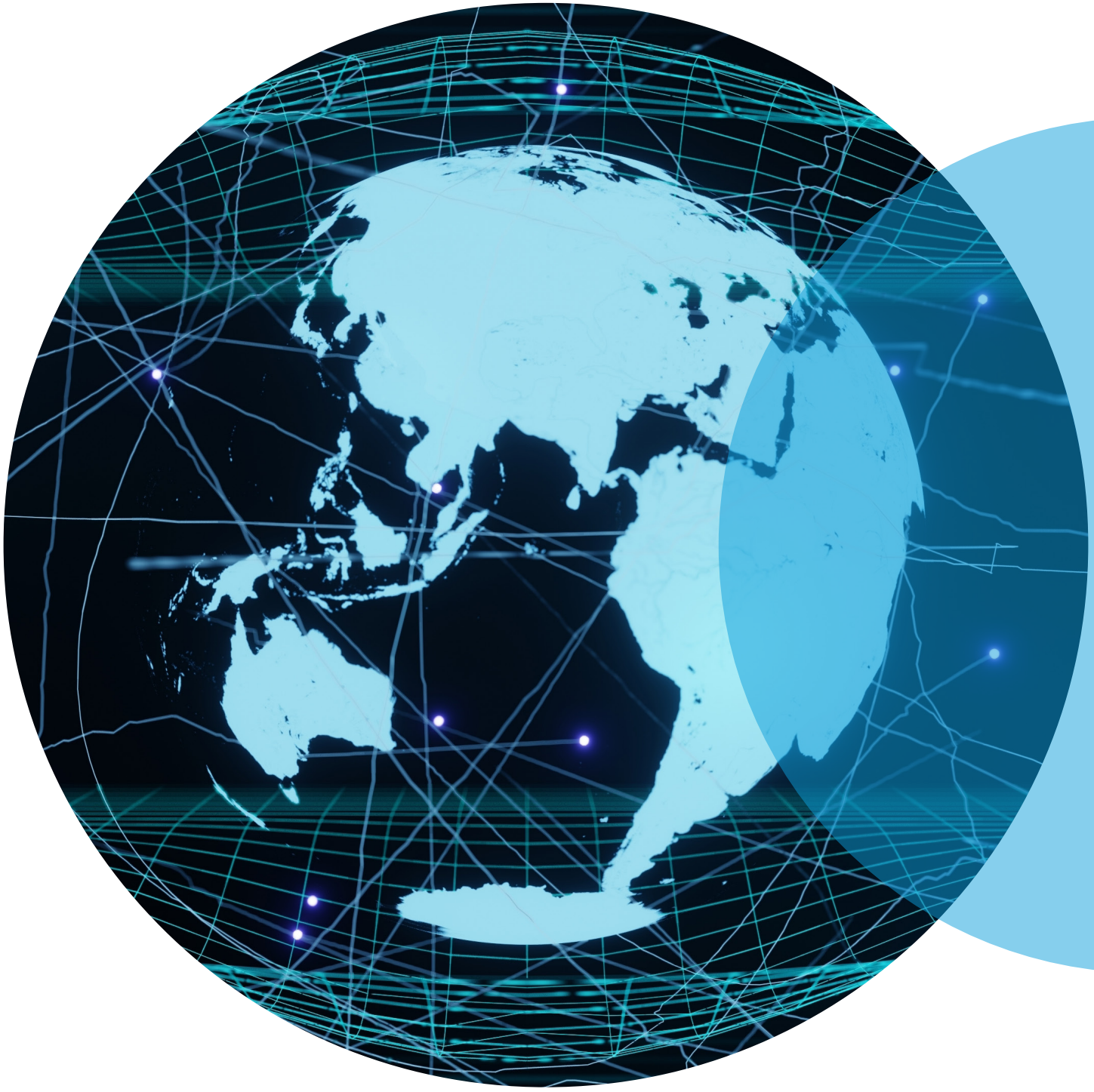
Hybrid CoE Paper 22

Cross-cutting technologies in Chinese space activities: Raising the risk of hybrid threats



Hybrid CoE

Mélusine Lebret, Theodora Ogden, James Black – December 2024

Hybrid CoE Papers are finalized pieces of analysis on a topic related to hybrid threats, based on one or several research questions. They may be either conceptual analyses or based on a concrete case study with empirical data.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 www.hybridcoe.fi

ISBN 978–952–7591–14–7 (web)
ISBN 978–952–7591–15–4 (print)
ISSN 2670–2053 (web)
ISSN 2814–7227 (print)

December 2024

Cover photo: CESM I Studio / Shutterstock.com

Hybrid CoE's mission is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

Contents

List of abbreviations

AI – Artificial Intelligence
ASAT – Anti-Satellite
CCS – Counter Communications System
C2 – Command and Control
C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CHIPS – Creating Helpful Incentives to Produce Semiconductors (US Act)
EW – Electronic Warfare
GEO – Geosynchronous Equatorial Orbit
GPS – Global Positioning System
IO – Information Operations
ISR – Intelligence, Surveillance, and Reconnaissance
LEO – Low Earth Orbit
MCF – Military-Civil Fusion
PNT – Positioning, Navigation, and Timing
PLA – People's Liberation Army
PLASSF – PLA Strategic Support Force
QKD – Quantum Key Distribution
QUESS – Quantum Experiments at Space Scale
S&T – Science and Technology
SATCOM – Satellite Communications
SDA – Space Domain Awareness
SSA – Space Situational Awareness
UN OEWG – United Nations Open-Ended Working Group

