in the 2016 U.S. presidential election, or the Kremlin’s use of false and misleading narratives to justify military action against Ukraine ahead of its invasion of the country in 2022 are but two examples (Box 2).[13] Another is the Iranian government’s reported use of “cyber-enabled influenced operations”, including the use of AI-generated images and videos, to undermine Israel and “create general confusion and lack of trust” in the context of the ongoing Israel-Hamas war.[14]

BOX 2. **RUSSIA’S INTERNET RESEARCH AGENCY (IRA)**

A Russian company engaged in propaganda and influence operations through social media platforms on behalf of Russian business and political interests. It is known for its involvement in disseminating disinformation and misinformation to shape public opinion and influence political discourse, both domestically within Russia and internationally in countries such as the United States. The IRA employs various tactics, including creating fake social media accounts, posting comments, sharing memes, and amplifying certain narratives, to spread ideologically loaded messages and manipulate online discussions.

Major powers are not the only actors interested and able to play with people's cognition using the latest available technology, as shown by the growing use of deceptive-AI in democratic processes.

The *2023 Freedom of the Net* report identified cases of AI-based disinformation in at least 16 countries during the coverage period.[15] In Slovakia, for instance, the fake audio recording of the leader of the pro-Western Progressive Slovakia party discussing election rigging and proposing the doubling of beer prices spread rapidly on social media, and according to pundits, could have directly contributed to the party's electoral defeat.[16]

While the examples above may not be considered pure or effective cases of cognitive warfare, they do illustrate an emerging trend: the intent and increasing ability of a variety of state and non-state actors to manipulate our thoughts and perceptions to drive behavior in a particular direction, leveraging the power of social media and emerging technologies. This all takes place in a fertile ground, at a time when the attention economy has already taken a toll on our cognition and our ability to think critically, trust in institutions is at an unprecedented low and societal polarization is at its peak, making people vulnerable to attacks that seek to fuel a further "balkanization of reality". [17]

In a year where approximately a quarter of the world's population is heading to the polls and democracy is at stake, understanding and addressing the mechanisms and potential risks of cognitive warfare becomes particularly relevant.

IDENTIFYING **SIGNALS**: ELEMENTS SHAPING THE FUTURE OF COGNITIVE WARFARE

IDENTIFYING **SIGNALS:** ELEMENTS SHAPING THE FUTURE OF COGNITIVE WARFARE

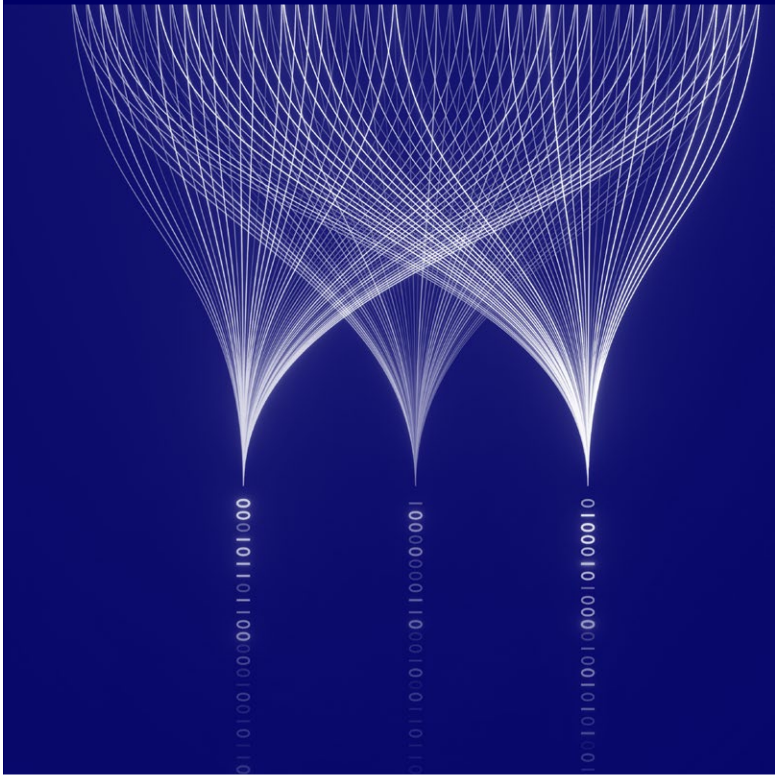
In order to grasp what cognitive warfare could entail in the forthcoming decades, we must first understand two of the driving forces behind its development.

