Testimony before the U.S.-China Economic and Security Review Commission

Hearing on "Deterring PRC Aggression Towards Taiwan"

Fiona S. Cunningham, Ph.D.

Assistant Professor of Political Science and International Affairs
George Washington University

Stanton Nuclear Security Fellow
Carnegie Endowment for International Peace

February 18, 2021

Commissioner Goodwin, Commissioner Talent, members of the commission, thank you for inviting me to appear before you today to discuss deterring the People's Republic of China (PRC) military actions targeting Taiwan. I have been asked to comment on the Cross-Strait military balance. My testimony will examine how authoritative and other Chinese sources define the goals and employment of the People's Liberation Army's (PLA) information operations capabilities, including for space, cyber, electronic, and psychological warfare, the role of PRC commercial actors in those operations, the challenges those capabilities pose for Taiwan and the United States, and provide several recommendations for Congress to consider.

PLA Information Operations in a Taiwan Contingency

The PLA's information operations capabilities include its space, cyber, electronic and psychological warfare capabilities. These capabilities can be used for stand-alone operations to achieve strategic deterrence, or for operational effects in combination with the PLA's general purpose conventional capabilities for land, sea, or air operations. When employed for stand-alone operations, these capabilities enable the PLA to take escalatory steps below the threshold of armed conflict in peacetime or nuclear conflict during a local conventional war, exploiting an adversary's hesitancy to cross those key thresholds.[1] The PLA also views these capabilities as integral to its ability to win local informatized wars because they degrade an adversary's ability to exploit information in conventional operations.[2]

The PRC is vulnerable to space, cyber, psychological and electronic warfare operations, which constrains the PLA's employment of these capabilities against a sophisticated adversary like the United States. It remains unclear whether the PLA has the ability to integrate effects from space, cyber, electronic warfare, and psychological operations, and integrate those operations with conventional operations, to achieve the joint effects its doctrinal writings aspire to. The main foci of PLA developments in these information capabilities in the future are likely to be enhancing capabilities and the capability to integrate effects in joint operations, adjusting its capabilities and employment to account for its growing vulnerability in these domains, and its improving conventional capabilities.

PLA information operations pose three key challenges for Taiwan and the United States. First, when used for strategic deterrence, they create escalation risks. Second, designing appropriate responses to these attacks is challenging because they occur below key conflict thresholds that the United States and Taiwan may be hesitant to cross. Third, when used for operational effects, these capabilities pose challenges for U.S.-Taiwan operations to defend Taiwanese territory and interests from PRC attacks. To address these challenges, Congress should support crisis stability talks with the PRC and invest in open-source research of PLA plans and capabilities.

[1] For more detailed arguments about China's use of space and cyber capabilities for strategic deterrence in local wars, see Fiona S. Cunningham, "Maximizing Leverage: Explaining China's Strategic Force Posture Choices in Limited Wars" (Ph.D. Dissertation, Cambridge, M.A., Political Science Department, Massachusetts Institute of Technology, 2018).

[2] China's current military strategic guideline is "winning informatized local wars." See M. Taylor Fravel, *Active Defense: China's Military Strategy Since 1949* (Princeton, N.J., 2019), chap. 7.

Goals and Employment of PLA Information Operations

The PLA's information operations capabilities serve two goals: strategic deterrence and achieving operational effects in a conflict.[3]

Strategic Deterrence

The PLA's information operations capabilities are a key component of its capabilities for strategic deterrence. The PLA was first tasked with developing capabilities and operations to carry out strategic deterrence in local wars in 1993, which includes "information deterrence" and "space deterrence" alongside conventional and nuclear deterrence.[4] The objectives of PLA strategic deterrence are to prevent the outbreak of war, reduce the severity of an outbreak of war, stop escalation, and prevent or reduce the damage inflicted in a war.[5] PLA writings indicate that military means of deterrence should be coordinated with non-military means, such as diplomatic, economic, and political actions.[6]