Summary

This Hybrid CoE Paper addresses China's use of cross-cutting technologies as part of hybrid threats in space and emanating from space. First, an understanding of Chinese strategy and doctrine is important to characterize activities across domains, including information operations. Next, the Paper assesses cross-cutting technologies, including artificial intelligence (AI), quantum technologies, and advances in hardware, as well as the associated risks (e.g., escalation), including to Chinese systems themselves. Finally, the Paper examines the implications for NATO and EU member states across domains in the event of hybrid threats to their space capabilities.

Introduction

China's rapid technological advances in recent years have raised concerns in the United States, the European Union (EU) and the North Atlantic Treaty Organization (NATO) about how China's increasing strengths in science and technology (S&T) may challenge Western interests and values.[1] The competition over S&T has spilled over into space, where the development and integration of new technologies into space capabilities is key to achieving military and commercial advantages in this fast-changing domain.[2] Increasingly, innovation is focused not only on space-specific technologies (e.g., new forms of spacecraft propulsion), but also on cross-cutting technologies with a broad range of applications across multiple domains.[3]

Prominent examples of cross-cutting technologies include artificial intelligence (AI), quantum technologies, or hardware (e.g., robotics, semiconductors), all of which are seeing sizeable investments in both China and the West in the race for S&T advantage. Such technologies are critical enablers and drivers of improvements in space-related capabilities such as space domain awareness (SDA), satellite communications (SATCOM), Earth observation/intelligence, surveillance, and reconnaissance (EO/ISR), and on-orbit operations (e.g., rendezvous and close-proximity missions, or active debris removal). Many of these applications and use cases are benign. However, advances in these cross-cutting technologies also bolster China's capacity to undertake more coercive activities in and through the space domain, contributing to hybrid threats.[4]

Hybrid threat operations[5] against space assets and ground infrastructure may seek space domain dominance or deterrence through a variety of domains and means, leveraging cyber, electromagnetic capabilities, or the information environments, for example. Attacks on key assets and infrastructure may target space-based systems, their ground infrastructure, or data transfer links. This is possible kinetically, through physical attacks; or non-kinetically, through cyberattacks and electronic weapons. The future strategic environment of space is also shaped by the inherent dual-use function

1 T. Chhabra, R. Doshi, R. Hass & E. Kimball. *Global China: Technology* (Brookings, 2020). https://www.brookings.edu/articles/global-china-technology/.

2 Cross-cutting technologies refer to cross-cutting, non-space technologies – such as AI, robotics, semiconductors, and other technological innovations that can be utilized to enhance space capabilities, but which are also widely applied in other domains.

3 James Black, Theodora Ogden, Mélusine Lebret, Andy Skelton, Zsofia Wolford & Henri van Soest. *Implications of Emerging Technology for UK Space Regulation Policy* (Santa Monica, Calif.: RAND Corporation, 2024). https://www.rand.org/pubs/research_reports/RRA3121-1.html.

4 Terrence K. Kelly, David C. Gompert & Duncan Long. *Smarter Power, Stronger Partners, Volume I: Exploiting U.S. Advantages to Prevent Aggression* (Santa Monica, Calif: RAND Corporation, 2016). https://www.rand.org/pubs/research_reports/RR1359.html.

5 Hybrid CoE identifies hybrid threats as the targeting of democratic vulnerabilities through coordinated, diverse means, but also as exploiting the thresholds of detection and attribution, and various interfaces (e.g., war-peace, local-state), as well as exerting an influence on decision-making to advance strategic goals while undermining targets. Hybrid CoE, *Hybrid Threats as a Concept* (n.d.). https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

of space technologies, which can be used for both military and civilian purposes.[6]

This Hybrid CoE Paper summarizes the impact of cross-cutting technologies on China's wider space capabilities and the implications for hybrid threats. This analysis takes stock of the existing evidence and knowledge of the relevant cross-cutting space technologies that the People's Liberation Army (PLA) is using or is likely to use in the coming decade, underpinned by an increasingly collaborative strategy with the private space industry in line with China's concept of military-civil fusion (MCF)[7]. As China strives to deploy state-of-the-art technologies as a capability multiplier for space, it becomes increasingly important to examine how these technologies can amplify hybrid threats, as well as the implications for EU and NATO member states and their international partners. The research for this short study draws on academic articles, reports, and policy documents identified through a targeted literature review.[8] Hybrid CoE's conceptual framework, based on the definition of hybrid threats, was used to guide the analysis.[9] The objective is to equip readers with a foundational understanding of China's use of cross-cutting technologies in space as a basis for future research. First, the Paper briefly examines China's strategy and activities in the space domain, and how cyber and electronic warfare capabilities are combined with space capabilities. It then assesses how China is implementing its strategy, including through investments in cross-cutting technologies such as artificial intelligence (AI), quantum, and orbital hardware, together with the implications of these investments. The Paper also addresses the challenges that Chinese space systems are encountering, for example due to orbital debris, military escalation, supply-chain disruptions, and strategic dilemmas. Finally, the Paper identifies the implications for NATO and EU member states in relation to China's use of cross-cutting technologies in space as part of hybrid threats.