The first is the increased knowledge about how the brain works and the fundamental processes behind our mental shortcuts and cognitive biases. This is the result of recent advances in neuroscience, behavioral economics, and psychology. We now know that the subconscious mind, which operates below conscious awareness, regulates bodily functions, emotions, and most decision-making processes. Because the conscious mind requires significant energy and capacity, only a small fraction of decisions (about 2%) is rational, with the rest influenced by subconscious factors such as repetition, automatic responses, biases, and fallacies.[18] Cognitive attacks attempt to leverage these subconscious mental shortcuts to influence how we perceive and interpret our environment, thereby "affecting not what we think but how we think".[19]

Second, this manipulation is increasingly possible thanks to progress in nanotechnology, biotechnology, information technology and cognitive sciences, including neurotechnology (NBIC), and the datafication of our societies.[20] Whether it's browsing social media, shopping online, or even engaging in casual conversations with AI chatbots like ChatGPT, we are constantly producing and sharing vast amounts of personal data about our preferences, behaviors, and emotional states. This helps generate increasingly granular user data and bolster the information available for accurate profiling and micro-targeting for various purposes, from selling us a product to influencing our electoral choices.[21] With an "avalanche of brain-tracking devices" about to hit the market in the form of wearables, access to our neural data (Box 3) will give actors even greater access to our subconscious.[22]

BOX 3. **NEURAL DATA**

Information derived from the activity of neurons in the nervous system, providing insights into an individual's mental processes and states. This data can be collected through various means such as wearable devices and advanced neurotechnology and holds significant importance in understanding and shaping human cognition, behavior, and decision-making processes.



If advances in cognitive science and access to our data give ill-intended actors the knowledge required for cognitive attacks, emerging technologies such as Generative AI, Brain-Computer-Interfaces (BCIs), and augmented and virtual reality (AR/VR) technologies create the capacity to apply that knowledge efficiently and at a scale (Box 4).

BOX 4.

Generative AI
Generative AI refers to algorithms capable of generating various content forms, including text, images, audio, and videos. Widely accessible tools like ChatGPT, deepfake technology, and voice cloning are now available to a broad spectrum of users, enabling both state and non-state actors of all sizes to target individual consumers and large institutions alike.

Brain Computer Interfaces (BCIs)
Technologies that enable direct communication between the brain and external devices, such as a computer or prosthetic limb. Invasive BCIs, such as deep brain stimulation (DBS), involve surgical procedures and are primarily used in medical settings for therapeutic interventions. Non-invasive neurotechnologies such as EEG do not require surgery and have become increasingly accessible due to advancements in sensor technology. These non-invasive BCIs are used for various applications, from medical diagnostics to consumer devices for device control, self-neuromonitoring, and personalized entertainment.

Augmented and Virtual Reality (AR/VR)
Immersive technologies that alter or enhance the user's perception of reality. AR allows digital information to be displayed onto the physical environment, enabling users to interact with virtual elements in real-time. VR, on the other hand, creates entirely simulated environments that users can interact with using specialized headsets, providing a fully immersive experience.

In recent years, we have seen how AI algorithms have been used to recommend human-generated content based on data about user preferences to manipulate political opinions. The advent of Generative AI, with its ability to learn from its interlocutors and create highly realistic content in seconds, promises to amplify this phenomenon. The data collected on different individuals could be used to create personalized disinformation with little human intervention, increasing the efficiency and efficacy of influence operations.[23]

> For instance, chatbots such as ChatGPT could be used to hit very differently individuals within a target audience by "knowing through the use of which prompts, methods, and topics and at which times of the day an interlocutor is more susceptible to manipulation".[24]

In addition, AI-generated content, such as deepfakes and voice cloning, will only increase in authenticity, making it harder for people to tell what's real and what's not.