The PLA views strategic deterrence as operating during peacetime, crises, and wars. In peacetime, strategic deterrence actions provide warning and defense against a latent adversary. During a crisis, those actions coerce an adversary to back down and creates favorable conditions for the transition to war. During a war, they might coerce an adversary to come to terms.[7] PLA texts indicate that the targets and tempo of operations for strategic deterrence during crises should be carefully calibrated to coerce but not provoke an adversary into starting a war.[8] The targets of those operations in wartime could include high-value targets that would have a strong effect on adversary decision-makers and society, including civilian critical infrastructure.[9]

PLA texts are often silent about the inadvertent escalation risks that cyber and space attacks on high-value targets would pose. They caution that an adversary needs to be carefully studied, and targets and means carefully selected, to avoid provoking retaliation at a higher level of violence. Nevertheless, they appear confident that signaling with military capabilities could be calibrated to coerce an adversary without prompting it to further escalate the conflict.[10]

[3] Shou Xiaosong, ed., 战略学 *[The Science of Military Strategy]* (Beijing: Junshi Kexue Yuan Chubanshe, 2013), 118.

[4] Chen Zhou, 面向未来的国家安全与国防*[The Future National Security and Defense]* (Beijing: Guofang Daxue Chubanshe, 2008), 215.

[5] Ibid., 217; Shou, *The Science of Military Strategy*, 119.

[6] Xiao Tianliang, ed., 战略学 *[The Science of Military Strategy]*, revised (Beijing: Guofang Daxue Chubanshe, 2017), 135.

[7] Shou, *The Science of Military Strategy*, 119.

[8] Xiao, *The Science of Military Strategy*, 134.

[9] Zhou Xinsheng, ed., 军种战略教程 *[Study Guide to Military Service Strategy]* (Beijing: Junshi Kexue Yuan Chubanshe, 2013), 125.

[10] Fiona S. Cunningham and M. Taylor Fravel, "Dangerous Confidence? Chinese Views of Nuclear Escalation," *International Security* 44, no. 2 (2019): 103.

Operational Effects

The PLA frequently describes its goals for using space, cyber, and electronic warfare as attacking an adversary's information networks to gain a military advantage while protecting its own information networks to ensure continuing exploitation of information on the battlefield.[11] These capabilities would enable the PLA to seize "information superiority" with preemptive attacks on an adversary's information networks, sensors, and infrastructure at the outset of a conflict to create favorable conditions for subsequent land, air and sea operations.[12] Psychological warfare also creates favorable conditions for conventional operations by diminishing the cohesion and morale of an adversary's military and society.[13]

PLA texts suggest that the military advantage generated by these attacks would in theory enable it to carry out an island landing campaign, the campaign for an amphibious landing on Taiwan, as well as other PLA campaigns that could target Taiwanese interests, including a joint firepower campaign and naval blockade campaign. The PLA's primary campaign for achieving operational effects using these capabilities is its joint information operations campaign, described below, which would combine cyber, electronic, space, and psychological warfare to degrade an enemy's information capabilities.[14]

Cyber Operations

The PLA has developed offensive cyber capabilities and extensive cyber surveillance capabilities since the early 2000s. Development of its defensive cyber capabilities has lagged behind offense and surveillance. It has also prioritized situational awareness capabilities, including the ability to attribute cyber attacks, since approximately 2015.[15] The PRC officially acknowledged the PLA's building of defensively oriented cyber capabilities for the first time in 2015,[16] but does not officially acknowledge its possession of offensive cyber capabilities. PLA media, PLA research texts and Western media reports indicate that China has the capability to carry out offensive cyber operations on adversary tactical military networks and homeland critical infrastructure networks in both Taiwan and the United States.[17]

[11] Wang Houqing and Zhang Xingye, eds., 战役学 *[The Science of Military Campaigns]* (Beijing: Guofang Daxue Chubanshe, 2000), 168; Zhang Yuliang, ed., 战役学*[The Science of Military Campaigns]* (Beijing: Guofang Daxue Chubanshe, 2006), 151–52; Ye Zheng, ed. 信息作战学教程 *[Study Guide to Information Warfare]* (Junshi Kexue Yuan Chubanshe, 2013), 4.