6 James Black, Linda Slapakova & Kevin Martin. *Future Uses of Space Out to 2050: Emerging Threats and Opportunities for the UK National Space Strategy* (Santa Monica, Calif: RAND Corporation, 2022). https://www.rand.org/pubs/research_reports/RRA609-1.html.

7 The military-civil fusion refers to the development of civil programmes to benefit the military. See e.g., Conlan Ellis, Theodora Ogden, and James Black. 'China and space: How space technologies boost China's intelligence capabilities as part of hybrid threats'. Hybrid CoE Paper 21, 21 October 2024, 13.

8 The key Boolean search strings for the selection of papers were: "China space strategy", "China space technology", "China dual-use space technologies", "China sub-threshold space threats", "China space hybrid threats", "hybrid threats", "cross-cutting technologies". Sources dated before 2015 and containing only high-level information on dual-use technology were excluded.

9 Georgios Giannopoulos, Hanna Smith, and Marianthi Theocharidou. 'The landscape of Hybrid Threats: A conceptual model'. 5 February 2021. https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/.

China's strategic approach to hybrid warfare

In order to understand China's use of cross-cutting technologies in space, it is first necessary to frame China's strategic objectives and conceptual or doctrinal basis. China has long employed a wide range of hybrid threat tactics, embedding them throughout its strategic planning and viewing them holistically as part of a broader approach to interstate competition.[10] In 2003, China adopted the Three Warfares doctrine, which emphasized the need to move beyond the build-up of traditional military capabilities (still a major priority for the PLA) and to develop hybrid threat capabilities for "psychological warfare, public opinion warfare, and legal warfare".[11] Much has also been written about the concept of Unrestricted Warfare – a set of ideas proposed by two colonels in the PLA air and ground forces in a 1999 treatise that has since proven influential, but which has not technically been incorporated into formal Chinese doctrine.[12] This concept focuses on the securitization of all policy domains and the use of all levers, both military and non-military, above and below the threshold of open conflict, to achieve an advantage for China.[13]

Within this overarching approach to strategic competition – and understanding the role of hybrid threats in it – the PLA has also developed a set of military concepts and a doctrine that influence Chinese space operations. The PLA has focused its recent modernization programmes on enhancing its capabilities and readiness to fight future "informatized" and "intelligentized" wars and to achieve information dominance below the threshold of open warfare. In 2016, China released its State Plan for Informatization in the Period of the 13th Five-Year Plan, which seeks to develop space-based infrastructure to provide high-speed global internet and information services through communications satellites in Low Earth Orbit (LEO) and higher orbits, as well as a network of floating platforms high in the atmosphere.[14] In addition, concerns persist that China is increasing its control over pathways of information sharing, with the ability to intercept, censor or shut down communications through AI-enabled bulk data collection and surveillance.[15] The PLA places significant emphasis on diminishing or preventing an adversary through information operations (IO) during the initial stages of a

10 Office of the Secretary of Defense. A*nnual Report to Congress. Military and Security Developments Involving the People's Republic of China* (2020). https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINAMILITARY-POWER-REPORT-FINAL.PDF.

11 James Black, Alice Lynch, Kristian Gustafson, David Blagden, Pauline Paillé & Fiona Quimbre. *Multi-Domain Integration in Defence: Conceptual Approaches and Lessons from Russia, China, Iran and North Korea* (Santa Monica, Calif: RAND Corporation, 2022). https://www.rand.org/pubs/research_reports/RRA528–1.html.

12 Qiao Liang and Wang Xiangsui. *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999).

13 David Kilcullen. *The Dragons and the Snakes: How the Rest Learned to Fight the West* (Glasgow, UK: Bell & Bain Ltd., 2020).

14 Mark Stokes, Gabriel Alvarado, Emily Weinstein & Ian Easton. *China's Space and Counterspace Capabilities and Activities*. The U.S.-China Economic and Security Review Commission, 30 March (2020). https://www.uscc.gov/sites/default/files/2020–05/China_Space_and_Counterspace_Activities.pdf.

15 IISS. *Cyber Capabilities and National Power: A Net Assessment. International Institute for Strategic Studies* (2021). https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf.

conflict, increasing intensity as the conflict progresses.[16] This tactic exists within the framework of "informatized warfare".[17] With the rise of AI, the Chinese military strategy has evolved into "intelligentized warfare" due to advanced AI technologies that enhance the interconnectivity of information networks deployed between space and terrestrial capabilities.[18] China's improved intelligence and military capabilities, combined with its IO and economic warfare potential, pose considerable hybrid threats to EU and NATO countries.

