EMERGING TECHNOLOGIES, EMERGING CHALLENGES — THE POTENTIAL EMPLOYMENT OF NEW TECHNOLOGIES IN FUTURE PLA NC3



Recommended Citation

Elsa B. Kania, "EMERGING TECHNOLOGIES, EMERGING CHALLENGES — THE POTENTIAL EMPLOYMENT OF NEW TECHNOLOGIES IN FUTURE PLA NC3", NAPSNet Special Reports, September 05, 2019, https://nautilus.org/napsnet/napsnet-special-reports/emerging-technologie--in-future-pla-nuclear-command-control-and-communications/

ELSA B. KANIA

SEPTEMBER 5, 2019

I. INTRODUCTION

In this essay, Elsa Kania assesses how emerging technologies--including artificial intelligence, cloud computing, fifth-generation telecommunications, and quantum communications--may affect China's nuclear command, control, and communications (NC3). Kania concludes: "Although certain of these technologies could enhance China's confidence in its NC3 in ways that may prove stabilizing, there are also reasons for concern that the potential introduction of such complex, untested technologies could also create new risks and exacerbate the threat of miscalculation."

Elsa B. Kania is a Research Fellow with the Center for Security and Emerging Technology at Georgetown University and an Adjunct Senior Fellow with the Technology and National Security Program at the Center for a New American Security. She is also a PhD student in the Department of Government at Harvard University.

A podcast with Elsa Kania, Peter Hayes, and Philip Reiner on China's NC3 and emerging technologies is found **here**.

Acknowledgments: The workshop was funded by the John D. and Catherine T. MacArthur Foundation.

This report is published simultaneously here by Nautilus Institute and here by Technology for Global Security and is published under a 4.0 International Creative Commons License the terms of which are found here.

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

Banner image is by Lauren Hostetter of Heyhoss Design

II. NAPSNET SPECIAL REPORT BY ELSA B. KANIA

EMERGING TECHNOLOGIES, EMERGING CHALLENGES — THE POTENTIAL EMPLOYMENT OF NEW TECHNOLOGIES IN FUTURE PLA NC3

SEPTEMBER 5, 2019

Summary

This paper presents an initial assessment of the implications of certain emerging technologies for the future of nuclear command, control, and communications (NC3). In particular, this examination of the potential for new technological developments in NC3 is informed by an assessment of the strategic objectives and current research underway by the Chinese People's Liberation Army (PLA)

at a time when Chinese nuclear posture is evolving dynamically. I evaluate how the PLA's advances in and approach to emerging technologies—including artificial intelligence, cloud computing, fifth-generation telecommunications, and quantum communications—may contribute to its future command and control of nuclear and conventional operations. This analysis considers initial indicators of how the PLA is starting to explore and/or may choose in the future to leverage these emerging technologies in various elements of its NC3 architecture, including for early warning, decision support, improved targeting, and secure communications. Although certain of these technologies could enhance China's confidence in its NC3 in ways that may prove stabilizing, there are also reasons for concern that the potential introduction of such complex, untested technologies could also create new risks and exacerbate the threat of miscalculation.

Introduction

China and the United States confront shared concerns and distinct challenges as each seeks to pursue new directions in its development and modernization of NC3. The U.S. military must reckon with aging systems that are facing new threats, particularly in space and cyberspace, as the 2018 Nuclear Posture Review highlighted.[1] General Hyten of U.S. Strategic Command has emphasized, " We have to modernize the entire architecture. And so, as you see the modernization plans coming in; make sure, number one, it's the 21st century information architecture."[2] By contrast, China must not only address similar issues of modernization but also remains in the process of developing and operationalizing new elements of its NC3 apparatus, including the introduction and construction of capabilities for strategic early warning. Possessing less of an extensive architecture of legacy systems—and currently undertaking a transition from a monad to a triad in its nuclear posture—China might undertake distinct approaches to its NC3 relative to other nations. Perhaps, as a result, China may prove more open to leveraging certain emerging technologies, including to compensate for current shortcomings in its military capabilities. This paper leverages a range of open sources, particularly Chinese-language materials, including textbooks to authoritative commentaries and technical publications, and builds upon the existing literature to evaluate some of these trends and potential developments.[3]

New Directions and Challenges for China's NC3 Systems

The future trajectory of China's NC3 architecture will be shaped by its strategic concerns and evolving missions.[4] At present, the PLA is at a stage in the development of its nuclear arsenal that is uniquely transitional. Traditionally, the former Second Artillery Force, which has been elevated to become the PLA Rocket Force (解放军火箭军) in the course of recent military reforms, has been solely responsible for China's "lean and effective" arsenal, which was aimed towards a minimal requirement often characterized as "assured retaliation."[5] However, the PLA is currently transitioning from this initial 'monadic' posture, which initially involved exclusively intercontinental ballistic missiles (ICBMS),[6] to a full triad.[7] There is a more capable fleet of Type 096 SSBNs under development, which will result in a more credible sea-based deterrent, augmenting the Type 094 SSBNs already in service, for the PLA Navy (PLAN).[8] Meanwhile, the PLA Air Force (PLAAF) plans to field a new strategic bomber, likely to be known as the H-20, in the years to come, which could be armed with new air-launched ballistic missiles that include a nuclear payload.[9] In the process, the PLA Navy and Air Force appear to be embracing their new status and missions as "strategic service s," undergoing transformations that will contribute to their capabilities to bolster deterrence and war-fighting.[10] At the same time, ongoing developments that are intended to enhance the PLA's future capabilities have included progress in MIRVS and hypersonic glide vehicles, as well as techniques such as chaff, decoys, and jamming.[11] The current debate and emerging concerns about the potential feasibility of counterforce capabilities could result in a redoubling of such developments.[12]

These new strategic capabilities raise questions of command and control that the PLA likely remains in the process of resolving. For example, the PLA Rocket Force, under the direct command and control of the Central Military Commission (CMC), is the only service that has extensive historical experience with NC3. The PLARF may be inclined to seek to defend this nuclear "monopoly," from the perspective of bureaucratic competition, but it remains to be seen what role, if any, the PLARF may have with regard to the new elements of this triad.[13] Currently, the PLARF does employ the PLA's integrated command platform (一体化指挥平台), through which it can connect and coordinate with other services under the aegis of the new theater commands (战区) that have responsibility for operations,[14] at least for units and missions involving conventional capabilities.[15] To date, no nuclear units are known to have been connected to the integrated command platform,[16] yet there appears to be some degree of interdependence among relevant C4ISR systems in ways that could create a degree of risk.[17] The PLARF also possesses its own dedicated systems for nuclear forces that are intended to be resilient and redundant, evidently involving a combination of radio, fiber-optic cables, and satellites, but this existing architecture may require improvement and modernization as it fields and deploys a growing number of mobile missiles.[18]

If the PLAN and PLAAF do take on new responsibilities for NC3, the fielding of these systems will involve requirements for the construction of NC3 systems *de novo*, which could introduce distinct difficulties. Presently, China's communications with its Type 094 SSBNs are known to use very low frequency (VLF) communications, involving at least two main stations for transmission.[19] Reportedly, the PLA constructed its first military-grade super low frequency transmission station in 2009, and a new project that will introduce the capability for extremely low frequency communications with submarines is just being completed as of late 2018.[20] However, ensuring secure and reliable underwater communications with SSBNs may prove quite challenging for the PLA, including raising questions of procedures for delegation. Meanwhile, the PLAAF's future employment of strategic bombers may be influenced by its past tendency towards often highly scripted exercises that have involved a tightly controlled approach to command.[21] The PLA also could start to integrate aircraft not unlike the U.S. military's TACAMO, perhaps building upon current developments in airborne early warning and control aircraft, to facilitate these functions.[22] As the PLA looks to adapt and expand its NC3 architecture, there are a number of potential technical and organizational characteristics, including issues of trust and a preference for high-level, centralized command of strategic capabilities that may influence its approach.[23]

As the PLA's strategy, doctrine, and force posture continue to evolve in response to the geopolitical environment and today's technological transformations, these shifts could influence its approach to NC3.[24] As the 2015 defense white paper, "China's Military Strategy" highlighted at the time, "China will optimize its nuclear force structure, improve strategic early warning, command and control, missile penetration, rapid reaction, and survivability and protection."[25] This commitment to continued modernization reflects a response to assessments of new trends in the capabilities of potential adversaries, including concerns about U.S. efforts in missile defense and conventional prompt global strike (CPGS), and technological developments.[26] The PLA's focus on improving strategic early warning indicates a recognition that these capabilities have been a relative weakness for the PLA and their construction has proven challenging.[27] Consequently, Chinese military academics and strategists appear to be concerned with the threat of a 'false negative' if a nuclear attack or surprise attack against strategic missiles by an adversary with more sophisticated capabilities were to go undetected.[28] The PLA intends to construct a space-based system for early warning and strategic surveillance capable of detecting indicators of a potential nuclear attack.[29] The estimates of feasible timeframes for this drive to improve early warning capabilities tend to vary, and it is difficult to evaluate the progress of this process, which could change the calculus for the PLA.[30]