The risks of manipulation and distortion of reality will additionally be enlarged as AR/VR technologies such as *Apple Vision Pro*[25] or *Meta Quest Pro*[26], and BCIs such as Elon Musk's *Neuralink* become widespread. The latter promise immersive experiences and the ability to control objects with our thoughts. This does not only raise the stakes of privacy invasion—as the technologies require access to vast amounts of biometric and physiological data to properly function.[27] It may also enable actors to hack the "reality" around us, or even directly our moods and reactions, to shape our behavior. In fact, several countries have already explored "brain-hacking" applications such as mood regulation and stress resilience, aiming to optimize their soldiers' performance and decision-making on the battlefield.[28]

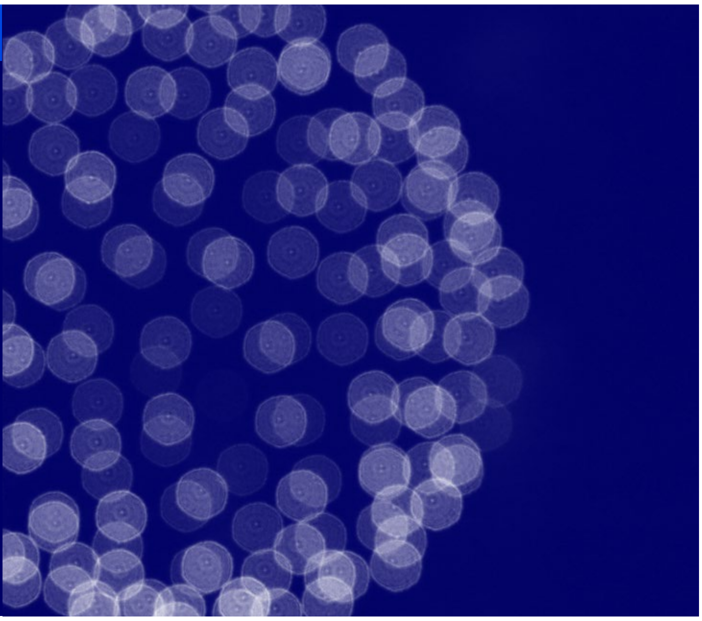
How exactly might these technologies be used by revisionist actors to wage cognitive warfare in the near future? Given current trends, one plausible scenario involves combining generative AI with AR/VR technology, along with neural data from other wearables, to further disrupt our collective perception of reality and sow internal discord. In *Chronicle of a Cultural Death Foretold*, The Red Team Defense Initiative presents a fictional future scenario in which society would be divided into an archipelago of community-based alternative reality zones known as “safe spheres”.[29] Initially created for recreation, these safe spheres would foster the development of echo chambers that reinforce ‘groupthink’ (Box 5), while making it more difficult for different groups to agree on what is real and what is not. In this future scenario, state and non-state actors would capitalize on this balkanization of reality to create further confusion and chaos when a new virus appears in France.[30] They would use generative AI to create fake messages and simulations based on the known fears and beliefs of users, to prevent the government from evacuating citizens from contaminated areas, and to incite riots and violence across the country.

In such a future, liberal democracies would be on the verge of becoming failed states because the nation-state would no longer be able to provide protection, and different groups in society would not be able to communicate or cooperate as they would perceive reality differently. Today, attempts to manipulate individual and group cognition are already threatening liberal democracies and international security. As *Financial Times* senior columnist Tim Harford suggested, the mere acknowledgement of the existence of deepfakes and disinformation is already making us more “cynical” and “skeptical” of everything around us, including our neighbors and democratic institutions.[31]

Participants agreed that a society cannot function without public trust and a basic shared understanding of reality, and that if we want to protect the international liberal order from the risks of cognitive warfare and its enabling technologies, we need to act now.

BOX 5. **GROUPTHINK**

The tendency in a group where members often prioritize harmony and conformity over critical evaluation of ideas or alternative viewpoints. When individuals in a group have similar backgrounds and are shielded from dissenting opinions, it hampers their ability to engage in independent and rational thinking. This closed-minded approach can be exploited by individuals or entities aiming to create discord or influence public opinion, capitalizing on the echo chambers and divisions present within society.