[12] Zhang, *The Science of Military Campaigns*, 151–7.

[13] Ibid., 203

[14] Ibid., 157–61.

[15] State Council Information Office of the People's Republic of China, *China's Military Strategy* (Beijing: Renmin Chubanshe, 2015).

[16] Ibid.

[17] Shane Harris, "China's Cyber-Militia," *National Journal*, May 31, 2008, https://www.nationaljournal.com/s/636724/chinas-cyber-militia?mref=search-result ;Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage" (Washington, D.C.: Northrop Grumman Corp for the U.S.-China Economic and Security Review Commission, March 7, 2012), 21, 23–24; J. Michael Cole, "China's Shifting Cyber Focus on Taiwan," The Diplomat, April 30, 2013, https://thediplomat.com/2013/04/chinas-shifting-cyber-focus-on-taiwan/; Sean Lyngaas, "Taiwan Accuses Chinese Hackers of Aggressive Attacks on Government Agencies," CyberScoop, August 19, 2020, https://www.cyberscoop.com/taiwan-china-hacking-apt40/.

PLA writings have been enthusiastic about the effectiveness of offensive cyber operations against a conventionally superior military such as the United States since the early 2000s. That enthusiasm has endured despite a dramatic growth in the PRC's vulnerability to cyber attacks between 2000 and 2010.[18] Cyber operations take aim at the "soft underbelly" of an information-dependent adversary's military and society. Cyber capabilities are also viewed as the "strategic commanding heights" of future joint operations because they provide the linkages both within the multi-domain battlespace, and between military conflict and politics, economics, technology and culture.[19]

PLA texts describe the use of cyber attacks for both strategic deterrence and operational effects. Some PLA texts describe attacks on an adversary's critical infrastructure in a crisis as a form of "information deterrence."[20] The PLA might have raised the threshold for such attacks from a crisis to a conflict in recognition of the emerging international consensus that such attacks would be an act of war.[21] Cyber attacks are described as one means for attacking an enemy's systems in local wars under informatized conditions. Other means include electronic warfare, another "soft kill" option, "hard kill" options, and the "three warfares." According to one 2013 PLA textbook, cyber attack methods would include "systems intrusion, computer virus attacks, attacks to cut off servers, and network deception attacks," focusing on enemy communications hubs, radar stations, computer network nodes, and important civilian networks (民用网络系统).[22]

Counterspace Operations

The PLA began to test counterspace weapons in approximately 2005-6.[23] Since then, it has developed and tested a wide array of kinetic and non-kinetic counterspace weapons.[24] The PLA's investments in space-based support for its own conventional operations has also increased dramatically. PLA texts observe that China's capabilities to defend its space assets, including space situational awareness capabilities, have lagged behind its development of attack and support capabilities.[25] The PLA does not officially acknowledge its counterspace capabilities. It remains unclear from open sources which PLA counterspace capabilities are operational and which are still in development.

PLA texts recognized that China's own valuable space assets made it vulnerable to counterspace attacks even when it had only a few dozen satellites in orbit in the early 2000s. As a consequence, the PLA envisages that any space hostilities would be limited.[26] Chinese

[18] Ariel (Eli) Levite and Jinghua Lü, "Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?" *China Military Science*, January 24, 2019, https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213.
[19] Wang Kebin, "坚定不移走中国特色信息强军之路 [Resolutely Take the Path of Strengthening the Military by Informatization with Chinese Characteristics]," *Zhongguo Junshi Kexue [China Military Science]* 2 (2015): 3.
[20] Xiao, *The Science of Military Strategy*, 133–34.
[21] Chuanying Lu, "Forging Stability in Cyberspace," *Survival* 62, no. 2 (2020): 130.
[22] Zhou, *Study Guide to Military Service Strategy*, 125.
[23] Michael R. Gordon and David S. Cloud, "U.S. Knew of China's Missile Test, but Kept Silent," *The New York Times*, April 23, 2007.
[24] Defense Intelligence Agency, "Challenges to Security in Space" (Washington, D.C.: Defense Intelligence Agency, January 2019), 20–21.
[25] Xiao, *The Science of Military Strategy*, 397–98.
[26] Shou, *The Science of Military Strategy*, 186.