If China's posture were to evolve towards that of "launch on warning" (预警即发射) in the future, this change would demand and depend upon much more reliable early warning systems. In this regard, it is significant that China Electronics Technology Corporation (CETC) at the Zhuhai Air Show in the fall of 2018 CETC revealed a range of new radar- and satellite-based early warning defense systems, claiming that these systems have improved datalinks that can enable real-time sharing and integration of intelligence for enhanced situational awareness.[31] In its totality, these systems and their integration are aimed to fulfill a range of operations, variously intended for anti-missile operations, space attack and defense, theater joint operations, far seas warfare, and global surveillance and strike.[32] Of these, the anti-missile early warning system is intended "to acquire full-process intelligence of targeted ballistic missiles to support strategic counterattacks and anti-missile operations."[33] The design of these systems, which provide "multi-source fusion and comprehensive integration" of information, is intended to anticipate the demands of future warfare, involving information dominance (信息主导), system of systems coordination, and all-domain operations. However, beyond the reporting and advertising, there is only limited technical information available about these systems.

The PLARF's new emphasis on "rapid reaction" (快速反应) appears to imply the capability for a faster counterattack. Such a posture could be considered consistent with China's traditional "no first use" pledge and commitment to only engage in second strikes (后发制人), according to some authoritative assessments, including the 2013 edition of *The Science of Military Strategy*, released by the PLA's Academy of Military Science.[34] This concept appears to imply a shift towards or become tantamount to a posture of launch on warning, involving the launch of a retaliatory strike upon reliably distinguishing that an enemy has launched a nuclear attack to limit the damage to PRC nuclear power and to improve the survivability of counterattack capabilities—but cannot be fully confirmed.[35] Notably, the 2015 edition of *Science of Military Strategy*, produced by the PLA's National Defense University, emphasizes, "rapid response is a prerequisite for second strikes, and to improve rapid response capabilities, the level of alertness of strategic missile units must be increased, and always maintaining a state of high alert" (高度戒备状态).[36] This text characterizes rapid response as "the degree of rapidity of strategic missile forces in the implementation of combat operations," which depends upon factors that include capabilities for strategic reconnaissance, the rapid judgment of the commander on enemy operations, the degree of alertness of missile units, and the level of training of troops, as well as NC3 capabilities.[37]

Since the PLA launched an agenda of historic reforms in late 2015, the Rocket Force has continued to progress in its modernization and informatization.[38] Since the 1990s, the development of systems for command automation (指挥自动化), essentially analogous to C4ISR, which could convey commands, integrate intelligence, and enable real-time monitoring, has been a clear priority and persistent challenge for the PLA. In particular, the PLARF has focused on "accelerat[ing] the construction of an informatized combat system," promoting capabilities for command and control and for reconnaissance and early warning.[39] As the Rocket Force's former commander General Wei Fenghe (魏凤和) has emphasized, it will be important to "promote the rapid integration, efficient sharing, and deep linkages of combat information of various elements of each system, and improve the strategic deterrence and actual combat capability based on information systems."[40] At the same time, the PLARF is responding to Xi Jinping's high-level emphasis on military innovation, including through exploring new methods and theories of warfare, considering trends in the form of warfare towards remote, precision, intelligentized (智能化), stealthy, and unmanned weaponry that are expected to become particularly prominent.[41] Given the PLARF's strategic requirement of "combining nuclear and conventional (capabilities) and all-domain deterrence and war-fighting" (核常兼备、全域慑战), there could be a degree of "entanglement" in its C4ISR systems that may pose new risks, yet this issue is not unique to China.[42]

Looking forward, Chinese strategists recognize that the military competition is intensifying in ways that necessitate continued modernization in China's strategic deterrence (战略威慑).[43] To some extent, China's continued modernization of its nuclear arsenal constitutes a response to concerns about survivability that have been exacerbated by advances in U.S. missile defenses and potential counterforce capabilities.[44] These advances in China's nuclear forces has included the introduction of more advanced weapons systems, such as the DF-31AG, which may possess greater mobility and thus survivability and could be armed with multiple independently targetable re-entry vehicle (MIRV) warheads.[45] Concurrently, China is pursuing advances in hypersonic weapons that may be dual-capable and possess higher levels of autonomy.[46] The active research focusing on new techniques for autonomous control, as well as improved automatic target recognition, in advanced weapons systems, could prove relevant to future directions in the development of nuclear and conventional capabilities alike.[47] The emphasis and direction of the latest U.S. Nuclear Posture Review, as well as the Missile Defense Review, may intensify these concerns and could contribute to a redoubling of China's expansion and modernization of its nuclear arsenal, including the requisite improvements in NC3.[48]

Risks of Errors and Biases in China's NC3 Systems

These progressive evolutions in China's nuclear posture, doctrinal concepts, and concurrent technological developments will impact the risks of errors that could be exacerbated in the course of these changes. China has approached the challenge of deterrence from the perspective of a weaker state that is confronting a powerful adversary (强敌) with superior capabilities. Traditionally, China has taken a pragmatic and minimalist approach to its nuclear arsenal yet concerns of survivability appear to be changing assessments of the fundamental requirements. Consequently, Chinese strategists have been deeply concerned with increasing strategic early warning and surveillance capabilities.[49] This focus on the risks of false negatives, which involve a failure to launch when an attack occurs, could guide the direction of future Chinese NC3 developments.[50] Relative to the U.S. and Russian militaries, the Chinese military seems to have less concern and less historical experience with the risks of false positives, which would involve a mistaken launch when there is not an attack underway.[51] Although the introduction of new technologies, particularly the use of artificial intelligence (AI), to enhance situational awareness, could prove stabilizing,[52] there is also a risk that the limitations and potential vulnerabilities or idiosyncrasies of these emergent technologies and capabilities could render an accident or miscalculation more likely.

Throughout its history, China has maintained a "no first use" policy with striking consistency that seems unlikely to change in the foreseeable future.[53] At first glance, China's NC3 profile appears to be relatively conditioned towards negative controls that are primarily procedural in nature.[54] Based on the most recent assessments, Chinese warheads continue to be stored separately from weapons systems in secure and central locations by the PLA Rocket Force.[55] The PLA Navy may have to mate warheads with nuclear submarines for future nuclear patrols, and it remains to be seen how the PLA Air Force will approach the management of warheads in the future, including the question of whether the Rocket Force may end up having authority over the totality of the triad.[56] Although there has not been definitive evidence to date that China uses permissive action links (PALs), such controls are likely within its technological capabilities. The Rocket Force remains directly under the control of the Central Military Commission (CMC), rather than the PLA's regional theater commands (or "war zones," 战区), and the prospect of delegation of the authority for nuclear launch to lower levels appears relatively unlikely at present.[57]

Pending any conclusive evidence or additional confirmation, it seems most likely that the PLAN and PLAAF's nuclear capabilities will be commanded directly through the Central Military Commission, consistent with the paradigm of in use for the Rocket Force and the former Second Artillery Force

throughout its history. This centralized approach to command and control could contribute to reducing the possibility of an accident. In all likelihood, a nuclear attack could only be authorized by Xi Jinping, in his capacity as Chairman of the Central Military Commission and General Secretary of the Chinese Communist Party. However, it is difficult to ascertain whether certain aspects of this profile may change in the future, as China explores new directions in command automation and introduces a more robust fleet of SSBNs and new strategic bombers into its arsenal.

Potential Employment of Emerging Technologies in PLA NC3

This section will consider certain emerging technologies, including artificial intelligence, cloud computing, fifth-generation telecommunications, and quantum communications, providing an initial evaluation of their relevance and feasibility of their application to the future of NC3.[58] While discussing the technical potential and challenges of these various technologies, I will examine in particular how China might employ them in the future, given the particular constraints and challenges that are relevant to its current force construction. To the extent feasible, I draw upon the available technical literature and look to develop reasonable assessments that are informed by data and current trends.