BUILDING **STRATEGIES:** PROTECTING THE MIND

BUILDING **STRATEGIES:** PROTECTING THE MIND

During the roundtable discussion, participants identified three areas of priority action:

A. CULTIVATING AWARENESS AND UNDERSTANDING OF THE THREATS

In recent years, a growing number of studies have examined the concept of cognitive warfare and its risks, with NATO, through its Science & Technology Organization and the Allied Command Transformation, leading much of the exploratory work.[32] Foresight exercises, such as the future scenario by the Red Team Defense Initiative mentioned above, also help us think about and prepare for potential developments in the coming decades.[33] Yet, participants to the discussion agreed that while we are somehow aware of the threat of cognitive warfare, efforts to conceptualize it remain fragmented, and there is generally limited understanding of its mechanisms and implications, among citizens and policymakers alike.

To inform policymakers, it is imperative that academia, industry, and the defense sector accelerate their efforts to define cognitive warfare and better understand how the brain and emerging technologies can be exploited by state and non-state actors. Using terminology from physical domains of war can hinder understanding and governance of non-physical domains like cyber and cognitive warfare. Therefore, attention should be given to developing a language that accurately describes activity in the cognitive domain, including defining thresholds for terms such as "attack," "weapon," or "injury."[34]

As has already occurred with cyberwarfare, a paradigm shift away from a purely physical and coercive understanding of warfare to include non-physical and subversive activities is essential for effective policy making in this domain.[35]

When raising awareness on the risks of cognitive warfare among citizens, careful consideration of the approach is necessary to avoid counterproductivity. As highlighted by participants, asking citizens not to believe in anything they read or hear can lead to skepticism and apathy. Instead, citizens should be encouraged to critically evaluate information sources. Providing resources and tools for fact-checking and critical thinking can empower individuals to navigate the information landscape effectively. Techniques like 'prebunking' have proven useful in helping people identify and resist manipulative content (Box 6).[36]

BOX 6. **PREBUNKING**

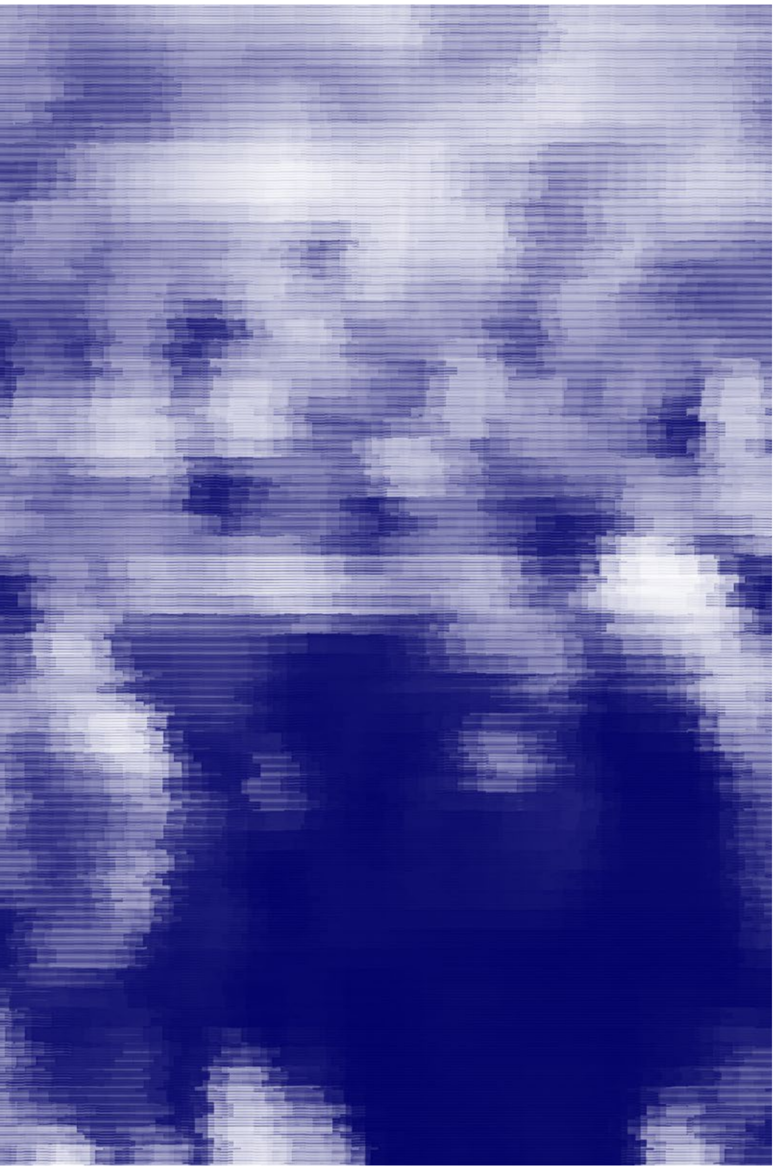
A proactive approach to countering misinformation and manipulation attempts before they happen. It involves three key steps:

