CHERN POLICY BRIEF
2022/01
December 2022

China's omnipresence:

Open RAN is no solution to the "5G China challenge"*

The question of whether to include Huawei technology in the rollout of Europe's 5G infrastructure has increased awareness of the vulnerabilities that stem from technological dependence on China. The high level of market concentration in the Radio Accession Network (RAN) market has led to Open RAN being presented as a solution, as it disaggregates the components of RAN. However, while Open RAN is a promising technological concept, it does not solve the "China challenge" as it neither reduces reliance on China nor necessarily offers a higher degree of network security.

Key recommendations

- **Consider whether and when to support Open RAN.** Before providing financial support for the development of Open RAN, governments should carefully consider the structures and activities of the Open RAN community that they are supporting. This is essential to avoid unintended geopolitical outcomes. Support for Open RAN might be useful, but would not mitigate geopolitical concerns.
- **Get fit to assess more complex RAN.** Open RAN is technologically more complex, which increases the demand for proper regulation, assessment, testing and certification. The European Union and its members states should provide additional resources to regulators to enable them to identify critical network components and their functionalities.
- **Invest in analyses of the RAN ecosystem.** Open RAN shifts the responsibility for supply chain security, and ensuring the quality, reliability and trustworthiness of suppliers and equipment, from vendors to several actors, including public agencies. This will require detailed knowledge and expertise on supply chains, vendors and potential chokepoints, and therefore demand additional public investment by the European Union (EU) and its member states.
- **Pool European resources for an EU regulator.** Smaller EU member states will find it increasingly difficult to oversee their wireless networks once Open RAN gains significant market share. However, the EU is highly interconnected and the challenges to network security and dependence in one member state will be problematic for the entire EU. We suggest pooling resources across the EU to fund a European regulator.

**This is the short version of a paper published by the Digital Power China (DPC) research consortium available here. We are grateful for the help we received from Isabeau Höhn in the writing of this paper.*

cost EUROPEAN COOPERATION IN SCIENCE & TECHNOLOGY
Funded by the European Union
CHERN China in Europe Research Network CA18215
https://china-in-europe.net/

In recent years, the latest generation of wireless infrastructure, widely known as 5G, has become a subject of geopolitical competition.[1] A group of states spearheaded by the United States (US) argues that Chinese technology suppliers, notably Huawei and ZTE, are not trustworthy. The concern is that the Chinese party-state ultimately controls technology firms headquartered in the People's Republic of China (PRC), allowing authoritarian leaders in Beijing to take advantage of network insecurities and technological overdependency for political ends. Several states have therefore either explicitly or de facto excluded Huawei and ZTE from the rollout of their 5G infrastructure.

The resulting challenge is the risk of a further consolidation of the highly concentrated Radio Access Network (RAN) equipment market. While there are already more RAN vendors, only four companies are "full-stack" vendors that offer tightly integrated solutions for radio, transport, core network and management software – Sweden's Ericsson, Finland's Nokia, and China's Huawei and ZTE.[2] Thus, in the west, the exclusion of Huawei and ZTE reduces the market options to two dominant players. Banning Chinese suppliers could create network security vulnerabilities linked to reduced vendor diversity.[3]

Some policymakers hope that a new technological concept, "Open RAN", could help to resolve this dilemma.[4] In contrast to currently deployed single-vendor solutions, Open RAN is intended to enable multi-vendor single RAN site implementation.[5] Open RAN hardware and software components of a Radio Access Network are disaggregated and can be provided by separate suppliers, enabling mobile operators to freely pick individual RAN components from a range of sources. In theory, this could increase network diversity because disaggregation multiplies vendor choice. Such hopes have led some governments, such as in the US and Japan, to approve major subsidies for the development of Open RAN.[6]

In reality, however, things are not that simple. There are major pitfalls to the Open RAN approach and neither network security vulnerabilities nor overdependence on Chinese suppliers would be automatically resolved by using Open RAN technology.