Artificial Intelligence

Today's advances in AI have noteworthy implications for the future of NC3. Of course, the potential applications of AI to enhance nuclear capabilities are hardly novel, dating back to U.S. and Soviet initial development of and experimentation with AI systems during the Cold War.[59] In particular, while accounts vary, the Soviet Union had explored the construction of a system for fully automated counterstrikes, known as the "Dead Hand," and to have deployed a system known as "Perimetr," which had leveraged some kind of AI, particularly for communications, and involved delegation but kept a human in the loop.[60] As a general-purpose technology that can enable and augment existing missions and capabilities, AI appears to possess great potential in such applications as early warning, decision support, and the targeting and guidance of advanced weapons systems, not to mention key supporting functions, such as logistics and predictive maintenance.[61] Certain of these applications could prove stabilizing, enabling improved situational awareness, such as through data fusion and the rapid integration of information, in ways that might mitigate the risks of miscalculation in a crisis scenario. However, AI technologies also remain inherently vulnerable to exploitation and manipulation, including through the corruption of data or attacks against the underlying hardware, based on research that is currently underway.[62] These advances raise concerns about the risks of an error and questions of safety, surety, and assurance that remain largely unresolved at this point.[63]

Xi Jinping has called for the PLA to accelerate the advancement of "military intelligentization" (军事智能化).[64] Chinese strategists recognize the strategic potential of military applications of AI for a range of applications. There are initial indications that the PLA is actively exploring options for the integration of AI into its C4ISR systems, particularly to support command decision-making.[65] In an authoritative commentary, the CMC Joint Staff Department has called for the PLA to advance intelligentized command decision-making in its construction of a joint operations command system, through taking advantage of the potential of AI, as well as big data, cloud computing, and other advanced technologies.[66] Certain Chinese defense academics anticipate that the advent of AI in warfare will increase the speed and tempo of operations in ways that absolutely necessitate greater integration of AI technologies into command and control, perhaps complementing or ultimately surpassing human intelligence.[67] For instance, Lieutenant General Liu Guozhi (刘国治), director of the Central Military Commission Science and Technology Commission, has anticipated "human-machine hybrid intelligence" will be the highest form of future intelligence.[68] Unsurprisingly, there has been active research underway to explore these directions in application of big data and AI to command information systems, including a new laboratory in which Baidu has partnered with the

China Electronics Technology Group Corporation.[69]

The PLA believes AI could be critical to enhancing—or perhaps someday displacing—human intelligence in creating tactics and strategies in warfare. Consequently, humans might transition from being 'in' the loop, to 'on' the loop, and even out of the loop in the future.[70] Certain PLA thinkers anticipate a transition in warfare to an era of 'algorithmic confrontation' among AI systems.[71] It remains to be seen how the PLA might approach these technological developments in the context of nuclear decision-making, including potentially to improve early warning and situational awareness. Potentially, the PLA Rocket Force could leverage intelligent decision support systems or could explore options for intelligent command and control.[72] For instance, the PLA might leverage AI technologies to enhance the decision-making of fighter pilots or the commanders of submarines. According to credible reporting, the computer systems on PLAN nuclear submarines will be updated with an AI decision-support system that is designed reduce commanding officers' workload and mental burden,[73] potentially building upon robust research in underwater acoustic target identification.[74] The PLA's advances in AI-enabled decision support might be applied to its future NC3 as well. AI technologies might be applied in support of combat mission planning, including to coordinate selection of targets.[75] For instance, the PLARF Engineering University contributed to an international workshop on AI and evidential reasoning that was convened to focus on intelligent reasoning and decision-making.[76] In addition, advances in the use of AI in war-gaming and military simulations may be relevant to anticipating dynamics on the actual battlefield, since such scenarios of game confrontation can generate data and insights that may be valuable.[77]

The PLA's approach to leveraging AI could be shaped by concerns over current shortcomings in its operational capabilities. With regard to NC3, current inadequacies in Chinese early warning and situational awareness appear to be motivating the employment of AI technologies to augment these capabilities. To date, there has also been apparent progress in research involving the AI-enabled mining and processing of data from remote sensing satellites,[78] which may already be in use, at least to a limited degree, by the PLA Rocket Force and Strategic Support Force.[79] For instance, PLARF research in remote sensing has explored the use of adversarial networks in a new framework for domain adaptation and classification based on deep convolutional neural networks,[80] as well as to hyperspectral image classification.[81] Reportedly, several technology companies have already launched "AI satellites" that include AI chips for on-board intelligent processing of data, which can increase the speed of processing in ways that might accelerate targeting.[82] Although not all of these developments have direct and immediate relevance to NC3, the initial direction of the PLA's employment of AI may prove indicative of the future integration of these technologies with its nuclear posture. In particular, the ability of algorithms to rapidly identify patterns in data, including from remote sensing, appears to be a major focus of academic research and publications, including from a number of students and researchers associated with the Rocket Force Engineering University.[83] For instance, the application of machine learning to hyper-spectral image classification, including in support of remote sensing applications, can contribute to battlefield environmental support.[84] In addition, greater automation in targeting could be applied to facilitate ballistic missile defense.[85]

The PLA is also actively advancing the use of AI in support of targeting and missile guidance of conventional—and potentially dual-capable—nuclear weapons. Recognizing the criticality of data fusion and intelligence to future operational advantage, PLA researchers are exploring options to leverage AI technologies to train on and learn from target features acquired by a range of sensors.[86] For instance, the application of machine learning to improve automatic target recognition (ATR), including with the use of convolutional neural networks in Synthetic Aperture Radar (SAR) image target recognition, is recognized as an opportunity to build upon prior research to enhance precision in targeting.[87] PLA researchers are also exploring the improvement of algorithms to facilitate the

tracking of moving targets.[88] Increasingly, advanced Chinese weapons systems are also becoming more autonomous and "intelligentized" in their guidance and targeting.[89] The sophistication of Chinese aerospace capabilities, including cruise missiles and hypersonic weapons systems, will be augmented through the use of AI technologies to enable intelligent autonomous control (智能自主控制).[90] Moreover, the extreme speed of hypersonic weapons systems may create an incentive for a pragmatic transition towards higher degrees of autonomy. In many cases, the technical advances in question may be relatively incremental, enhancing guidance and targeting in weapons systems that may be nuclear or dual-capable to increase their precision.

In the aggregate, such developments could contribute to enhancing China's strategic deterrence, including through augmenting NC3, but there is not yet unambiguous evidence that the PLA has integrated—or will in the near future—incorporate AI into its current NC3 architecture. Certainly, given the PLA's active interest and investments in relevant research and development, it would not be surprising to see AI take on a greater role in supporting China's NC3 in the future, though there could continue to be a level of opacity that engenders uncertainty. At present, the impact of AI on the risks of false positives and false negatives is difficult to ascertain. Certainly, the introduction of AI, including to enhance Chinese early warning capabilities and strategic intelligence, could prove stabilizing, potentially increasing China's confidence in its capability for rapid response to a nuclear attack. However, the impact of AI could also increase the risks of a false positive, given the demonstrated shortcomings and vulnerabilities of AI systems at present, which could be exacerbated by the paucity of data available in this context.

Cloud Computing

In an era in which data is critical to battlefield advantage, the potential benefits of cloud computing are clear. The centralization of data storage in remote servers can contribute to more effective data management, while facilitating AI deployment. This new approach to military information management can overcome the barriers and stovepipes that might otherwise impede the effective integration of data across organizations. In a complex operational environment, cloud computing also could enable commanders to reach "scientifically coordinated operational decisions" through the sharing of important information.[91] If designed and implemented with high levels of cyber security, the introduction of cloud computing can have the dual advantages of facilitating access to data and improving security overall. Potentially, the distributed character of the cloud may also provide an advantage in a highly contested environment, since an attack on a single point wouldn't compromise the entire cloud or interrupt access to information.[92]

At present, the PLA also appears to be exploring the introduction of cloud computing into its C4ISR architecture, which may have some relevance to its future NC3 systems as well.[93] Based on available publications, several research institutes in the PLA are starting to explore and experiment with option for a cloud architecture for command information systems.[94] There are also a number of companies that are engaged in supporting the PLA's transition to the cloud. In early 2016, the China Institute for Command and Control (CICC) signed a strategic cooperation agreement with the Chinese Academy of Science's Sugon (曙光, *Shuguang* or 'Dawning').[95], [96] At the time, Dai Hao (戴浩), chair of CICC and also a researcher with the PLA's 61st Research Institute, highlighted that this partnership would enable advances in the "cloud-ization" ("云"化) and intelligentization of China's military command and information systems.[97] In particular, Dawn's big data and cloud computing technology were seen as providing advanced technological support and cloud service systems to China's joint operations command mechanism and the construction of military command information systems. Increasingly, a number of tech companies, including Ganyun S&T (乾云科技) and Meihou Cloud (美猴云), are also starting to pursue opportunities to contribute to military cloud computing.[98]

