Frontier Assessments Unit

Research Report

LJ EADS, RYAN CLARKE, ROBERT MCCREIGHT, HANS ULRICH KAESER

DECEMBER 2023

Unraveling China's 6G Ambitions and the Dual Role of U.S. Experts in Global Tech Supremacy

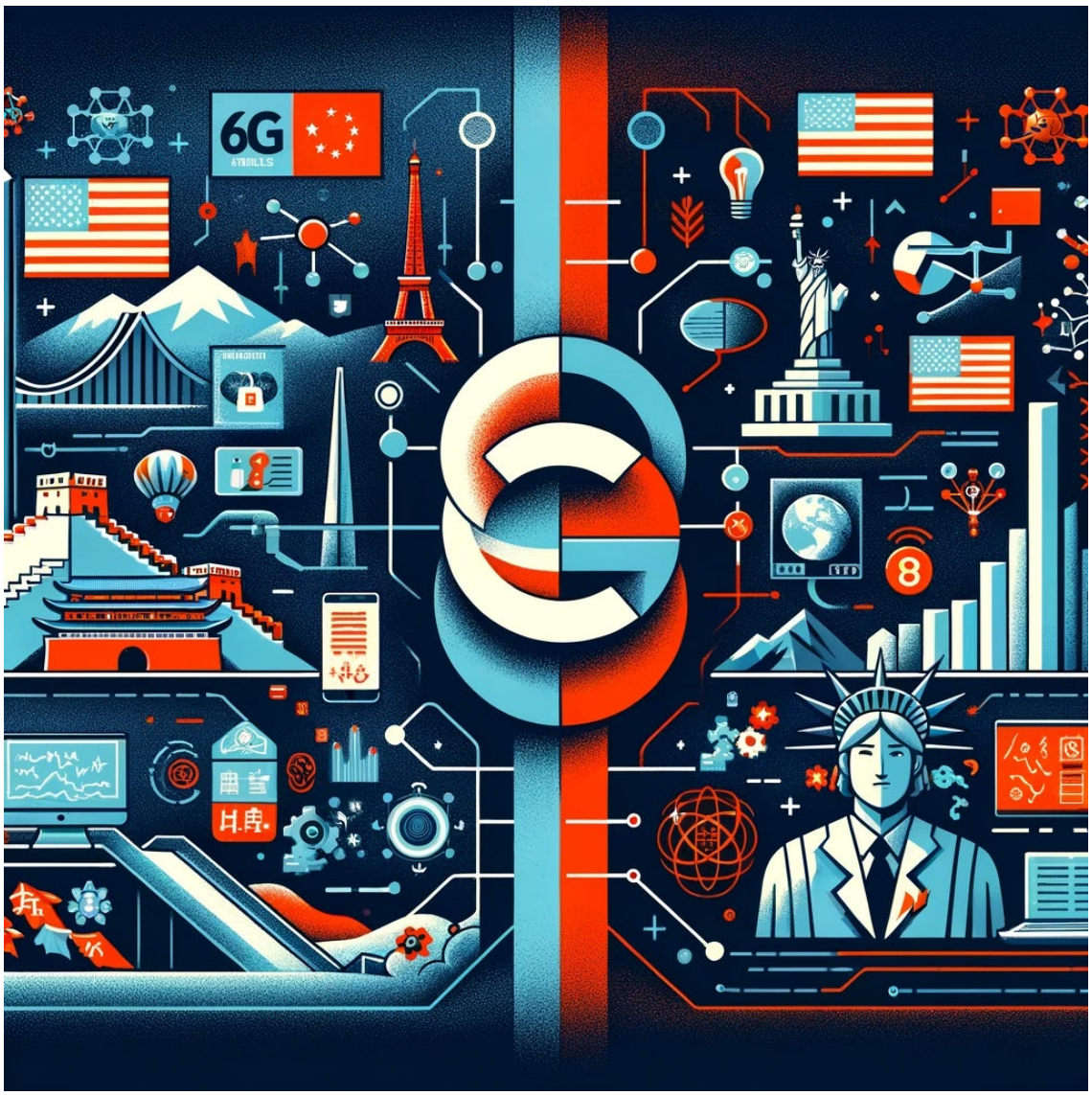

Table of Contents

Executive Summary

This report delves into the intricate dynamics of global technological competition, with a specific focus on the **CCP's ambitious strides in 6G technology** and the complex involvement of U.S. talent. It uncovers the critical role of institutions like the **Eastern Institute of Technology** and the **Eastern Institute of Advanced Study** in China's tech expansion, particularly highlighting the development of the **Ningbo Oriental University of Science and Technology**. This development is a testament to China's strategic planning and significant investment in research and innovation.

Central to the narrative is China's **Kunpeng Plan**, a strategic talent acquisition initiative reminiscent of the **Thousand Talents Program**. The plan's aggressive approach to attract global talents, including U.S. 6G researchers like **Bodong Shang**, indicates a direct challenge to the U.S.'s technological dominance. Shang's move from U.S. defense-funded research to a key role in Chinese technological initiatives raises alarm about the potential transfer of sensitive technologies and knowledge.

A significant part of the report focuses on **Lingjia Liu**, a close associate of **Bodong Shang**, and a prominent U.S. scientist with deep ties in future telecommunications research. His extensive background and role **leading the National Spectrum Consortium (NSC)** place him at the forefront of U.S. technological research on **5G and Beyond 5G** funded by the **Department of Defense (DoD)**. However, his collaborations with entities like **Purple Mountain Laboratories** and relations to **talent and technology transfer programs**, while also linked to the **Chinese military and Huawei**, cast a shadow over these associations, highlighting the dual-use potential of scientific research in areas critical to national defense.