---

[1] Jan-Peter Kleinhans. Europe's 5G challenge and why there is no easy way out. TechNode. 25 June 2019. https://technode.com/2019/06/25/europes-5g-challenge-and-why-there-is-no-easy-way-out/; Tim Nicholas Rühlig, John Seaman and Daniel Voelsen. *5G and the US–China Tech Rivalry: A Test for Europe's Future in the Digital Age.* SWP Comment no. 29. Berlin: SWP, 2019.

[2] Daryl Schooler and Jaimie Lendermam. "Mobile operators have many 5G network vendor options". Omdia. 15 January 2021. https://omdia.tech.informa.com/-/media/tech/omdia/marketing/commissioned-research/pdfs/mobile-operators-have-many-5g-network-vendor-options.pdf.

[3] Council of the European Union. Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G. 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019XG1210(02); Deutscher Bundestag. Experten gegen Ausschluss von Anbietern beim Mobilfunkstandard 5G. 2019. https://www.bundestag.de/dokumente/textarchiv/2019/kw46-pa-auswaertiges-5g-665414.

[4] Mike Dano. "AT&T, Microsoft, others get behind Trump's anti-Huawei agenda". Light Reading. 2 April 2020. https://www.lightreading.com/security/atandt-microsoft-others-get-behind-trumps-anti-huawei-agenda-/d/d-id/757286.

[5] While mobile operators use different RAN vendors for different geographic sites, mixing RAN components from different vendors in a single site (base station) is typically not possible today.

[6] Broszio, S., "Europe urged to act now to build Open RAN Ecosystem". T. 18 Nov. 2021. https://www.telekom.com/en/media/media-information/archive/recommendations-for-open-ran-640862.

Are Chinese vendors a risk to European 5G networks?

The role of Chinese wireless technology vendor Huawei in 5G networks has triggered controversy in the west and some parts of Asia. Critics raise two primary concerns. First, as 5G and future generations of mobile infrastructure will be more software-defined, the need for constant maintenance work on such infrastructure will only increase. Thus, the west would not only be giving up the ability to construct its critical infrastructure, but also relying on a Chinese vendor to maintain it. Critics argue that the EU would be entrusting the maintenance of its critical infrastructure to a technology company from an authoritarian state that is not a security ally of Europe.[7]

Second, the highly complex nature of 5G networks increases the attack surface considerably. Critics fear that the use of Huawei equipment provides the company with privileged knowledge and access. Chinese party-state agencies would gain increased opportunities for espionage and the sabotage of wireless networks in Europe.[8] If 5G and 6G are the future backbone of a broad digitization of society and the economy, shutting down 5G networks would disable not just mobile telephony, but autonomous driving, the machine-to-machine communications essential to industrial production, and smart home and smart health applications.[9]

These concerns assume that Huawei (and ZTE) are not private sector companies like any other. Loopholes in Huawei's governance structure reinforce concerns that the company is ultimately controlled by the Chinese Communist Party.[10] Hence, network insecurities and technological dependencies could become political tools in the hands of the authoritarian leaders in Beijing.[11] Huawei refutes these accusations and argues that ownership of the company lies not with the Chinese state but almost exclusively with its employees.[12] Huawei's claims may be correct, but the problem is that ownership in Huawei's case does not come with control over the firm. The use of Huawei equipment in human rights infringements of Muslim minorities in China's Xinjiang province has fuelled these concerns.[13]

In essence, however, the issue of trustworthiness demonstrates that the problem is not Huawei, but China. To some observers, Open RAN is the solution to this problem: But does Open RAN reduce the risk of technological overdependence on China? In addition, will Open RAN improve network security?