For purposes of strategic early warning and situational awareness, this potential improvement in PLA capabilities to integrate and process key data could be advantageous, perhaps enhancing and accelerating decision-making in ways that could be stabilizing. Indeed, the introduction of cloud computing can enable real-time data transmission, resource sharing, and command and control that can facilitate greater coordination among units. However, such consolidation of information could exacerbate the risks of compromise of highly sensitive information, at worst creating a single point of failure, which may be a concern in the U.S. Department of Defense's potential transition to cloud platform.[99] Unsurprisingly, in the process, the PLA is closely tracking and often influenced and informed by the precedent of U.S. developments, including the notion of a "combat cloud" or cloud operations.[100] The PLA's adoption of cloud computing appears to remain relatively limited at present, but could increase in the future in the course of initiatives to implement intelligentization that will require more effective management of 'military big data.'[101]

Fifth-Generation Telecommunications

As China progresses in the nationwide deployment of 5G, the Chinese military may also reap the full benefits of the high speed, low latency, and high throughput of this new generation of telecommunications. While concern over 5G has concentrated thus far primarily on the economic implications, the potential for dual-purpose and military applications of these technologies constitutes another important dimension of its strategic significance. Evidently, those promising applications are not lost upon the Chinese military. China's initial exploration of synergies between defense and commercial developments in 5G could be a trend worth watching. For instance, the advancement of 5G in China today is associated with its national strategy for military-civil fusion (军民融合). For instance, there is a new "5G Technology Military-Civil Fusion Applications Industry Alliance" (5G技术军民融合应用产业联盟), which involves key tech companies, like ZTE, and the China Aerospace Science and Industry Corporation (CASIC), a state-owned defense conglomerate.[102]

Going forward, 5G could contribute to future battlefield communications through enabling a new leap in the rate and stability of information transmission in ways that can enhance the timeliness and integration of information. Potentially, 5G will provide the rapid transmission and bandwidth required to realize the potential of the Internet of Things and AI on the future battlefield. In this regard, the advent of 5G for military purposes could contribute to the realization of military intelligentization (军事智能化), though which the PLA seeks to leverage the potential applications of AI technologies in military affairs. Just as 5G can enable massive inter-machine communication in smart cities, similar levels of networking among sensors and devices could be advantageous on a highly "informatized" battlefield, enabling improved situational awareness through advances in data analytics and perhaps real-time coordination or command and control.[103]

Potentially, China's deployment of 5G technologies at a national level could provide more extensive coverage and augment information support capabilities for the PLA. In this regard, an integrated infrastructure for 5G could provide a significant operational advantage with potential relevance for NC3. In theory, if designed and implemented appropriately, 5G may be more secure and faster. The speed that this new generation of telecommunications may provide could be valuable to NC3, especially in scenarios where time is of the essence. While there are initial indications that China may explore various military applications of 5G, including its initial employment in drills for emergency mobilization, it remains to be seen whether and to what extent 5G might be used in the context of NC3, such as to enhance situational awareness through facilitating data fusion and rapid communications.

Quantum Cryptography and Communications

The PLA has started to leverage its new and expanding infrastructure for quantum communications

for military purposes that could augment future command and control. The national backbone network that enabled quantum key distribution (QKD) has progressively expanded, from the Beijing-Shanghai "Trunk" to a range of local area networks. The PLA appears to be exploring and perhaps expanding its employment of quantum communications.[104] Potentially, the experience that Chinese scientists and engineers are gaining in building and operationalizing these systems could be applied to the development of a dedicated infrastructure for NC3. Chinese scientists plan to launch a whole constellation of quantum satellites in low and high earth orbit in the years to come, which will enable the scaling up of this system.[105] These developments have been characterized as a priority of China's agenda for military-civil fusion.[106] Of course, while there are indications that the PLA could expand its use of these systems, whether these technologies would be extended to communications for nuclear purposes is essentially impossible to verify with high confidence.

The apparent enthusiasm for the promise of supposedly unhackable communications extends to the highest echelons of Chinese leadership, including Xi Jinping himself. It is not unreasonable to postulate or hypothesize that strategic communications of particular sensitivity may already or could in the future be secured using quantum key distribution, such as between Xi Jinping, in his capacity as chair of the Central Military Commission, and the Joint Staff Department's Joint Operations Command Center, to the five regional theater commands and perhaps even to certain critical units in the field, given that the PLA is also testing mobile quantum communications.[107] Among the advantages of such a transition would be "future-proofing" highly sensitive information of relevance to China's nuclear arsenal against the risks of future decryption by a capable quantum computer. [108] However, it is worth noting that China's development of quantum-resistant algorithms remains relatively limited compared to current attempts underway in the United States.

Going forward, quantum communications can be employed underwater, providing new options for communications with submarines. As China continues to develop its SSBN fleet, quantum communications could be leveraged as a solution to enable secure and nearly undetectable communications that might resolve otherwise challenging problems of command and control. Presently, as Chinese scientists and academics have noted, the development of quantum communications underwater remains at a fairly nascent stage, since there are major obstacles to its reliable realization.[109] According to one Chinese defense academic, "it is certain that once underwater quantum communication is engineered, it will completely disrupt the submarine communication and command and even the combat mode."[110] The use of blue-green lasers for communications can serve as a basis for underwater quantum communications, providing greater assurance for the security of communications. However, this technology remains far from mature, limited by some basic constraints that will likely include water quality.[111] The military maritime applications of quantum technology may extend far beyond NC3, but it is clear that the potential for secure, high-capacity, and long-distance communications leveraging entanglement could have relevance in command and fire control in a combat scenario.[112]

The PLA recognizes that improvements in capabilities for military communications could be integral to future capabilities, and quantum communications could prove advantageous given their potential resistance and survivability in the face of electromagnetic interference, yet it may remain vulnerability to interference from light).[113] While there are currently limitations to the speed and efficiency of most known types of quantum communications, these obstacles could be overcome in the course of future developments. The potential for "stealth transmission" that cannot be readily detected— and thus less subject to adversary countermeasures—could also prove advantageous. In the future, the PLA could leverage quantum technology to augment the information architecture for military C4ISR.[114] For instance, the China Aerospace Science and Industry Corporation has become active in the development of dual-use networks for quantum communications, which may be used to transmit classified military information between command centers and units in the field.[115] Chinese

defense academics anticipate that there might be new stealthy quantum communications systems integrated among command and control with reconnaissance and early warning systems.[116] Hypothetically, a system based on quantum teleportation for the exchange of information can be constructed among various operational command and control systems, while also integrating early warning and reconnaissance, "thus constructing a communication network for quantum information battlefields, with its large channel capacity and super features such as high communication speed playing an irreplaceable role in the future information war."[117] In such an architecture, the realization of advances in quantum radar and sensing, which have been reported to have the capability to overcome stealth or detect nuclear submarines, may also have disruptive impact on future targeting, which may have implications for survivability.[118]

However, there are also reasons for strong skepticism that quantum cryptography and communications would be suitable for use in NC3 in the near or even long term. U.S. experts and scientists remain relatively skeptical that this is an apt application, given concerns of reliability and survivability.[119] At present, these technologies remain challenging to operationalize in real-world conditions. The entanglement among photons that is leveraged to transmit a cryptographic key or to convey information directly is fragile and could possess potential vulnerability to spoofing or interference.[120] While this mechanism does provide "provable" security, the costs and tradeoffs may not be favorable. Thus, a reliance upon quantum technology to support NC3 seems unwise, absent further verification of survivability, but quantum cryptography and communications—or future quantum networking to facilitate information integration—may have some role to play in future generations of NC3 systems nonetheless.

Conclusions and Implications

Presently, the U.S. and China militaries are both exploring new directions in their NC3 architectures that could result in perhaps parallel but distinctive approaches to the employment of these emerging technologies. Despite their novelty, the impact of these strategic technologies, which have become a new frontier of rivalry, can be explored and evaluated based on traditional frameworks that consider potential sources of risk and error. There are reasons for a degree of optimism that certain advances may reduce the risk of errors. For instance, the use of AI could improve early warning and strategic reconnaissance, while the adoption of cloud computing could enable the integration of data that may facilitate situational awareness, and the advent of 5G could enable newly capable battle networks with the high speed and extreme connectivity required for the future "intelligentized" battlefield. Looking to the status of advances in quantum technology, quantum communications may provide newly secure and resilient communications, including underwater to SSBNs, while quantum computing presents a more distant threat to cyber security, and current advances in quantum sensing promise improved detection.

At the same time, the inherent complexity and uncertainty of these nascent, untested technologies also raises questions about new risks to stability. The reliability of AI depends upon the quality of data, efficacy of training, and parameters of operation, and mistakes in algorithms that may be difficult to predict or prevent false positives that may exacerbate the risks of accidental escalation. The introduction of cloud computing could improve decision-making but also might increase vulnerability to cyber threats, depending upon the security practices in its implementation. So too, the use of 5G in future battle networks could improve capability and create potential vulnerabilities based on their design. Ultimately, the actual impact of these technologies will depend upon the strategic choices that militaries make in their application and employment of emerging capabilities, particularly with regard to questions of safety and assurance. In this regard, it will be important to start to explore, including through existing mechanisms for dialogue and engagement, the potential

for new risks and options for best practices to improve surety.

