REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
12-05-2023	FINAL	N/A

4. TITLE AND SUBTITLE

Uncovering the Social Cybersecurity Arsenal: Defending Against China's "Weapons of Mass Persuasion"

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Lieutenant Colonel Elizabeth Pham, United States Marine Corps

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Writing & Teaching Excellence Center
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

China's global media information warfare campaign is quickly challenging U.S. National Security interests in Asia. China recognizes that social media is the quickest way to influence the most significant number of people, and unfiltered access to information with unregulated social media platforms makes democratic societies vulnerable to cyber-enabled malicious influence activities. To defend against China's coercive influence operations, the United States must implement a social cybersecurity and information warfare campaign. An Artificial Intelligence/Machine Learning (AI/ML)-enabled social cybersecurity solution can help characterize the social network and combat cyber-enabled threats. The iterative testing of a social cybersecurity playbook during military exercises and diplomatic engagements can better visualize and evolve actions and reactions within the social, digital network. Last, the United States should pursue a multilateral strategy with key allies and partners to challenge Beijing's aggressive global media offensive. The goal is to block China's efforts to thwart U.S. national security interests by pursuing a coordinated, comprehensive, and proactive strategy that combines social science with technology, joint and interagency efforts, and multilateral cooperation.

15. SUBJECT TERMS (Key words)
Information Warfare
Information Operations
Social Media
Social Cybersecurity
Influence Operations

16. SECURITY CLASSIFICATION OF:	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
			Director, Writing Center

a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	N/A		401-841-6499

Standard Form 298 (Rev. 8-98)

Title: Uncovering the Social Cybersecurity Arsenal: Defending Against China's "Weapons of Mass Persuasion"

INTRODUCTION

Beijing believes that the time has come for China to "reclaim its status as a great power"[1] and challenge a U.S.-led global order that aims to contain the ascent of Sino-centric power.[2] With this rise, China is carrying out an international media campaign that portrays its actions as courageous efforts in the fight against Western hegemony.[3] By grandstanding the Chinese Communist Power's (CCP's) perceived moral and legal justifications, they can better influence public opinion to champion Beijing's actions and potentially denounce any critics for lacking virtue. This polarizing tactic creates virtue-signaling echo chambers that can convince target audiences of Beijing's principled intent to resolve matters and dampen any notion of being vilified as a pariah. Most notably, China is positioning its emboldened and more aggressive domestic and foreign policies (i.e., territorial claims in the East and South China Seas, unification with Taiwan, modernization of its military capabilities, etc.) as moral and justified actions to preserve national security, sovereignty, and regional stability.[4]

China's rise as a great power competitor reignited sociopolitical divides between authoritarian and democratic governments. However, the "ideological cold war"[5] between Beijing and Washington is taking place on the digital battlefield using social media to employ

---

[1] Joshua Kurlantzick, *Beijing's Global Media Offensive: China's Uneven Campaign to Influence Asia and the World* (New York: Oxford University Press, 2023), 6.
[2] Kurlantzick, *Beijing's Global Media Offensive*, 6.
[3] Kurlantzick, *Beijing's Global Media Offensive*, 4-10.
[4] Kurlantzick, *Beijing's Global Media Offensive*, 4-10; Josh Baughman, *How China Wins the Cognitive Domain*, China Aerospace Studies Institute (Montgomery, Alabama: China Aerospace Studies Institute, January 23, 2023) https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/CASI%20Articles/2023-01-23%20How%20China%20Wins%20the%20Cognitive%20Domain.pdf.
[5] Susan L. Shirk, *Overreach: How China Derailed Its Peaceful Rise* (New York: Oxford University Press, 2023), 263.

"weapons of mass persuasion"[6] and seize key terrain in the cognitive domain to break each other's will to resist or fight.[7] China recognizes that social media is the quickest way to influence the most significant number of people, and unfiltered access to information with unregulated social media platforms makes democratic societies vulnerable to cyber-enabled malicious influence activities.[8]

To defend against China's coercive influence operations, the United States must implement a social cybersecurity and information warfare campaign. First, China's social media posture and influence activities within social cyberspace have potential malicious implication to national security. However, an Artificial Intelligence/Machine Learning (AI/ML)-enabled social cybersecurity solution can help characterize the social network and combat cyber-enabled threats. The iterative testing of this social cybersecurity playbook during military exercises and diplomatic engagements can better visualize and evolve actions and reactions within the social, digital network. These iterations will help develop countermeasures against deceitful propaganda that could threaten national security interests. Last, the United States should pursue a multilateral strategy with key allies and partners to challenge Beijing's aggressive global media offensive. The goal is to block China's efforts to thwart U.S. national security interests by pursuing a coordinated, comprehensive, and proactive strategy that

---

[6] The phrase "weapons of mass persuasion" was taken from the title of a new book about targeting the human mind through social media. The source is discussed in this article. Sander Van Der Linden, "Weapons of Mass Persuasion: Tracing the Story of Psychological Targeting on Social Media," *Behavioral Scientist*, April 10, 2023, https://behavioralscientist.org/weapons-of-mass-persuasion-tracing-the-story-of-psychological-targeting-on-social-media/.