---

[7] Mathieu Duchâtel and Francois Godement. *Europe and 5G: The Huawei Case.* Paris: Institut Montaigne, 2019.
[8] Dan Sabbagh and Jon Henley, "Huawei poses security threat to UK, says former MI6 chief". *The Guardian*. 16 May 2019. https://www.theguardian.com/technology/2019/may/16/huawei-poses-security-threat-to-uk-says-former-mi6-chief; Tom Uren, "The technical reasons why Huawei is too great a 5G risk". ASPI. 14 June 2018. https://www.aspi.org.au/opinion/technical-reasons-why-huawei-too-great-5g-risk; and Cassel Bryan-Low. "Special report – Hobbling Huawei: Inside the US war on China's tech giant". Reuters, 21 May 2019, https://www.reuters.com/article/us-huawei-usa-5g-specialreport/special-report-hobbling-huawei-inside-the-u-s-war-on-chinas-tech-giant-idUSKCN1SR1EU.
[9] James A. Lewis. *How 5G Will Shape Innovation and Security: A Primer.* Washington, DC: CSIS, 2018.
[10] Tim Rühlig. *Who Controls Huawei? Implications for Europe.* Stockholm: Swedish Institute of International Affairs, 2020.
[11] Jan-Peter Kleinhans. "Whom to trust in a 5G world? Policy recommendations for Europe's 5G challenge". Stiftung Neue Verantwortung. 5 December 2019. https://www.stiftung-nv.de/en/node/2717.
[12] Raymond Zhong. "Who owns Huawei? The company tried to explain: It got complicated". *New York Times*. 25 April 2019. https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html.
[13] Danielle Cave, Fergus Ryan and Vicky Xiuzhong Xu. *Mapping More of China's Tech Giants: AI and Surveillance.* Barton: ASPI, 28 November 2019. https://www.aspi.org.au/report/mapping-more-chinas-tech-giants.

Does Open RAN reduce technological dependency on China?

The idea that a disaggregation of RAN technology will minimize western dependence on Chinese technology is optimistic at best. Whether we consider single-vendor or Open RAN technology, China remains best positioned in the global market. The barriers to market entry for Radio Access Network technology, as well as its components, are high. Entry requires expertise and is capital intensive.

The global market share of Open RAN is still small.[14] It is estimated that 15 percent of global RAN could be Open RAN by 2026.[15] Others predict that Open RAN will only become a significant trend in the sixth generation of mobile infrastructure (6G). Either way, China's party-state will be able to sustain an uneven playing field by the very same means it has used to support Huawei.

According to the *Wall Street Journal*, Huawei has received at least US$75 billion in tax breaks, financing and soft loans in the past 25 years. The company has benefited from US$36 billion in cheap loans, credit lines and other support from state lenders alone, and avoided US$25 billion in taxes between 2008 and 2018.[16] Huawei has denied these numbers, but there can be little doubt that the company has profited from preferential treatment in a largely shielded domestic market,[17] public procurement policies, tax breaks, soft loans, subsidies and export credits.[18]

Huawei is by no means the most party-state controlled Chinese technology vendor. In China, it is not ownership but the degree of "state capture" that is pivotal. Through significant support from the party-state, state-owned and privately owned firms enjoy the same treatment regarding market access, state subsidies, procurement and the exercise of political guidance. Based on publicly available information, 95 of the top 100 private sector firms in China and eight of the top ten internet companies have a founder or de facto controller who is currently or was formerly a member of a central or local party or party-controlled state organ.[19] This is not to deny that firms in China have agency. However, strategically important companies are best thought of as an integral part of the PRC's political economy.

Although this high level of state control[20] may not apply to all firms across all sectors, the risk of party-state control in strategic sectors such as RAN technology is high. It would be irrational to believe that this holds only for single-vendor but not for Open RAN solutions. In fact, the strategic deliberations of state-run think tanks suggest that China sees Open RAN as an opportunity to circumvent US sanctions.

---

[14] StrandConsult. "Debunking 25 myths of Open RAN". 2021. https://strandconsult.dk/debunking-25-myths-of-openran/

[15] Peter Cohen. "Open RAN will have 15% RAN market share by 2026, report". RCR Wireless News. 24 January 2022. https://www.rcrwireless.com/20220124/open_ran/open-ran-revenues-forecast-to-15-of-ran-market-report

[16] Chuin-wei Yap. "State support helped fuel Huawei's global rise". *Wall Street Journal*, 25 December 2019. https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

[17] Gareth Owen. "Mixed fortunes for Ericsson and Nokia in China 5G RAN tender". Counterpoint. 23 July 2021. https://www.counterpointresearch.com/ericsson-nokia-china/.

[18] US Congressional Research Service. *China's Recent Trade Measures and Countermeasures: Issues for Congress*. Updated 10 December 2021. https://sgp.fas.org/crs/row/R46915.pdf.