III. ENDNOTES

[1] U.S/ Department of Defense, "Nuclear Posture Review," February 2018, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCL-AR-POSTURE-REVIEW-FINAL-REPORT.PDF.

[2] Ibid.

[3] My research seeks to build upon the excellent foundation of Fiona Cunningham's paper within this series, "Nuclear Command, Control, and Communications Systems of the People's Republic of China," and Lora Saalman's research on the impact of emerging technologies on China's nuclear posture, including, "Fear of false negatives: AI and China's nuclear posture," *Bulletin of the Atomic Scientists*, April 24, 2018, https://thebulletin.org/landing_article/fear-of-false-negatives-ai-and-chinas--uclear-posture/.

[4] Please note that I use the phrase "NC3" as a useful shorthand throughout this paper given the focus of this project, while recognizing PLA definitions and terminology differ slightly. For instance, the concept of "strategic command and control" (战略指挥控制), which does not refer exclusively to nuclear systems, is more prevalent in PLA writings. Similarly, the term "strategic C3I system" is defined as, "the C3I system at a country's highest-level military command structure that implements uninterrupted command and control of armed force. It is primarily made up of intelligence gathering systems (or intelligence and surveillance systems), strategic warning systems, communications network systems, and all levels of command center computer automated data management, display, and command monitoring control systems." See: Jing Zhiyuan, (ed.), *China Strategic Missile Force Encyclopedia* [中国战略导弹部队百科全书], China Encyclopedia Press, 2012, 739, qtd. in Fiona Cunningham's paper within this series, "Nuclear Command, Control, and Communications Systems of the People's Republic of China."

[5] Fiona S. Cunningham and M. Taylor Fravel, "Assuring Assured Retaliation: China's Nuclear Posture and US-China Strategic Stability," *International Security* 40, no. 2 (2015): 7-50.

[6] For excellent evaluations of China's nuclear posture, including its historical trajectory and evolution, see: Jeffrey G. Lewis, *Paper Tigers: China's Nuclear Posture*, Routledge, 2014. John Wilson Lewis and Litai Xue. *China Builds the Bomb*. Vol. 3. Stanford University Press, 1991. John Wilson Lewis and Litai Xue. *China's Strategic Seapower: The Politics of Force Modernization in the Nuclear Age*. Stanford University Press, 1996.

[7] For a more detailed assessment, see: Eric Heginbotham, Michael S. Chase, Jacob L. Heim, Bonny Lin, Mark R. Cozad, Lyle J. Morris, Christopher P. Twomey et al. *China's Evolving Nuclear Deterrent: Major Drivers and Issues for the United States*. Rand Corporation, 2017.

[8] For relevant reporting on China's development of a strategic bomber, see: "New strategic bomber to make PLA Air Force a strong force," China Military Online, February 17, 2017, http://english.chinamil.com.cn/view/2017-02/17/content_7491722.htm. For an argument from a prominent defense academic regarding the importance of long-distance counterstrike capabilities, see: Jiang Yamin [蒋亚民], *China's Fist: On Long-Arm Counterstrike* [中国的拳头：论长臂反击], Military Science Press [军事科学出版社], 2014.

[9] See: Ankit Panda, "Revealed: China's Nuclear-Capable Air-Launched Ballistic Missile," *The Diplomat*, April 10, 2018, https://thediplomat.com/2018/04/revealed-chinas-nuclear-capable-

air-launched-ballistic-missile/. For the Pentagon's latest assessment, see Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2019," https://media.defense.gov/2019/May/02/2002127082/-1--1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

[10] For PLA media and commentary that highlight these themes, see: "The Strategic Air Force's New Track" [战略空军的新航迹], China Military Online, May 9, 2018, http://www.81.cn/jfjbmap/content/2018-05/09/content_205618.htm. "People's Navy: Sailing for 70 Years" [人民海军：扬帆奋进70年], China Military Network, April 16, 2019, http://www.js7tv.cn/news/201904_178847.html.

[11] For the authoritative assessment on the issue, see: Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2019," https://media.defense.gov/2019/May/02/2002127082/-1--1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf

[12] Keir A. Lieber and Daryl G. Press. "The new era of counterforce: Technological change and the future of nuclear deterrence." *International Security* 41, no. 4 (2017): 9-49.

[13] For one perspective on this debate, see: David C. Logan, *China's Future SSBN Command and Control Structure*. National Defense University Washington United States, 2016.

[14] In particular, the Joint Staff Department's Information Support/Assurance Base (信息保障基地) appears to possess primary responsibility for the integrated command platform.

[15] For one description of how the integrated command platform is starting to be leveraged for joint operations, see: "The integrated command platform enables close links among different parts of command and operations" [一体化指挥平台让异地指挥作战各环节紧密衔接], *PLA Daily*, May 11, 2016, http://military.people.com.cn/n1/2016/0511/c1076-28341807.html.

[16] See Fiona Cunningham's paper within this series: "Nuclear Command, Control, and Communications Systems of the People's Republic of China."

[17] For the relevant academic literature on these issues, see: James Acton, "Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks," *Arms Control Today* 47, no. 10 (2017): 42-42. 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 (2018): 56-99.

[18] See Fiona Cunningham's excellent assessment within this collection of papers for a much more detailed analysis.

[19] Ibid, and see also: "Does China have an effective sea-based nuclear deterrent?", https://chinapower.csis.org/ssbn/

In particular, see: "Very Low Frequency (VLF) Stations," https://www.smeter.net/stations/vlf--.php

[20] Stephen Chen, "China's new antenna is five times the size of New York City, but some fear it could be a cancer risk," *South China Morning Post*, December 31, 2018, https://www.scmp.com/news/china/science/article/2180071/chinas-ne--antenna-five-times-size-new-york-city-it-also-cancer.

[21] I am very grateful and indebted to Ken Allen of the China Aerospace Studies Institute for his insights on these issues of training and command culture.

[22] For instance, the KJ-500 is widely in use, and the carrier-borne KJ-600 is currently under development. For further details on these aircraft, see: "China's aircraft carrier's new bodyguard KJ-600 shipborne early warning aircraft" [中国航母的新保镖 空警-600舰载预警机], China Military Network, September 2, 2018, https://military.china.com/aerospace/special/11162362/20180920/33958715.html.

[23] Elsa B. Kania, "Artificial Intelligence in Future Chinese Command Decision Making," in AI, China, Russia, and the Global Order: A Strategic Multilayer Assessment (SMA) Periodic Publication, December 2018, p. 145, https://nsiteam.com/social/wp-content/uploads/2018/12/AI-China-Russia-Global-WP_FINAL.pdf.

[24] For instance, the PLA is currently undertaking changes to its operational regulations (作战条令), which is roughly analogous to doctrine, that may be completed later in 2019 or early 2020, and a new defense white paper is expected to be issued in 2019 as well.

[25] Ministry of National Defense of the People's Republic of China [中华人民共和国国防部], "China's Military Strategy" [中国的军事战略]," May 26, 2015.

[26] See also: Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2019," https://media.defense.gov/2019/May/02/2002127082/-1--1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

[27] See, for instance: Expert: China's People's Liberation Army's Early Warning Capability Construction Confronts Multiple Challenges" [专家：中国解放军预警能力建设面临多重挑战], China Military Online, August 2, 2013, http://military.china.com.cn/2013-08/02/content_29602761.htm.

[28] For an authoritative textbook that alludes to these concerns, see: Xiao Tianliang [肖天亮] (ed.), *The Science of Military Strategy* [战略学], National Defense University Press, 2015. For an excellent piece on the issue, see: Lora Saalman, "Fear of false negatives: AI and China's nuclear posture," *Bulletin of the Atomic Scientists*, April 24, 2018 https://thebulletin.org/landing_article/fear-of-false-negatives-ai-and-chinas-nuclear-posture/.

[29] Xiao Tianliang [肖天亮] (ed.), *The Science of Military Strategy* [战略学], National Defense University Press, 2015. Lt. Gen. Xiao Tianliang has been the vice commandant of the PLA's National Defense University. His views may be influential with Chinese leaders, including Xi Jinping, considering that he was invited to present at a 2014 Politburo study session on new trends in the Revolution in Military Affairs (RMA). It is unusual that this textbook was revised and re-released in 2017, since that is a departure from the usual cycle of these textbooks' publication.

[30] For instance, in her paper in this series, Dr. Fiona Cunningham estimated that progress in early warning capabilities could require at least ten years.

[31] "CETC reveals radar early warning systems for wars," *Global Times*, November 5, 2018, http://www.globaltimes.cn/content/1126030.shtml.