[7] Josh Baughman discusses a People's Liberation Army (PLA) daily article called "A Brief Analysis of the Basic Meaning of Cognitive Domain Operations," where the PLA discusses that "Cognitive domain operations take the human brain as the main combat space, and focus on striking, weakening, and dismantling the enemy's will to fight, using human psychological weaknesses such as fear, anxiety, and suspicion as a breakthrough point, focusing on soft-kill methods to create an atmosphere of insecurity, uncertainty, and mistrust within the enemy, and increasing their internal friction and decision-making doubts." Baughman, *How China Wins the Cognitive Domain.*

[8] Baughman, *How China Wins the Cognitive Domain.*

combines social science with technology, joint and interagency efforts, and multilateral cooperation.

CHINA'S USE OF FOREIGN AND DOMESTIC SOCIAL MEDIA PLATFORMS

As of January 2023, the top 15 most prominent social media platforms in the world are owned by both the U.S. and China, with a total reach of at least 3.86 billion followers or 48% of the world's population.[9] With nearly half of the world using American and Chinese-based social media platforms, the fight for the social narrative between these two superpowers cannot be ignored. The CCP uses its access to Western-based social media platforms, such as *Twitter*, *Facebook*, *Instagram*, *Snapchat*, *WhatsApp*, *YouTube*, etc., to conduct influence campaigns and gather intelligence information to coercively manipulate target audiences.[10] In 2019, despite the ban on *Twitter* and *Facebook* in mainland China, China's largest state-owned news sources, such as *China Global Television Network* (*CGTN*), *China's Daily*, *People's Daily*, and *Xinhua's Facebook* pages, had the highest number of international followers across all global news sites—beating the *BBC News*, *CNN*, and the *New York Times*.[11] In addition, *CCTN* added 40 times more *Facebook* followers than *CNN* and twice as many followers on *Twitter* than the internationally popular *Al Jazeera English* platform.[12] China is also buying its way into Western-owned social

---

[9] Of the top 15 most prominent social media platforms, Russia owns only one with approximately 700 million users. The other 14 platforms are shared between the U.S. (eight platforms in the top 15) and China (6 platforms in the top 15). To achieve the 48%, the author took the total number of social media users (3.96 billion), divided it by the total estimated world population (approximately 8.03 billion), and multiplied the result by 100 to achieve 48%. However, China is allowing Russia increased access to its state-owned social media platforms and social media accounts on Western-owned platforms and thus this total reach may be more of less than what is stated here in this paper. S. Dixon, "Most Popular Social Networks Worldwide as of January 2023, Ranked by Number of Monthly Active Users," *Statista*, February 14, 2023, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/; Current World Population, Worldometer, accessed May 6, 2023, https://www.worldometers.info/world-population/.

[10] Kurlantzick, *Beijing's Global Media Offensive*, 21-32, 159-162, 228-246.

[11] "China is Using Facebook to Build a Huge Audience Around the World," *The Economist*, April 10, 2019, https://www.economist.com/graphic-detail/2019/04/20/china-is-using-facebook-to-build-a-huge-audience-around-the-world.

[12] Kurlantzick, *Beijing's Global Media Offensive*, 176-177.

media feeds via electronic commerce and paid-for content promotions that appear as sponsored information by either the news feed or the platform itself.[13] China also funds *Facebook* social media content farms that seed and grow disinformation with fake accounts.[14] It is estimated that a topic with eight "likes" on *Facebook* can reach an average of six million users.[15] These content farms actively recruit followers en masse or penetrate groups with similar or shared interests to initially gain trust and then gradually and increasingly inject content that criticizes U.S. political leadership and democratic institutions.[16]

In 2020, the CCP used bots and fake personas to spread disinformation on Western-owned social media platforms that disproportionally criticized the U.S. and Europe's initial COVID-19 response. Beijing also included an attempt to falsely accuse the U.S. of creating the virus as a military bioweapon and tied these accusations to failures within democracies to manage pandemic responses. Furthermore, Russian propaganda infiltrated Chinese-owned social media platforms, amplified the messages on U.S.-owned sites, and exacerbated Beijing's COVID-19 disinformation efforts. Meanwhile, China overwhelmingly praised Beijing's leadership for its actions to protect its citizens and stop the spread of the virus. Due to rising U.S. and foreign discord, *Twitter* removed nearly 170,000 fake accounts and personas tied to COVID-19 disinformation influence actions and Hong Kong protests.[17]

TikTok, *WeChat*, and *Weibo* are Chinese-owned social media platforms that are significant disinformation threat vectors. *TikTok* is the fastest-growing social media video streaming application that has quickly amassed over 1.05 billion users and is currently the

---

[13] Kurlantzick, *Beijing's Global Media Offensive*, 177-180.
[14] Kurlantzick, *Beijing's Global Media Offensive*, 242-243.
[15] Linden, "Weapons of Mass Persuasion."
[16] Kurlantzick, *Beijing's Global Media Offensive*, 242-243.
[17] Kurlantzick, *Beijing's Global Media Offensive*, 243-246, 282-284.

world's most visited site.[18] However, *TikTok* faces scrutiny by U.S. lawmakers for its AI-enabled data harvesting capability that collects sensitive user information.[19] Additionally, due to *TikTok's* growing reach and popularity, U.S. officials are concerned that the information gained could make users susceptible to foreign intelligence actions and undue influence by Russian and Chinese propagandists.[20] In 2022, Russian bots and trolls flooded China's *TikTok* platform with videos that attempted to bolster Russian support against supposed "Western-fueled aggression"[21] while sowing anti-Ukrainian messages.[22] China increasingly enables Russian propaganda to infiltrate advertising spaces on Chinese social media platforms to spread misinformation, disinformation, and conspiratorial theories regarding the war in Ukraine.[23]