Many of China's investments in cross-cutting technologies have broad applications that reinforce the connections between activities across space, cyber and the electromagnetic spectrum. The PLA views offensive cyber capabilities as a fundamental element of an integrated approach to information operations and wider strategic competition, and employs cyberattacks to support military operations, including against space assets. In realizing its vision of "information-led" operations becoming "machine-led", the PLA has been forming information warfare units since 2005 to create cyber means to attack adversarial computer systems and networks deployed in space, and to devise strategies and precautions to protect friendly assets at the same time.[19] In line with the principles of "system destruction warfare", China uses cyber capabilities to target other countries' space-enabled C4ISR systems and to pursue information dominance, seeking to undermine adversaries' ability to establish good situational awareness or make timely, informed decisions, skewing the competitive balance in China's favour.[20] The PLA also places a high value on electronic warfare (EW), which is used to suppress or deceive enemy equipment and operations.[21] Chinese operations aim to use a mix of dazzling (e.g., with lasers), spoofing and, in particular, jamming.[22] Regular exercises involving jamming techniques aim to degrade or deny SATCOM, EO/ISR, and positioning, navigation and timing (PNT) services, such as the US's Global Positioning System (GPS) or the EU's Galileo.[23]

The military doctrine of "system destruction warfare" seeks to weaken, confuse or paralyze the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems of Beijing's adversaries to render them unable or unwilling to oppose

16 Black et al. *Multi-Domain Integration in Defence*.

17 U.S. Department of Defence. 'Military and Security Developments Involving the People's Republic of China'. (2023). https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

18 Ibid.

19 Ibid.

20 Defense Intelligence Agency. 'Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion'. (2022). https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf.

21 Office of the Secretary of Defence. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2020* (2020). https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINAMILITARY-POWER-REPORT-FINAL.PDF.

22 J. Engstrom. *Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army seeks to wage Modern Warfare* (Santa Monica, Calif: RAND Corporation, 2018). https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1708/RAND_RR1708.pdf.

23 Office of the Secretary of Defence. *Annual Report to Congress*.

Chinese operations.[24] This systems-thinking approach also exploits the interconnectedness of hybrid threat activities across all domains.[25] This also links to the PLA's notion of systems confrontation, which requires "comprehensive dominance" to be achieved across all domains through the implementation of multifunctional operational systems and the coordination of offensive or subversive actions.[26] Many of these ideas are given institutional form through the organizational structures and remit of the PLA's Strategic Support Force (PLASSF), which was established in 2015 to bring together capabilities across cyber, electronic, and space operations to achieve information dominance over China's adversaries.

Economic tools, such as creating economic dependencies, are also included in China's hybrid threat strategy around the space domain. Through the provision of space-dependent dual-use technology, China strategically embeds other states within its supply chain. Selling this kind of technology through contracts with confidentiality clauses that allow lenders to influence debtors' policies also threatens countries' sovereign borrowing.[27] For example, in 2014, as part of its Belt and Road Space Information Corridor project, China provided Pakistan with a heavily subsidized signal operated by BeiDou, one of the main state-owned Chinese navigation satellite systems. This initiative aimed to replace GPS for critical systems in the region, while posing a threat to Pakistan's use of American GPS in 2023.[28]

24 Engstrom. *Confrontation and System Destruction Warfare*.

25 James Scouras, Edward Smyth & Thomas Mahnken. *Cross-domain deterrence in US-China Strategy*. Johns Hopkins Applied Physics Laboratory. (2017). https://www.jhuapl.edu/sites/default/files/2022–12/CrossDomainWeb.pdf.

26 Engstrom. *Confrontation and System Destruction Warfare*.

27 Jakub Pražák. 'On the Threshold of Space Warfare', *Astropolitics*, Vol. 20, Issue 2–3, (2022): 175–191, https://doi.org/10.1080/14777622.2022.2142351.

28 Jana Robinson, Patrik Martínek, Jakub Pražák & Kristína Sikoraiová. *China Deploys BeiDou to Project Power and Influence*. Prague Security Studies Institute, 8 March (2021). https://www.pssi.cz/publications/44-pssi-perspective-8-china-deploys-beidou-to-project-power-and-influence.

Implementation of cross-cutting technologies as part of China's space strategy

China's approach to competition draws on innovation in a range of cross-cutting technologies, and across many domains and means. Given that these are extensive, this Paper provides a non-exhaustive overview of three emerging areas for consideration, selected based on their importance and prominence in the literature on cross-cutting space technologies. They include artificial intelligence (AI), quantum technologies, and advances in orbital hardware. Advances in cross-cutting technologies are improving Chinese hardware and space-based systems at a rapid rate, posing hybrid threats in space and on Earth.

Artificial intelligence

AI refers to machines that can independently perform various functions, simulating human cognitive abilities. This critical technology can be used for problem-solving, automating repetitive tasks, or enhancing situational awareness and decision-making, while providing valuable insights into large quantities of data. Chinese advances in AI in space capabilities contribute to hybrid threats through increased ability to analyze EO/ISR data, the automation of orbital operations, as well as the ability to claim plausible deniability and machine error in the event of hostile actions against US or European satellites.

