RAND

Research Report

RUSSELL HANSON, ADAM R. GRISSOM, CHRISTOPHER A. MOUTON

The Future of Indo-Pacific Information Warfare

Challenges and Prospects from the Rise of AI

In today's globally interconnected environment, the advent of advanced artificial intelligence (AI) language models creates both anticipation for their potential benefits and apprehension over their possible misuse. This concern intensifies when considering the strategic ambitions of the People's Republic of China (PRC) in the Indo-Pacific region. The PRC aims to assert its dominance, striving to establish a hegemonic system that caters to the priorities of the Chinese Communist Party (CCP).[1]

The PRC's strategy "envisions Beijing weakening U.S. alliances, expanding its own network of client states, renovating and leading regional multilateral institutions, and deepening the region's integration into a Chinese-led economic, political, and technological order."[2] It is within this broader strategic context that the potential misuse of AI language models becomes particularly troubling, especially because the United States has struggled to maintain its information warfare capabilities since the end of the Cold War.[3] The United States now faces the growing threat of AI-powered disinformation campaigns that could supercharge the building of believable personas and can generate endless tailored content across a variety of mediums.[4]

Brad Smith, president of Microsoft, underscores the gravity of this situation. He warned, "We're going to have to address in particular what we worry about most [from] foreign cyber influence operations, the kinds of activities that are already taking place by the Russian government, the Chinese, the Iranians."[5] Smith's statement highlights the emerging threats in the digital landscape and the need for vigilance, particularly considering the actions of the PRC in the Indo-Pacific region and the fact that U.S. adversaries, such as China and Russia, have been investing heavily in information operations and strategic communications.[6]

KEY FINDINGS

- The development of AI technologies, particularly advanced language models, has drastically expanded the scope of possible disinformation campaigns. These technologies could enhance the People's Republic of China's ability to conduct information operations at an unprecedented scale and sophistication.
- The information environment necessitates constant vigilance to detect and neutralize disinformation campaigns early. Advanced AI tools could be instrumental in this endeavor, helping to analyze, characterize, and visualize the constantly changing information environment.
- Timely warnings can significantly dampen the effects of malign operations and are critical to combating them. Promoting true narratives and exposing falsehoods can help inoculate populations against disinformation, creating societal resilience that curbs the effect of repeated false information.
- The efforts to counter disinformation should be multinational. Collaboration with partner nations is crucial not only to increase the effectiveness of these operations but also to create a combined front against malign activities. Local knowledge, trusted by local populations, forms a crucial part of this strategy.
- As the landscape of information warfare evolves with technology and global geopolitics, future information operation strategies will need to be dynamic, collaborative, and proactive, combining vigilance, rapid response, and multinational cooperation to counter threats effectively.

Information Operations and the PRC

In the face of growing geopolitical tensions, the PRC has been increasingly opportunistic in its approach to subversion. China views modern warfare as being centered on the struggle for information dominance, which is considered the most important of the traditional "three dominances," along with air dominance and sea dominance.[7] Psychological warfare, a key part of information operations, is one aspect of the broader Three Warfares concept, which also consists of public opinion warfare and legal warfare.[8]

Several instances exemplify China's opportunistic approach to subversion: exploiting the discord between Bangkok and Washington following the 2014 coup in Thailand, filling the aid vacuum in Cambodia in the aftermath of the 2021 crackdown by Prime Minister Hun Sen, establishing the United Wa State Army in the ungoverned areas of eastern Myanmar, and extending proxy maritime militia operations around the Natuna Islands during the peak of the coronavirus disease 2019 (COVID-19) global pandemic.[9] Although these instances each highlight different facets of subversion led by varying PRC actors, they all share a common thread: a distinctive opportunism.

In the broader context, China maintains a robust, meticulously coordinated infrastructure for print, broadcast, and digital propaganda. The CCP Central Propaganda Department and the United Front Work Department underpin these efforts, yet a variety of other actors also participate. Inspired by the Russian model, China has made efforts to flood the information space with its own narratives, strategically using its media assets to disseminate disinformation and subtly influence overseas audiences.[10] Together, these actions create a complex tapestry of overt, gray, and covert messages designed to captivate diverse overseas audiences.[11] The result is a series of orchestrated campaigns that intentionally disseminate disinformation, instigate dissent in targeted nations, reinforce pro-PRC influencers, and contest adversaries' narratives.[12]