The report emphasizes the broader implications for **U.S. national security**, noting the complex nature of international scientific collaborations and the potential risks they pose. It underscores the need for stringent vetting processes for international collaborations, particularly with entities tied to **foreign military or state-sponsored research institutions**.

Strategic policy recommendations include enhanced oversight of research projects, strict control of information sharing, and a comprehensive understanding of the end-use of collaborative research outputs. The **United States** is urged to maintain strategic vigilance, monitor collaborations, and ensure that partnerships with foreign entities do not compromise U.S. strategic advantages or national security.

In conclusion, the report asserts the critical need for the U.S. to navigate the fine line between fostering open scientific collaboration and protecting sensitive technologies from foreign exploitation. By implementing robust measures, the U.S. can safeguard its technological supremacy and national security in the face of complex global research environments and emerging technological rivalries.

The CCP's 6G Quest: A Global Technological Supremacy Race[1] [2]

China's aggressive push towards 6G technology signifies a crucial aspect of the global tech supremacy battle, especially with the United States. With its early initiatives in 6G research, forming the **IMT-2030 (6G) Promotion Group** in 2018, China is laying a robust foundation for dominating this advanced technology. The two-phase strategy, focusing first on foundational research until 2025 and then on standardization and commercialization from 2026 to 2030, highlights China's methodical approach towards integrating 6G in various sectors. This strategy not only underscores China's aspirations to lead in 6G but also poses a formidable challenge to U.S. technological dominance. If the U.S. doesn't match or exceed these efforts, it risks losing its position at the forefront of wireless communication innovation, which could have significant implications for its economic and strategic influence globally.

Most recently **Huawei's** exhibition at **MWC Shanghai trade show** focused heavily on 5.5G technology, a transitional step between 5G and 6G, also called **"Beyond 5G"** or **"5G Advanced,"** that the company is preparing to bring on the market in the second half of 2024. Huawei says 5.5G will offer a tenfold improvement in network performance over standard 5G, enabling faster Internet of Things devices, more efficient factories and transportation systems, and 3D content creation. China is a global standout in the reach of its 5G network. China had 634 million 5G users and over 2.73 million base stations at the end of April, each accounting for roughly 60% of the global total, according to the **Ministry of Industry and Information Technology**. The current focus on developing key technologies, such as high-performance terahertz core chips and devices, terahertz channel propagation characteristics and transmission, and high-performance terahertz communication test platforms, is aimed at transforming China's electronic information and communications industry. This development aligns with the strategies proposed at the **20th National Congress of the CCP** to expedite the creation of a network power and digital China, thereby advancing the country's technological and digital infrastructure.[3] [4]

Strategic Implications of China's 6G Development for the United States

The emergence of 6G technology, spearheaded by China, presents multifaceted strategic implications for the United States, spanning economic, security, and geopolitical dimensions.

---

[1] IMT-2030 (6G) Promotion Group Officially Released the White Paper on "6G Vision and Candidate Technologies", http://www.caict.ac.cn/english/news/202106/t20210608_378637.html

[2] TAKASHI KAWAKAMI and SHIHO MIYAJIMA, Nikkei, China seeks leg up in 6G standards race with faster wireless tech, Huawei touts '5.5G' at MWC Shanghai under shadow of decoupling risk, 2023-06-30, https://asia.nikkei.com/Business/Telecommunication/China-seeks-leg-up-in-6G-standards-race-with-faster-wireless-tech

[3] Yi Lianhong: Showing responsibilities as an "important window" in order to accelerate the construction of a cyber powerhouse, Digital China (易炼红：为加快建设网络强国数字中国展现"重要窗口"担当), Cyberspace Administration, 2023-08-06, http://www.cac.gov.cn/2023-04/03/c_1682162937256512.htm

[4] Chen Zhi, Han Chong, Special topic of this issue: 6G terahertz communication technology (本期专题：6G太赫兹通信技术), mobile communications, https://app.dataabyss.ai/web/2023%2F0527%2F22552220.html

1. **Economic and Technological Leadership:** China's advancements in 6G threaten to shift the epicenter of technological innovation and economic power towards Asia. This shift poses a direct challenge to the U.S., which has historically led in technology and communications. The U.S. risks losing its competitive edge in crucial sectors like telecommunications, artificial intelligence, and the Internet of Things (IoT) as 6G technologies drive the next digital revolution.
2. **National Security Implications:** The increasing reliance on telecommunication infrastructure for national security makes China's control over 6G a significant concern. The potential risks extend beyond conventional cybersecurity and data privacy issues to encompass broader aspects of espionage and digital sovereignty. In response, the U.S. needs to bolster its digital infrastructure security to mitigate these emerging threats.
3. **Global Standards and Regulation:** China's leadership in 6G also positions it to significantly influence the setting of international telecommunications standards. This influence has far-reaching implications, as it could skew the regulatory and standards landscape in favor of Chinese technologies and protocols, potentially disadvantaging Western companies, and interests.

The U.S. must strategically navigate this evolving 6G landscape by bolstering its technological innovation, reinforcing cybersecurity measures, and actively participating in global standards-setting forums. Failing to do so could result in diminished global influence and compromised national security in an increasingly interconnected digital world.

Global Tech Domination: The Eastern Institute's Role in the CCP's 6G Ambitions and the U.S. Technology Rivalry[5] [6]

The global technological landscape is in the midst of an intense competition between the United States and China. Central to this rivalry is the strategic acquisition of companies and intellectual property, with institutions like the **Eastern Institute of Technology (EIT)** and its affiliate, the **Eastern Institute of Advanced Study (EIAS)**, being at the forefront. The EIT and EIAS are pioneering the development of **The Ningbo Oriental University of Science and Technology**, marking a significant expansion in China's research-intensive university sector. Funded by the **Yu Renrong Education Foundation**, the university aims for completion by 2025 and seeks to establish itself as a center of elite standards and global outlook.