With over 1.3 billion users worldwide, *WeChat* is the largest Chinese-owned social media platform that allows users a single location to communicate, shop, request ride-share services, conduct business transactions, and receive news alerts.[24] In mainland China alone, it is estimated that over 45 billion messages are exchanged between *WeChat* users daily.[25] *WeChat* is also prolific in several Asian countries and is known to push pro-CCP domestic and foreign policy content from major Chinese news sites (i.e., *Xinhua*, *Global Times*, and *CCTN*) that suppress, curtail, or omit content critical of Beijing.[26]

---

[18] *TikTok* is the world's 6th most powerful social media platform, with over 1.05 billion registered users and growing. *TikTok* features short video clips that promote dance moves, social challenges, and memes that attract mass appeal amongst predominately younger demographics between the ages of 16-24. Dixon, "Most Popular Social Networks Worldwide as of January 2023"; Kurlantzick, *Beijing's Global Media Offensive*, 228-231, 283.
[19] Brian Fung, "TikTok collects a lot of Data," *CNN Business*, March 24, 2023, https://www.cnn.com/2023/03/24/tech/tiktok-ban-national-security-hearing/index.html.
[20] Fung, "TikTok collects a lot of Data."
[21] "War via TikTok: Russia's New Tool for Propaganda Machine," *CBS News,* February 26, 2022, https://www.cbsnews.com/news/russia-tiktok-social-media-propoganda-disinformation/.
[22] "War via TikTok."
[23] Kurlantzick, *Beijing's Global Media Offensive*, 161-162.
[24] Dixon, "Most Popular Social Networks Worldwide as of January 2023"; Kurlantzick, *Beijing's Global Media Offensive*, 228-230.
[25] Kurlantzick, *Beijing's Global Media Offensive*, 229.
[26] Kurlantzick, *Beijing's Global Media Offensive*, 232-235.

The U.S. must be prepared to fight against China's proliferation of misinformation and disinformation on social media, which threatens to sow political discord, incite chaos, and manipulate the cognitive domain for political gains. However, U.S. solutions to counter Chinese disinformation should be cautious of suppressing social media platforms or censoring free speech but rather find ways to maneuver within the infosphere safely. The U.S. should explore the potential for incorporating Artificial Intelligence/Machine Learning (AI/ML) and the social science discipline of social cybersecurity to understand better the threats, vulnerabilities, and opportunities associated with countering malign influence campaigns in the digital network.

SOCIAL CYBERSECURITY: COMBATING AN ORDER OF BATTLE THAT CONSISTS OF BOTS, TROLLS, SOCK-PUPPETS, CYBORGS, DEEP FAKES, AND MEMES.

Social cybersecurity is a discipline that studies how cyber-mediated changes impact human behavior, society, culture, and politics and aims to develop a cyberinfrastructure that helps societies preserve their character in an information environment with cyber threats.[27] As depicted in Figure 1, social cybersecurity focuses on identifying and characterizing the actors (the "who"), the methods, maneuvers, and threat vectors used for manipulation (the "how"), the communication objectives and desired outcomes (the "why"), as well as the measures and countermeasures that either enable information flow or secure malicious or undue influence activities (the "impact").[28] The focus is on how information is engineered and moves within the social media digital network to influence and manipulate human perceptions.

---

[27] Social cybersecurity revolves around human interactions in the cognitive domain, but it also incorporates computer science, AI, engineering, mathematics, and statistics. Social cybersecurity differs from cybersecurity or computer security as it does not focus on protecting hardware, computer systems, or cloud computing devices from cyber threats. Kathleen M. Carley, "Social Cybersecurity: An Emerging Science," *Computational and Mathematical Organization Theory* 26, no. 4, (November 2020): 366, https://doi.org/10.1007/s10588-020-09322-9.

[28] The first step begins with discovering the threat on the social media platform. The next step encompasses the heart of the social analysis that identifies the threat, the BEND applicable information, and social network maneuvers and finds the targeted actors and groups. The last step is to evaluate the intent and overall communications objectives

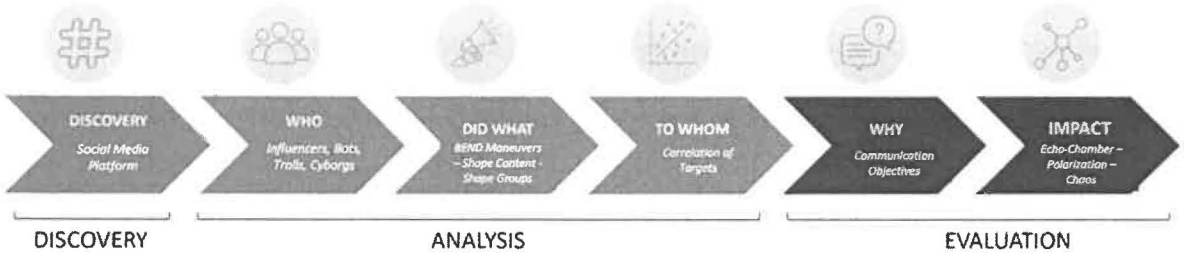

Figure 1. Social Cybersecurity "Methodology for Discovery, Analysis, and Evaluation" [29]

The Center for Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University developed a social cybersecurity social media analysis method that can serve as the basis for a comprehensive social cybersecurity playbook—The BEND framework.[30] This social cybersecurity BEND method, aided by AI/ML tools, outlines how information and networks are manipulated or "maneuvered" in the social media infosphere.[31]

---

and the desired result that would be compared to the overall final impact of the original threat. Carley, "Social Cybersecurity: An Emerging Science," 366-367.