There have been numerous recent examples that highlight China's application of opportunistic subversion in the information environment. The Chinese consulate in New York is accused of discretely paying influencers on social media to promote the Beijing Winter Olympics.[13] Similarly, Chinese state-run news and media companies have paid influencers and creators—both monetarily and with lucrative views—to run pro-PRC stories on their channels.[14] The blurred lines between the PRC and Chinese social media companies potentially gives China access to troves of data on the U.S. public as well as influences what content the U.S. public does and does not see.[15] Members of the PRC Ministry of Public Security were recently charged with operating troll farms to target and attack dissidents whose views were unfavorable to the PRC.[16] In 2020, Twitter disclosed "23,750 accounts that comprise . . . [a] highly engaged core network" and "approximately 150,000 accounts that were designed to boost this content, e.g. the amplifiers."[17]

The PRC's approach to subversion begins with strategic, long-term investments in relationships with regional economic, political, and military elites.[18] When conditions turn favorable for transforming these investments into functional assets and initiatives, Beijing reacts swiftly.[19] This opportunistic strategy is evident in its territorial expansions in the South China Sea, where the PRC has justified its actions with economic and political rationales, a tactic reminiscent of Russia's approach in Crimea.[20] The aim is to exert influence and cement the new status quo before the United States or other global actors can mount a meaningful response. The COVID-19 pandemic highlights another opportunistic operation by the PRC to attempt to redirect blame for the virus onto the United States and sow discord among U.S. allies.[21] Considering the PRC's sophisticated subversion capabilities, extensive network, and opportunistic tactics, the subversion gap in the Indo-

Abbreviations

AI	artificial intelligence
CCP	Chinese Communist Party
COVID-19	coronavirus disease 2019
DoD	U.S. Department of Defense
LLM	large language model
PRC	People's Republic of China

Pacific presents a significant risk: It threatens to fracture the counter-hegemonic coalition in the region. Beijing's goal appears to be to chip away at the coalition, weakening the existing U.S. regional strategy. Current attempts by the U.S. Department of Defense (DoD) to bolster conventional deterrence seem insufficient to thwart Beijing's subversive actions.

Artificial Intelligence and Cognitive Bias

Recently, the world has been captivated by the rapidly improving capabilities of AI large language models (LLMs), such as OpenAI's ChatGPT, Google's Bard, and Meta's Llama 2. These models are trained on enormous corpuses of open-source data collected from the internet and contain many billions of parameters.[22] The capacity of LLMs to generate coherent, well-structured, and persuasive sentences, imitating human writing, has rightfully alarmed experts. Lisa Costa, the chief technology and innovation officer for the U.S. Space Force, succinctly describes this phenomenon: "It creates these definitive short sentences that we typically identify as very knowledge-based, and so when we read these sentences, they sound . . . exactly right."[23] She warns, however, that "we should not confuse sentence structure with knowledge."[24] Costa's commentary highlights a cognitive bias, known as *cognitive fluency bias*, an extensive subject in academic research. Cognitive fluency bias—when people mistakenly equate polished presentation for authenticity—can mislead. This bias is deeply rooted, often influencing one's perceptions and decisions without their conscious knowledge. Cognitive fluency bias is especially prone to "truthiness," a term popularized by Stephen Colbert and further studied by Eryn Newman.[25] Newman characterizes *truthiness* as "how smart, sophisticated people use unrelated information to decide whether something is true or not."[26] Truthiness illustrates how high-quality presentation—whether through well-crafted text or compelling visuals—can make statements appear more truthful. In Newman's words, "When things feel easy to process, they feel trustworthy."[27]

State actors are increasingly harnessing digital technologies to launch malign information campaigns, using online tools and advanced information operations to promote their agendas.

Malign actors can use AI-generated content to capitalize on cognitive fluency bias and truthiness, manipulating people's intuitive thinking. These "gut feelings"—the cognitive mechanisms for rapid and often accurate decisionmaking—are rooted in the brain's evolved heuristics for judgments.[28] The presentation style of AI-generated content projects an impression of intelligence and aligns with the heuristic to accept certain statements at face value, without considerable scrutiny to differentiate fact from fiction.[29] The consequences for disseminating false information in a way that bypasses scrutiny are concerning, especially as AI language models can be employed to craft messages targeting vast segments of the population. Studies have also shown that repeating information causes it to appear more reliable, a phenomenon called the "illusory-truth effect."[30] AI-generated content promoted by state-run botnets can then prove a potent combination. The internet, given its global reach, has become a major platform for foreign interference through the exploitation of truthiness. State actors are increasingly harnessing digital technologies to launch malign information campaigns, using online tools and advanced information operations to promote their agendas.[31] In response, some nations, such as Singapore, have devised measures, such as the Foreign Interference (Countermeasures) Act, which grants officials the authority to investigate and counter these activities,

especially when they emanate from foreign sources.[32] The goal of these measures is to curb and mitigate the proliferation of such malign information campaigns.