The university's strategic development, spanning 378 acres and costing around 30 billion yuan ($4.2B USD), is backed by national authorities and involves both provincial and municipal administrations. Led by **Chen Shiyi**, a globally recognized educator and former **Los Alamos National Laboratory** employee, the institution is poised to make significant contributions to China's ambitions in innovation, technological advancement, and economic influence. **Chen is**

[5] Eastern Institute of Advanced Study – Teachers List. https://www.eias.ac.cn/?teachers_category=teachers-list

[6] EIT School Planning and Preparation Progress (EIT办学规划及筹建进展), EIT办学规划及筹建进展.pptx, accessed 2023-10-30

the headmaster of EIT where talent recruitment plans are paying American scientists million-dollar salaries and providing other lucrative benefits for their knowledge of cutting-edge technology that China has been unable to generate independently. The program has hired some of the United States' most experienced scientists. EIT is backed financially and politically by the regional CCP in Ningbo, south of Shanghai.[7] The intensifying engagement of the CCP in U.S. academic circles, particularly through initiatives like **MIT's McGovern Institute for Brain Research**, underscores a disturbing pattern of talent recruitment strategies. **The Shong Fund**, established in 2015 to encourage scientific collaboration between MIT and Chinese institutions, may inadvertently act as a channel for transferring sensitive AI research, potentially useful for military purposes, to the PLA. Such collaborations, while aimed at fostering academic exchange, risk becoming a part of the CCP's broader strategy to co-opt intellectual expertise and research for its military objectives, especially considering the ties of some of these Chinese entities to the PLA.[8]

The Kunpeng Plan and Strategic Talent Acquisition

The **Kunpeng Plan**, part of the **EIT Global Recruitment Program**, represents China's aggressive approach to talent acquisition, similar to the **Thousand Talents Program**. The plan, along with Ningbo City's tailored policies, offers extensive incentives to attract global talents, a move that directly challenges the U.S.'s position in the technological race. The recruitment of figures like **Bodong Shang** from **Carnegie Mellon University** (See Figure 1 for Bodong

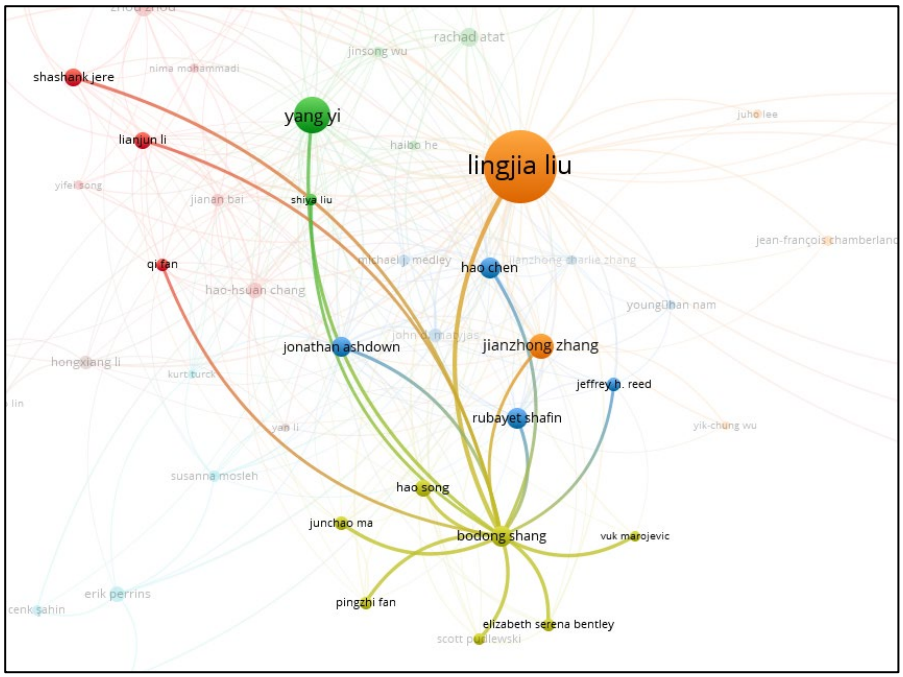

Figure 1: Bodong Shang holds 60 Research Connections, 185 Co-Authorship Links, 363 Total Co-Authorships, 11 Clusters Note: Lingjia Liu is his most frequent co-author.

[7] LJ EADS, RYAN CLARKE, HANS ULRICH KAESER, ROBERT MCCREIGHT, The Next Phase of U.S.-China Rivalry in the Era of Strategic Dual-Use Talent Acquisition and Technological Advancement: The Eastern Institute of Technology and Eastern Institute of Advanced Study, Frontier Assessments Unit, October 2023, https://www.frontierassessments.com/publications/project-one-ephnc-8rh5g-yx8x3-5zkfs

[8] LJ EADS, RYAN CLARKE, XIAOXU SEAN LIN, Illuminating Ties: The McGovern Institute's Engagement with the PLA in Brain-Inspired AI Research, The CCP BioThreats Initiative, August 2023

Shang's Co-Author Network), with his expertise in **Aerial Reconfigurable Intelligent Surfaces** and **6G networks**, exemplifies the strategic importance of such talent acquisitions. [9] [10] Shang's move to EIT, given his previous associations with U.S. defense and national research entities, raises significant concerns about international research collaborations and potential technology transfer. His expertise in areas funded by the **U.S. Air Force Research Laboratory (AFRL)** and the **National Science Foundation (NSF)** is of strategic importance, and his relocation represents a potential shift in the balance of technological capabilities between the U.S. and China. While Shang contributed to research funded by the AFRL and NSF, he collaborated with **Lingjia Liu** from **Virginia Tech**. Liu, serving as the principal investigator, worked alongside Shang on a project titled **"UAV Swarm-Enabled Aerial Reconfigurable Intelligent Surface: Modeling, Analysis, and Optimization"**. [11]