China is bolstering its informatization strategy through AI to advance its military capabilities and industry.[29] Strengthened by AI, the Chinese theory of victory implements the PLA's integrated combat forces to achieve success primarily in "system-vs-system operations", which involve hybrid threat objectives such as information dominance, precision strikes, and joint operations.[30] China has been using a combination of physical and non-kinetic space means to advance its military interests in maritime Asia, including the expansion of its coast guard and maritime militia through its independently constructed, developed, and exclusively operated AI-enabled BeiDou satellite navigation system.[31] This system now offers a global positional accuracy standard of 10 metres, with even higher accuracy within 5 metres in the Asia-Pacific region. Along with providing precise PNT, BeiDou notably includes a Regional Short Message Communication service, which enables user tracking and text messaging, facilitating mass communication among users.[32] These additional capabilities of the system enhance the military Command and Control (C2) readiness of the PLA. Alongside reinforcing China's own military capabilities, the increasing integration of AI into Chinese space services to enhance their effectiveness also supports wider efforts to promote their use by countries involved in Beijing's Digital Silk Road initiative.

29 Shira Efron, Howard J. Shatz, Arthur Chan, Emily Haskel, Lyle J. Morris & Andrew Scobell. *Evolving Israel-China Relationship* (Santa Monica, Calif: RAND Corporation, 2019). https://www.rand.org/pubs/research_reports/RR2641.html.

30 Black et al. *Multi-Domain Integration in Defence*.

31 Christopher Paul, James Dobbins, Scott W. Harold, Howard J. Shatz, Rand Waltzman & Lauren Skrabala. *A Guide to Extreme Competition with China* (Santa Monica, Calif: RAND Corporation, 2021). https://www.rand.org/pubs/research_reports/RRA1378–1.html.

32 Defense Intelligence Agency. 'Challenges to Security in Space'. https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf.

Quantum technologies

Quantum technologies are the result of the quantum effects of quantum mechanics and encompass quantum computing, sensing, measurement, simulation, and materials. Quantum computing uses qubits, which are the fundamental units of information, unlike the regular bits used in conventional computing. Qubits enable quantum computers to operate with greater complexity and speed because qubits have the ability to exist in multiple states simultaneously (on, off, or a mix of both) and exhibit entanglement, linking particles like photons and electrons even when they are far apart. The result is processing power that far outstrips today's supercomputers and enables a new form of encryption that is theoretically unhackable.[33] Quantum technologies have the potential to transform computing, communications, navigation, encryption, and sensing, which could greatly enhance the communications and operational efficiency of space-based systems.

China is one of the leading players in the global race to harness quantum technologies to bolster intelligence capabilities and enable data transmission at ultra-high speeds, while preventing interception by enemies. Chinese advances in quantum computing threaten to bring about a post-decryption world, incentivizing China to acquire encrypted data from or about foreign space capabilities in the hope of decrypting them in the future.

China is prioritizing the development of quantum communication networks through the Quantum Experiments at Space Scale (QUESS) project.[34] The project builds on China's previous work on the Mozi quantum satellite, which was launched in 2016 and is able to establish long-distance quantum key distribution communication – a secure communication method that uses quantum mechanics to generate and share encryption keys and detect interference – between ground stations across distances of 1,200 km.[35] In partnership with Austrian research institutes, QUESS aims to enable long-distance quantum communication through high-speed Quantum Key Distribution (QKD), as well as Quantum entanglement distribution.[36] The Jinan-1 satellite, launched into Low Earth Orbit in 2022, is capable of generating quantum keys up to three times faster than the Mozi satellite.[37] China's planned subsequent medium- and high-orbit quantum satellites are under development to upscale quantum experiments and realize quantum entanglement distribution

33 D. Lague. 'U.S. and China race to shield secrets from quantum computers'. Reuters (2023). https://www.reuters.com/investigates/special-report/us-china-tech-quantum/.

34 U.S. Department of Defense. *Military and Security Developments Involving the People's Republic of China.* (2023). https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

35 Harun Šiljak. 'China's quantum satellite enables first totally secure long-range messages'. *The Conversation*, 16 June, 2020. https://theconversation.com/chinas-quantum-satellite-enables-first-totally-secure-long-range-messages-140803.

36 EOPortal. *QUESS*. (2021). https://www.eoportal.org/satellite-missions/quess#mission-status.

37 SatNews. 'China launches new satellite in 'important step' towards global quantum communications network'. (2022). https://news.satnews.com/2022/07/31/china-launches-new-satellite-in-important-step-towards-global-quantum-communications-network/.

over greater distances.[38] If successful, China may become the first nation to achieve quantum C2 or to unencrypt the transmitted data of its adversaries at a faster pace than effective defenses can be implemented.