The implications of cognitive fluency bias and truthiness ripple out beyond individual decision-making and can affect the sociopolitical landscape and expand the potential for large-scale misuse of AI-driven language models for malicious information operations.

Monitoring the Information Environment

In recognizing the severity of this threat, DoD has underlined the need for constant vigilance in monitoring the information environment. DoD's 2016 *Strategy for Operations in the Information Environment* calls for enhancing capabilities to "monitor, analyze, characterize, assess, forecast, and visualize" the information environment.[33] This guidance aligns with the Observe and Orient stages of the Observe-Orient-Decide-Act (OODA) loop, a strategic concept developed by U.S. military strategist Colonel John Boyd.[34] *Observation* represents the crucial first step in the early detection of subversion attempts and issuing of warnings about potential disinformation campaigns. *Orientation* involves understanding the complex interplay between cognitive biases and the information produced by AI language models. Together, observation and orientation lay the foundation for informed decisionmaking and effective action against malign information operations.

Examples of information-sharing initiatives, such as the European External Action Service's Rapid Alert System, highlight the importance of international collaboration in addressing disinformation threats.[35] Launched in March 2019, the Rapid Alert System aimed to facilitate common situational awareness and responses to disinformation spread across European Union member states. However, its effectiveness has been limited because of a lack of trust and engagement among member states.[36] In the United States, the Department of State's Global Engagement Center is tasked by law to "[identify] current and emerging trends in foreign propaganda and disinformation."[37] However, the Global Engagement Center has been observed as "[lacking] the necessary political and institutional clout to direct a coordinated effort."[38]

Monitoring the information environment is not a task that the United States should undertake alone.

The advent of new AI and machine learning technologies offer an opportunity to enhance observation capabilities by monitoring and analyzing vast amounts of data to help detect patterns and anomalies that could signal a subversion attempt or disinformation campaign. In practice, the development of specialized units within the military or intelligence communities dedicated to information warfare can also provide the expertise needed to interpret and act on this data.

The existing network of joint, intergovernmental, and interagency relationships supporting information operations in the Indo-Pacific region is a product of past strategic priorities, which significantly differ from current needs. The authorities and permissions governing these relationships—including Title 10 and Title 50,[39] along with the support systems that sustain them—are not fully aligned in the region. This misalignment creates operational challenges and underscores the necessity for new types of collaborations with interagency partners. Recognizing this, the National Security Strategy specifically calls for an integrated approach and a pivot from the existing structures to those that can effectively synchronize the myriad tools at the nation's disposal.

Furthermore, monitoring the information environment is not a task that the United States should undertake alone. As stated in the National Security Strategy, "to solve the toughest problems the world faces, we need to produce dramatically greater levels

of cooperation" and "assemble the strongest possible coalitions to advance and defend a world that is free, open, prosperous, and secure."[40] Collaboration with allies and partners around the world is crucial for sharing intelligence, building a collective understanding of threats, and coordinating responses. Working together in this way can help build a more robust, collective defense against the destabilizing potential of malign information operations.

Issuance of Advanced Warnings

The crucial task of issuing timely warnings represents an important countermeasure against malign information operations.[41] Drawing from cognitive inoculation principles, it is observed that preemptive warnings about possible disinformation significantly reduce the risk of people falling for these malign attempts.[42] Warnings serve an important function: They alert audiences about potential misinformation, which in turn stimulates critical evaluation of the information encountered. In this context, the cognitive bias of perceived truthfulness is attenuated to skepticism.[43]

In the process of issuing effective warnings, attention should be given to not only debunking false narratives but to also endorsing true ones.[44] Warnings perform a dual function in this context: They counter misinformation while simultaneously promoting validated information. These warnings guide audiences toward trustworthy sources and equip them with tools to verify the information that they encounter. Therefore, ensuring that true narratives are effectively promoted is a critical element of this process. Importantly, a warning's efficacy hinges on the credibility of the entity issuing it. This highlights the significance of fostering public trust and maintaining the authorities' integrity, particularly those authorities likely to issue warnings.[45] It is here that collaboration with allies and partners becomes essential. Local knowledge and trust gained through these partnerships can greatly enhance the warnings' credibility and contribute to the resilience of these societies against disinformation campaigns.

Issuing warnings is a dynamic process, not a one-off event. Adapting to the rapidly evolving information environment is key, requiring the ability to promptly detect and respond to emerging disinformation campaigns. Leveraging advanced AI and machine learning technologies can support these efforts by monitoring the information environment, identifying threats, and swiftly issuing relevant warnings.[46] In addition, local partners can play a critical role because they are often better positioned to respond quickly to real-time events. Their responsiveness can contribute to a warning system's overall effectiveness.