1. Alerting people to an impending attempt to manipulate them;
2. Providing them with a small dose of the manipulation technique or narrative;
3. Emphatically refuting the false claims or manipulation attempts.

This strategy aims to equip individuals with the skills to recognize and defend themselves against misinformation when they encounter it.

Raising awareness about the importance of not sharing data too easily, and understanding how data is collected, is essential for preventing micro-targeting and risks posed by technologies like neurotech.

Moreover, raising awareness about the importance of not sharing data too easily, and understanding how data is collected, is essential for preventing micro-targeting and risks posed by technologies like neurotech. These awareness initiatives should be promoted across various aspects of life, including schools, workplaces, and public spaces, to ensure widespread understanding of potential threats and foster responsible data-sharing practices among citizens.



B. GOVERNING COGNITIVE WARFARE AND ITS ENABLING TECHNOLOGIES

While it is important to raise awareness among citizens about the mechanisms and threats of cognitive warfare, some participants emphasized that the responsibility for protecting against these threats should rest with policymakers.

Policymakers need to develop a comprehensive governance framework that addresses both the enablers of cognitive warfare and the consequences of its use.

In this regard, recent initiatives by national governments and international organizations to govern AI and other enablers of cognitive warfare represent significant steps forward. For instance, through its forthcoming AI Act, considered the world first comprehensive AI law, the European Union directly prohibits uses of AI whose "risk is deemed unacceptable directed", including uses aimed at "cognitive behavioral manipulation" (Box 7).[37] Through its Executive Order on AI, the Biden Administration, in turn, has incorporated provisions for labeling AI-generated content to inform users of its origin.[38] Beyond AI, governance efforts focused on the mind are also starting to emerge, most importantly in the concept of neurorights, championed by the Neurorights Foundation and UNESCO[39]. Although still in their early stages, these efforts seek to address ethical dilemmas related to the use of neurotechnology, such as how to ensure mental privacy, autonomy, and integrity, essential to prevent cognitive warfare.

Nonetheless, most of these legislative initiatives and recommendations still need to be enforced and remain limited in scope. They seek to promote responsible innovation and curb technology misuse but do not specifically address the use of these technologies as

It is essential to establish a clear legal basis for cognitive warfare, including a clear definition of the concept and an elaboration of its various forms and tactics.

weapons of warfare. Similarly, due to their predominant focus on the physical domain of warfare, international humanitarian law) and arms control agreements do not directly address the tools or hybrid tactics that may be employed in cognitive warfare.[40] For instance, as highlighted by Dr. Giordano, the Biological Weapons Convention and the Chemical Weapons Convention do not contain any provisions for neuroweapons or new techniques in biotechnology that could impact the mind such as gene editing.[41]

In developing a legal framework to effectively regulate cognitive warfare, policymakers must consider several key elements.