China's Calculated Move in Strategic 6G Talent Recruitment

Introduction to Lingjia Liu

Lingjia Liu (刘令嘉)[12] [13] is a prominent figure in electrical and computer engineering, with a comprehensive academic and professional background. He graduated **from Shanghai Jiao Tong University** with a Bachelor of Science in Electronic Engineering and earned a Ph.D. in Electrical and Computer Engineering from **Texas A&M University**. Liu's professional journey includes significant roles at the **University of Kansas** as an Associate Professor and at the **Mitsubishi Electric Research Laboratory** and **Samsung Research America**, where he contributed notably to 3GPP LTE/LTE-Advanced standards, particularly in multiuser MIMO and Coordinated Multi-Point (CoMP) transmission/reception.

At **Virginia Tech**, Liu serves as a Professor and Bradley Senior Faculty Fellow in the Bradley Department of Electrical and Computer Engineering and leads **Wireless@Virginia Tech**. His research spans emerging technologies for **6G cellular networks**, involving machine learning,

---

[9] 'Report Claims To Detail China's Decades-Long Recruitment Of Leading LANL Scientists', Los Alamos Reporter, 2022-09-22.
https://losalamosreporter.com/2022/09/22/report-claims-to-detail-chinas-decades-long-recruitment-of-leading-lanl-scientists/

[10] Bodong Shang, IEEE Author Profile, https://ieeexplore.ieee.org/author/37085769308

[11] B. Shang, E. S. Bentley and L. Liu, "UAV Swarm-Enabled Aerial Reconfigurable Intelligent Surface: Modeling, Analysis, and Optimization," in IEEE Transactions on Communications, vol. 71, no. 6, pp. 3621-3636, June 2023, doi: 10.1109/TCOMM.2022.3173369.

[12] *RMcCreight has identified this expert as just one among numerous potential targets for the CCP's strategic talent and technology acquisition. These experts often include Non-CCP Intellectuals and possibly covert CCP intellectuals functioning in dual loyalty roles. Occupying positions as academics, technology advisors, and scientists, they subtly operate within universities, government entities, and think tanks. They may discreetly serve as conduits for PLA intelligence and cooperatively facilitate clandestine technology transfer to the CCP. Or, for example, he could be an Unwitting Target of the CCP's talent and technology acquisition efforts, possibly unaware of the broader strategic implications of his collaborations. Alternately he might be seen as a Dual Loyalty Non-CCP target holding dual loyalty roles, driven by a genuine desire to contribute positively to China's development, without being an actual CCP member. Current evidence indicates the existence of many such individuals operating freely in academia, industry, think tanks and elsewhere, with further identifications, affiliations and disclosures anticipated.*

[13] Lingjia Liu, IEEE Author Profile, https://ieeexplore.ieee.org/author/37293117400

massive MIMO, and mmWave communications. He has been recognized for his contributions with several awards and honors, including the Miller Professional Development Award for Distinguished Research and the Research Excellence Award from Virginia Tech. He is a member of the **Executive Committee of the National Spectrum Consortium**, significantly contributing to 5G and Beyond 5G research in the U.S.

Liu's academic contributions are extensive, with over 200 publications, including book chapters, journal publications, and conference papers. He has made significant technical contributions to major 4G standards and holds numerous U.S. patents and essential intellectual property rights in these standards. His research has received substantial funding from various agencies, including **AFRL/AFOSR, DARPA, IARPA, NSF, and OUSD(R&E)**, totaling over **$132 million**, with Liu as the principal investigator on projects worth over **$27 million**.[14]

Lingjia Liu's current research projects have received significant grants, including a project on **Learning-Based ORAN Testing** funded by **NTIA's Wireless Innovation Fund** with a budget of over **$2 million**, and a project on **Mobile Distributed MIMO** funded by **OUSD(R&E)** with a budget of **$9.2 million**. He has been recognized as the **Bradley Senior Faculty Fellow by Virginia Tech**, an acknowledgment of his research excellence.[15]

Lingjia Liu's Involvement with the National Spectrum Consortium[16]

Lingjia Liu's position as an **executive committee member** with the **National Spectrum Consortium (NSC)** places him at a critical junction of U.S. technological research and development. The NSC, a collaborative body that brings together industry, academia, and government to advance spectrum management and technology, plays a vital role in shaping future U.S. communications and defense capabilities. NSC has funded 128 projects with a total of $1.6B in government funding. Liu's involvement in this consortium, given his expertise in telecommunications and electronic engineering, is significant. His research, particularly in the context of emerging technologies for 6G cellular networks and beyond, is of strategic importance to the U.S. in maintaining its edge in global communications technology.

The NSC has been instrumental in collaborating with the **U.S. Department of Defense (DoD)** and other federal entities on strategic spectrum management, notably through the **Partnering to Advance Trusted and Holistic Spectrum Solutions (PATHSS)** working group. Established in response to a **Congressional mandate in the Infrastructure Investment and Jobs Act**, PATHSS is tasked with exploring spectrum sharing possibilities in the 3.1 to 3.45 GHz frequency band. Since November 2021, the group has united a diverse group of stakeholders, including the DoD, NTIA, FCC, and representatives from telecom, academia, military equipment manufacturing, and the NGO sector. Operating through public and classified subgroups, PATHSS enhances information sharing and builds trust for future spectrum sharing initiatives.