[29] This figure and methodology were adapted from two documents. The first was a research paper from the Center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University that applied the methods of social cybersecurity and the BEND framework to two case studies involving social media (*Twitter*) in Indonesia. The methodology (discovery, analysis, and evaluation) and the arrow graphic and circle icons were used as the baseline that will be applied to this paper. The other document was from a brief from Dr. Kathleen Carley of the Center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University. The BEND Framework outlined in this brief was applied to this figure to explain better the BEND methods and how it fits into an overall social cybersecurity analysis tool that can be used to create future influence and counter-influence playbooks. Adya Danaditya, Lynnette Hui Xian Ng, and Kathleen M. Carley, "From Curious Hashtags to Polarized Effect: Profiling Coordinated Actions in Indonesian Twitter Discourse," *Social Network for Analysis and Mining* 12, no. 105: 5. https://doi.org/10.1007/s13278-022-00936-2; Kathleen M. Carly, "Social Cybersecurity: A New Approach to Understanding How Bots and Memes are Used to Spread Disinformation and Alter Groups in Social Media," (presentation, Computational Analysis of Social and Organizational Systems, Carnegie Mellon University, Pittsburgh, Pennsylvania, September 25, 2019), https://www.cylab.cmu.edu/_files/documents/ml-1-3-kcarley-social-cybersecurity.pdf.

[30] Carley, "Social Cybersecurity: An Emerging Science," 368, 371-374; David M. Beskow and Kathleen M. Carley, "Social Cybersecurity: An Emerging National Security Requirement," *Military Review: The Professional Journal of the U.S. Army, Army University Press* 99, no. 2 (March-April 2019): 117-120, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b/; Danaditya, Ng, and Carley, "From Curious Hashtags to Polarized Effect," 5.

[31] There are two types of maneuvers: Information maneuvers and social network maneuvers. Information maneuvers focus on shaping the content and understanding what and how subjects are being discussed. Social network

Table 1 shows the BEND framework, which outlines 16 ways (or communication objectives) that information warfare campaigns use social media to shape perceptions in the cognitive domain. The first category of these objectives aims to manipulate the narrative. It includes what is being discussed and how the information is perceived between various actors or within topic-oriented community groups. It is further broken down into four positive objectives or the "four E's" (Engage, Explain, Excite, Enhance) and four negative objectives or the "four D's" (Dismiss, Distort, Dismay, Distract). The "four E's" and "four D's" are maneuvers that use selective language to evoke emotional responses, dismiss or encourage discourse, introduce relevant or irrelevant information, or distort or reinterpret the underlying themes and messages shared between groups.[32]

Examples of common information maneuver tactics and their correlations to the BEND framework include the following:

The Sleeper Effect, where ideas and information are introduced into a group, leaves a lasting impression and becomes unconsciously embedded in one's mind. The information may be "distorted," cause "dismay," or attempt to "excite" actors and further encourage "enhancing" the topic further as the information gains more traction over time.[33]

---

maneuvers focus on shaping relationships within the community and understanding who is communicating with whom and who are key leaders and influencers of a group. These maneuvers are not independent or exclusive of each other—Influence campaigns use multiple maneuvers to achieve various communication objectives. Carley, "Social Cybersecurity: An Emerging Science," 368, 371-374; Beskow and Carley, "Social Cybersecurity: An Emerging National Security Requirement," 117-125; Kathleen M. Carley, "Socially Influence Campaigns: The Coordination of Events using Bots and Misinformation," (presentation, The CMU Centers for Informed Democracy and Social Cybersecurity, Computational Analysis of Social and Organizational Systems, Carnegie Mellon University, Pittsburgh, Pennsylvania, June 25, 2021), https://prepare-vo.org/sites/preparevo/files/Kathleen_Carley_slides.pdf.

[32] The BEND term is derived from the amalgamation of the letters "E," "D," "B," and "N." Each letter is part of an alliteration representing 16 communication objectives or information and social network maneuvers. Carley, "Social Cybersecurity: An Emerging Science," 368, 371-374; Beskow and Carley, "Social Cybersecurity: An Emerging National Security Requirement," 118-125.

[33] Keyshawn Shaahid, "What is the Sleeper Effect? How does Media use it one YOU," *Illumination's Mirror*, May 26, 2022, https://medium.com/illuminations-mirror/what-is-the-sleeper-effect-how-does-media-use-it-one-you-65f3b7615787.