assessments of the effectiveness of using direct-ascent ASAT weapons for operational effects have also diminished over time.[27] The PLA is aware of the fragility of the space environment and the close relationship between certain space capabilities, computer networks, and nuclear capabilities.[28] These texts suggest that the PLA might prefer to employ non-kinetic counterspace capabilities for limited attacks (possibly with reversible effects) if employed for operational effects, while relying on kinetic weapons such as its direct-ascent ASAT capability for strategic deterrence in a conflict.

PLA texts indicate that counterspace weapons could deter at least three kinds of unwanted adversary actions by holding an adversary's satellites at risk: harassment of China's space capabilities,[29] an adversary's conventional military operations,[30] and degradation of China's nuclear retaliatory capability.[31] Descriptions of the PLA joint information warfare campaign from 2006 included counterspace capabilities, but provided no details about the kinds of attacks (e.g. kinetic or non-kinetic) that might be employed.[32]

Electronic Warfare

The PLA established an electronic warfare capability in the late 1970s.[33] By 2009, it had a basic capability to disrupt U.S. space-based information support for military operations.[34] Electronic warfare operations would involve both soft kill capabilities such as electronic jamming, as well as hard kill capabilities such as anti-radiation missiles, high-powered laser weapons and electromagnetic pulse weapons.[35]

PLA texts frequently describe the employment of electronic warfare for operational effects as well as deterrence at an operational rather than strategic level.[36] One PLA text describes the goal of electronic warfare as to "weaken and damage the effectiveness of an enemy's use of electronic equipment, and protect the effectiveness and regular functioning of one's own electronic equipment."[37] Electronic warfare would "damage and interfere with an enemy's command and

[27] Tong Zhao, "Practical Ways to Promote U.S.-China Arms Control Cooperation" (Washington, D.C.: Carnegie Endowment for International Peace, October 2020).
[28] Zhang Shibo,战争新高低 *[The New High Ground of Warfare]* (Beijing: Guofang Daxue Chubanshe, 2016), 29.
[29] Shou, *Zhanlue Xue*, 182.
[30] Jiang Lianju, ed., 空间作战学教程 *[Study Guide to Space Warfare]* (Beijing: Junshi Kexue Yuan Chubanshe, 2013), 127.
[31] Deng Lizhong, "信息条件下第二炮兵核导弹作战运用理论研究 [Research on the Combat Role of Second Artillery Nuclear Missile Forces under Informatized Conditions]" (Masters Thesis, Beijing, National Defense University, 2004), 41–42.
[32] Zhang, *The Science of Military* Campaigns, 114, 135.
[33] Liu Jixian,叶剑英年谱 *[Chronology of Ye Jianying]*, vol. 2 (Beijing: Zhongyang Wenxian Chubanshe, 2007), 1098.
[34] John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," China Strategic Perspectives (Washington, D.C.: Institute for National Strategic Studies, National Defense University, September 2018), 8.
[35] Xiao, *The Science of Military Strategy*, 230–31.
[36] Electronic warfare operations may be strategic if targeting adversary satellites. John Costello and Peter Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations," in *China's Evolving Military Strategy*, ed. Joe McReynolds (Washington, D.C.: Jamestown Foundation, 2016), 167–68.
[37] Xiao, *The Science of Military Strategy*, 230. See also Ye, *Study Guide to Information Warfare*, 90–91.