[32] "CETC Released "Radar Five Major Operational Early Warning Systems" to show you every corner of the world" [中国电科发布"雷达五大作战预警体系"带你看遍全球每个角落], *Global Times*, November 5, 2018, http://webcache.googleusercontent.com/search?q=cache:J0EUlrj8yDIJ:www.sohu.com/a/274974961_162220+&cd=5&hl=en&ct=clnk&gl=us.

[33] "CETC reveals radar early warning systems for wars," *Global Times*.

[34] Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部] (ed.), *The Science of Military Strategy* [战略学.p. 363.

[35] That is, the term "rapid response" has occurred across a number of writings of varying degrees of authoritativeness, including the 2013 and 2015 editions of The Science of Military Strategy produced respectively by the PLA's Academy of Military Science and National Defense University.

[36] Xiao Tianliang [肖天亮] (ed.), *The Science of Military Strategy* [战略学], National Defense University Press, 2015, p. 355, 378.

[37] Ibid.

[38] For an authoritative assessment of the post-reform PLARF, see: Mark Stokes, "Reform and Reorganization of the PLA Rocket Force," *forthcoming*.

[39] Wei Fenghe [魏凤和] and Wang Jiasheng [王家胜], "Keeping in mind the words and listening to the party's command; working hard to build a powerful modern Rocket Force" [牢记训词 听党指挥 努力建设强大的现代化火箭军], *Seeking Truth* [求是], January 31, 2016, http://www.qstheory.cn/dukan/qs/2016-01/31/c_1117915676.htm

[40] Ibid.

[41] Chen Yonghua [陈永华], "Missile Warfare, Opening the Veil to the Road to Winning" [导弹战，揭开"面纱"谋胜道], *PLA Daily*, December 29, 2016. The author had been the political commissar of a PLARF missile brigade previously.

[42] James M. Acton, "Escalation through Entanglement: how the vulnerability of command-an--control systems raises the risks of an inadvertent nuclear war," *International Security* 43, no. 1 (2018): 56-99.

[43] It is worth noting that China's concept of strategic deterrence includes not only nuclear deterrence but also conventional deterrence and information deterrence, among other elements. Some discussions of the elements of strategic deterrence even highlight the value of "people's warfare," a concept that dates back to the time of Mao Zedong, as an element of China's strategic deterrence today. See, for instance: Xiao Tianliang [肖天亮] (ed.), *The Science of Military Strategy* [战略学], National Defense University Press, 2015/2017.

[44] For instance, see this reporting on some responses to the 2018 Nuclear Posture Review: Minnie Chan, "China needs more nuclear warheads to deter US threat, military says," *South China Morning Post*, January 30, 2018, https://www.scmp.com/news/china/diplomacy-defence/article/2131261/chin--needs-more-nuclear-warheads-deter-us-threat. For a similar argument, see: "Hypersonic missiles Can Defeat US Missile Defenses," *Cankao Xiaoxi*, February 23, 2014, http://ihl.cankaoxiaoxi.com/2014/0207/343864.shtml.

[45] Richard D. Fisher Jr., "DF-31AG ICBM can carry multiple warheads, claims China's state media," IHS Jane's Defence Weekly, https://web.archive.org/web/20180719154222/http://www.janes.com:80/article/72971/df-31ag-icbm-can-carry-multiple-warheads-claims-china-s-state-media. See also: "China DF-31AG ICBM Debut" [中国东风31AG洲际导弹亮相], Sina Military, July 24, 2017, http://mil.news.sina.com.cn/jssd/2017-07-24/doc-ifyihrit1272002.shtml.

[46] For context and more detailed assessments, see Lora Saalman's excellent research on hypersonics, including: Lora Saalman, "China's Calculus on Hypersonic Glide," Stockholm International Peace Research Institute, August 15, 2017, https://www.sipri.org/commentary/topical-backgrounder/2017/chinas-calculus-hypersonic-glide

[47] The sources in question are available upon request. Some of the prominent research has been undertaken at Beihang University and the National University of Defense Technology, among a growing number of institutions.

[48] For more detailed analyses of Chinese reactions to these reviews, see: Michael S. Chase**,** **"**Chinese Views on the 2018 Nuclear Posture Review, and Their Implications," *China Brief*, Volume 18: Issue 4, March 12, 2018,

https://jamestown.org/program/chinese-views-on-2018-npr/.

[49] Xiao Tianliang [肖天亮] (ed.), *The Science of Military Strategy* [战略学], National Defense University Press, 2015, p. 355.

[50] See again: Lora Saalman, "Fear of false negatives: AI and China's nuclear posture," Bulletin of the Atomic Scientists, April 24, 2018, https://thebulletin.org/landing_article/fear-of-false-negati-es-ai-and-chinas-nuclear-posture/.

[51] For discussion of the U.S. history of false alarms and accidents, see: Eric Schlosser, *Command and control: Nuclear weapons, the Damascus accident, and the illusion of safety*. Penguin, 2013.

[52] Ibid.

[53] M. Taylor Fravel, *Active Defense: China's Military Strategy Since 1949*. Princeton University Press, 2019.

[54] This characterization draws upon the framework from: Jerome M. Conley, *Nuclear Command and Control in the 21st Century*, 2007.

[55] For an authoritative assessment of the post-reform PLARF, see: Mark Stokes, "Reform and Reorganization of the PLA Rocket Force," *forthcoming*.

[56] "Expert: PLA Rocket Force may have strategic nuclear submarine, bomber," China Military Online, January 8, 2016, http://english.chinamil.com.cn/news-channels/pla-daily-commentary/2016-01/08/content_6850119.htm

[57] However, PLA Rocket Force units that have conventional capabilities can reportedly be commanded by theater commands for joint operations, and it is unknown whether missiles and units that are dual-capable may influence

[58] Please note that this listing and assessment is not intended to be comprehensive but rather considers a series of technologies that may have relevance to different aspects of this challenge.

[59] Edward Geist and Andrew J. Lohn. "How Might Artificial Intelligence Affect the Risk of Nuclear War?," RAND, 2018, https://www.rand.org/pubs/perspectives/PE296.html.

[60] Ibid.

[61] See context and discussion in this article: Dmitry Dima Adamsky, “The 1983 nuclear crisis–lessons for deterrence theory and practice,” *Journal of Strategic Studies* 36, no. 1 (2013): 4--.

[62] See, for instance: Zou Minhui, Yang Shi, Chengliang Wang, Fangyu Li, WenZhan Song, and Yu Wang. "Potrojan: powerful neural-level trojan designs in deep learning models." *arXiv preprint arXiv:1802.03043* (2018). Zhao, Mengchen, Bo An, Yaodong Yu, Sulin Liu, and Sinno Jialin Pan. "Data poisoning attacks on multi-task relationship learning." In *Thirty-Second AAAI Conference on Artificial Intelligence*. 2018.

[63] For context on AI safety issues, see: Dario Amodei, Chris Olah, Jacob Steinhardt, Paul Christiano, John Schulman, and Dan Mané. "Concrete problems in AI safety." *arXiv preprint arXiv:1606.06565* (2016).

[64] “Xi Jinping’s Report at the Chinese Communist Party 19thNational Congress” [习近平在中国共产党第十九次全国代表大会上的报告], Xinhua, October 27, 2017, http://www.china.com.cn/19da/2017-10/27/content_41805113_3.htm.

[65] For a more detailed discussion and assessment, see: Elsa B. Kania, “Artificial Intelligence in Future Chinese Command Decision-Making,” in “AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives,” A Strategic Multilayer Assessment (SMA) Periodic Publication, December 2018, https://nsiteam.com/social/wp-content/uploads/2019/02/A--China-Russia-Global-WP_FINAL.pdf.

[66] CMC Joint Staff Department [中央军委联合参谋部], “Accelerate the Construction of a Joint Operations Command System with Our Nation’s Characteristics—Thoroughly Study Chairman Xi’s Important Sayings When Inspecting the CMC Joint Operations Command Center [加快构建具有我军特色的联合作战指挥体系—— 深入学习贯彻习主席视察军委联指中心时的重要讲话], *Qiushi* [求是], August 15, 2016, http://www.qstheory.cn/dukan/qs/2016-08/15/c_1119374690.htm.

[67] Looking forward, “on the future battlefield, with the continuous advancement of AI and human-machine fusion (人机融合) technologies, the rhythm of combat will become faster and faster, until it reaches a “singularity” (奇点): the human brain can no longer cope with the ever-changing battlefield situation, unavoidably a great part of decision-making power will have to be given to highly-intelligent machines,” from the perspective of one Chinese defense academic.

[68] “National People’s Congress Representative Liu Guozhi: Artificial Intelligence Will Accelerate the Process of Military Transformation” [人大代表刘国治：人工智能将加速军事变革进程].