Smokescreen, where content is introduced to a group that "distracts" them from paying attention to the original subject or hides the original content.[34]

Hashtag Latching is where potentially irrelevant and unrelated information is linked or tied to a #hashtag that can support any knowledge network maneuvers.[35]

Threadjacking or the fierce "hijacking" of a conversation or information discussed within a group with the intent to abruptly change the subject or move the conversation in a different direction than was originally intended. This tactic can support any of the information maneuver communication objectives.[36]

Clickbaiting attempts to introduce controversial, sensational, and potentially salacious information that is misleading, deceptive, or inaccurate with the desire to increase the number of "clicks" or peak user interest that will, in turn, give the information higher priority and "excite" or "dismay" and potentially "enhance" the group to continue discussing the topic.[37]

The second category focuses on manipulating the social network or interactions between actors or topic-oriented community groups. It is further broken down into four positive objectives or the "four B's" (Back, Build, Bridge, Boost) and four negative objectives or the "four N's" (Neutralize, Nuke, Narrow, Neglect). The "four B's" and "four N's" are maneuvers that expand or limit the number of followers, influencers, or thought leaders within a group, make topic-oriented groups seem smaller or larger than they are, connect groups to other actors, sever or isolate fractions within groups, and create new or dismantle existing groups within the network.[38]

---

[34] Beskow and Carley, "Social Cybersecurity: An Emerging National Security Requirement," 117-125.
[35] Beskow and Carley, "Social Cybersecurity: An Emerging National Security Requirement," 117-125.
[36] Beskow and Carley, "Social Cybersecurity: An Emerging National Security Requirement," 117-125.
[37] Ann Gynn, "Is Clickbait Ever Used for Good?" *Content Marketing Institute*, July 7, 2020, https://contentmarketinginstitute.com/articles/clickbait-headlines-good-tactic/.
[38] Carley, "Social Cybersecurity: An Emerging Science," 372-373.

Examples of common social network maneuvers and their correlations to the BEND framework include the following:

Co-opting with Super-Spreader (Opinion Leaders) or Super-Friends, where links and associations with social media influencers can help the spread of a narrative that can create a "back" campaign that increases the agency of an opinion leader or "boost" the size of a group or even "bridge" groups together based on increasing shared interests.[39]

The appearance of consensus, where information is promoted as being agreed upon by the majority of the group, and therefore, the information should be believed and followed by everyone in the group. This tactic can "build" and "bridge" communities over shared interests or "nuke" and "narrow" groups based on the desired communication objectives.[40]

Bridging actors and communities, where topic-oriented groups are eventually linked to other topic-oriented groups by slowly injecting and infiltrating one group's idea(s) into the other until both groups are wholly joined.[41]

---

[39] Beskow and Carley, "Social Cybersecurity: An Emerging National Security Requirement," 117-125.
[40] Beskow and Carley, "Social Cybersecurity: An Emerging National Security Requirement," 117-125.
[41] Beskow and Carley, "Social Cybersecurity: An Emerging National Security Requirement," 117-125.

	Information Maneuver		Network Maneuver	
	Knowledge network manipulation		Social network manipulation	
	Things you can do by affecting what is being discussed		Things you can do by affecting who is talking/listening to whom	
Positive	**Engage**	Discussion that brings up a related but relevant topic	**Back**	Actions that increase the importance of the opinion leader
Positive	**Explain**	Discussion that provides details on or elaborates the topic	**Build**	Actions that create a group or the appearance of a group
Positive	**Excite**	Discussion that brings joy/happiness/cheer/enthusiasm to group	**Bridge**	Actions that build a connection between two or more groups
Positive	**Enhance**	Discussion that encourages the group to continue with the topic	**Boost**	Actions that grow the size of the group or make it appear that it has grown
Negative	**Dismiss**	Discussion about why the topic is not important	**Neutralize**	Actions that limit the effectiveness of opinion leader such as by reducing the number who can or do follow or reply or attend to
Negative	**Distort**	Discussion that alters the main message of the topic	**Nuke**	Actions that lead to a group being dismantled
Negative	**Dismay**	Discussion about a topic that will bring worry/sadness/anger to group	**Narrow**	Actions that lead to the group becoming sequestered from other groups
Negative	**Distract**	Discussion about a totally different topic and irrelevant	**Neglect**	Actions that reduce the size of the group or make it appear that the group has grown smaller

Table 1. The "BEND" Framework: Describing Social Cybersecurity Maneuvers [42]

To effectively apply the BEND framework, it is essential to use AI/ML-enabled social network analysis tools to process and decipher large amounts of data at high speed with relevance. The opponents in the cognitive domain are not limited to human users but also include AI programs that manifest as bots, trolls, sock-puppets, and cyborgs that can create and disseminate content such as deep fakes, memes, and written propaganda.[43] Software programs

[42] This table is taken directly from the cited source. Beskow and Carley, "Social Cybersecurity: An Emerging National Security Requirement," 123.

[43] A bot is an AI-created social media profile that can mimic basic human actions on social media platforms including retweets, likes, follow, friend, reply, etc. According to Dr. Kathleen Carley from the Computational Analysis of Social and Organizational Systems Department at Carnegie Mellon University, there are 11 different

such as *BotHunter*, *MemeHunter*, and *NetMapper* are crucial in analyzing bot characteristics, processing images, and understanding the sentiment and meaning of words in context, respectively.[44] Network analysis and visualization tools like *Netanomics ORA-PRO* are essential in characterizing overall network structures and interactions between groups and platforms.[45] These AI/ML programs are examples of the many technologically advanced tools readily available for employment. Therefore, utilizing an AI/ML-enabled social cybersecurity method, such as the BEND framework, for social media analysis can serve as the foundation for building a comprehensive social cybersecurity playbook that can be implemented today. With this playbook, users can quickly and precisely analyze social media networks and identify opportunities to exploit adversarial influence campaigns in real-time.