control system, influencing the regular employment of its weapons equipment systems, delay and pin down an adversary's combat operations, to seize favorable conditions for victory."[38] In recognition of the PLA's vulnerability to electronic countermeasures, teaching texts emphasize that defense is equally important to offense in the contest for superiority in the electromagnetic domain in contemporary warfare.[39]

Psychological Warfare

Since the early 2000s, the PLA has combined its psychological warfare (心理战) capabilities with "public opinion warfare" and "legal warfare" as part of its "three warfares" concept. The PLA views these three capabilities as intimately related and complementary.[40] The target of psychological operations is the enemy's state, society, and its military knowledge and decision-making systems. In contrast, legal warfare and public opinion warfare aim to shape the views of international society and public opinion.[41]

The PLA envisages using psychological warfare for both strategic deterrence and operational effects. Psychological offense-defense (心理攻防) refers to "employing specific information and media, … [to] exert influence over a targeted opponent's psychology and behavior, according to strategic intentions and combat tasks."[42] One PLA text indicates that the aim of psychological warfare is to shatter the enemy's morale, weaken its combat effectiveness, and influence and divide enemy factions," to reduce the cost of a military victory or avoid having to fight a war at all.[43] Psychological warfare could be employed as part of the strategic deterrence action of "creating a war atmosphere" to pressure and deter an adversary with actions indicating that war is imminent.[44] In general, armed attacks serve as a backstop for the three warfares. In wartime, however, one PLA text specifies that psychological operations should be combined with armed attacks to strengthen and expand their effects.[45]

Prominent cyber-enabled information operations and increased Chinese dependence on the internet have drawn the attention of analysts to China's own vulnerabilities to psychological warfare. A former PLA official attributed the Arab Spring uprisings to the United States facilitated by the social media platforms of U.S. companies.[46] According to one Chinese cybersecurity expert, the Russian 2016 U.S. election meddling raised the possibility of interference in Chinese internal affairs, including Chinese Communist Party leadership

[38] Xiao, *The Science of Military Strategy*, 230.
[39] Ye, *Study Guide to Information Warfare*, 94.
[40] Elsa B. Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," Center for International Maritime Security, August 25, 2016, http://cimsec.org/plas-latest-strategic-thinking-three-warfares/27468.
[41] Xiao, *The Science of Military Strategy*, 234–35.
[42] Ibid., 233.
[43] Ibid., 234.
[44] Ibid., 131.
[45] Ibid., 234, 236.
[46] Hao Yeli, "对美国加快网络战发展的几点思考 [Some Thoughts on the U.S. Rapid Development of Cyber Warfare]," *Waiguo Junshi Xueshu [Foreign Military Arts]*, no. 8 (2015), 3.

transitions.[47] A PLA researcher also noted that foreign states could leverage online content to weaken PLA loyalty to the Party.[48] It remains unclear whether these perceptions of societal and military vulnerability to psychological warfare might constrain PLA employment of psychological warfare in the same manner that cyber and space vulnerability have influenced PLA employment of those capabilities, or not in a similar manner to electronic warfare.

The Joint Information Warfare Campaign

PLA texts envisage that cyber attacks, electronic warfare, and psychological warfare capabilities could be used in combination for joint operations to limit an adversary's ability to exploit information in a future local war. The official *Military Terminology of the Chinese People's Liberation Army* defines information operations (信息作战) as follows: "comprehensively employing electronic warfare, cyber warfare (网络战), psychological warfare, etc. to form operations to attack or confront an adversary. The goal is to interfere with and damage enemy information and information systems in the cyber and electromagnetic domain, influence and weaken an enemy's capabilities for information gathering, transmission, management, exploitation and decision-making, and ensure the stable functioning of one's own information systems functions, information security and accuracy of decisions."[49]

PLA textbooks published from 2006-2013 outline a joint information warfare campaign. The campaign was largely aspirational at the time those texts were published. China lacked the organizational structure to implement such a campaign,[50] while its capabilities were likely too rudimentary to have the desired effects on an adversary's military networks. Since 2013, however, China has developed capabilities and an organizational structure better equipped to coordinate the effects of each component of the campaign and with the conventional joint operations.[51]