[69] “China Electronics Science and Technology Group and Baidu Company established the “Joint Laboratory for Intelligent Command and Control Technology”” [中国电科28所与百度公司成立“智能指挥控制技术联合实验室”], January 23, 2018, www.sohu.com:a:218485100%E2%80%AD_%E2%80%AC779538.

[70] These concepts (i.e., of humans being in, on, or out of the loop) originate in U.S. discussions of the role of humans in decision-making, reflecting the PLA’s close attention to U.S. policies and debates.

[71] See, for instance: Chen Hanghui [陈航辉], “Artificial Intelligence: Disruptively Changing the Rules of the Game” [人工智能：颠覆性改变“游戏规则], China Military Online, March 18, 2016, http://www.81.cn/jskj/2016-03/18/content_6966873_2.htm.

[72] The PLA as a whole is actively exploring options to leverage AI in support of command and control, particularly decision-making. For some of the existing literature on the topic based on

technical research and conceptual writings, see, for instance: Huang Jianming [黄建明], Hao Dongbai [郝东白], Zou Zhenning [邹振宁], “Aiming at the intelligentized and innovative command concept” [瞄准智能化创新指挥理念], China Military Online, September 27, 2018, http://www.mod.gov.cn/jmsd/2018-09/27/content_4825747.htm. See also: Zhang Xiaohai [张晓海], and Cao Xinwen [操新文], “Military Intelligent Decision Support System Based on Deep Learning” [基于深度学习的军事智能决策支持系统], Command Control and Simulation [指挥控制与仿真] 40, no. 2 (2018): 1-7.

[73] For my prior analysis on the topic, see: Elsa Kania, “Chinese Sub Commanders May Get AI Help for Decision-Making,” Defense One, February 12, 2018, https://www.defenseone.com/ideas/2018/02/chinese-sub-commanders-may-get-ai-help-decision-making/145906/?oref=d-river. For English-language reporting on the topic, see: Stephen Chen, “China’s plan to use artificial intelligence to boost the thinking skills of nuclear submarine commanders,” *South China Morning Post*, February 4, 2018, https://www.scmp.com/news/china/society/article/2131127/chinas-plan-use-artificial-intelligence-boost-thinking-skills.

[74] For a paper that provides an overview of the topic by researchers from the China Shipbuilding Industry Corporation, see: Qiang Chaochao [强超超] and Wang Yuanbin [王元斌], “Current Status and Development of the Target Recognition Technology” [水声目标识别技术现状与发展], *Command Information System and Technology* [指挥信息系统与技术] 9, no. 2 (2018): 73-78.

[75] Zhao Guohong [赵国宏], “Recognition of Several Issues in Combat Mission Planning” [作战任务规划若干问题再认识], *Journal of Command and Control* [指挥与控制学报], 3, no. 4 (2017): 265-272.

[76] “Evidence Reasoning and Artificial Intelligence Summit Forum” [证据推理与人工智能高峰论坛宣传册], December 26, 2017, https://new.qq.com/omn/20171226/20171226G0DFLD.html.

[77] Elsa Kania, “PLA Advances in AI-Enabled War-Gaming, China Brief,

[78] Li Ming [李明], “Artificial Intelligence Applications in Space Systems” [人工智能在空间系统的应用], Guangming Daily [光明日报], June 14, 2018, http://webcache.googleusercontent.com/search?q=cache:SWEs8zdUKJwJ:epaper.gmw.cn/gmrb/html/2018-06/14/nw.D110000gmrb_20180614_2-13.htm+&cd=29&hl=en&ct=clnk&gl=us. Li Ming is the deputy director of the Fifth Academy of the China Aerospace Science and Technology Group.

[79] “Remote Sensing Big Data Intelligent Processing and Mining Theories, Methodologies, and Major Applications” [遥感大数据智能处理与挖掘理论方法及重大应用] from the 2018 National Science and Technology Progress Award Nomination Content [2018年度国家科学技术进步奖提名公示内容].

[80] See: Xu Suhui [许夙晖] et al., “Unsupervised Remote Sensing Domain Adaptation Method with Adversarial Network and Auxiliary Task” [结合对抗网络与辅助任务的遥感影像无监督域适应方]. Some of the authors are affiliated with the Rocket Force Engineering University.

[81] For recent research on these issues, see: Fu Guangyuan [付光远], Pei Hongjun [辜弘炀], and Wang Hongqiao [汪洪桥], "Hyperspectral image classification based on weighted K-nearest neighbor and convolutional neural networks” [基于加权 K 近邻和卷积神经网络的高光谱图像分], *Computer Application Research [*计算机应用研究], 8 (2018): 76.

[82] “Chinese commercial space start-ups launch two AI satellites in a hundred days”

[中国商业太空初创企业百天内发射两颗AI卫星], *Global Times*, November 26, 2018, http://smart.huanqiu.com/ai/2018-11/13645096.html?agt=15422.

[83] For several examples of such research, see: Liu Xing [刘星], Chen Jian [陈坚], Yang Dongfang [杨东方], and He Hao [贺浩], "Scene-coupled air-to-ground multi-task remote sensing image intelligent detection algorithm" [场景耦合的空对地多任务遥感影像智能检测算法], *Optics Journal* [*光学学报]* 38, no. 12 (2018): 1215008. Xu Suhui [许夙晖] et al., "Unsupervised Remote Sensing Domain Adaptation Method with Adversarial Network and Auxiliary Task" [结合对抗网络与辅助任务的遥感影像无监督域适应方法].

[84] For an example of this research, see: Yang Guopeng [杨国鹏], "Hyperspectral image classification based on machine learning methods" [基于机器学习方法的高光谱影像分类研究], PhD, PLA Information Engineering University, 2010.

[85] See, for instance: Qu Chenghua [曲成华], Zhang Cheng [张程], Wu Jinhai [吴金海], and Shi Xinhu [史新虎], "Research on Regional Anti-Missile Warfare Accusation Center System Based on Artificial Intelligence" [基于人工智能的区域反导作战指控中心系统研究], http://webcache.googleusercontent.com/search?q=cache:qHZelT47m3EJ:kns.cnki.net/kcms/detail/detail.aspx%3Ffilename%3DKJSJ201814001%26dbcode%3DCJFQ%26dbname%3DCJFDTEMP%26v%3D+&cd=1&hl=en&ct=clnk&gl=us. The authors include those affiliated with the CETC 38th Research Institute, the former General Armaments 63726 Unit, and the Taiyuan Satellite Launch Center.

[86] See, for instance: "2017 Target Recognition and Artificial Intelligence Forum" [2017目标识别与人工智能高峰论坛], April 22, 2017, http://www.csoe.org.cn/meeting/trai2017/.

[87] For one of a number of publications on these topics, see: Tian Zhuangzhuang, Zhan Ronghui, Hu Jiemin, *et al*., "SAR ATR based on convolutional neural networks," *Journal of Radars*, 2016, 5(3): 320–325. DOI: 10.12000/JR16037.

[88] For an example of such research, see: Xing Yunlong [邢运龙], Li Aihua [李艾华], Cui Zhigao [崔智高], and Fang Hao [方浩], "Improved Kernel Correlation Filtering Moving Target Tracking Algorithm" [改进核相关滤波的运动目标跟踪算法], *Infrared and Laser Engineering* [红外与激光工程] 45, no. S1 (2016): 214-221.

[89] There is concern with foreign developments and accelerating indigenous capabilities: Ding Yu [丁宇] and Yan Xiusheng [闫秀生], "Intelligent long-range anti-ship missile capability and technical analysis" [智能化远程反舰导弹能力及技术分析], Optoelectronic Technology and Applications [光电技术应用] 34, no. 2 (2019): 1. On the subject of hypersonics developments, see: For an authoritative assessment, see: Lora Saalman, "China's Integration of Neural Networks into Hypersonic Glide Vehicles," December 2018, https://nsiteam.com/social/wp-content/uploads/2018/12/AI-China-Russia-Global-WP_FINAL.pdf. For research on techniques for adaptive control that leverage neural networks: Zhai Ziyang [甄子洋], Zhu Ping [朱平], Jiang Wei [江驹], and Tao Gang [陶钢] "Research progress of near-space hypersonic vehicles based on adaptive control" [基于自适应控制的近空间高超声速飞行器研究进展], Journal of Astronautics [宇航学报] 39, no. 4 (2018): 355-367.

[90] See: Lora Saalman, "China's Integration of Neural Networks into Hypersonic Glide Vehicles," in " AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives," A Strategic Multilayer Assessment (SMA) Periodic Publication, December 2018, https://nsiteam.com/social/wp-content/uploads/2019/02/AI-China-Russia-Global-WP_FINAL.pdf. "Announcement of Admissions for Doctoral Candidates in Flight Dynamics and Control, National University of Defense Technology" [2018年国防科技大学飞行动力学与控制方向博士研究生招生公告],

January 25, 2018.