[14] Lingjia Liu, Ph.D. Virginia Tech Webpage and News, https://computing.ece.vt.edu/~lingjialiu/doku.php?id=news
[15] Lingjia Liu, Ph.D. Virginia Tech Webpage and Biography, https://computing.ece.vt.edu/~lingjialiu/doku.php
[16] National Spectrum Consortium Executive Committee Page, https://www.nationalspectrumconsortium.org/working-groups/

PATHSS has conducted in-depth examinations of spectrum usage, addressing the needs of both federal security and commercial wireless services. With over 50 commercial members and contributions from academic and non-traditional entities, the group has made significant progress in optimizing spectrum usage. PATHSS is poised to deliver recommendations that will guide DoD and federal policy decisions on spectrum management, demonstrating NSC's critical role in harmonizing defense and commercial interests in this field.

Liu plays a significant role in the **NSC 5G Working Group**, serving as a task group co-chair. This group is central to the NSC's efforts in advancing 5G/NextG capabilities for federal mission-critical networks. The primary objectives of the 5G Working Group are to enhance agility, resiliency, and situational awareness in the deployment of these advanced communication networks.

The group's approach includes gathering stakeholders and ideas from various sectors to refine the development and assessment processes of **5G/NextG** technologies. A key focus of the group is to identify commercial use cases and capabilities, particularly those emerging in Release 17, which could be beneficial for the DoD and other federal entities. This involves evaluating the suitability of capabilities developed by the 3rd Generation Partnership Project (3GPP) to meet the specific needs of federal mission-critical networks.

Moreover, the 5G Working Group is responsible for pinpointing specific requirements that may necessitate further standardization efforts beyond Release 17. This proactive identification aids in shaping future standards and technologies related to 5G, ensuring that they align with the critical needs of federal networks.

Liu's involvement as a co-chair in the **Proximity Services/Sidelink (ProSe/Sidelink-TTNT) Task Group** under the **5G Working Group** indicates his active engagement in the technical aspects of 5G development. The group meets bi-weekly on Fridays at 11:30 am EST, under the leadership of **Chair Brian Daly from AT&T** and **Vice-Chair Sumit Roy the Beyond 5G program lead from OUSD R&E**.

The direct collaboration with a OUSD R&E innovation leader such as Sumit Roy raises concerns about potential technology and knowledge transfer risks, especially considering the substantial investments by the OUSD R&E in Beyond 5G technologies. The involvement of a key figure like Liu, who has ties to Chinese research institutions, underscores the need for stringent safeguards to prevent unintended dissemination of sensitive research and technologies that are critical to U.S. national security and technological leadership.

The DoD's Innovate Beyond 5G (IB5G) Program recently kicked off three new projects that continue to advance DoD collaborative partnerships with industry and academia for 5G-to-NextG wireless technologies. "The DoD has a vital interest in advancing 5G-to-NextG wireless technologies and concept demonstrations," said Dr. Sumit Roy, IB5G Program Director. "These efforts represent our continuing investments via public and private sector collaboration on

research & development for critical Beyond 5G technology enablers necessary to realize high performance, secure, and resilient network operations for the future warfighter."[17]

Lingjia Liu's Collaborations: Entanglement with Technology Transfer and Chinese Defense Programs[18]

Lingjia Liu's association with the NSC and his collaborative ties with **Bodong Shang**, who is actively recruiting global talent for Chinese technological initiatives, raises concerns about the inadvertent transfer of sensitive information and technology. The NSC's collaborative nature, while fostering innovation, also potentially opens channels for the flow of critical knowledge and technology to entities with direct ties to the Chinese military, such as Purple Mountain Laboratories. This inadvertent transfer of information can occur through shared research, publications, or even informal exchanges within the academic and scientific community. (See Figure 2 for Lingjia Liu's Co-Author Network).