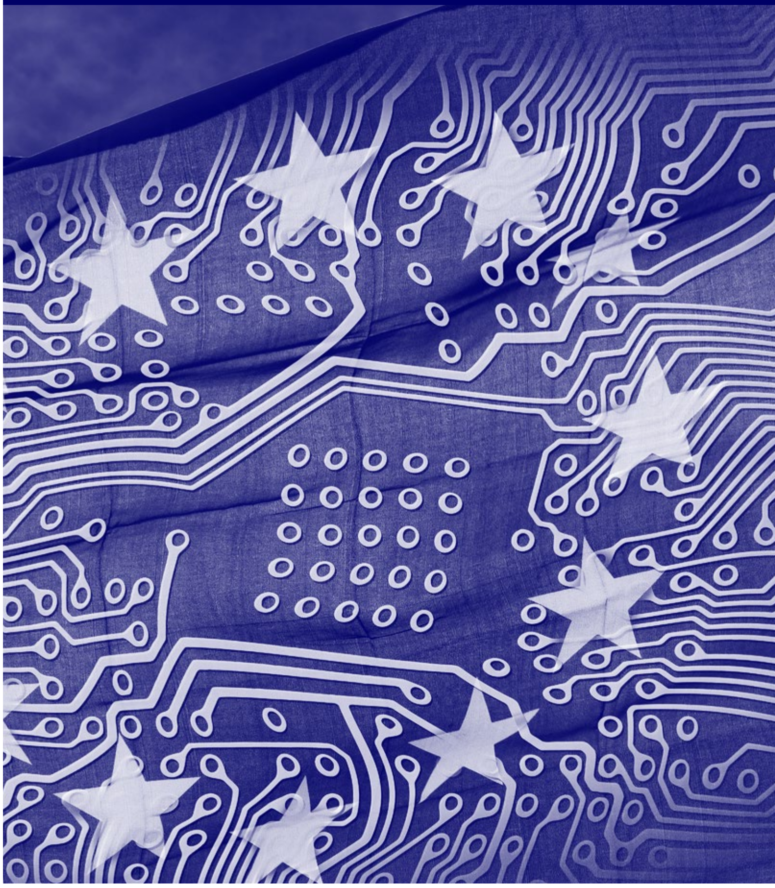
First, as suggested above, it is essential to establish a clear legal basis for cognitive warfare, including a clear definition of the concept and an elaboration of its various forms and tactics. This definition should include not only traditional forms of information warfare, but also newer techniques facilitated by emerging technologies such as AI and neurotechnology.

Second, as already pointed out in discussions on the cyberspace, policymakers need to determine not whether but *how* or in which cases existing international law applies to the cognitive domain.[42] Which actions, for instance, should be deemed unlawful and prohibited by the UN Charter or trigger Article 5 of the North Atlantic Treaty?

Finally, in cases when current frameworks do not apply, new legal frameworks should be developed. The latter should specify what actions or tactics constitute acts of aggression, and address accountability and responsibility, outlining the obligations of state and non-state actors involved in cognitive warfare activities. This includes mechanisms for attribution, accountability for malicious acts, and avenues for recourse or retaliation in response to cognitive warfare incidents.

BOX 7. **EU AI ACT**

The first comprehensive legal framework globally, aiming to promote trustworthy AI by ensuring adherence to fundamental rights and ethical principles while addressing risks associated with impactful AI models. It categorizes AI systems into four risk levels, imposing strict obligations on high-risk applications such as those used in critical infrastructures, education, and law enforcement. Through transparency requirements, future-proof strategies, and enforcement by the European AI Office, the Act seeks to position Europe as a leader in ethical AI development and implementation.



C. CAPTURING THE POWER OF EMERGING TECH TO STRENGTHEN SOCIETAL AND DEMOCRATIC RESILIENCE

To prevent any risk to individuals, groups, or systems, we must confront both internal vulnerabilities and the threat of any potential actor exploiting those vulnerabilities to cause harm or achieve a specific goal. While the previous sections focused on how to understand and govern the threat of cognitive warfare, we should also tackle the vulnerabilities that cognitive warfare seeks to exploit. During the discussion, there was broad consensus that, in order to fully prevent the risks of cognitive warfare, we must address the current failures of our liberal democracies as well as our cognitive biases. This requires a comprehensive set of actions, ranging from political reform to critical thinking education.

While more research is needed on the specific set of actions that need to be taken in this regard, participants agreed that the same knowledge and technologies that enable cognitive warfare can help us address the vulnerabilities in our system. For example, complex AI systems hold the promise of strengthening democratic processes by enabling effective participation, deliberation and collaboration through understanding wide-scale sentiment and social conversations or enabling town hall-style democratic exchange at scale[43]. VR experiences, in turn, could be used—and are already being used—to provide unconscious bias training. By immersing individuals in scenarios from alternate perspectives, VR enables users to identify biases previously overlooked[44]. This underscores the potential of emerging technologies to contribute to societal and democratic resilience.

Realizing this potential hinge upon robust collaboration among diverse stakeholders, from technology developers and policy makers to sociologists and venture capitalists. They should work to identify the various vulnerabilities in our system and how technology can help address them.