[19] Curtis J. Milhaupt and Wentong Zheng, "Beyond ownership: State capitalism and the Chinese firm", *The Georgetown Law Journal* vol. 103, no. (2015).

[20] Tim Rühlig. *China's Foreign Policy Contradictions*. New York: Oxford University Press, 2022, chapters 2 & 5.

Such considerations mirror the reality in the most influential Open RAN community that exists: the O-RAN Alliance. The O-RAN Alliance was established by five mobile operators, including China Mobile, in 2018. Today, it has three main work streams: a "specification effort" that develops technical specifications based on existing technical standards on open interfaces; a "software community" that is developing open-source software for the RAN in close cooperation with the Linux Foundation; and a "testing and integration effort", which ensures the interoperability of Open RAN technology developed by the Alliance.[21]

The O-RAN Alliance united two earlier organizations: the US-based xRAN Foundation and China's C-RAN. It has also established a formal liaison with the Telecom Infra Project (TIP), which involves hundreds of participants from around the world, including from China.[22] China Unicom is particularly prominent in the TIP, and leads the Indoor 5G NR Small Cell Subgroup.[23] However, while only 20 percent of O-RAN Alliance members are Chinese entities,[24] the O-RAN Alliance is anything but free from Chinese influence.

Not only are 36 company participants in the O-RAN Alliance headquartered in China, but some of its most active members are subject to US sanctions. A recently published analysis finds that at least two-thirds of the Chinese O-RAN Alliance members have elements of state-ownership, and six are outright public institutions or agencies. At least 16 O-RAN Alliance members have public links to the Chinese security apparatus.[25] Strikingly, all three of China's main mobile operators, China Mobile, China Telecom and China Unicom, participate in the O-RAN Alliance. All are state-owned and supervised by the Ministry of Industry and Information Technology (MIIT). All have participated in the provision of telecom infrastructure linking islands in the South China Sea that China claims in breach of international law. In the East China Sea, the three companies have reportedly provided an upgrade of signals intelligence and location services to the People's Liberation Army (PLA).[26]

The case of China Mobile is particularly problematic. China's largest mobile operator is a founding member of the O-RAN Alliance with permanent membership on its Board of Directors and Executive Committee. The company also co-chairs ten of the 14 O-RAN Alliance working groups,[27] and is a member of the Alliance's influential Technical Steering Committee.[28] In 2016, China Mobile signed an agreement on civil-military fusion with the PLA.[29] In 2021, it was forced to delist from the New York Stock Exchange following US sanctions as a company that is part of the Chinese Military-Industrial

[21] O-RAN Alliance. About us. [n.d.]. https://www.o-ran.org/abouthttps://www.o-ran.org/about.
[22] Telecom Infra Project. "Our community". [n.d.]. https://telecominfraproject.com/members/.
[23] RWR Advisory Group. *Chinese Companies Active in the Architecture of Open RAN*. Washington, DC. 1 April 2021. https://www.rwradvisory.com/wp-content/uploads/2021/04/RWR_ORAN_Report_4-2021.pdf.
[24] RWR Advisory Group. *Chinese Companies Active in the Architecture of Open RAN*. Washington, DC. 1 April 2021. https://www.rwradvisory.com/wp-content/uploads/2021/04/RWR_ORAN_Report_4-2021.pdf.
[25] Hosuk Lee-Makiyama. European Centre for International Political Economy. "China's participation in O-RAN". January 2022. https://ecipe.org/blog/chinas-participation-o-ran/.
[26] RWR Advisory Group. *Chinese Companies Active in the Architecture of Open RAN*. Washington, DC. 1 April 2021. https://www.rwradvisory.com/wp-content/uploads/2021/04/RWR_ORAN_Report_4-2021.pdf.
[27] Hosuk Lee-Makiyama. European Centre for International Political Economy. "China's participation in O-RAN". January 2022. https://ecipe.org/blog/chinas-participation-o-ran/.
[28] O-RAN Alliance. About us. [n.d.]. https://www.o-ran.org/abouthttps://www.o-ran.org/about.
[29] RWR Advisory Group. *Military Ties of Major Chinese State-owned Telcom Companies: China Mobile, China Unicom, China Telecom*. Washington, DC. 2 February 2021. https://www.rwradvisory.com/wp-content/uploads/2021/02/RWR_China_Telco_CCMCs.pdf.

complex.[30] Whatever one might think of Huawei there is less evidence of party-state influence over the widely criticized company compared to O-RAN Alliance members such as China Mobile.