"BENDING" CHINA WITH THE SOCIAL CYBERSECURITY PLAYBOOK

A potential approach to counter China's global influence operations through social media is to continuously apply, test, refine, and iterate the AI-enabled social cybersecurity playbook in real time. Two actionable opportunities exist for the U.S. to seize immediately. The first

---

types of bots, including amplifier bots, chaos bots, intimidation bots, news bots, Russian- and Iranian-specific bots, etc. Bots can also evolve to mask tactics or be repurposed by bot creators to coordinate influence campaigns automatically. Trolls are human personas that purposefully push content to sow discord and chaos within and between groups. Sock-puppets are fake identities or groups that try to make specific agendas that usually attack bots, trolls, and cyborgs. Cyborgs are human-controlled bots, where humans can determine when and where they would like to control a bot and thus making interactions in social media seem more "human." Deep fakes are digitally altered media (voice, photo, or video) that falsely depicts human activity and is used for disinformation. Memes are images or videos altered with a script or writing to invoke a shared cultural or behavioral sentiment. David Beskow and Kathleen Carley," Investing in Social Cybersecurity," *Naval Science and Technology: Future Force* 6, no. 2 (2020): 17-19, https://www.nre.navy.mil/media/document/future-force-vol-6-no-2-2020; Bryan Ek, Lucas A. Overbey, and Michael Grass, "Combating Misinformation: An Ecological Approach," *Naval Science and Technology: Future Force* 6, no. 2 (2020): 39, https://www.nre.navy.mil/media/document/future-force-vol-6-no-2-2020.

[44] *BotHunter* can analyze bot characteristics to look for the digital signatures of malicious bots that show high levels of activity across multiple accounts, friends, likes, followers, etc., and can process over 4.5 million tweets in 60 minutes and pending software, can process 60 million tweets in one day or 24 hours. *MemeHunter's* algorithms can process over 7,000 images per hour. Language technologies like *NetMapper* are essential to understanding the sentiment and meaning of words in context and deciphering a statement's true intent and meaning. Beskow and Carley, "Investing in Social Cybersecurity," 18; Carley, "Social Cybersecurity: An Emerging Science," 375.

[45] Carley, "Social Cybersecurity: An Emerging Science," 374.

opportunity is aimed at China's media offensive in Taiwan. Beijing's influence campaigns primarily focus on coercing Taiwan to peacefully accept unification, persuading the international community to support China's pursuit of Taiwan, and deterring any U.S.-led military intervention that could disrupt Beijing's unification plans.[46] The U.S. could apply the playbook to identify critical actors, analyze social media information flow, and characterize the messages exchanged between China and Taiwan. According to a 2021 study by RAND, China uses Taiwan as a testing ground to develop disinformation and misinformation attack vectors on social media.[47] China creates fake social media profiles and uses CCP content farms to encourage political and civil discord, consistently ridicule Taiwan's leadership, and portray them as incompetent and weak.[48] Beijing also tries to instill fear by pushing the narrative that the U.S. will not come to Taiwan's aid in case of attack.[49] An interviewee in Taiwan claimed that China conducts thousands of media cyber-attacks daily.[50] China's sophisticated and aggressive disinformation campaign against Taiwan provides real-time opportunities to measure the impact of Beijing's influence actions and potentially reveal areas for exploitation.[51]

The second opportunity to test, evaluate, and refine counter-influence tactics using the cybersecurity playbook is during USINDOPACOM Theater Security Cooperation (TSC) Operations, Activities, and Investments (OAIs). Specifically, large-scale joint military,

---

[46] The article discusses China's three roads to unification. However, with the third road, China must be prepared to use brute military force to compel unification with Taiwan forcefully. Dan Blumenthal and Fred Kagan, "China Has Three Roads to Taiwan: The U.S. Must Block Them All," *The Hill*, March 13, 2023, https://thehill.com/opinion/national-security/3896916-china-has-three-roads-to-taiwan-the-us-must-block-them-all/.
[47] Scott W. Harold, Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung, *Chinese Disinformation Efforts on Social Media*, RR4373Z3, (Santa Monica, CA: RAND, 2021), x.
[48] When applying the BEND framework, this could potentially be "distort," "dismay," and "neutralize" maneuvers. Harold et al., *Chinese Disinformation Efforts on Social Media*, 4.
[49] This could potentially be "distort" and "dismay" maneuvers when applying the BEND framework. Harold et al., *Chinese Disinformation Efforts on Social Media*, 4.
[50] Harold et al., *Chinese Disinformation Efforts on Social Media*, 66.
[51] Kurlantzick, *Beijing's Global Media Offensive*, 244.

interagency, and multilateral operations inside the First Island Chain would elicit reactions from the CCP, and potentially neighboring North and Southeast Asia countries, that create a target-rich environment to challenge China's information and influence campaigns. This approach would offer real-time feedback on China's knowledge and network manipulation within the BEND framework, allowing the U.S. to validate China's social media information warfare capabilities outside of Taiwan. To better understand how to implement the playbook, characterize the digital network, and find ways to counter China's media offensive, iterative testing of a social cybersecurity playbook during military exercises and diplomatic engagements is essential. These iterations help develop countermeasures against deceitful propaganda undermining integrated operational and national defense objectives.