[91] “Cloud Computing Powers Informatized Warfare” [云计算为信息化战争助力], PLA Daily, July 6, 2018, http://military.people.com.cn/n1/2018/0706/c1011-30130697.html.

[92] Wei Wenhui [魏文辉], Zhang Xiaobing [张晓冰], and Li Renbo [李仁波], “Cloud Computing Powers Informatized Warfare” [云计算为信息化战争助力], *PLA Daily*, July 6, 2018, http://www.xinhuanet.com/mil/2018-07/06/c_129908426.htm.

[93] For one analysis of potential applications of cloud computing, see: Zhao Fei [赵菲], Liu Junjie [刘俊杰], “Application of Cloud Computing in the Construction of Command Information System” [云计算在指挥信息系统建设中的应用], *Communication Technology* [通信技术], No. 4, 2012, http://www.cqvip.com/qk/94433x/201204/41468633.html. The authors are affiliated with the Navy Command Informatization Department (海军司令部信息化部).

[94] Yu Airong [于爱荣], et al., “Analysis and Research on the Architecture of Command Information System in the Age of Cloud Computing” [云计算时代下的指挥信息系统体系架构分析与研究], http://cpfd.cnki.com.cn/Article/CPFDTOTAL-ZHKZ201507002030.htm.

[95] “China Command and Control Society Joins Hands with CAS Dawn” [中国指挥与控制学会联手中科曙光], China New Network, January 15, 2016, http://www.chinanews.com/mil/2016/01-15/7718692.shtml.

[96] “Shuguang – Company Profile” [曙光 一公司介绍], http://www.sugon.com/about/intro.html.

[97] “Accelerate the “Cloud-ization” and Intelligentization of Military Command Information Systems” [推进军事指挥信息系统“云”化和智能化], *Global Times*, January 17, 2017, http://www.js7tv.cn/news/201601_33024.html

[98] “Ganyun S&T Indigenous Cloud Computing Products Displayed at the Qingdao Military-iCivil Fusion S&T Innovation Show” [乾云科技自主云计算产品亮相首届青岛军民融合科技创新成果展], October 12, 2018, http://www.massclouds.com/index.php?m=content&c=index&a=show&catid=7&id=860. “Meiyun Cloud won the “Cloud Computing Service Best Practice Award” for 2017 Military-Civilian Fusion Industry” [美猴云获2017年军民融合产业“云计算服务最佳实践奖], August 25, 2017, https://web.archive.org/web/20190705015905/https://www.jianshu.com/p/dc03b43adcf7.

[99] For a great assessment of these risks, see: Jackie Schneider, “JEDI: Outlook for Stability Uncertain as Pentagon Migrates to the Cloud,” *Bulletin of the Atomic Scientists* (blog), June 21, 2018, https://thebulletin.org/2018/06/jedi-outlook-for-stability-uncertain-as-pentagon-migrate-.

[100] Wu Guohui [吴国辉], “Cloud Combat”: Bringing a New Revolution in Air and Space Combat” [云作战”：带来空天作战新革命], China National Defense Report [中国国防报], March 7, 2016, http://zlzy.81.cn/qy/2016-08/19/content_7232206_2.htm. The author is a professor at the PLA’s National Defense University.

[101] For more on the PLA’s interest in big data for defense, see: Big data builds the strongest “military brain”” [大数据构筑最强“军事大脑], *Qiushi* [求是], July 12, 2018, https://web.archive.org/web/20190505163610/http://www.qsjournal.com.cn/junshiguofang/46518.html.

[102] “5G Technology Military-Civil Fusion Applications Industry Alliance Established in Beijing” [5G技术军民融合应用产业联盟在北京成立], *Economic Network* [经济网], November 5, 2018,

http://www.ceweekly.cn/2018/1105/239477.shtml. “CASIC: Promoting the application of 5G technology in the military and civilian fields” [航天科工：推动5G技术在军民领域的应用], Economics Daily [经济日报], November 2, 2018, http://www.ce.cn/xwzx/gnsz/gdxw/201811/02/t20181102_3069I220.shtml.

[103] “When communication is paralyzed, can the PLA resume command with 5G?” [通讯陷入瘫痪，解放军能不能用5G恢复指挥？], CCTV, June 17, 2019, http://military.cctv.com/2019/06/17/ARTIQE70Hgi9NzGxbt1OrXIh190617.shtml

[104] The PLA has used QKD at least experimentally since as early as 2009, and reportedly possessed the capability to use quantum communications in a wartime scenario in 2015, according to Chinese scientist Pan Jianwei.

[105] “Quantum Innovation Research Institute Proposed Five-Year Objectives; Will Launch Many Micro and Nano-Quantum Satellites” [量子创新研究院提五年目标 将发多颗微纳量子卫星], China Daily, February 23, 2018, http://cn.chinadaily.com.cn/2018-02/23/content_35725867.htm.

[106] “Thirteenth Five-Year Science and Technology Military-Civil Fusion Development Special Plan” (Full Text) [“十三五”科技军民融合发展专项规划》全文], September 26, 2017, http://www.aisixiang.com/data/106161.html.

[107] “Chinese military-use quantum mobile phones will be entering trial usage” [中国军用量子手机将投入试用], Military Observer, June 29, 2018, http://mil.news.sina.com.cn/china/2018-06-29/doc-iheqpwqy6243500.shtml.

[108] “In the future, underwater operations, how to maintain the ‘letter from a distance’ with the outside world”[未来水下作战，如何在水下保持与外界“飞鸿传书”], Xinhua, March 3, 2019, http://www.xinhuanet.com/mil/2019-03/01/c_1210070679.htm.

[109] “Seawater quantum communication is far from military applications” [海水量子通信离军事应用尚远], *S&T Daily* [*科技日报],* https://web.archive.org/web/20190705022129/http://www.xinhuanet.com/tech/2017-09/06/c_1121611142.htm.

[110] Ibid. The academic in question is Wang Qun (王群), a professor at the National Security and Military Strategy Research Center of the National University of Defense Technology.

[111] For a more detailed discussion of potential considerations: Raymond Wang, “Quantum Communications and Chinese SSBN Strategy,” *The Diplomat*, November 04, 2017, https://thediplomat.com/2017/11/quantum-communications-and-chinese-ssbn-strategy/.

[112] Hu Zhi-qiang [胡志强] and Hu Qian-jin [胡前进], “Discussion on the Application of Quantum Communication in the Ocean in Military Field, Second China Command and Control Conference Volume, 2014.

[113] “The ultimate weapon for deciphering information security “quantum communication”,” *PLA Daily*, April 12, 2017.

[114] Ibid.

[115] “China adds new line to its quantum communications network,” *Asia Times*, November 22, 2018, http://www.atimes.com/article/china-adds-new-line-to-its-quantum-communications-network/.

[116] “Quantum Technology: Archimedes Pivot of the Military Revolution” [量子技术：军事革命的阿基米德支点], China Social Sciences Network [中国社会科学网], January 19, 2017.

[117] Wang Junze [王军责], “Quantum Technology: Making Informatized Warfare Change Its Face” [量子技术：让信息化战争变了容颜], China National Defense Report, January 8, 2014, http://www.81.cn/jkhc/2014-01/08/content_5726287.htm.

[118] Elsa Kania and John Costello, “Quantum Hegemony? — China’s Ambitions and the Challenge to American Innovation Leadership,” Center for a New American Security, November 2017, https://www.cnas.org/publications/reports/quantum-hegemony

[119] Of course, views vary, but this comment is based on my attendance of a workshop at which this question was discussed and subsequent conversations with a number of U.S. and international quantum scientists.

[120] For a technical assessment of these potential vulnerabilities, see: Li Hongxin [李宏欣] et al., “Security Analysis on Measurement-Device-Independent Quantum Key Distribution Protocol” [数学与物理 测量设备无关量子密钥分发方案安全性研究], November 6, 2017, https://webcache.googleus-ercontent.com/search?q=cache:5RdMZfkrqLUJ:https://image.hanspub.org/xml/22813.xml+&cd=17&hl=en&ct=-clnk&gl=au.

IV. NAUTILUS INVITES YOUR RESPONSE

The Nautilus Asia Peace and Security Network invites your responses to this report. Please send responses to: nautilus@nautilus.org. Responses will be considered for redistribution to the network only if they include the author’s name, affiliation, and explicit consent

---

View this online at: https://nautilus.org/napsnet/napsnet-special-reports/emerging-technologie--in-future-pla-nuclear-command-control-and-communications/

Nautilus Institute
608 San Miguel Ave., Berkeley, CA 94707-1535 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org