> Only by working together to reduce the current weaknesses of our liberal democracies will we be able to adequately protect them from the risks of cognitive warfare.

ENDNOTES

1 Bernard Claverie and François Du Cluzel, rep., "Cognitive Warfare": *The Advent of the Concept of "Cognitics" in the Field of Warfare*, March 2022, https://www.researchgate.net/publication/359991886_Cognitive_Warfare_The_Advent_of_the_Concept_of_Cognitics_in_the_Field_of_Warfare.

2 Claverie and Du Cluzel, *"Cognitive Warfare": The Advent of the Concept of "Cognitics" in the Field of Warfare*.

3 "Cognitive Warfare: Beyond Military Information Support Operations," Allied Command Transformation: NATO's Strategic Warfare Development Command, May 2023, https://www.act.nato.int/articles/cognitive-warfare-beyond-military-information-support-operations.

4 Kathy Cao et al., "Countering Cognitive Warfare: Awareness and Resilience," NATO Review, May 20, 2021, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html#:~:text=In%20cognitive%20warfare%2C%20the%20human.

5 Cornelis van der Klaauw, rep., *The 21st-Century Game Changer*: Cognitive Warfare, 2023, https://www.jwc.nato.int/application/files/7216/9804/8564/CognitiveWarfare.pdf.

6 Claverie and Du Cluzel, *"Cognitive Warfare": The Advent of the Concept of "Cognitics" in the Field of Warfare*.

7 rep., Munich Security Report 2024, 2024, https://securityconference.org/en/publications/munich-security-report-2024.

8 Carlos Cantafio Apitz and Branka Marijan, rep., *On Geopolitics and Innovation: How the Military Technology Race between the United States and China Will Shape Global Security*, October 2023, https://tinyurl.com/2fdd3bwa.

9 rep., *China's Military Strategy in the New Era* (The National Institute for Defense Studies, 2021), https://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2021_A01.pdf.

10 Josh Baughman and Peter W. Singer, "China Gears up for Cognitive Warfare," Defense One, April 7, 2023, https://www.defenseone.com/ideas/2023/04/china-gears-cognitive-warfare/384876.

11 Nita Farahany, "Tiktok Is Part of China's Cognitive Warfare Campaign," The Guardian, March 25, 2023, https://www.theguardian.com/commentisfree/2023/mar/25/tiktok-china-cognitive-warfare-us-ban.

12 Koichiro Takagi, "New Tech, New Concepts: China's Plans for AI and Cognitive Warfare," War on the Rocks, April 15, 2022, https://warontherocks.com/2022/04/new-tech-new-concepts-chinas-plans-for-ai-and-cognitive-warfare.

13 Philip N. Howard et al., rep., *The IRA, Social Media and Political Polarization in the United States*, 2012-2018, 2018, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf#page=1.

ENDNOTES

14 "Iran Surges Cyber-Enabled Influence Operations in Support of Hamas," Microsoft Security, March 5, 2024, https://www.microsoft.com/en-us/security/business/security-insider/reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas.

15 Allie Funk, Kian Vesteinsson, and Adrian Shahbaz, "The Repressive Power of Artificial Intelligence," Freedom House, 2023, https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence#generative-ai-supercharges-disinformation.

16 Peter Conradi, "Was Slovakia Election the First Swung by Deepfakes?," The Times, October 7, 2023, https://www.thetimes.co.uk/article/was-slovakia-election-the-first-swung-by-deepfakes-7t8dbfl9b.

17 "Ledger of Harms," Ledger of Harms, June 2021, https://ledger.humanetech.com.

18 Astrid Groenewegen, "Kahneman Fast And Slow Thinking Explained," SUE: Behavioural Design, 5AD, https://suebehaviouraldesign.com/kahneman-fast-slow-thinking.

19 Cornelis van der Klaauw, rep., The 21st-Century Game Changer: Cognitive Warfare, 2023, https://www.jwc.nato.int/application/files/7216/9804/8564/CognitiveWarfare.pdf.

20 Francois du Cluzel, rep., Cognitive Warfare, a Battle for the Brain, 2023, https://tinyurl.com/ynpupeh7.

21 https://www.gcsp.ch/publications/peace-mind-cognitive-warfare-and-governance-subversion-21st-century.