Orbital hardware

Technologies such as robotics and semiconductors enable the development of orbital hardware with the potential for use in anti-satellite systems, active debris removal, space tugs, and in-orbit maintenance and repairs. Although such systems have the potential to bring about improvements, such as the removal of orbital debris, the refuelling of space systems and moving defunct satellites into graveyard orbit, there are associated concerns about the dual-use or dual-purpose aspect of these capabilities.

In recent years, China has tested space-based maintenance technologies for satellite inspection and repair, while exploring options for orbital debris removal. Although the objectives of such programmes may serve a wider civilian purpose, there are dual-use implications for such systems if operationalized to target functional satellites. Shijian-21, a Chinese dual-use satellite with a robotic arm that can be used for both civilian and military purposes – including interfering with operational satellites – was launched into Geosynchronous Equatorial Orbit (GEO) in late 2021, and towed a defunct BeiDou navigation satellite to a high graveyard orbit in early 2022.

Since 2006, government-linked Chinese academia has been exploring aerospace engineering concepts related to space-based kinetic weapons (e.g., re-entry techniques, payload separation, delivery vehicles, and transfer orbits for the purpose of targeting etc.).[39] As a result of this research, in 2021, China successfully executed the first fractional orbital launch[40] of an intercontinental ballistic missile with a hypersonic glide vehicle, demonstrating the longest flight time (over 100 minutes) and the greatest distance flown (approximately 40,000 kilometres) of any Chinese land attack weapon system to date.[41]

38 J. Pao. 'China making the quantum future in space'. *Asia Times*, 3 June, 2023. https://asiatimes.com/2023/06/china-to-boost-quantum-research-in-space/.

39 Defense Intelligence Agency. 'Challenges to Security in Space'.

40 Fractional orbital launch systems deliver a payload into LEO, which then orbits the Earth as required before re-entering the atmosphere to strike targets in a more unpredictable and hard-to-detect manner than traditional ballistic missiles, which follow a predictable parabolic arc from launch site to target. Ritwik Gupta. 'Orbital hypersonic delivery systems threaten strategic stability'. *Bulletin of the Atomic Scientists*. (2023).

41 U.S. Department of Defense. 'Military and Security Developments'.

Risks to Chinese systems

Although China is deriving considerable benefits from advances in cross-cutting technology, some risks to Chinese systems remain. Besides natural hazards such as space weather, human-generated debris poses a growing risk to all assets in space. China's 2007 test launch of a direct ascent anti-satellite (ASAT) attack – a missile-targeted assault – on a defunct Chinese weather satellite generated the largest-ever debris field in space of more than 3,000 trackable pieces, increasing space debris by 25%.[42] The International Space Station is still forced to manoeuvre to avoid some of this debris today.[43] Likewise, China's Tiangong space station is susceptible to space junk, sustaining damage to its core module earlier this year and experiencing a partial loss of power supply due to debris striking the solar wing's power cables.[44] The increase in space activities contributes to the risk of space debris and damage to assets, requiring mitigation measures by the Chinese government, ranging from Space Situational Awareness (SSA) and monitoring of the space environment to reinforcing systems and components.[45]

In addition to the risk of accidental collisions, there is also the risk of unintended conflict in outer space due to hostile Chinese activities or incidents that provoke miscalculation and escalation – triggering a Western response. There is also a risk that Chinese systems might fall victim to fratricide, which remains a constant concern for EW capabilities with a wide beamwidth (as opposed to systems that only hit targets along a narrow beam in line of sight). When used in counterspace operations, Chinese Counter Communications Systems (CCS) and jammers may also inadvertently disrupt other Chinese satellites, including PNT systems. To address this weakness, and the threats posed by US and allied EW capabilities, the PLA is looking to improve the defenses of Chinese satellites, conceal their operations centres, enhance the ability to manoeuvre satellites when under attack, and use civilian satellites for military purposes to provide both deniability and redundancy, alongside stockpiling other satellites in reserve to fill coverage gaps during wartime.[46] The Chinese military is also concerned that friendly air defense units could accidentally jam BeiDou satellites, calling for coordinated transparency on electronic jamming across the PLA to reduce the risk.[47]

China is also encountering supply chain risks, particularly for critical semiconductors essential to space technologies. Taiwan is the global leader in semiconductor manufacturing, outstripping all other competitors, including China. Despite increased spending on the semiconductor industry and aiming to reach 70% self-sufficiency in chip manufacture by 2025, China is

42 ESA. 'About Space Debris' (n.d.). https://www.esa.int/Space_Safety/Space_Debris/About_space_debris; Greg Hadley. 'Saltzman: China's ASAT Test Was "Pivot Point" in Space Operations', Air & Space Forces, 13 January, 2023, https://www.airandspaceforces.com/saltzman-chinas-asat-test-was-pivot-point-in-space-operations/.

43 Hadley. 'Saltzman: China's ASAT Test'.

44 Elizabeth Howell. 'China's Tiangong space station damaged by debris strike: report'. Space.com, 24 April, 2024. https://www.space.com/china-tiangong-space-station-space-debris-measures.