Although effective, warnings cannot exist as a standalone solution to counter malign information operations. A multifaceted strategy—incorporating digital literacy improvement, fact-checking promotion, and critical thinking skill enhancement—is vital to successfully combat these operations. Within the context of a DoD campaign to counter disinformation, it is crucial to recognize the constitutional, legal, and political complexities that arise when considering increased DoD involvement because these efforts might blur the boundaries between foreign and domestic information spaces.

Warnings serve an important function: They alert audiences about potential misinformation, which in turn stimulates critical evaluation of the information encountered.

Partner Information Operations

In the face of pervasive AI-driven threats, developing partnerships and conducting collaborative operations have never been more crucial. By augmenting partner nations' capabilities, DoD can significantly reinforce the resilience against disinformation and subversion attempts. This partnered approach recognizes the complex and dynamic nature of the information environment.

A core objective should be to enhance partner nations' ability to execute successful information operations independently. Equipping these forces with the knowledge, strategies, and tools to operate effectively within the information environment will not only counteract disinformation but will also foster global literacy about malign information operations. A critical consideration for the United States, in increasing its involvement, is to carefully balance the provision of accurate information to counter foreign disinformation campaigns against the risk of inadvertently supporting narratives that might be construed as propaganda, potentially aggravating the situation.

Next, the United States should consider a shared database that documents and tracks the PRC's malign information activities. This shared resource can expose patterns, identify vulnerabilities, and aid in the strategic formation of responses. It would establish a sharing foundation of knowledge for countering disinformation and integrating partner nations through an irregular warfare approach applied to information operations, increasing the collective stance against malign information operations.

The lessons derived from both irregular warfare (IW) and information warfare (IW) have significant implications for countering malign information operations.[47] A fusion of these two IW principles—which we refer to as the IW^2 concept—can provide unique insights for operations below the threshold of armed conflict. This approach underscores the benefits of partnered operations. It leverages U.S. partners' unique local knowledge and capabilities, enhancing their ability to safeguard their sovereignty, disrupt adversary subversion, and counter AI-driven disinformation. Harnessing the IW^2 framework can enhance deterrence, foster commitment to shared security objectives, and help position the United States as the preferred partner of choice.[48] Several facilitating elements stand out in these operations. The capacity to train partner forces outside their countries creates a secure space for them to acquire the necessary skills and prepare for future information operations. Training outside the partner country can improve operational security and afford efficiencies by centralizing resources. Information-sharing can build trust and enhance the security of both the partner nation and the United States. Similarly, an increased ability for U.S. forces to work in sync with partner forces, developing cultural sensitivity and language skills, reflects the advantages of the collaborative nature of our recommended approach.

In the face of pervasive AI-driven threats, developing partnerships and conducting collaborative operations have never been more crucial.

Increased funding for multinational exercises can underscore U.S. commitment and offer shared learning opportunities and practical skills application. In the same vein, securing public support within partner nations for cooperation with the U.S. military becomes essential. It aligns with the need for timely warnings and the promotion of accurate narratives. The backing of local populations can foster enduring collaboration, bolstering the collective defense against malign information operations.

Partner information operations represent an important tool in U.S. efforts to counteract subversion and future AI-driven disinformation campaigns. The promotion of digital literacy, issuance of timely warnings, constant vigilance in monitoring the information environment, and conducting of collaborative

operations collectively construct a robust defense against disinformation campaigns.

A Measure-Countermeasure Dynamic

Measure-countermeasure dynamics have been central throughout historical and technological evolution. The design of new offensive capabilities leads to the development of corresponding defensive strategies, which in turn catalyzes the creation of even more-advanced offensive methods. The rise of aviation, the anthrax bioweapon threat, International Traffic in Arms Regulations, and the Cold War arms race illustrate how this dynamic has shaped the responses to emerging threats. In each instance, countermeasures did not eradicate threats; instead, they prompted continually evolving ways to mitigate risks. Today, AI language models present novel challenges that bring this dynamic into focus, forcing governments to react to the advent and proliferation of LLMs.[49] Devising the countermeasure to these challenges in a timely manner is critical because the window to enact defensive policies might be short.[50]

In 2017, the PRC released an AI roadmap outlining its ambition to define ethical norms and AI security policies by 2025 and become the world's leading AI innovation center by 2030.[51] Although achieving these goals might be unlikely, they serve as a motivating force for the United States to counter the PRC's efforts to shape global AI perspectives to its advantage.[52] In this light, taking steps to influence the AI measure-countermeasure dynamic will be critical to countering malign information operations.

To effectively engage with the measure-countermeasure dynamic in the AI space, continuous monitoring of the information environment is crucial for early detection and neutralization of threats. Timely issuance of warnings is another critical countermeasure to identify and counter false narratives, fostering societal resilience against disinformation. A unified, international approach that leverages local knowledge and narratives is necessary to counter malign operations while the power to strengthen awareness and resilience in this era of digital advancement is harnessed. Promoting transparency and accountability in the development and deployment of AI systems is essential to establishing international norms and standards, which help create a global effort to address AI-enabled threats. Multilateral engagement with U.S. partners can create a coordinated approach strengthening the countermeasure to malign information operations.

Recognizing the emerging threat posed by AI-enabled information operations, the United States must understand the risks, implement necessary countermeasures, and continue to leverage these tools in a safer and more secure manner. Time is critically important, and responding sooner gives the United States the upper hand in the measure-countermeasure dynamic. The role of AI language models, as both measure and countermeasure, underlines the complexity of the challenge but also illuminates the path to managing it effectively. By engaging proactively, the United States can develop robust warning systems and counteract potential threats, enhancing national security while reaping the rewards of technological innovation.

Promoting transparency and accountability in the development and deployment of AI systems is essential to establishing international norms and standards.

Conclusions

In the evolving information environment, the role of advanced AI technologies has drastically expanded the scope of possible disinformation campaigns. Notably, efforts by the PRC have demonstrated the need for a concerted and strategic response from the United States and its allies. To this end, a potential strategy emerges, built on a combination of monitoring, issuing warnings, and conducting partner operations.

Continuous monitoring of the information environment is the foundation of this strategy, a prerequisite for the early detection and neutralization of disinformation campaigns. A proactive stance, underpinned by advancements in AI and machine learning techniques, can aid in better understanding the dynamic information environment and staying ahead of potential threats.

A robust warning system that promotes truth while spotlighting disinformation forms the second pillar of this approach. Timely and effective warnings can help inoculate the public against false narratives and mitigate the impact of disinformation campaigns. The power of truth cannot be underestimated; it is a robust tool in negating the effects of falsehoods.

Finally, partnering with international allies multiplies the strength of these efforts. As the PRC's activities span the globe, so too must the counter-efforts. U.S. allies not only provide valuable local knowledge but also amplify a collective message in the face of disinformation. The coordination of partner nations is central to building an integrated front against malign information operations.

The challenges posed by AI-driven disinformation are immense, particularly in the face of adversarial competitors, such as the PRC. It is important to note that this problem transcends regional boundaries and is, in fact, a global concern. However, the combination of monitoring, warning issuance, and partner operations offers a promising strategy to secure the information environment, promote truth, and counter the evolving threats to our free and open societies.

Notes

[1] Xi, "New Asian Security Concept for New Progress in Security Cooperation."

[2] Heath, Grossman, and Clark, *China's Quest for Global Primacy*, p. xvi.

[3] Magnuson, "U.S. Still Playing Catch Up in Information."

[4] Sedova et al., "AI and the Future of Disinformation Campaigns."

[5] Bartz, "Microsoft Chief Says Deep Fakes Are Biggest AI Concern."

[6] Magnuson, "U.S. Still Playing Catch Up in Information."

[7] Beauchamp-Mustafaga, *Chinese Next-Generation Psychological Warfare*.

[8] Kania, "The PLA's Latest Strategic Thinking on the Three Warfares."

[9] On the general approach, see Medeiros, *China's International Behavior*. On specific cases, see Detsch, "Washington Worries China is Winning Over Thailand"; Ciorciari, "Cambodia in 2020"; and Lintner, *The Wa of Myanmar and China's Quest for Global Dominance*.

[10] Chin et al., "When Dragons Watch Bears."

[11] Brady, "Guiding Hand"; Parton, "Revealing China's 'Hidden Hand'"; Stokes and Hsiao, *The People's Liberation Army General Political Department*.

[12] See the Hong Kong, Taiwan, and COVID-19 case studies in DiResta et al., *Telling China's Story*, pp. 19–33.

[13] "China Discreetly Paid for U.S. Social Media Influencers to Tout Beijing Winter Olympics."

[14] Mozur et al., "How Beijing Influences the Influencers."

[15] Barinka and Flatley, "How TikTok Became a US-China National Security Issue."

[16] Office of Public Affairs, U.S. Department of Justice, *40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents*.

[17] "Disclosing Networks of State-Linked Information Operations We've Removed."

[18] DiResta et al., *Telling China's Story*.

[19] Fitzgerald, "China in Xi's 'New Era'"; Siriphon, "Chinese Dream, Emerging Statecraft, and Chinese Influence in the Mekong Region."

[20] Chin et al., "When Dragons Watch Bears."

[21] Matthews, Migacheva, and Brown, *Superspreaders of Malign and Subversive Information on COVID-19*, p. 28.

[22] Roose, "How Does ChatGPT Really Work?"

[23] "Generative A.I. and the Promise of Productivity."

[24] "Generative A.I. and the Promise of Productivity."

[25] The Colbert Report, "The Word—Truthiness."

[26] Newman, "Psychology Explains Why People Are So Easily Duped."

[27] Newman, "Psychology Explains Why People Are So Easily Duped."

[28] Gigerenzer, *Gut Feelings*.

[29] Talboy and Fuller, *Challenging the Appearance of Machine Intelligence*.

[30] Begg, Anas, and Farinacci, "Dissociation of Processes in Belief."

[31] Gleicher et al., *The State of Influence Operations 2017–2020*.

[32] Republic of Singapore, Foreign Interference (Countermeasures) Act 2021.

[33] U.S. Department of Defense, *Department of Defense Strategy for Operations in the Information Environment*.

[34] Phillips, "Revisiting John Boyd and the OODA Loop in Our Time of Transformation."

[35] Pamment, *The EU's Role in Fighting Disinformation*.

[36] Pamment, *The EU's Role in Fighting Disinformation*.

[37] Public Law 114-328, National Defense Authorization Act for Fiscal Year 2017; Section 1287, Global Engagement Center.

[38] Cohen et al., *Combating Foreign Disinformation on Social Media*.

[39] U.S. Code, Title 10, Armed Forces; U.S. Code, Title 50, War and National Defense.

[40] White House, *National Security Strategy*.

[41] Jalbert, Newman, and Schwarz, "Only Half of What I'll Tell You Is True."

[42] Pilditch et al., "Psychological Inoculation Can Reduce Susceptibility to Misinformation in Large Rational Agent Networks."

[43] Greene, Flynn, and Loftus, "Inducing Resistance to Misleading Information."

[44] van der Linden, "Misinformation."

[45] Handley-Miner et al., "The Intentions of Information Sources Can Affect What Information People Think Qualifies as True."

[46] García Lozano et al., "Veracity Assessment of Online Data."

[47] Chin et al., "When Dragons Watch Bears."

[48] U.S. Department of Defense, *Summary of the Irregular Warfare Annex to the National Defense Strategy*.

[49] Mouton and Lucas, "Taking the Measure of AI and National Security."

[50] Polyakova and Boyer, *The Future of Political Warfare*.

[51] Webster et al., "Full Translation: China's 'New Generation Artificial Intelligence Development Plan.'"

[52] Cheng and Zeng, "Shaping AI's Future? China in Global AI Governance."

References

Barinka, Alex, and Daniel Flatley, "How TikTok Became a US-China National Security Issue," *Washington Post*, September 15, 2023.

Bartz, Diane, "Microsoft Chief Says Deep Fakes Are Biggest AI Concern," Reuters, May 25, 2023.

Beauchamp-Mustafaga, Nathan, *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*, RAND Corporation, RR-A853-1, 2023. As of August 30, 2023: https://www.rand.org/pubs/research_reports/RRA853-1.html

Begg, Ian Maynard, Ann Anas, and Suzanne Farinacci, "Dissociation of Processes in Belief: Source Recollection, Statement Familiarity, and the Illusion Of Truth," *Journal of Experimental Psychology: General*, Vol. 121, No. 4, December 1992.

Brady, Anne-Marie, "Guiding Hand: The Role of the CCP Central Propaganda Department in the Current Era," *Westminster Papers in Communication and Culture*, Vol. 3, No. 1, 2006.

Cheng, Jing, and Jinghan Zeng, "Shaping AI's Future? China in Global AI Governance," *Journal of Contemporary China*, Vol. 32, No. 143, 2023.

Chin, Christopher H., Nicholas P. Schaeffer, Christopher J. Parker, and Joseph O. Janke, "When Dragons Watch Bears: Information Warfare Trends and Implications for the Joint Force," *Joint Force Quarterly*, Vol. 109, 2nd Quarter 2023.

"China Discreetly Paid for U.S. Social Media Influencers to Tout Beijing Winter Olympics," CBS News, April 8, 2022.

Ciorciari, John D., "Cambodia in 2020: Preventing a Color Revolution," *Asian Survey*, Vol. 61, No. 1, January/February 2021.

Cohen, Raphael S., Nathan Beauchamp-Mustafaga, Joe Cheravitch, Alyssa Demus, Scott W. Harold, Jeffrey W. Hornung, Jenny Jun, Michael Schwille, Elina Treyger, and Nathan Vest, *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions*, RAND Corporation, RR-4373/1-AF, 2021. As of September 8, 2023: https://www.rand.org/pubs/research_reports/RR4373z1.html

The Colbert Report, "The Word—Truthiness," video, *Comedy Central*, October 17, 2005. As of September 7, 2023: https://www.cc.com/video/63ite2/the-colbert-report-the-word-truthiness

Detsch, Jack, "Washington Worries China is Winning Over Thailand," *Foreign Policy*, June 17, 2022.

DiResta, Renee, Carly Miller, Vanessa Molter, John Pomfret, and Glenn Tiffert, *Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives*, Stanford Internet Observatory, 2020.

"Disclosing Networks of State-Linked Information Operations We've Removed," X Blog, June 12, 2020. As of September 13, 2023: https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020

Fitzgerald, John, "China in Xi's 'New Era': Overstepping Down Under," *Journal of Democracy*, Vol. 29, No. 2, April 2018.

García Lozano, Marianela, Joel Brynielsson, Ulrik Franke, Magnus Rosell, Edward Tjörnhammar, Stefan Varga, and Vladimir Vlassov, "Veracity Assessment of Online Data," *Decision Support Systems*, Vol. 129, February 2020.

"Generative A.I. and the Promise of Productivity," video, Fortune, May 18, 2023. As of September 7, 2023: https://fortune.com/videos/watch/mpw-next-gen-2023---generative-a.i.-and-the-promise-of-productivity-/9cf405d4-2407-4291-b289-5c415cc71b87

Gigerenzer, Gerd, *Gut Feelings: The Intelligence of the Unconscious*, Penguin, 2008.

Gleicher, Nathaniel, Margarita Franklin, David Agranovich, Ben Nimmo, Olga Belogolova, and Mike Torrey, *The State of Influence Operations 2017–2020*, Facebook, May 2021.

Greene, Edith, Marlene S. Flynn, and Elizabeth F. Loftus, "Inducing Resistance to Misleading Information," *Journal of Verbal Learning and Verbal Behavior*, Vol. 21, No. 2, April 1982.

Handley-Miner, Isaac J., Michael Pope, Richard Kenneth Atkins, S. Mo Jones-Jang, Daniel J. McKaughan, Jonathan Phillips, and Liane Young, "The Intentions of Information Sources Can Affect What Information People Think Qualifies as True," *Scientific Reports,* Vol. 13, 2023.

Heath, Timothy R., Derek Grossman, and Asha Clark, *China's Quest for Global Primacy: An Analysis of Chinese International and Defense Strategies to Outcompete the United States*, RAND Corporation, RR-A447-1, 2021. As of December 20, 2023: https://www.rand.org/pubs/research_reports/RRA447-1.html

Jalbert, Madeline, Eryn Newman, and Norbert Schwarz, "Only Half of What I'll Tell You Is True: Expecting to Encounter Falsehoods Reduces Illusory Truth," *Journal of Applied Research in Memory and Cognition*, Vol. 9, No. 4, December 2020.

Kania, Elsa, "The PLA's Latest Strategic Thinking on the Three Warfares," *China Brief*, Vol. 16, No. 13, August 22, 2016.

van der Linden, Sander, "Misinformation: Susceptibility, Spread, and Interventions to Immunize the Public," *Nature Medicine*, Vol. 28, No. 3, March 2022.

Lintner, Bertil, *The Wa of Myanmar and China's Quest for Global Dominance*, Silkworm, 2021.

Magnuson, Stew, "U.S. Still Playing Catch Up in Information," *National Defense*, February 11, 2022.

Matthews, Miriam, Katya Migacheva, and Ryan Andrew Brown, *Superspreaders of Malign and Subversive Information on COVID-19: Russian and Chinese Efforts Targeting the United States*, RAND Corporation, RR-A112-11, 2021. As of December 27, 2023: https://www.rand.org/pubs/research_reports/RRA112-11.html

Medeiros, Evan S., *China's International Behavior: Activism, Opportunism, and Diversification*, RAND Corporation, MG-850-AF, 2009. As of December 27, 2023: https://www.rand.org/pubs/monographs/MG850.html

Mouton, Christopher, and Caleb Lucas, "Taking the Measure of AI and National Security," *The National Interest*, September 19, 2023.

Mozur, Paul, Raymond Zhong, Aaron Krolik, Aliza Aufrichtig, and Nailah Morgan, "How Beijing Influences the Influencers," *New York Times*, December 13, 2021.

Newman, Eryn, "Psychology Explains Why People Are So Easily Duped," *Washington Post*, June 30, 2014.

Office of Public Affairs, U.S. Department of Justice, *40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents*, press release, April 17, 2023.

Pamment, James, *The EU's Role in Fighting Disinformation: Taking Back the Initiative*, Carnegie Endowment for International Peace, July 15, 2020.

Parton, Charles, "Revealing China's 'Hidden Hand,'" *Journal of Democracy*, Vol. 31, No. 4, October 2020.

Phillips, Mark S., "Revisiting John Boyd and the OODA Loop in Our Time of Transformation," *Defense Acquisition Magazine*, Vol. 50, No. 5, September–October 2021.

Pilditch, Toby D., Jon Roozenbeek, Jens Koed Madsen, and Sander van der Linden, "Psychological Inoculation Can Reduce Susceptibility to Misinformation in Large Rational Agent Networks," *Royal Society Open Science*, Vol. 9, No. 8, August, 2022.

Polyakova, Alina, and Spencer Phipps Boyer, *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, Brookings Institution, March 2018.

Public Law 114-328, National Defense Authorization Act for Fiscal Year 2017; Section 1287, Global Engagement Center, December 23, 2016.

Republic of Singapore, Foreign Interference (Countermeasures) Act 2021, November 26, 2021.

Roose, Kevin, "How Does ChatGPT Really Work?" *New York Times*, March 28, 2023.

Sedova, Katerina, Christine McNeill, Aurora Johnson, Aditi Joshi, and Ido Wulkan, "AI and the Future of Disinformation Campaigns," Center for Security and Emerging Technology, December 2021.

Siriphon, Aranya, "Chinese Dream, Emerging Statecraft, and Chinese Influence in the Mekong Region," *International Journal of Asian Studies*, Vol. 18, No. 2, July 2021.

Stokes, Mark, and Russell Hsiao, *The Peoples' Liberation Army General Political Department: Political Warfare with Chinese Characteristics*, Project 2049 Institute, October 14, 2013.

Talboy, Alaina N., and Elizabeth Fuller, *Challenging the Appearance of Machine Intelligence: Cognitive Bias in LLMs and Best Practices for Adoption*, arXiv, 2023.

U.S. Code, Title 10, Armed Forces.

U.S. Code, Title 50, War and National Defense.

U.S. Department of Defense, *Department of Defense Strategy for Operations in the Information Environment*, June 2016.

U.S. Department of Defense, *Summary of the Irregular Warfare Annex to the National Defense Strategy*, 2020.

Webster, Graham, Rogier Creemers, Paul Triolo, and Elsa Kania, "Full Translation: China's 'New Generation Artificial Intelligence Development Plan,'" *New America*, August 1, 2017.

White House, *National Security Strategy*, October 2022.

Xi Jinping, "New Asian Security Concept for New Progress in Security Cooperation," remarks at the Fourth Summit of the Conference on Interaction and Confidence Building Measures in Asia, Shanghai Expo Center, May 21, 2014.

About This Report

As humanity increasingly embraces the digital age, artificial intelligence (AI) and its capabilities are having profound impacts on all facets of society, including information warfare. This impact is particularly relevant in the Indo-Pacific region, where the rise of AI-powered disinformation and malign information campaigns can pose significant challenges to national security and stability. The People's Republic of China (PRC), with its advanced AI technology and extensive information operations, is a significant factor shaping this dynamic landscape. In this report, the authors address the timely issue of AI-powered information warfare in the Indo-Pacific and its implications for regional and global security. Specifically, the authors delve into the appropriate strategies required for an effective near-term response and mitigation of the potential threats. By examining the PRC's tactics, the authors provide an exploration into the future of information warfare in the region and how defense organizations and their partners can adapt and respond to these evolving challenges.

The research reported here was completed in December 2023 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

RAND National Security Research Division

This research was conducted within the Acquisition and Technology Policy Program of the RAND National Security Research Division (NSRD), which operates the RAND National Defense Research Institute (NDRI), a federally funded research and development center (FFRDC) sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise. This research was made possible by NDRI exploratory research funding that was provided through the FFRDC contract and approved by NDRI's primary sponsor.

For more information on the RAND Acquisition and Technology Policy Program, see www.rand.org/nsrd/atp or contact the director (contact information is provided on the webpage).

Acknowledgments

We extend our gratitude to Caitlin Lee and Aaron Frank for their roles in management oversight and quality assurance reviews. Additional thanks go to Michael Spirtas for providing us the opportunity to conduct this research. Our appreciation also goes to Karin Suede for her exceptional assistance in coordinating the administration of this project. We are grateful to Megan McKeever for her meticulous management of our budgets. Special thanks are owed to the military professionals who specialize in the information environment; their generous contributions of time and expertise have been critical. All errors are the sole responsibility of the authors.

For more information on this publication, visit www.rand.org/t/RRA2205-1.

www.rand.org

RR-A2205-1