22 Nita Farahany, "Wearable Brain Devices Will Challenge Our Mental Privacy," Scientific American, March 27, 2023, https://www.scientificamerican.com/article/wearable-brain-devices-will-challenge-our-mental-privacy.

23 Thor Benson, "This Disinformation Is Just for You," Wired, August 1, 2023, https://www.wired.com/story/generative-ai-custom-disinformation.

24 Rickli, Mantellassi, and Glasser, *Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st Century.*

25 "Introducing Apple Vision Pro: Apple's First Spatial Computer," *Apple*, June 2023, https://www.apple.com/newsroom/2023/06/introducing-apple-vision-pro.

26 "Meta Quest pro: Premium Mixed Reality," Meta, accessed March 14, 2024, https://www.meta.com/es/en/quest/quest-pro.

27 Luke Heemsbergen, "Editing Memories, Spying on Our Bodies, Normalising Weird Goggles: Apple's New Vision Pro Has Big Ambitions," The Conversation, January 29, 2024, https://theconversation.com/editing-memories-spying-on-our-bodies-normalising-weird-goggles-apples-new-vision-pro-has-big-ambitions-221910.

28 Jean-Marc Rickli, "Neurotechnologies and Future Warfare," RSiS: Nanyang Technological University, 2023, https://www.rsis.edu.sg/rsis-publication/rsis/ai-governance-and-military-affairs-neurotechnologies-and-future-warfare/#.YAp-Oi2ZPEZ.

29 "Chronicle of a Cultural Death Foretold," The Red Team, accessed March 14, 2024, https://redteamdefense.org/en/season-1/chronicle-of-a-cultural-death-foretold.

30 ibid.

31 Tim Harford, "It's Only a Matter of Time before Disinformation Leads to Disaster," Financial Times, 2024, https://www.ft.com/content/0afb2e58-c7e2-4194-a6e0-927afe0c3555.

32 "Cognitive Warfare: Beyond Military Information Support Operations," Allied Command Transformation: NATO's Strategic Warfare Development Command.

33 "Chronicle of a Cultural Death Foretold," The Red Team.

34 Rickli, Mantellassi, and Glasser, *Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st Century.*

35 Rickli, Mantellassi, and Glasser, *Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st Century.*

36 Nahal Toosi, "Pre-Bunking, Micro-Dosing and Liberating," Politico, 2023, https://www.politico.com/newsletters/global-insider/2023/08/04/pre-bunking-micro-dosing-and-liberating-00109753.

37 "Artificial Intelligence Act: Council and Parliament Strike a Deal on the First Rules for AI in the World," *Council of the European Union*, 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai.

38 "FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence," *The White House*, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/#:~:text=The%20Executive%20Order%20establishes%20new,around%20the%20world%2C%20and%20more.

39 "Ethics of Neurotechnology," UNESCO, accessed March 14, 2024, https://www.unesco.org/en/ethics-neurotech.

40 Rickli, Mantellassi, and Glasser, Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st Century.

41 1. James Giordano, "Is Neuroscience the Future of Warfare?," Defence IQ, August 29, 2023, https://www.defenceiq.com/defence-technology/articles/neuroscience-and-future-warfare-1.

42 Aurel Sari, "International Law and Cyber Operations: Current Trends and Developments," Council of Europe, 2023, https://rm.coe.int/64th-cahdi-pr-aurel-sari-presentation/1680aaaf48.

43 "AI4Democracy," The Center for the Governance of Change, 2023, https://www.ie.edu/cgc/research/ai4democracy.

44 "How Virtual Reality is tackling unconscious bias", Learning People, accessed March 14, https://www.learningpeople.com/uk/resources/blog/how-virtual-reality-is-tackling-unconscious-bias.

UNIVERSITY

CENTER FOR THE
GOVERNANCE OF
CHANGE

WRITTEN BY:
Irene Pujol Chica and Quynh Dinh Da Xuan

RECOMMENDED CITATION:
Pujol, I. & Dinh, Q., “The Battle for the Mind: Understanding and Addressing Cognitive Warfare and its Enabling Technologies”, IE CGC, April 2024

Photos: Lennart Preiss/MSC, Unsplash, Shutterstock