45 Ibid.

46 Kevin McCauley. 'China's PLA Increasing Use of Simulators and Simulations'. EO Watch Commentary, 1 May, 2022. https://community.apan.org/wg/tradoc-g2/fmso/m/oe-watch-articles-2-singular-format/416133.

47 Stokes et al. *China's Space and Counterspace Capabilities*.

currently at approximately 16% self-sufficiency, importing the majority of its chips.[48] However, Western-imposed sanctions are restricting China's ability to import semiconductors and chip-making technologies. The US CHIPS and Science Act, passed in 2022, prohibits technology sales to Chinese companies and is expected to limit China's growth in the semiconductor market, thereby restricting the implementation of MCF.[49]

China's MCF strategy also creates a dilemma for Chinese industry and leadership. While MCF is strengthening China's industrial defense base, the strategy also poses risks to its space industry. The hesitance of Western countries to cooperate with China's space industry in the face of MCF could affect the sector in the long run, with fewer opportunities to trade and learn from other nations.[50]

48 David Sacks. 'Will China's Reliance on Taiwanese Chips Prevent a War?'. Council on Foreign Relations, 6 July, 2023, https://www.cfr.org/blog/will-chinas-reliance-taiwanese-chips-prevent-war.

49 Jeremy Mark and Dexter T. Roberts. 'United States–China semiconductor standoff: A supply chain under stress'. Atlantic Council (2023.) https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/united-states-china-semiconductor-standoff-a-supply-chain-under-stress/.

50 Masaaki Yatsuka, 'The complex impact of China's military-civil fusion in space', Think China, 4 July, 2022. https://www.thinkchina.sg/technology/complex-impact-chinas-military-civil-fusion-space.

Conclusions and implications for NATO and EU member states

China's use of cross-cutting technologies as part of its hybrid threat activities remains a major concern for the US, Europe, and their allies and partners. The military strategy implemented by the PLA incorporates both covert and overt methods of influence. Cyber and electronic strategic means are highly important to China as part of its hybrid approach, making vulnerabilities in these areas arguably the greatest threat to allied satellite systems.[51] Accordingly, EU and NATO countries need to take measures to limit disruption through cyber and electronic means and to mitigate the risks posed by cross-cutting technologies in the context of hybrid threats.

Cyber resilience is important to mitigate potential threats, particularly emanating from the integration of cross-cutting technologies in China's arsenal, including AI and quantum. EU policymakers meet with their US counterparts annually to update their cyber and space strategies against the latest threats and to explore options to enhance cooperation with allies.[52] Further collaboration is needed to share good practice and to update on the most pressing threats. It is also important that lessons are transferred across government and industry. The US Satellite Cybersecurity Act of 2022 proposes a list of "best practices" to be maintained by the Cybersecurity and Infrastructure Security Agency to advise the private sector. In addition, the proposed Act directs the US Government Accountability Office to assess federal government action to support the cybersecurity of the commercial satellite industry.[53] Considering the interconnected nature of space sectors, which comprise a complex network of public and private actors, ensuring resilience across the board remains critical to countering cyber threats emanating from China.

Competitors and allies alike seem more willing to accept the potential dangers of cross-cutting technologies such as AI and automated systems – and could become heavily dependent on these capabilities.[54] Eventually, such cross-cutting technologies deployed across space, cyber, and the information environment may sway the defense strategies of other nations, erode trust in institutional infrastructures, strain international relations, and diminish significant competitors.[55] The EU AI Act, proposed in 2021, is set to be the world's first comprehensive legislation on AI, promoting innovation and the safe, reliable, and transparent use of AI.[56] Similarly, the NATO AI

51 Secure World Foundation. 'Global Counterspace Capabilities: An Open Source Assessment'. (2020). https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf.

52 European Commission. 9th EU-US Cyber Dialogue in Brussels – press statement. 7 December, 2023. https://digital-strategy.ec.europa.eu/en/library/9th-eu-us-cyber-dialogue-brussels-press-statement.

53 U.S. Congress. S.3511 – Satellite Cybersecurity Act. 30 March, 2022. Senate, Homeland Security and Governmental Affairs. https://www.congress.gov/bill/117th-congress/senate-bill/3511.

54 Michael J. Mazarr, Ashley L. Rhoades, Nathan Beauchamp-Mustafaga, Alexis A. Blanc, Derek Eaton, Katie Feistel, Edward Geist, Timothy R. Heath, Christian Johnson, Krista Langeland, Jasmin Léveillé, Dara Massicot, Samantha McBirney, Stephanie Pezard, Clint Reach, Padmaja Vedula & Emily Yoder. *Disrupting Deterrence: Examining the Effects of Technologies on Strategic Deterrence in the 21st Century* (Santa Monica, Calif: RAND Corporation, 2022). https://www.rand.org/pubs/research_reports/RRA595-1.html.

55 Paul et al. *A Guide to Extreme Competition with China*.

56 European Parliament. EU AI Act: first regulation on artificial intelligence. (2023). https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

Strategy[57] seeks to promote responsible behavior and protect members against the malicious use of AI. Regulation, cooperation and sharing good practice remain important to ensure that allies and partners are equipped to overcome the challenges posed by AI threats, including in the space domain. The UK, US, EU, Australia and China signed the Bletchley Declaration last year, agreeing that unrestricted AI usage poses a risk to humanity.[58] International collaboration, including with China, remains central to addressing AI as a global challenge.