It is likely that the joint information warfare campaign remains one of the campaigns the PLA is preparing to fight in a future local war. The Central Military Commission (CMC) recently issued a new set of *Joint Operations Regulations for the Chinese People's Liberation Army (Trial)* which updated existing PLA-wide doctrine reflected in textbooks published during the 2000s.[52] Although no information about the content of these updated regulations is publicly available, there are hints of the PLA's continuing intent to integrate the effects of its information warfare capabilities in future campaigns. In 2017 the PLA paraded an information operations group at the Zhuruihe training facility, which included an Information Support Formation and Electronic Reconnaissance Formation, both from its newly-created Strategic Support Force (SSF), as well

[47] Lu Chuanying, "黑客干预美国大选 国际网络安全冲突升级 [Hackers Interfere in U.S. Election, International Cybersecurity Conflicts Escalate]," Shanghai Institutes for International Studies, January 5, 2017, http://www.siis.org.cn/Research/Info/3895.

[48] Zhang Lizhong, "论信息网络时代部队思想政治工作 [On the Ideological and Political Work of the Armed Forces in the Mobile Internet Era]," *Zhongguo Junshi Kexue [China Military Science]* 4 (2016): 95–103.

[49] Junshi Kexue Yuan [Academy of Military Science], 中国人民解放军军语 *[Military Terminology of the Chinese People's Liberation Army]* (Beijing: Junshi Kexue Yuan Chubanshe, 2011), 259.

[50] Costello and Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations," 187–88.

[51] Costello and McReynolds, "China's Strategic Support Force: A Force for a New Era," 40–41.

[52] "China's Guidelines on Joint Operations Aim for Future Warfare: Defense Spokesperson," *China Military Online*, November 27, 2020, http://english.scio.gov.cn/pressroom/2020-11/27/content_76954237.htm.

as an Electronic Countermeasures Formation from the PLA Army and an Unmanned Aerial Vehicle Formation from the PLA Army and Air Force.[53] The SSF consolidated space, cyber, electronic warfare and three warfares units scattered throughout the PLA into a unified organization reporting directly to the CMC.[54] It remains unclear what degree of coordination among cyber, electronic, and psychological warfare operations is facilitated within the SSF. The organizational structure coordinating the information warfare campaign components within the SSF with components in other parts of the PLA also remains unclear.[55]

The Role of PRC Commercial Actors

PRC commercial actors might assist the PLA's information operations with personnel or equipment, likely under the guise of the PRC's efforts to enhance military-civilian fusion (军民融合). In 2017, the PRC established a Central Civil-Military Integration Development Committee, chaired by Xi Jinping, which elevated the importance of the concept both within and outside of the PLA.[56] Commercial actors may provide specialized personnel for PLA reserve and militia units supporting PLA space, cyber, electronic warfare, and psychological operations.[57] Where PLA media and Western analysts have identified commercial actors contributing to these PLA capabilities, they have tended to serve in support rather than combat roles.[58] Commercial actors may also support the PLA in its development of weapons equipment, defense and situational awareness capabilities. For example, reducing reliance on foreign-produced information communications and technology (ICT) products has been a key thrust of China's cyber defense efforts to reduce its vulnerability to cyber attacks.[59] The first Chinese actors to demonstrate improvements in the country's cyber situational awareness capabilities were also Chinese cybersecurity companies, who publicly attributed cyber intrusions into Chinese companies to U.S. government agencies.[60]

[53] Dennis J. Blasko, Elsa B. Kania, and Stephen Armitage, "The PLA at 90: On the Road to Becoming a World-Class Military?" *China Brief* 17, no. 11 (August 17, 2017), https://jamestown.org/program/the-pla-at-90-on-the-road-to-becoming-a-world-class-military/.

[54] "专家:战略支援部队将贯穿作战全过程 是致胜关键 [Expert: Strategic Support Force Is the Key to Victory throughout the Complete Process of War," *Renmin Wang*, January 5, 2016, http://military.people.com.cn/n1/2016/0105/c1011-28011251.html; Costello and McReynolds, "China's Strategic Support Force: A Force for a New Era"; Elsa B. Kania and John Costello, "Seizing the Commanding Heights: The PLA Strategic Support Force in Chinese Military Power," *Journal of Strategic Studies* (2020): 1–47.

[55] The Joint Staff Department Network-Electronic Bureau, formed out of the former General Staff Department Fourth Department headquarters, could play such a role. See Kania and Costello, "Seizing the Commanding Heights," 12.

[56] Huang Panyue, "Xi to Head Civil-Military Integration Body," *Global Times*, January 23, 2017, http://eng.chinamil.com.cn/view/2017-01/23/content_7462990.htm.

[57] Xiao, *The Science of Military Strategy*, 397, 403.

[58] Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York, N.Y: Oxford University Press, 2015), 208; John Dotson, "Military-Civil Fusion and Electromagnetic Spectrum Management in the PLA," *China Brief* 19, no. 18 (October 8, 2019).

[59] Adam Segal, "Seizing Core Technologies: China Responds to U.S. Technology Competition," *China Leadership Monitor*, June 1, 2019, https://www.prcleader.org/segal-clm-60.

[60] "The CIA Hacking Group (APT-C-39) Conducts Cyber-Espionage Operation on China's Critical Industries for 11 Years," *Qihoo 360 Threat Intelligence Center* (blog), March 2, 2020, https://blogs.360.cn/post/APT-C-39_CIA_EN.html.

Future Developments

Three factors are likely to characterize future PLA developments in the use of space, cyber, electronic, and psychological warfare. First, the PLA is likely to continue to develop the sophistication of its capabilities and operations. It is also likely to improve its ability to integrate these capabilities with each other and conventional joint operations to amplify their effects on Taiwanese and U.S. decision-making.[61] Second, as the PLA continues to pursue informatization, it will rely more on information networks and space operations to support its conventional operations. As a result, it will become more vulnerable to adversary space, cyber, electronic warfare and psychological operations. The PRC more broadly will remain vulnerable to cyber attacks, counterspace operations, and psychological warfare as economic, governmental and societal actors remain dependent on the internet, information networks, and civilian space assets for key functions. This combination of increasing capability and vulnerability creates incentives for greater precision, caution, and attention to escalation management in the PLA's employment of these capabilities. Third, as the PLA's general purpose conventional capabilities and ability to carry out operations such as an island landing campaign improves, it is likely to rely less on strategic deterrence to achieve its political aims. Its use of space, cyber, electronic and psychological warfare capabilities may also focus more on enhancing the operational effects of conventional operations than strategic deterrence.

Challenges for the United States and Taiwan

PLA employment of space, cyber, electronic warfare, and psychological warfare capabilities for strategic deterrence and operational effects pose a number of challenges for the United States and Taiwan. Three key challenges are highlighted below: the risk of escalation, the difficulty of crafting appropriate responses, and complications for conventional operations.

First, PLA space, cyber, electronic and psychological warfare attacks create escalation risks, especially when they are used to pursue strategic deterrence goals in a crisis or conflict. The PLA invested in these capabilities in part because they provide it with coercive options to compensate for an unfavorable cross-Strait balance in conventional military capabilities without directly confronting U.S. advantages in conventional operations and nuclear weaponry.[62] These capabilities could increase the intensity of a crisis right up to the threshold of armed conflict or, when used in a conflict, up to the threshold of a nuclear war.[63]

PLA officers' apparent confidence that they could finely calibrate the use of force for strategic deterrence to force an adversary to back down but not escalate to an armed conflict or a higher level of violence during a war could lead to Chinese miscalculations of U.S. or Taiwanese reactions to such an attack.[64] Accidental or unauthorized use of information operations capabilities poses a second type of escalation risk. Third, there is a risk of inadvertent escalation

[61] State Council Information Office of the People's Republic of China, "China's National Defense in the New Era," July 2019, 12–14.

[62] Cunningham, "Maximizing Leverage: Explaining China's Strategic Force Posture Choices in Limited Wars."

[63] Ibid., Costello and Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations," 189.

[64] Cunningham and Fravel, "Dangerous Confidence? Chinese Views of Nuclear Escalation."

if the United States or Taiwan discovers PLA intelligence-gathering activity in space, cyberspace or either country's information platforms in a crisis that cannot be distinguished from preparations for an attack in a timely manner.[65] Finally, there is a risk of inadvertent escalation if PLA space, cyber, or electronic warfare capabilities are used to damage components of the U.S. nuclear arsenal or its supporting information systems.[66]

Second, designing effective and proportionate responses to the use of PLA information operations capabilities is challenging. Threatening retaliatory strikes to deter these attacks are unlikely to be effective if they involve the United States or Taiwan crossing key thresholds of armed conflict or nuclear war. Nevertheless, increasing PRC vulnerability to symmetrical, in-kind attacks offers the United States and Taiwan an increasing number of proportionate response options while also increasing the constraints on the PLA to conduct such attacks for fear of such retaliation. Other response options include investing in resilience, redundancy and defenses of U.S. and Taiwanese assets the PLA is likely to target.[67]

Third, these information operations will complicate U.S., Taiwanese and other allied efforts to defend territory and other interests such as commercial shipping if the PRC uses them in concert with conventional military operations. The United States and Taiwanese militaries are likely to be operating in a degraded information environment from the outset of any future U.S.-China conflict.

Policy Recommendations

The analysis above yields the following recommendations for Congress:

First, Congress should support executive efforts to pursue crisis stability talks with the PRC. Crisis stability talks would enable the United States to communicate its concerns about the potential for escalation resulting from PLA use of information capabilities, explore mechanisms for crisis communications, and learn about the PLA's escalation thresholds. Nuclear dialogues at the 1.5-track level have increased awareness of inadvertent escalation risks among China's arms control community.[68] This success could be replicated in these non-nuclear domains.

Second, Congress should support and encourage open-source analysis of Chinese military strategy within U.S. and allied academic and policy organizations.[69] The Chinese government

[65] Ben Buchanan and Fiona S. Cunningham, "Preparing the Cyber Battlefield: Assessing A Novel Escalation Risk in a U.S.-China Crisis," *Texas National Security Review* 3, no. 4 (2020).

[66] James M. Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (Summer 2018): 56–99.

[67] Benjamin W. Bahney, Jonathan Pearl, and Michael Markey, "Antisatellite Weapons and the Growing Instability of Deterrence," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Erik Gartzke and Jon R. Lindsay (New York, N.Y: Oxford University Press, 2019), 138–43; Jacquelyn G. Schneider, "Deterrence in and through Cyberspace," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Gartzke and Lindsay, 104–15.

[68] Zhao Tong and Li Bin, "The Underappreciated Risks of Entanglement: A Chinese Perspective," in *Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks*, ed. James M. Acton (Washington, D.C.: Carnegie Endowment for International Peace, 2017), 69.

[69] M. Taylor Fravel, "Testimony before the U.S.-China Economic and Security Review Commission," hearing on "A 'World-Class' Military: Assessing China's Global Military Ambitions," June 20, 2019, 13.

provides very little official information about its information warfare capabilities and operations. Open-source analysis of unofficial Chinese-language materials is therefore a key method for understanding PLA actions in a future conflict. Numerous Chinese-language materials are available on these topics that reveal PLA thinking about the goals, employment and future of these capabilities. The timely and systematic collection, translation, and wide dissemination of these materials outside of government would increase literacy about Chinese military strategy within the U.S. and allied policy communities and contribute to informed public debate about China policy.