In sum, the concept of Open RAN prevents neither a dominant Chinese market presence in strategic segments of Open RAN equipment nor an unlevel playing field. The only foreseeable shift that will result from Open RAN is the strengthening of cloud providers. These are not European but mostly US or Chinese firms.[31] If anything, this is not in Europe's interests.

Does Open RAN provide better network security?

Critics of Huawei are concerned that the Chinese equipment manufacturer or other Chinese actors could use advanced knowledge of deployed RAN technology for espionage or to sabotage the wireless network and the critical infrastructure it connects.[32] As argued elsewhere, however, the Chinese security services are advanced enough to conduct espionage or sabotage operations with or without the deployment of Huawei equipment.[33] This applies to Open RAN equipment too. Hence, the exclusion of Chinese vendors when deploying mobile networks provides only a limited increase in network security.

Encryption is a more effective tool than the exclusion of Chinese suppliers to combat espionage and increase the confidentiality of data. Furthermore, while Chinese cyberespionage is a crucial challenge, the overwhelming share of cyberespionage is carried out through phishing rather than mobile infrastructure.[34] The most effective means to reduce the risk of a kill switch is to increase the cost for a malign actor through vendor diversification. In a diverse network, an attacker needs to identify and exploit vulnerabilities in the equipment of not just one but several vendors.[35] At least in theory, the disaggregation of equipment in an Open RAN scenario increases network diversity and improves network security. Importantly, however, Open RAN does not just facilitate network diversification – it also comes with two risks.

---

[30] US Department of the Treasury. Issuance of Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China & related FAQs; Introduction of Non-SDN Chinese Military-Industrial Complex Companies List. 3 June 2021. https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210603.

[31] Jean-Christophe Plantin. "The political hijacking of open networking: The case of open radio access network". *European Journal of Communication*, vol. 36, no. 4 (2021), pp. 404–17.

[32] Jan-Peter Kleinhans. "Whom to trust in a 5G world? Policy recommendations for Europe's 5G challenge". *Stiftung Neue Verantwortung*. 5 December 2019. https://www.stiftung-nv.de/en/node/2717

[33] https://www.ui.se/globalassets/butiken/ui-paper/2020/ui-paper-no.-5-2020.pdf.

[34] Reporting of previous Chinese hacks are indicative: PwC, "Operation Cloud Hopper," PwC, accessed: 2020-03-28, at: https://www.pwc.co.uk/cyber-security/pdf/cloudhopper-report-final-v4.pdf; Brian Barrett, "How China's Elite Hackers Stole the World's Most Valuable Secrets," Wired, accessed: 2020-03-28, at: https://www.wired.com/story/doj-indictmentchinese-hackers-apt10/; FireEye. "Mandiant APT1. Exposing One of China's Cyber Espionage Unites". FireEye, accessed: 2020-03-28, at: https://www.fireeye.com/content/dam/fireeyewww/services/pdfs/mandiant-apt1-report.pdf; Thomas Brewster, "Chinese trio linked to dangerous APT3 hackers charged with stealing 407GB of data from Siemens". Forbes. 27 November 2017. https://www.forbes.com/sites/thomasbrewster/2017/1 1/27/chinese-hackers-accused-of-siemens-moodystrimble-hacks/.

[35] UK Department for Digital, Culture, Media and Sport. *UK Telecoms Supply Chain Review Report*. July 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.

First, Open RAN requires a community of operators, vendors and researchers to develop open interfaces and software. This is not necessarily problematic. Cooperative technical standard-setting has not substantially compromised IT, cybersecurity or network security. Rather, transparency and security standards have improved all these. Similarly, the development of open interfaces for Open RAN seems fairly harmless as it provides little information on the actual equipment but focuses on the interfaces that are necessary for interoperability.

It appears to be riskier when code is jointly developed, as is the case in the O-RAN Alliance's Software Community. Here, the complexity of RAN code provides multiple options for backdoors not only in a single piece of code, but also in the combination of it. It is unrealistic to expect to be able to constantly review the code provided by all the participants in an Open RAN software community. A proper security review of RAN code is impossible, even by experts in code analysis.[36] In the end, the trustworthiness of software suppliers is indispensable.[37] As a consequence, Open RAN software is only as secure as the participants in any given Open RAN software community are trustworthy. Strikingly, some of the members of the O-RAN Alliance are more obscure and probably less trustworthy than Huawei.[38]

The characteristics of the members of the O-RAN Alliance outlined above indicate that trustworthiness cannot be assumed in Open RAN communities. Legally, all Chinese actors are obliged to cooperate with the Chinese security services under Article 7 of the Intelligence Law.[39] Chinese intelligence has little interest in the cooperation of most companies. However, it seems likely that they would be tempted to gain information from suppliers of critical infrastructure to third countries.

Second, while providing more options for vendor diversification, the deployment of Open RAN presents additional network security challenges. These largely stem from the greater complexity of different Open RAN network functions linked to different suppliers interacting with each other.[40] Such increased complexity enlarges the attack surface of the RAN.[41] At the same time, however, at least in theory, the high level of virtualization has the potential to increase security. While the high level of virtualization and encapsulation of Open RAN solutions could potentially increase network security, however, Open RAN development does not exclusively focus on security considerations. Interoperability, openness and time-to-market are also crucial.[42]

---

[36] UK Department for Digital, Culture, Media and Sport. *UK Telecoms Supply Chain Review Report*. July 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.

[37] Jan-Peter Kleinhans. "5G vs. national security: A European perspective". Stiftung Neue Verantwortung. February 2019. https://www.stiftung-nv.de/sites/default/files/5g_vs._national_security.pdf.

[38] US Congressional Research Service. "China's Recent Trade Measures and Countermeasures: Issues for Congress". Updated 10 December 2021. https://sgp.fas.org/crs/row/R46915.pdf.

[39] Peking University Law Database, National Intelligence Law of the People's Republic of China (2018 Amendment) [Effective]. PKULaw. https://en.pkulaw.cn/display.aspx?cgid=313975&lib=law.

[40] Bundesamt für Sicherheit in der Informationstechnik."Open-RAN Risikoanalyse". 22 November 2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/5G/5GRAN-Risikoanalyse.html?nn=520690

[41] European Commission. "Cybersecurity of Open Radio Access Networks". 11 May 2022. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks.

[42] European Telecommunications Network Operators' Association. *State of Digital Communications, 2022*. February 2022. https://www.etno.eu/downloads/reports/state_of_digi_2022.pdf.

Conclusion

In summary, Open RAN does not necessarily increase network security. The collective development of code, as is the case in the O-RAN Alliance Software Community, requires a high degree of trust. Given that several Chinese members of the O-RAN Alliance are less trustworthy than Huawei, this initiative carries obvious risks to network security. The deployment of more diverse RAN technology to increase network security comes with new vulnerabilities linked to increased technological complexity.

Depending on how Open RAN is developed and deployed, geopolitical concerns can be mitigated to some extent. However, the EU and its member states should neither dismiss Open RAN nor place too high hopes on the concept.

This publication is based upon work from COST Action CA18215 - China In Europe Research Network, supported by COST (European Cooperation in Science and Technology).

COST (European Cooperation in Science and Technology) is a funding agency for research and innovation networks. Our Actions help connect research initiatives across Europe and enable scientists to grow their ideas by sharing them with their peers. This boosts their research, career and innovation.
https://www.cost.eu/

https://china-in-europe.net/

Get in touch with the authors:

Tim Rühlig, German Council on Foreign Relations
ruehlig@dgap.org

Jan-Peter Kleinhans, Stiftung Neue Verantwortung
jkleinhans@stiftung-nv.de

cost EUROPEAN COOPERATION IN SCIENCE & TECHNOLOGY

Funded by the European Union

CHERN China in Europe Research Network CA18215