The global race for quantum, while led by China, is seeing considerable growth from Europe. Since its launch in 2018, the Quantum Flagship – Europe's EUR 1 billion, decade-long research and innovation programme – has brought together government, industry and start-ups to explore promising quantum solutions.[59] Programmes such as the European Quantum Internet Alliance, which is designing a pan-European multi-node quantum communication system through quantum entanglement and teleportation, are operating at the cutting edge of technology.[60] It remains important for the US, Europe and their allies to continue to invest and cooperate towards securing a quantum future, particularly if China gains first-mover advantage in this area. Ensuring secure encryption in key segments of the communication chain remains essential to building resilience in C2, particularly in times of conflict. Even though quantum-secured information will remain vulnerable to the exploitation of other weak links, QKD could potentially protect sensitive communications against interception.[61]

In developing critical hardware, it is also essential for the US, Europe and their allies to ensure resilience and security across supply chains, particularly for components, parts and resources. There is a balance to be struck between enabling international scientific collaboration, and protecting IP and cross-cutting technology. Although European governments have been among the largest beneficiaries of Chinese foreign direct investment, they are gradually tightening investment screening measures, which is affecting Chinese investment accordingly.[62] Despite the financial ramifications of restricting such investment, evidence suggests that these subsidies alter the global economy, limit European industries' market access

57 NATO. Summary of NATO's revised Artificial Intelligence (AI) strategy. (2024). https://www.nato.int/cps/en/natohq/official_texts_227237.htm.

58 Kiran Stacey and Dan Milmo. 'UK, US, EU and China sign declaration of AI's "catastrophic" danger', *The Guardian*, 1 November, 2023, https://www.theguardian.com/technology/2023/nov/01/uk-us-eu-and-china-sign-declaration-of-ais-catastrophic-danger.

59 J. Dargan. 'New Report Shows Quantum Technologies Thriving In Europe', *The Quantum Insider*, 10 February, 2023, https://thequantuminsider.com/2023/02/10/new-report-shows-quantum-technologies-thriving-in-europe/.

60 Ibid.

61 Michael J. D. Vermeer & Evan D. Peet. *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption* (Santa Monica, Calif: RAND Corporation, 2020). https://www.rand.org/pubs/research_reports/RR3102.html.

62 A. Kratz, Zenglein, M., Sebastian, G. and Witzke, M. 'Chinese FDI in Europe: 2022 Update', Rhodium Group, 9 May, 2023, https://rhg.com/research/chinese-fdi-in-europe-2022-update/.

for cross-cutting technology, and pose risks related to IP and technology transfer.[63]

Diplomatic discourse, international treaties and agreements remain key to maintaining the rule of law and de-escalating potential conflicts. Initiatives such as the UN Open-Ended Working Group (UN OEWG) on agreed norms of responsible space behavior, while lacking attribution and enforcement mechanisms, remain important in establishing international principles and defining the tolerance threshold of spacefaring nations. Fora such as the Combined Space Operations (CSpO) Initiative[64] or NATO can help generate a better understanding of China's activities in this domain. It remains important for allies and partners to collaborate and develop resilience and strategies to counter China's hybrid threats, while signaling their commitment to security in space.

63 J. McBride and A. Chatzky. 'Is "Made in China 2025" a Threat to Global Trade?', Council on Foreign Relations, 13 May, 2019, https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

64 This forum is composed of Australia, Canada, France, Germany, New Zealand, the United Kingdom and the United States.

Authors

Mélusine Lebret is a Research Assistant at RAND Europe in the Defence, Security & Justice (DSJ) research group and the coordinator of the RAND Europe Space Hub. Mélusine conducts qualitative and quantitative policy research on space governance, artificial intelligence security, and technologies deployments, mainly through future and foresight methods. Her space work is conducted across Europe and the US in English, French and Italian. She holds an M.Sc. in culture and conflict studies from the LSE and a B.A. in economics and Russian, from UCL.

Theodora Ogden is a Senior Analyst at RAND Europe in the Defence, Security & Justice (DSJ) research group and the deputy lead for the RAND Europe Space Hub, where she focuses on emerging technologies for defence and space as an operational domain. In 2022, she was the inaugural Interplanetary Initiative fellow at Arizona State University, and prior to RAND she worked at NATO HQ SACT. She holds an LLM and MSc in crisis management and is currently working towards her MBA.

James Black is Assistant Director of the Defence, Security & Justice (DSJ) research group at RAND Europe, where he leads the Defence Strategy, Policy, and Capability research portfolio. He also serves as the European lead for the RAND Space Enterprise Initiative, leads the RAND Europe Space Hub, and advises the Centre for Defence Economics and Acquisition. He holds a double MA-MSc in international security from Sciences Po and the LSE, and a BA Hons in history from the University of Cambridge.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats