Hybrid CoE Paper 21

China and space: How space technologies boost China's intelligence capabilities as part of hybrid threats

Hybrid CoE

Conlan Ellis, Theodora Ogden, James Black – October 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 978–952–7591–12–3 (web)
ISBN 978–952–7591–13–0 (print)
ISSN 2670–2053 (web)
ISSN 2814–7227 (print)

October 2024

Cover photo: testing / 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

Abbreviations

C2 – command and control
C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
EO – Earth observation
ISR – intelligence, surveillance, and reconnaissance
MCF – military-civil fusion
PNT – positioning, navigation, and timing
SATCOM – satellite communications
SDA – space domain awareness
SLV – spacecraft and space launch vehicle
SSA – space situational awareness
SST – space surveillance and tracking
TTPs – tactics, techniques, and procedures

Summary

This Hybrid CoE Paper explores China's rapidly proliferating space-based intelligence capabilities and their contribution to hybrid threats. It begins by examining the role of space in Chinese strategy and doctrine, highlighting the trends in Chinese space capability and operations, and aiming to provide readers with a foundational understanding of Chinese intelligence-gathering capabilities. This is further developed by explaining the military-civil fusion model, and analyzing China's space and intelligence activities within the context of hybrid threats. Lastly, the Paper presents the implications for EU and NATO member states, particularly in the areas of competition, resilience and deterrence.

Introduction

Over the last decade, the People's Republic of China has emerged as a strategic competitor to the United States, the European Union (EU), and the North Atlantic Treaty Organization (NATO), presenting a systemic challenge to the existing international order.[1] This rebalancing of power is also acutely felt in the space domain, where China has invested heavily in developing a national space programme that aims to surpass Russia's and rival that of the US.[2] The dual-use nature of most space capabilities and China's promotion of a 'military-civil fusion' (MCF) model – which promotes technology transfer between the military and civilian spheres[3] – have raised concerns about the potential for China's expanding space capabilities to contribute to hybrid threats.[4]

As outlined by Hybrid CoE,[5] hybrid threats are characterized by:[6]

- Coordinated and synchronized actions that deliberately target the systemic vulnerabilities of democratic states and institutions through a wide range of means.
- Activities that exploit the thresholds of detection and attribution, as well as the different interfaces (e.g., war-peace, internal-external security, local-state, and national-international).
- Activities aimed at influencing different forms of decision-making at the local (regional), state, or institutional level, and designed to further and/or fulfil the agent's strategic goals while undermining and/or hurting the target.

This encompasses a broad spectrum of activities across different domains, including space, which is closely interconnected with other domains, and relied upon by Western

1 NATO, 'Strategic Concept 2022' (2022), https://www.nato.int/strategic-concept/.
2 Defense Intelligence Agency (DIA), '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; US DoD, 'Military and Security Developments involving the People's Republic of China', Annual Report to Congress (2023), https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.
3 Mark Hilborne, 'China's Space Programme: A Rising Star, A Rising Challenge, China in the World', King's College London (2020), https://www.kcl.ac.uk/lci/assets/kssppolicyno.2-final.pdf.
4 Scott Harold, Yoshiaki Nakagawa, Junichi Fukuda, John A. Davis, Keiko Kono, Dean Cheng, and Kazuto Suzuki, 'The U.S.-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains', Santa Monica, CA: RAND Corporation (2017), https://www.rand.org/pubs/conf_proceedings/CF379.html; Bonny Lin, Cristina L. Garafola, Bruce McClintock, Jonah Blank, Jeffrey W. Hornung, Karen Schwindt, Jennifer D. P. Moroney, Paul Orner, Dennis Borrman, Sarah W. Denton, and Jason Chambers, 'Competition in the Gray Zone: Countering China's Coercion Against U.S. Allies and Partners in the Indo-Pacific', Santa Monica, CA: RAND Corporation (2022), https://www.rand.org/pubs/research_reports/RRA594-1.html.
5 Georgios Giannopoulos, Hanna Smith, and Marianthi Theocharidou, 'The Landscape of Hybrid Threats: A Conceptual Model', Hybrid CoE (2021), https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/.
6 Hybrid CoE, 'Hybrid Threats as a concept' (n.d.), https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

nations for communications, navigation, and connectivity. A recurring theme across these diverse activities is the need for effective intelligence to enable situational awareness and guide decision-making, both by the aggressor and those states targeted in a hybrid threat scenario.[7] In turn, space capabilities have emerged as a key enabler of modern intelligence-gathering, reflecting the unique opportunities associated with the use of space as the 'ultimate high ground'.[8]

This Hybrid CoE Paper focuses on the role of space-based intelligence capabilities through China's rapid development of satellite technologies. This includes a mix of Chinese civilian and military agencies, as well as various forms of overt, covert or deniable cooperation between Chinese state entities and a growing array of commercial, private or proxy actors, all contributing to hybrid threats.[9] To explore the contribution of Chinese space-based intelligence capabilities to the hybrid threat landscape, a scan of a range of academic and government publications relating to developments in the Chinese space sector was conducted. The goal is to provide readers with a foundational understanding of the type of hybrid threats posed by the rapid advances in Chinese intelligence-gathering capabilities operating in and through the space domain.

First, the Paper examines the role of space in Chinese strategy and doctrine, followed by a discussion of the trends in Chinese space capabilities and operations. It then explores military-civil fusion and its influence on space, intelligence and hybrid threats. Finally, the Paper summarizes the implications for EU and NATO member states in terms of competition, resilience and deterrence.

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

8 Benjamin Lambeth, 'Multi-Domain Integration in Defence: Conceptual Approaches and Lessons from Russia, China, Iran and North Korea', Santa Monica, CA: RAND Corporation (2003), https://www.rand.org/pubs/research_reports/RRA528–1.html.

9 DIA, 'Challenges to Security in Space'.

The role of space in Chinese strategy and doctrine

In 2022, the State Council Information Office (SCIO) released a white paper publicly outlining its intentions for China's space programme.[10] It reaffirmed China's commitment to becoming a "Great Space Power".[11] The SCIO makes it clear that China's developing space capabilities work to defend national security, stating that China will only use outer space "for peaceful purposes, and opposes any attempt to turn outer space into a weapon or battlefield or launch an arms race in outer space".[12] A 2020 RAND report outlines China's four major grand strategic aims: upholding and preserving territorial boundaries; preventing the Indo-Pacific region from being controlled by external powers; establishing a global atmosphere that promotes economic growth; and participating in shaping the global international order.[13] China's growing space capabilities, including those for intelligence purposes, serve to strengthen its influence across these aims, while increasing its hybrid threat capabilities. Modernization efforts seek to turn the People's Liberation Army (PLA) into a modern force by 2035 and 'world class' by 2049. Investments in satellite-based intelligence-gathering capabilities, as well as other space infrastructure and communications, contribute to plans to digitize the PLA for 'informatized' and 'intelligentized' local wars and hybrid threat operations in the future.[14]

The development of space capabilities and intelligence-gathering functions, as well as strengths in related areas such as cyber or electronic warfare, is an essential component of 'systems warfare'.[15] This term reflects the PLA's conceptualization of interstate competition and conflict as a continuous effort to undermine, disrupt, confuse, paralyze, and ultimately outthink and outmanoeuvre the adversary's own decision-making processes and structures.[16] Such concepts concerning the role of space and intelligence in hybrid threats draw on a mix of systems thinking, cognitive science and the latest advances in areas such as artificial intelligence,[17] while also incorporating historically

10 State Council Information Office (SCIO), 'China's Space Program: A 2021 Perspective' (2022), http://english.scio.gov.cn/whitepapers/2022–01/28/content_78016877_7.htm.

11 Samantha Lu, Briana Boland and Lily McElwe, 'Introduction', in *CCP Inc. in Argentina: China's International Space Industry Engagement*, Center for Strategic and International Studies (CSIS) (2023), http://www.jstor.org/stable/resrep47100.4.

12 SCIO, 'China's Space Program'.

13 Andrew Scobell, Edmund J. Burke, Cortez A. Cooper III, Sale Lilly, Chad J. R. Ohlandt, Eric Warner, and J.D. Williams, 'China's Grand Strategy: Trends, Trajectories, and Long-Term Competition', Santa Monica, CA: RAND Corporation (2020), https://www.rand.org/pubs/research_reports/RR2798.html.

14 Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, 'People's Liberation Army Operational Concepts', Santa Monica, CA: RAND Corporation (2020), https://www.rand.org/pubs/research_reports/RRA394–1.html.

15 Jeffrey Engstrom, 'Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare', Santa Monica, CA: RAND Corporation (2018), https://www.rand.org/pubs/research_reports/RR1708.html; Black et al., 'Multi-Domain Integration in Defence'.

16 Burke et al., 'People's Liberation Army Operational Concepts'; US DoD, 'Military and Security Developments'.

17 Nathan Beauchamp-Mustafaga, 'Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States', Santa Monica, CA: RAND Corporation (2023), https://www.rand.org/pubs/research_reports/RRA853–1.html.

embedded strands of Chinese thought.[18] This ensures a distinctive Chinese approach to thinking about hybrid threats, and to understanding how activities in space contribute to China's pursuit of strategic advantage.[19] It also reflects a perception by China that space-based activities by the US and its allies pose a direct threat to Chinese security and influence.[20] At the same time, it is clear to China that Western societies' dependence on space infrastructure is a critical vulnerability that could be exploited.[21]

18 This includes ideas such as 'Three Warfares' , 'unrestricted warfare' and Maoist or even Confucian influences. Giannopoulos et al., 'The Landscape of Hybrid Threats'; Burke et al., 'People's Liberation Army Operational Concepts'; Black et al., 'Multi-Domain Integration in Defence'.

19 Timothy Heath, Derek Grossman, and Asha Clark, 'China's Quest for Global Primacy: An Analysis of Chinese International and Defense Strategies to Outcompete the United States', Santa Monica, CA: RAND Corporation (2021), https://www.rand.org/pubs/research_reports/RRA447–1.html; Michael J. Mazarr, Bryan Frederick, John J. Drennan, Emily Ellinger, Kelly Elizabeth Eusebi, Bryan Rooney, Andrew Stravers, and Emily Yoder, 'Understanding Influence in the Strategic Competition with China', Santa Monica, CA: RAND Corporation (2021), https://www.rand.org/pubs/research_reports/RRA290–1.html; Bonny Lin et al., 'Competition in the Gray Zone'; Jonah Blank, Samuel Charap, Benjamin N. Harris, Timothy R. Heath, Niklas Helwig, Jeffrey W. Hornung, Lyle J. Morris, Ashley L. Rhoades, Ariane M. Tabatabai, and Sean M. Zeigler, 'Understanding the Emerging Era of International Competition Through the Eyes of Others', Santa Monica, CA: RAND Corporation (2022), https://www.rand.org/pubs/research_reports/RR2726z1.html; Timothy Heath, Eric Robinson, Christian Curriden, Derek Grossman, Sale Lilly, Daniel Egel, and Gabrielle Tarini, 'Disrupting the Chinese Military in Competition and Low-Intensity Conflict: An Analysis of People's Liberation Army Missions, Tasks, and Potential Vulnerabilities', Santa Monica, CA: RAND Corporation (2023), https://www.rand.org/pubs/research_reports/RRA1794–2.html.

20 Alexis A. Blanc, Nathan Beauchamp-Mustafaga, Khrystyna Holynska, M. Scott Bond, and Stephen J. Flanagan, 'Chinese and Russian Perceptions of and Responses to U.S. Military Activities in the Space Domain', Santa Monica, CA: RAND Corporation (2022), https://www.rand.org/pubs/research_reports/RRA1835–1.html.

21 Krista Langeland & Derek Grossman, 'Tailoring Deterrence for China in Space', Santa Monica, CA: RAND Corporation (2021), https://www.rand.org/pubs/research_reports/RRA943–1.html; Julia Brackup, Sarah Harting, and Daniel Gonzales, *Digital Infrastructure and Digital Presence: A Framework for Assessing the Impact of Future Military Competition and Conflict*, Santa Monica, CA: RAND Corporation (2022), https://www.rand.org/pubs/research_reports/RRA877–1.html.

Trends in Chinese space capability and operations

Chinese priorities in space include the rapid development of space infrastructure, with high-profile advances such as successful manned space missions, China's lunar exploration programme, heavy investment in deep space monitoring, and the creation of China's first independent low-orbit space station, Tiangong. Another key avenue of development has been China's construction of satellite networks – including for a range of satellite communications (SATCOM), Earth observation (EO), intelligence, surveillance and reconnaissance (ISR), and positioning, navigation and timing (PNT) functions – and the subsidiary technological infrastructure, systems and workforce skills that support these investments.

The number and sophistication of Chinese spy satellites in orbit have been advancing rapidly, long since surpassing Russian capabilities.[22] This growing fleet means that China now operates almost as many EO/ISR satellites as the rest of the world combined (excluding the United States).[23] In 2022, China launched 64 missions (about a third of the global total), putting it in second place behind the United States, which completed 76 launches in the same period.[24] Alongside military applications, satellites are also used for civilian purposes such as weather, climate or land use monitoring, and to support the BeiDou Global Navigation Satellite System.[25] Yet it is clear that many are intended to gather intelligence for use as part of hybrid threat or overt operations against China's competitors, building on concepts of systems warfare and continuous competition.

On 4 October 2023, China successfully deployed a trio of classified Yaogan-39 remote sensing satellites. The Yaogan satellites, while described by the Chinese Communist Party (CCP) as classified projects to conduct electromagnetic probes,[26] are also able to fulfil military and intelligence-gathering objectives, creating a sovereign Chinese small-sat constellation with high revisit rates[27] for signal intelligence missions or imaging tasks.[28] The October launch was the third of its kind within a short space of time, with six other Yaogan satellites launched in August and September. This rapid succession of launches continues the upward trend shown in Figure 1.

China has also invested heavily in improving its space intelligence. This is reflected in the development of space surveillance and tracking (SST) capabilities, and the pursuit of wider space situational awareness (SSA). Unlike the US, which has established a global footprint

22 J. Pupier, 'A2/AD chinois et liberté d'action aérienne dans le Pacifique occidental: gagner le conflit aéronaval à distance?' [Chinese A2/AD and freedom of air action in the Western Pacific: winning the air and naval conflict from a distance?] (2023), La Fondation pour la Recherche Stratégique, https://www.frstrategie.org/sites/default/files/documents/publications/autres/2023/Vortex-5-Fr.pdf.

23 DIA, 'Challenges to Security in Space'.

24 J. Pupier, 'A2/AD chinois'.

25 An alternative to the US's Global Positioning System [GPS], the Russian GLONASS, or the EU's Galileo. SCIO, 'China's Space Program'.

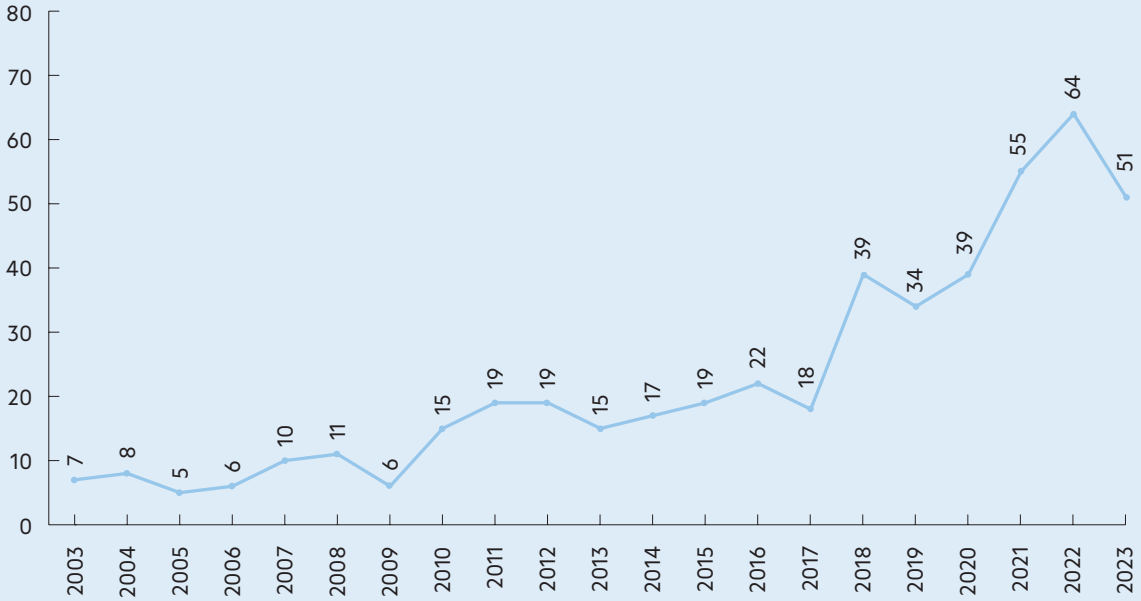
26 Probes designed to measure ambient electromagnetic fields.

27 The revisit rate refers to the interval in which data is captured. Satellites with high revisit rates capture multiple images with short time intervals.

28 Andrew Jones, 'China launches yet more classified Yaogan reconnaissance satellites to orbit' (2022), Space.com, https://www.space.com/china-launches-yaogan-satellites-december-2022.

Figure 1. Chinese orbital launches 2003–2023

Source: Space Stats (2023). Note that the data ends in September 2023.



for its Space Surveillance Network (SSN) by working with partner nations to host different sensors, China's network of radars and optical telescopes is largely confined to its borders, augmented by a maritime fleet of tracking ships.[29] Besides monitoring space weather or debris, this investment in SSA assists the Chinese military and security agencies in concealing terrestrial activities, such as those relating to hybrid threats, and in targeting and conducting hostile activities against foreign-owned space assets in orbit.[30]

China has also developed a spectrum of different counterspace capabilities. These range from the covert or deniable to the overt; from the kinetic to the non-kinetic; and from the reversible to the permanent in effect. China is known to have successfully tested direct-ascent anti-satellite (ASAT) missiles,[31] and reportedly continues to develop and deploy a range of cyber, electronic warfare, and orbital means of conducting surveillance, espionage, or attack missions against foreign spacecraft and associated networks or infrastructure.[32] This includes rendezvous and close proximity missions near other nations' satellites – presenting not only an opportunity for intelligence-gathering and sabotage or theft of sensitive technology, but also a form of coercion and hybrid threat. To this end, China exploits the ambiguity and deniability surrounding the dual-use nature of most space capabilities to mask the true intent of its threatening orbital activities.[33]

The steady growth in Chinese satellite operations has been accompanied by the expansion of ground support infrastructure to support China's on-orbit fleet and related functions, including spacecraft and space launch vehicle

29 Secure World Foundation, 'Global Counterspace Capabilities Report' (2023), https://swfound.org/counterspace/.

30 DIA, 'Challenges to Security in Space'.

31 Brian Weeden, '2007 Chinese Anti-Satellite Test Fact Sheet', Secure World Foundation (2010), https://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf.

32 DIA, 'Challenges to Security in Space'; Secure World Foundation, 'Global Counterspace Capabilities Report'.

33 Langeland & Grossman, 'Tailoring Deterrence for China'.

(SLV) manufacturing, launch operations, command and control (C2), and data transfer links.[34] The Chinese Academy of Sciences (CAS) also manages the Aerospace Information Research Institute (AIR), a research centre that has developed several large-scale projects on behalf of the Chinese ground segment, such as a network of ground stations for remote sensing satellites.[35] Although still currently under development, a "mega engineering project" approved in the 13th Five-Year Plan, the Space-Ground Integrated Information Network, aims to comprehensively integrate space and ground information networks, significantly advancing China's ability to exploit space data and leverage intelligence capabilities.[36]

34 DIA, 'Challenges to Security in Space'.
35 AIRCAS homepage, 2023, http://english.aircas.cn/home/.
36 Kai Lin Tai, 'Evaluating China's "Space-Ground Integrated Information Network" Project', *The Diplomat* (2022), https://thediplomat.com/2022/05/evaluating-chinas-space-ground-integrated-information-network-project/.

The military-civil fusion

The Chinese government is actively promoting the commercialization of its space sector, which has helped to spur growth alongside state-owned enterprises and programmes. Private Chinese companies are now investing heavily in the launch market, including exploring the potential for reusable rockets.[37] Almost all commercial space companies in China have some degree of state involvement – a trend dubbed 'commercialization with Chinese characteristics'.[38] China's strategy for modernizing its space capabilities involves prioritizing military-civil fusion (MCF) – the development of civil programmes to benefit the military – and the advancement of dual-use technology that can support both military and economic expansion. The commercial space industry has largely focused on the development of prioritized technologies, including capabilities such as advanced telecommunications, satellite infrastructure, autonomous systems, and subsystem-level rocket launches.[39] The Chinese government describes the purpose of commercial satellites as "one star with many uses", highlighting the importance of balancing strategic and economic needs.[40]

This drive to integrate public and private space activities poses obvious hybrid threats, given the potential for a wide range of covert and deniable activities by commercial and proxy actors working on behalf of the Chinese state. At the same time, it is important not to overstate the degree of integration implied by MCF, which remains as much an ambition as a reality. Chinese official sources often bemoan the persistent bureaucratic, cultural, information-sharing and other barriers to achieving their vision of MCF, and the lack of proper coordination of many academic and commercial entities with state institutions and their priorities.[41]

37 European Space Agency (ESA), 'China's Space Sector: Commercialisation with Chinese Characteristics' (2021), https://space-economy.esa.int/article/102/chinas-space-sector-commercialisation-with-chinese-characteristics.

38 ESA, 'China's Space Sector'.

39 Institute for Security and Development Policy, 'Made in China 2025' (2018), https://www.isdp.eu/wp-content/uploads/2018/06/Made-in-China-Backgrounder.pdf.

40 National Development and Reform Commission, Medium- and long-term development plan for national civil space infrastructure (2015–2025), (2015), https://www.ndrc.gov.cn/xxgk/zcfb/ghwb/201510/W020190905497791202653.pdf; B. Curcio, 'Developments in China's Commercial Space Sector' (2021), The National Bureau of Asian Research, https://www.nbr.org/publication/developments-in-chinas-commercial-space-sector/.

41 Elsa B. Kania and Lorand Laskai, 'Myths and Realities of China's Military-Civil Fusion Strategy', Center for a New American Security (2021), https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy.

Space, intelligence, and hybrid threats

Heavy Chinese investment in Earth Observation (EO), and in space situational awareness (SSA) in particular, contributes to hybrid threats in a variety of ways. Remote sensing satellites enable the collection of a range of different forms of intelligence, including imagery, electronic and signals intelligence.[42] Increasingly, the convergence of different EO/ISR, SATCOM and PNT technologies, along with other terrestrial telecommunications (e.g., mobile telephony and 5G), is also driving the generation of vast amounts of geospatial and open-source intelligence. This trend extends to the rollout of the internet of things, smart cities, smart grids, and smart logistics, all of which depend on access to space infrastructure and networks for critical functions.[43] By connecting distant humans or computing hardware, space technologies also enable other intelligence functions beyond the space domain, such as human or cyber intelligence.

China's satellite development efforts have had a significant impact on its Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) capabilities. Both for hybrid threat operations (such as harassing foreign ships around contested waters or islands in the South and East China Seas, or provocative military exercises or overflights) and for planning future combat operations, PLA doctrine relies heavily on incorporating information technology and networked operations with space-based networks serving as the backbone.[44] Although China has established increasingly sophisticated C4ISR networks such as Qu Dian and the Joint Information Distribution System, it has not yet fully realized its ambitions to utilize remote sensing, navigation, and communications satellites to support joint operations.[45] The Chinese Space-Ground Integrated Information Network (SGIIN) has the capability to improve the sharing of battlefield data and to shorten the military decision cycle by overcoming data stovepipes between various space systems through its comprehensive space-based network. Additionally, ground information ports can enhance joint operations and SSA by consolidating data from land, sea, air, and space domains.[46] Attempts to assert information dominance in space enable a "system-of-systems" approach to PLA operations, with command and control decisions optimized through real-time information gathering and sharing.[47] China's spy satellites enable constant monitoring of the entire Western Pacific region – including Taiwan – as well as potentially further afield, supporting efforts to project Chinese hybrid threats globally.

The intelligence and communications capabilities garnered through China's satellite development can also be seen as an avenue for Chinese grand strategy to control key

42 Giannopoulos et al., 'The Landscape of Hybrid Threats'.
43 James Black, 'Our Reliance on Space Tech Means We Should Prepare for the Worst', *Defense News* (2018), https://www.defensenews.com/space/2018/03/12/our-reliance-on-space-tech-means-we-should-prepare-for-the-worst/.
44 Larry Wortzel, 'The Chinese People's Liberation Army and Information Warfare', Strategic Studies Institute, US Army War College (2014), http://www.jstor.org/stable/resrep11757.
45 Tai, 'Evaluating China's "Space-Ground Integrated Information Network" Project'.
46 Ibid.
47 Langeland & Grossman, 'Tailoring Deterrence for China'.

information pipelines.[48] By controlling the pathways of information sharing, China can control which information passes through, and could create an information blackout by shutting down these pipelines. China has been active not only in promoting its satellite providers, but also in seeking to shape global standards and governance of space and the wider digital society in its favour.[49] This includes efforts to bolster its influence within the International Telecommunication Union (ITU), the United Nations agency responsible for allocating valuable orbital slots and spectrum.[50] It is also reflected in efforts to frustrate the UN Open-Ended Working Group on norms for responsible space behaviour, as well as attempts to shape regulatory frameworks or to promote the role of Chinese companies, such as Huawei, in building global digital infrastructure.[51] Efforts to shape legal, regulatory, normative, and technical standards around the information pipelines that underpin modern global society pose a direct hybrid threat to democratic nations resisting the creeping influence of more authoritarian values.[52]

The proliferation of Chinese satellite technology creates levers of influence over other nations in the ongoing strategic competition, while also putting China at an advantage should that competition ever escalate to outright armed conflict. For example, China has sought to integrate satellite networks into its Belt and Road Initiative (BRI) through its Digital Silk Road (DSR) initiative.[53] The DSR provides BRI partners with substantial investment in information and communication technologies, albeit with the risk that nations will be required to store data on servers based in China and be subject to checks by Chinese authorities.[54] The BRI Space Information Corridor exports Chinese satellite services to provide telecommunications and data-related business operations[55] to

48 Joshua Kurlantzick, 'How China Is Attempting to Control the "Information Pipes"', *The Diplomat* (2023), https://thediplomat.com/2023/03/how-china-is-attempting-to-control-the-information-pipes/.

49 Brackup et al., '*Digital Infrastructure and Digital Presence*'; Julia Brackup, Sarah Harting, Daniel Gonzales, and Brandon Corbin, 'Alternative Futures for Digital Infrastructure: Insights and Considerations for the Department of Defense'. Santa Monica, CA: RAND Corporation (2023), https://www.rand.org/pubs/research_reports/RRA1859–1.html.

50 Mark Scott and Clothilde Goujard, 'Digital Great Game: The West's Standoff Against China and Russia', *Politico* (2022), https://www.politico.eu/article/itu-global-standard-china-russia-tech/; Matt Sheehan and Jacob Feldgoise, 'What Washington Gets Wrong About China and Technical Standards', Center for Strategic and International Studies (2023), https://carnegieendowment.org/2023/02/27/what-washington-gets-wrong-about-china-and-technical-standards-pub-89110.

51 Brackup et al., 'Alternative Futures for Digital Infrastructure'.

52 Giannopoulos et al., 'The Landscape of Hybrid Threats'.

53 European Space Policy Institute (ESPI), 'China's 2016 White Paper on Space: An Analysis' (2017), https://www.espi.or.at/briefs/chinas-2016-white-paper-on-space-an-analysis/; Christopher Paul, James Dobbins, Scott W. Harold, Howard J. Shatz, Rand Waltzman, Lauren Skrabala, eds. Brian Bendlin, Lauren Skrabala, 'A Guide to Extreme Competition with China', Santa Monica, CA: RAND Corporation (2021), https://www.rand.org/pubs/research_reports/RRA1378–1.html.

54 James McBride, Noah Berman and Andrew Chatzky, *China's Massive Belt and Road Initiative*, Council on Foreign Relations (2023), https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

55 This includes, but is not limited to, GPS, agriculture tracking, disaster relief, port operations, telemedicine, transportation, financial services, and urban planning. For further information, see SCIO, 'China's Space Program'.

BRI states across the world, including in Africa, Asia, the Caribbean, Europe, and Latin America. This has allowed China to export the internet to areas that currently suffer from limited connectivity, with one company, StarTimes, offering digital and satellite TV services in 30 different countries.[56] But it also gives Beijing a powerful bargaining chip to influence BRI states, whether overtly or covertly. In this sense, China's space capabilities all contribute to a wider effort to shape, subvert and leverage the information environment in its favour.

The value of Chinese satellite systems extends beyond information operations and propaganda to their potential role in any future military conflicts. Information control is essential for modern strategic operations, and while traditionally the domain of government, the influence of private sector actors is rising in this area. China is actively aiming to provide a global alternative to the US Starlink satellites,[57] centralized under Guo Wang, which has sought approval for nearly 13,000 satellites in a filing to the ITU.[58] If Guo Wang successfully enters the global market as a competitor to Starlink, it could grant the Chinese government significant influence in peacetime, using the technology as a backbone for communications, as well as leverage in times of crisis through the ability to threaten or disrupt communications channels. While China's successful implementation of this technology remains to be seen, the use of commercial satellite technologies in modern strategic operations has opened up new possibilities for Chinese hybrid influence and the future of information control.

56 Paul, et al., 'A Guide to Extreme Competition with China'.

57 Ukraine's use of US Starlink satellites in the Russia-Ukraine war has drawn global attention to the growing strategic influence of commercial satellite technologies, as well as the associated vulnerabilities. Starlink offered a potential solution to Russian attacks against Ukrainian communication infrastructure, but also exposed the risks of relying on commercial technology when a Ukrainian attack on the Russian fleet in Sevastopol failed due to Elon Musk's refusal to extend Starlink coverage to Crimea. See: Julian Borger, 'Elon Musk ordered Starlink to be turned off during Ukraine offensive, book says', *The Guardian* (2023), https://www.theguardian.com/technology/2023/sep/07/elon-musk-ordered-starlink-turned-off-ukraine-offensive-biography.

58 Juliana Suess, 'Guo Wang: China's Answer to Starlink?', RUSI (2023), https://rusi.org/explore-our-research/publications/commentary/guo-wang-chinas-answer-starlink.

Implications for EU and NATO states

Hybrid threats, like China's space capabilities, are evolving at a rapid pace, although not all have been fully actualized. China does not yet have the capability to compete with Starlink in commercial satellite provision or to control the information flow in BRI states, despite its ambitions to do so. However, these capabilities are emerging, and China continues to demonstrate a willingness to develop and deploy not only intelligence-gathering but also counterspace capabilities that pose a significant threat to US, European and allied assets in space, as well as critical governmental, military, and societal functions on Earth.

New measures are needed to limit the current and potential future hybrid threats posed by Chinese investments in space and intelligence capabilities. Such measures should be proactive, given the rapid pace at which the Chinese threat is developing; collaborative, given the need for a coordinated response across different nations and in partnership with the private sector; and holistic, given the need to degrade both China's ability and its will to conduct hostile acts against other nations using space and intelligence capabilities in support of hybrid threats. This Paper emphasizes the need to promote competition, resilience and deterrence, underpinned by careful escalation management and signalling to avoid accidental crisis or conflict, while more robustly countering the Chinese hybrid threat in space.[59]

NATO and EU states still have significant advantages in space services due to their thriving commercial space industries. This aptly positions them to compete with Beijing's offering by providing innovative services, including remote sensing, SATCOM, PNT, and reusable launch, to countries involved in China's BRI.[60] Presenting an alternative to relying on Chinese space systems for services could hinder China's efforts to exert control over information pipelines, limiting potential disinformation strategies or blackouts. Similarly, democratic nations should seek to resist Chinese efforts to establish technical standards that unduly favour Chinese firms, and encourage China to engage constructively with international institutions and normative and regulatory frameworks as a responsible partner. This entails striking a balance between incentivizing China to engage in good faith, and avoiding the possible temptation to overreact to Chinese-led initiatives,[61] while maintaining a robust stance against any attempt by the CCP to dominate emerging governance arrangements for the world's digital infrastructure and enabling technologies.[62]

59 Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe, 'Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War', Santa Monica, CA: RAND Corporation (2019), https://www.rand.org/pubs/research_reports/RR2942.html; Langeland & Grossman, 'Tailoring Deterrence for China'; Stephen J. Flanagan, Nicholas Martin, Alexis A. Blanc, and Nathan Beauchamp-Mustafaga, 'A Framework of Deterrence in Space Operations', Santa Monica, CA: RAND Corporation (2023), https://www.rand.org/pubs/research_reports/RRA820–1.html.

60 Michael S. Chase, 'The Space and Cyberspace Components of the Belt and Road Initiative', NBR Special Report no. 80 (2019), https://www.nbr.org/publication/the-space-and-cyberspace-components-of-the-belt-and-road-initiative/.

61 Sheehan & Feldgoise, 'What Washington Gets Wrong'.

62 Brackup et al., 'Alternative Futures for Digital Infrastructure'.

In terms of resilience, states and companies can reduce the impact of their exposure to hybrid threats arising from advances in Chinese space and intelligence capabilities. To some degree, the proliferation of space-based intelligence opens up new opportunities for identifying, tracking, and attributing hybrid threat activities that would otherwise have remained unseen or at least ambiguous.[63] Yet for this "panopticon effect" of pervasive satellite surveillance to have a beneficial impact, domestic and international audiences must have confidence in the intelligence data and analysis with which they are presented. There are likely lessons to be learned from the role that commercial satellite imagery from companies such as Maxar has played in helping triangulate declassified US and UK military intelligence to debunk Russian propaganda claims and expose planned "false flag" attacks in Ukraine.[64]

More generally, democratic nations should improve the resilience of their societies to deal with Chinese information operations. This involves a wide variety of responses, starting with increased vigilance on Earth in terms of thinking about how overflying Chinese satellites might gain useful intelligence on critical facilities or movements. It also includes improved cybersecurity for spacecraft, networks and ground installations; improved space domain awareness (SDA); technical countermeasures in satellite designs; and revised tactics, techniques and procedures (TTPs) for space operations aimed at frustrating Chinese efforts to gather intelligence on the sensitive capabilities and technologies of Western satellites, including through rendezvous and close-proximity missions in orbit.

In terms of deterrence, some of the resilience and competitive measures outlined above should already contribute to what is known as deterrence by denial, making it more challenging for China to achieve the objectives of its hybrid threat operations in and through space. These should be paired with ongoing investment in a posture capable of credible deterrence by punishment.[65] This means that China must perceive that NATO allies possess both the capability and the will to employ counter-space or other retaliatory measures against it if its hybrid threat activities in and through space go too far.[66] Indeed, Chinese strategists believe that space is likely to be one of the primary arenas for military deterrence in the coming decades, given the opportunities for escalation, de-escalation and signalling in a manner that is "strategic, convenient, and controllable", without widespread risk to life.[67] Democratic nations – and sub-groupings such as the Combined Space Operations (CSpO) Initiative or NATO – need to build a clearer understanding of China's strategic culture, decision-making,

63 Hybrid CoE, 'Multidomain situational awareness: Using technology to outthink hybrid opponents' (2021), https://www.hybridcoe.fi/news/multidomain-situational-awareness-using-technology-to-outthink-hybrid-opponents/.

64 Army Technology, 'The Role of OSINT in the War in Ukraine' (2022), https://www.army-technology.com/analyst-comment/osint-war-in-ukraine/.

65 Langeland & Grossman, 'Tailoring Deterrence for China'.

66 Jonas Vidhammer Berge and Liselotte Odgaard, 'NATO in the Global Commons: Defending Outer Space Against Threats from China', *International Journal*, 78(4) (2023), https://doi.org/10.1177/00207020231217119.

67 Flanagan et al., 'A Framework of Deterrence'.

assets, vulnerabilities, and threat perceptions,[68] as well as communication mechanisms for engaging with Beijing and de-escalating in a crisis.[69] These can then be used to carefully calibrate both inducements and deterrent effects to shape Chinese behaviours without triggering an unwanted escalatory response.[70]

In summary, China's space development has not only advanced its technological capabilities, but has also created new avenues for hybrid threats. The development of satellite networks and infrastructure has allowed China to exert more control over the pathways of information sharing, creating levers of influence over foreign audiences (e.g., opinion towards the EU or NATO) and critical digital infrastructure. The expansion of Chinese intelligence gathering in, through and about space similarly serves to guide command and control, planning and decision-making for hybrid threat operations, including coercive and provocative acts in outer space itself.[71] **While it is not possible to prevent or deter all hybrid threats emanating from China's space operations, prudent actions could enhance the competitiveness and resilience of democratic societies, while deterring the more escalatory hybrid threats that risk unwanted crisis and conflict.**[72]

68 Bonnie L. Triezenberg, 'Deterring Space War: An Exploratory Analysis Incorporating Prospect Theory into a Game Theoretic Model of Space Warfare', Santa Monica, CA: RAND Corporation (2017), https://www.rand.org/pubs/rgs_dissertations/RGSD400.html.

69 Audrey Decker, 'US Space Command Wants Red Phones with China, Russia', *Defense One* (2023), https://www.defenseone.com/policy/2023/04/worlds-military-space-forces-need-talk-more-us-officials-say/385486/.

70 Berge & Odgaard, 'NATO in the Global Commons'.

71 DIA, 'Challenges to Security in Space'.

72 Morris et al., 'Gaining Competitive Advantage in the Gray Zone'.

Authors

Conlan Ellis is a Research Assistant in the Defence and Security team at RAND Europe, where he focuses on command and control and Chinese grand strategy. He received his MA in international relations from the University of Edinburgh, and his MPhil in politics and international studies from the University of Cambridge.

Theodora Ogden is a Senior Analyst at RAND Europe, 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 an MSc in crisis management and is currently working towards her MBA.

James Black is Assistant Director of the Defence and Security research group at RAND Europe, where he leads the Defence Strategy, Policy, and Capability research portfolio. He also serves as European lead for the RAND Space Enterprise Initiative 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