A MULTILATERAL APPROACH TO SOCIAL CYBERSECURITY: A UBIQUITOUS NATIONAL SECURITY INTEREST

Although China has predominately focused its information warfare offense against Taiwan,[52] countries like Singapore, Malaysia, Australia, New Zealand, South Korea, and select European nations have all been subjected to China's disinformation tactics.[53] Overseas Chinese propaganda proxy groups have pushed aggressive influence operations with "political astroturfing," or fake grassroots movements to counter anti-China policies or open seams and vulnerabilities to sow discord within democratic nations.[54] Evidence shows that China's *WeChat* platform monitors user conversations and activities outside mainland China, potentially censoring content critical of Beijing.[55] Consequently, the threat of China's coercive and manipulative influence offensive is ubiquitous. The U.S. can form and lead a multinational, joint,

---

[52] Harold et al., *Chinese Disinformation Efforts on Social Media*, 4.
[53] Kurlantzick, *Beijing's Global Media Offensive*, 101-102.
[54] Kurlantzick, *Beijing's Global Media Offensive*, 101-102, 127.
[55] Kurlantzick, *Beijing's Global Media Offensive*, 237.

and interagency task force to safeguard communication networks from disinformation campaigns and social cyber-attacks on social media. This task force strengthens collaboration and cooperation with key allies and partners and demonstrates U.S. resolve and credible commitment to regional security and stability. To engender trust and demonstrate transparency, all information sharing and social cybersecurity collaboration would be via publicly available, unclassified enclaves and cloud computing sites enabled by AI/ML systems. Additionally, allies and partners can help analyze the networks, provide real-time indications and warnings of potential social cyberspace attacks, and refine the social cybersecurity playbook and AI/ML systems with regional, language, and cultural inputs. Investing in allies, partnerships, and interagency relationships will result in force-multiplying effects that will allow the task force to out cycle China's ability to gain and maintain the initiative in spreading disinformation. Moreover, this task force would message a steadfast multilateral front that can challenge and deter China's gray zone activities in the information domain.

IS WHAT'S PAST TRULY PROLOGUE?

One may argue that China's disinformation campaign is focused on only two objectives—maintaining internal regime stability and unification with Taiwan. Moreover, there exists only anecdotal evidence to suggest that China has any interest in conducting disinformation operations on a global scale.[56] Furthermore, there is limited evidence to suggest that Beijing is conducting harmful influence operations or adopting Russia's "flamethrower"[57] tactics of using large-scale, sophisticated disinformation to incite fear, terror, chaos, and instability.[58] Instead, Beijing aims to demonstrate a prominence of "morality and jurisprudence"[59] and to be viewed as

---

[56] Harold et al., *Chinese Disinformation Efforts on Social Media*, 3.
[57] Kurlantzick, *Beijing's Global Media Offensive*, 103.
[58] Kurlantzick, *Beijing's Global Media Offensive*, 95-99, 240-241, 291.
[59] Baughman, "How China Wins the Cognitive Domain."

having a stable and secure government.[60] China only wants to "… tell China's story well…"[61] and show its rise as a responsible world power. Besides, China's use, thus far, of misinformation and disinformation through social media is still in its infancy, with little history of implementation and success.[62]

However, the rapid and exponential evolution of technological advances in cyber, space, and AI are transforming how humans receive and process information at an unprecedented speed. Thus, past failures and perceived lack of evidence should not drive the predictors of how China will behave in the future. China is learning fast and is increasingly investing in some of the world's most significant telecommunications infrastructure projects, the most capable digital and satellite communications, and the most prolific fiber-optic and mobile networks.[63] One might argue that the most successful influence operations are the ones that gradually and slowly change and influence perspectives over time–the most potent disinformation and misinformation campaigns are so insidious that those who are being targeted have little to no realization of being victimized. If left uncontested, China will have unfettered access to U.S. networks, allowing Beijing to slowly and gradually manipulate Western perspectives, break down mental resiliencies, and gain asymmetric advantages in the cognitive domain. An unrestricted spread of disinformation will surge civil discord, incite chaos, erode trust in societies, destabilize governments, and weaken alliances. Worst still, it will fuel fear among the populace, giving rise to authoritarianism and the suppression of free speech and civil liberties. This reality would play right into China's hands as the CCP seeks to promote and export its authoritarianism to reshape

---

[60] Baughman, "How China Wins the Cognitive Domain"; Kurlantzick, *Beijing's Global Media Offensive*, 95-99, 240-241.
[61] Shirk, *Overreach*, 232.
[62] Kurlantzick, *Beijing's Global Media Offensive*, 276-290.
[63] Kurlantzick, *Beijing's Global Media Offensive*, 276-290.

the world in its image.[64] It is time to take proactive measures to paralyze China's infectious media offensive.

CONCLUSION

Defending against gradual, insidious attacks of influence and persuasion camouflaged within truths with low observable signatures of deception is a long, complex, and daunting task. However, there is hope. The defense against China's global information warfare campaign will require a whole-of-government approach with cooperation and integration across various disciplines. The U.S. can harness together a powerful nexus of academia, social science experts, interagency professionals, AI/ML technocrats, media industry, military combatant commanders, and international partners and allies to collectively defend and preserve freedom, civil liberties, democratic institutions, and global stability. It is time to "speak truth to power" and uncover the collective social cybersecurity arsenal to defend against China's "weapons of mass persuasion."