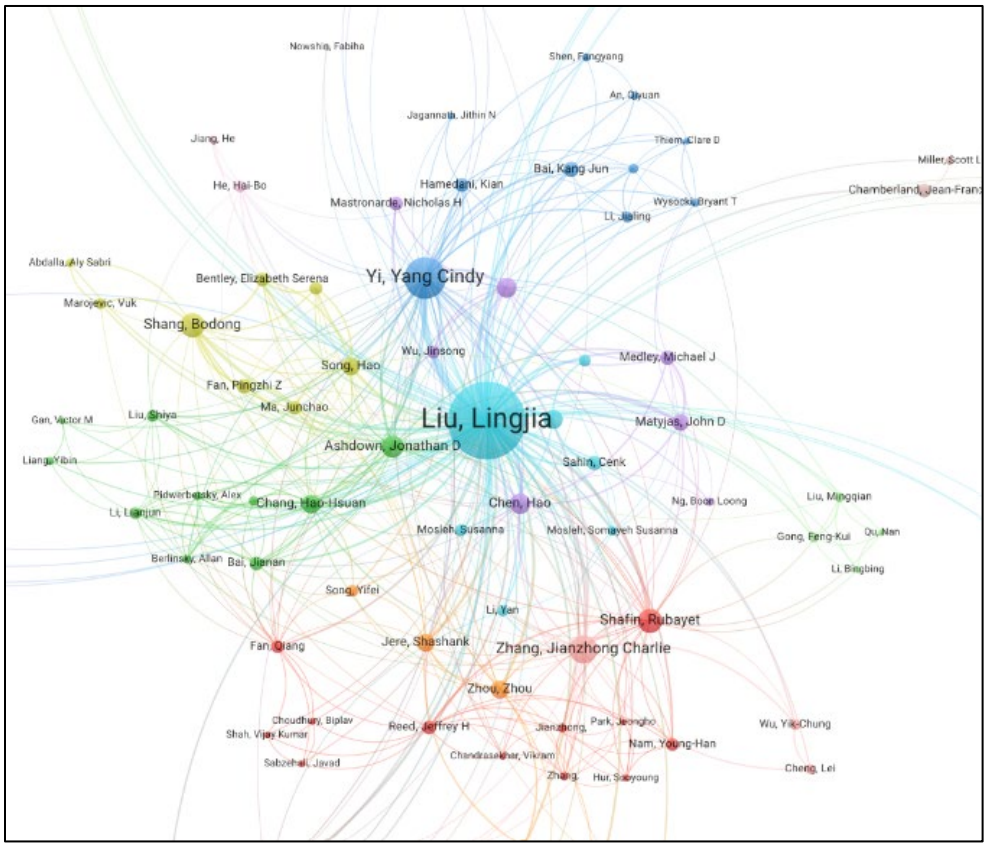

Figure 2: Lingjia Liu holds 100 Research Connections, 466 Co-Authorship Links, 1521 Total Co-Authorships, 19 Clusters.

Lingjia Liu's extensive expertise in **5G and NextG technologies** and his collaborative research on advanced surveillance technology underscore the sophisticated nature of his work in data processing and surveillance capabilities. However, his associations with individuals linked to the

[17] Department of Defense, Immediate Release, "Three New Projects for DOD's Innovate Beyond 5G Program", 2022-08-02, https://www.defense.gov/News/Releases/Release/Article/3114220/three-new-projects-for-dods-innovate-beyond-5g-program/

[18] Lingjia Liu, Data Abyss Author Profile, https://app.dataabyss.ai/openPerson/A5027237940

PLA and **Huawei**, coupled with the potential dual-use applications of this research, raise significant concerns. These connections bring into question the broader implications of such research, particularly in terms of its possible utilization in military contexts, underscoring the need for careful consideration of the end-use of technological advancements in sensitive fields.[19]

While collaborating with **Beijing Jiaotong University**, Liu published a report titled **"Understanding Images of Surveillance Devices in the Wild"** the research was conducted to enhance the image quality of CCTV systems suffering from low-light conditions, noise, and poor visual quality. Utilizing a web crawler to gather live webcam streams from public spaces, the authors develop ImCam, a framework combining a retinex model and generative adversarial network (GAN), to improve image quality. Their evaluation, involving 203,786 live streams and using classification systems like AlexNet and ResNet, demonstrates ImCam's effectiveness in enhancing CCTV image quality for practical security use.[20]
His co-author on this report from **Beijing Jiaotong University**, **Qiang Li**, has historically supported Chinese defense funded research such as with the study titled **"Towards Fine-grained Fingerprinting of Firmware in Online Embedded Devices"** funded by **China's National Defense Basic Scientific Research program**.[21] Qiang Li has produced extensive research as a Security Researcher for Beijing Jiaotong University. Li also published an interesting report on IP-based geolocation methods using a framework called GeoCAM that generates high-quality landmarks by automatically extracting the IP addresses and latitude/longitude of online webcams at large scale.[22] Beijing Jiaotong University is known for producing some of China's better hackers.

Liu while collaborating with **Bodong Shang** and other **Purple Mountain Laboratory** co-authors in 2021 published a report titled **"Cooperative Caching in HetNets with Mutual Information Accumulation"** which leveraged funding from the **111 project** (No.111-2-14). The 111 project is a project initiated in 2006 by the **Ministry of Education of the People's Republic of China (MOE)** and **State Administration of Foreign Experts Affairs (SAFEA)** to establish innovation centers for the purposes of technology transfer. **Plan 111** became an avenue for foreign technology transfer of both civilian and military application.[23] [24]

---

[19] X. You et al., "Toward 6G $\text{TK}\mu$ Extreme Connectivity: Architecture, Key Technologies and Experiments," in IEEE Wireless Communications, vol. 30, no. 3, pp. 86-95, June 2023, doi: 10.1109/MWC.004.2200482.
[20] Dai, Jiongyu and Li, Qiang and Wang, Haining and Liu, Lingjia, Understanding Images of Surveillance Devices in the Wild. Available at SSRN: https://ssrn.com/abstract=4431881 or http://dx.doi.org/10.2139/ssrn.4431881
[21] Q. Li, X. Feng, R. Wang, Z. Li and L. Sun, "Towards Fine-grained Fingerprinting of Firmware in Online Embedded Devices," IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, Honolulu, HI, USA, 2018, pp. 2537-2545, doi: 10.1109/INFOCOM.2018.8486326.
[22] Li, Qiang & Wang, Zhihao & Tan, Daiwei & Jinke, Song & Wang, Haining & Sun, Limin & Liu, Jiqiang. (2021). GeoCAM: An IP-based Geolocation Service through Fine-grained and Stable Webcam Landmarks. IEEE/ACM Transactions on Networking. PP. 10.1109/TNET.2021.3073926.
[23] J. Ma, B. Shang, L. Liu, C. Zhang and P. Fan, "Cooperative Caching in HetNets With Mutual Information Accumulation," in IEEE Networking Letters, vol. 3, no. 3, pp. 105-109, Sept. 2021, doi: 10.1109/LNET.2021.3072250.
[24] Wikipedia contributors, "Plan 111," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Plan_111&oldid=1167546147 (accessed November 30, 2023).

Liu actively collaborates with **Purple Mountain Laboratories** researchers such as **Junchao Ma**[25] who's current research interests are in **6G networks**. Junchao Ma and his colleagues such as Xiaohu You, Yongming Huang, and others at institutions like **Purple Mountain Laboratories**, **Southeast University in China**, and **Huawei** illustrate the cutting-edge exploration in the field of next-generation wireless networks. These researchers, with their diverse areas of expertise, are driving advancements in 6G technologies that include intelligent mobile communications, mmWave wireless communications, AI-aided optimization for wireless networks, and innovative solutions for THz communication. Ma's Huawei colleague is Jianjun Wu, the Chief Researcher and the Head of the **Future Network Architecture Laboratory** at **Huawei Technologies**. He is leading the 6G network architecture design in Huawei. He is also a co-founder of the **6GANA** (www.6g-ana.com), which aims to promote network Al as the key enabler of 6G networks to offer new services, such as Al4NET, NET4Al, AlaaS, etc.[26] [27]

Game Changer in Global Tech: The Dual Role of U.S. Scientists in China's 6G Ambitions

The involvement of U.S. scientists like **Lingjia Liu** with prominent Chinese 6G researchers is not just significant—it's a potential game-changer with startling implications. Liu, with his deep NSC connections, knowledge in machine learning, and advanced communication technologies, is inadvertently contributing to China's aggressive push in 6G development. This collaboration, while advancing technological frontiers, also poses a stark risk of strategic technology transfer, potentially undermining U.S. dominance in telecommunications. His engagement in research areas crucial to future telecom infrastructure, such as massive MIMO and IoT, could inadvertently fuel China's ascendancy in the global tech race, challenging the very technological leadership of the U.S. This complex intertwining of international research and national interests spotlights the precarious balance in global technological supremacy.

Purple Mountain Laboratories, situated in Nanjing, China, is an advanced research facility that plays a pivotal role in the development of next-generation technologies. Focusing primarily on future networks and endogenous security, the lab has garnered attention for its cutting-edge research in areas such as cybersecurity, communications technology, and artificial intelligence. Its strategic partnerships and collaborations extend globally, including with various U.S.-based institutions and researchers.

Purple Mountain Laboratories' collaborations with the **PLA** and **Huawei Technologies Co. Ltd.** are of particular interest. The PLA's involvement suggests a direct military interest in the research outcomes, particularly in areas such as cyber warfare and communication security. Huawei's participation, given its global presence and technological prowess, adds a layer of

[25] Junchao Ma, IEEE Author Profile, https://ieeexplore.ieee.org/author/37311283700
[26] J. Ma, B. Shang, L. Liu, C. Zhang and P. Fan, "Cooperative Caching in HetNets With Mutual Information Accumulation," in IEEE Networking Letters, vol. 3, no. 3, pp. 105-109, Sept. 2021, doi: 10.1109/LNET.2021.3072250.
[27] X. You et al., "Toward 6G $\text{TK}\mu$ Extreme Connectivity: Architecture, Key Technologies and Experiments," in IEEE Wireless Communications, vol. 30, no. 3, pp. 86-95, June 2023, doi: 10.1109/MWC.004.2200482.

complexity, considering the company's contentious position in global telecommunications and the ongoing scrutiny it faces from several Western countries, including the U.S.[28]

One of the more alarming aspects of **Purple Mountain Laboratories'** research portfolio includes its focus on offensive cyber capabilities. The lab has been involved in developing technologies for cyber warfare, including advanced methods for cyber-attacks like **Control-Flow Hijacking Attacks**. This type of research, especially when associated with military entities like the PLA, is a significant concern for U.S. national security, as it potentially enhances China's capabilities in cyber warfare and cyber espionage.[29] Purple Mountain Laboratories' collaboration with **PLA Unit 96941** and **No. 63 Research Institute of the National University of Defense Technology** on advanced cognitive radios signifies that Purple Mountain Laboratory is assisting the PLA directly on military grade spectrum capabilities. [30]

The research conducted by **PLA Unit 96941** has significant implications for defense applications, focusing on enhancing military capabilities and addressing security concerns. Their work on visualization and generative adversarial networks aids in improving battlefield situation awareness, thus facilitating better decision-making and strategic planning in military operations. The Units use of Convolutional Neural Networks (CNNs) contributes to the development of sophisticated feature extraction methods, crucial for target identification and object detection in defense systems. Additionally, their research in ground cloud classification and ecological interface design is particularly relevant for military operations in challenging weather conditions, affecting visibility and surveillance.[31]

Purple Mountain Laboratories' involvement with the PLA and its focus on areas such as cyber warfare, communication security, and artificial intelligence adds a layer of significant concern. Collaborative research or shared insights from the NSC, especially in the domain of spectrum management and NextG technology, could inadvertently end up benefiting these military-aligned research initiatives. The technological insights gained from such collaborations can enhance the PLA's capabilities in areas critical to modern warfare, including cyber operations, electronic warfare, and advanced communications.

---

[28] Y. Zhu et al., "SNWPM: A Siamese network based wireless positioning model resilient to partial base stations unavailable," in China Communications, vol. 20, no. 9, pp. 20-33, Sept. 2023, doi: 10.23919/JCC.fa.2023-0064.202309.

[29] MA Bolin, ZHANG Zheng, SHAO Yuwen, LI Bingzheng, PAN Chuanxing, JIANG Peng, WU Jiangxing. KMBox: Linux Kernel-based Heterogeneous Redundant Execution System Designed for Processes[J].Journal of Cyber Security,2023,8(1):14-25, https://app.dataabyss.ai/publication/fe85QosBAmNaFefFBl8Q

[30] Pan, Z., & You, X. (2021). Distributed dynamic spectrum access method for multiple heterogeneous users. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), Peking University Core. Affiliations include the State Key Laboratory of Mobile Communications, Southeast University, Unit 96941 of the Chinese People's Liberation Army, No. 63 Research Institute of the National University of Defense Technology, Purple Mountain Laboratory of Network Communications and Security.
https://app.dataabyss.ai/publication/rMisQYsBAmNaFefFprE9

[31] PLA Unit 96941 Data Abyss Page,
https://app.dataabyss.ai/affiliation/%E8%A7%A3%E6%94%BE%E5%86%9B96941%E9%83%A8%E9%98%9F

The Broader Implications for U.S. National Security

The situation involving Lingjia Liu, Bodong Shang, and their connections to entities like Purple Mountain Laboratories and Huawei, against the backdrop of U.S. and Chinese defense funding, underscores a critical challenge for U.S. national security. This complexity arises from the intertwining of open scientific exchange and the potential exploitation of sensitive technologies by foreign adversaries. The involvement of Chinese technology transfer programs, notably 111 project, adds another layer to this challenge, emphasizing the dual-use nature of scientific research. For the U.S., it is imperative to balance the encouragement of scientific innovation with safeguarding critical technologies and knowledge. This delicate equilibrium requires robust policies and vigilant oversight to prevent inadvertent technology transfers that could bolster the military or strategic capabilities of potential adversaries. The U.S. must remain vigilant in assessing collaborations and research initiatives, especially those in domains with profound defense and strategic consequences, to ensure that its technological and scientific advancements do not inadvertently empower rival nations in ways that could compromise national security interests.

Strategic Policy Recommendations

To effectively counter the risks identified in U.S.-China scientific collaborations, especially those with ties to military or state-backed entities, the United States needs a comprehensive strategic policy. This should include:

1. **Enhanced Vetting Processes**: Implementing stringent vetting procedures for international collaborations, particularly with connections to foreign defense or government-sponsored research institutions. This involves detailed scrutiny of the backgrounds and affiliations of individual researchers and organizations.
2. **Controlled Information Sharing**: Establishing strict guidelines on the type and extent of information shared in international collaborations to prevent unintended technology transfer.
3. **Research End-Use Monitoring**: Developing mechanisms to monitor and understand the end-use of collaborative research outputs, ensuring that they align with U.S. interests and do not inadvertently aid foreign military advancements.
4. **Community Awareness and Training**: Educating the U.S. scientific community about the risks associated with international collaborations, particularly with entities that may have dual-use research applications. This includes training researchers to recognize potential red flags in collaborations.
5. **Ethical Standards and Guidelines**: Creating clear and enforceable ethical standards and guidelines for international research partnerships to ensure they are in line with U.S. national security interests.
6. **Ongoing Monitoring of Collaborations**: Regularly monitoring and assessing the nature and implications of collaborations between U.S. researchers and institutions like Purple

Mountain Laboratories. This should involve a continuous review of joint projects and their alignment with U.S. strategic interests.

7. **Legislative and Regulatory Frameworks**: Strengthening legislative and regulatory frameworks to support these policies and actions. This could involve new laws or amendments to existing ones, ensuring they provide a solid legal basis for action against potentially harmful collaborations.
8. **International Diplomacy and Alliances**: Leveraging international diplomacy to build alliances and agreements that foster responsible scientific collaboration while protecting national security interests.

Through the implementation of these strategic measures, the United States will not only safeguard its technological edge but also fortify its national security. These actions are imperative in a world where technological prowess and information are pivotal battlegrounds. The U.S. must remain vigilant and proactive in its approach to international scientific collaborations, ensuring that its interests and global leadership in technology and innovation are robustly protected against emerging and sophisticated threats.

Surfacing Subterranean CCP Networks, Preventing Strategic Damage to National Security: The Role of the Frontier Assessments Unit

As this report draws to a close, it's imperative to acknowledge that while we have delved deep into the intricacies of China's technological ambitions and the complex roles played by various actors, many questions remain unanswered. The scope and scale of the challenges we face in understanding and countering the CCP's strategies are immense, underscoring the importance of continuous investigation and vigilance.

Our findings have highlighted the CCP's subtle infiltration into U.S. universities and organizations, particularly those identified as 'trusted research partners' by the Department of Defense. This infiltration raises profound concerns about the integrity and security of U.S. technological advancements and defense strategies. The CCP's talent recruitment efforts, exemplified by initiatives like the **111 Project and Kunpeng Plan**, are not just about harnessing intellectual capital; they symbolize a more profound campaign to influence and potentially control pivotal research and development sectors in the U.S.

The involvement of experts like **Bodong Shang, Chen Shiyi, Lingjia Liu**, and others, who occupy key positions in trusted U.S. institutions, further complicates the landscape. Their roles and affiliations necessitate a thorough reevaluation of how the U.S. engages with its intellectual assets and safeguards its scientific and technological repositories.

Looking ahead, our future reports will aim to unravel the deeper layers of the CCP's strategic campaigns. We plan to:

1. Investigate the full extent of the CCP's infiltration into U.S. universities and research institutions, with a focus on understanding how these entities might be unknowingly contributing to the CCP's broader strategic objectives.

2. Examine the origins, focus, and real-time impact of the CCP's talent recruitment efforts, seeking to uncover the underlying motives and long-term goals of these initiatives.
3. Continue to identify and scrutinize key experts and their roles within U.S. institutions, understanding their influence and potential connections to the CCP's strategic aims.
4. Provide a comprehensive analysis of the Kunpeng Plan, detailing its strategic focus and how it aims to influence and infiltrate U.S. defense institutions, universities, and trusted research partnerships.

In summary, the challenges we face in navigating the complexities of global technological supremacy, intellectual influence, and defense security are substantial. However, with diligent investigation, strategic foresight, and a commitment to uncovering the truth, we aim to contribute significantly to safeguarding our national interests and maintaining global technological leadership. The journey ahead is arduous, but our resolve to see these challenges through remains unwavering.