---

[64] Kurlantzick, *Beijing's Global Media Offensive*, 6.

BIBLIOGRAPHY

Baughman, Josh. *How China Wins the Cognitive Domain*. China Aerospace Studies Institute. Montgomery, Alabama: China Aerospace Studies Institute, January 23, 2023. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/CASI%20Articles/2023-01-23%20How%20China%20Wins%20the%20Cognitive%20Domain.pdf.

Beskow, David M. and Kathleen M. Carley. "Social Cybersecurity: An Emerging National Security Requirement." *Military Review: The Professional Journal of the U.S. Army, Army University Press* 99, no. 2 (March-April 2019: 117-127. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b/

Beskow, David and Kathleen Carley. "Investing in Social Cybersecurity." *Naval Science and Technology: Future Force* 6, no. 2 (2020): 16-21. https://www.nre.navy.mil/media/document/future-force-vol-6-no-2-2020

Blumenthal, Dan and Fred Kagan. "China Has Three Roads to Taiwan: The U.S. Must Block Them All." *The Hill*, March 13, 2023. https://thehill.com/opinion/national-security/3896916-china-has-three-roads-to-taiwan-the-us-must-block-them-all/.

Carley, Kathleen M. "Social Cybersecurity: An Emerging Science." *Computational and Mathematical Organization Theory* 26, no. 4 (November 2020): 365-381. https://doi.org/10.1007/s10588-020-09322-9.

Carly, Kathleen M. "Social Cybersecurity: A New Approach to Understanding How Bots and Memes are Used to Spread Disinformation and Alter Groups in Social Media." Presentation at Computational Analysis of Social and Organizational Systems, Carnegie

Mellon University, Pittsburgh, Pennsylvania, September 25, 2019. https://www.cylab.cmu.edu/_files/documents/ml-1-3-kcarley-social-cybersecurity.pdf.

Carley, Kathleen M. "Socially Influence Campaigns: The Coordination of Events using Bots and Misinformation." Presentation at the CMU Centers for Informed Democracy and Social Cybersecurity, Computational Analysis of Social and Organizational Systems, Carnegie Mellon University, Pittsburgh, Pennsylvania, June 25, 2021. https://prepare-vo.org/sites/preparevo/files/Kathleen_Carley_slides.pdf.

"Current World Population." Worldometer, accessed May 6, 2023. https://www.worldometers.info/world-population/.

Danaditya, Adya, Lynnette Hui Xian Ng, and Kathleen M. Carley. "From Curious Hashtags to Polarized Effect: Profiling Coordinated Actions in Indonesian Twitter Discourse." *Social Network for Analysis and Mining* 12, no. 105 (2022) https://doi.org/10.1007/s13278-022-00936-2.

Dixon, S. "Most Popular Social Networks Worldwide as of January 2023, Ranked by Number of Monthly Active Users." *Statista*, February 14, 2023. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

"China is Using Facebook to Build a Huge Audience Around the World." *The Economist*, April 10, 2019. https://www.economist.com/graphic-detail/2019/04/20/china-is-using-facebook-to-build-a-huge-audience-around-the-world.

Ek, Bryan, Lucas A. Overbey, and Michael Grass. "Combating Misinformation: An Ecological Approach." *Naval Science and Technology: Future Force* 6, no. 2 (2020): 38-41. https://www.nre.navy.mil/media/document/future-force-vol-6-no-2-2020.

Fung, Brian. "TikTok collects a Lot of Data." *CNN Business*, March 24, 2023. https://www.cnn.com/2023/03/24/tech/tiktok-ban-national-security-hearing/index.html.

Gynn, Ann. "Is Clickbait Ever Used for Good?" *Content Marketing Institute*, July 7, 2020. https://contentmarketinginstitute.com/articles/clickbait-headlines-good-tactic/.

Harold, Scott W., Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung. *Chinese Disinformation Efforts on Social Media*. RR4373Z3. Santa Monica, CA: RAND, 2021.

Kurlantzick, Joshua. *Beijing's Global Media Offensive: China's Uneven Campaign to Influence Asia and the World*. New York: Oxford University Press, 2023.

Linden, Sander Van Der. "Weapons of Mass Persuasion: Tracing the Story of Psychological Targeting on Social Media." *Behavioral Scientist*, April 10, 2023. https://behavioralscientist.org/weapons-of-mass-persuasion-tracing-the-story-of-psychological-targeting-on-social-media/.

Mazzarr, Michael J., Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, and Luke J. Matthews. *The Emerging Risk of Virtual Societal Warfare*. RR2614. Santa Monica, CA: RAND, 2019. https://www.rand.org/t/RR2714.

Shirk, Susan L. *Overreach: How China Derailed Its Peaceful Rise*. New York: Oxford University Press, 2023.

Shaahid, Keyshawn. "What is the Sleeper Effect? How does Media use it one YOU." *Illumination's Mirror*, May 26, 2022. https://medium.com/illuminations-mirror/what-is-the-sleeper-effect-how-does-media-use-it-one-you-65f3b7615787.

"War via TikTok: Russia's New Tool for Propaganda Machine." *CBS News,* February 26, 2022. https://www.cbsnews.com/news/russia-tiktok-social-media-propoganda-disinformation/.