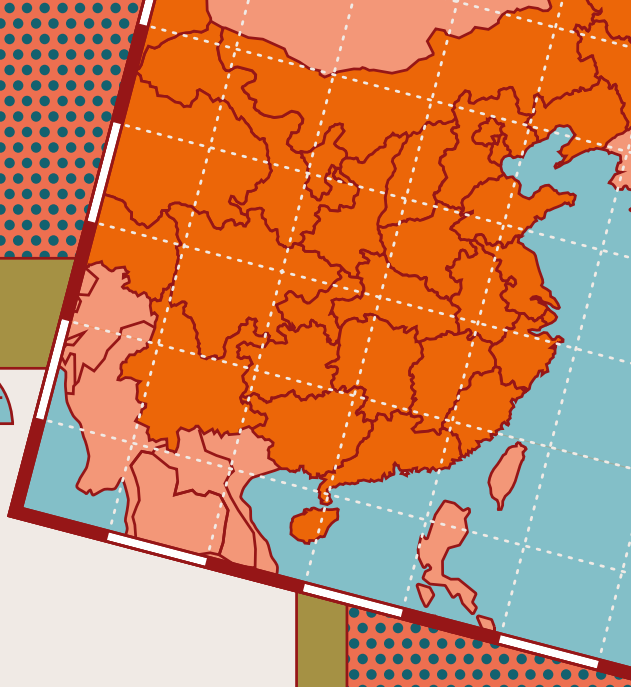
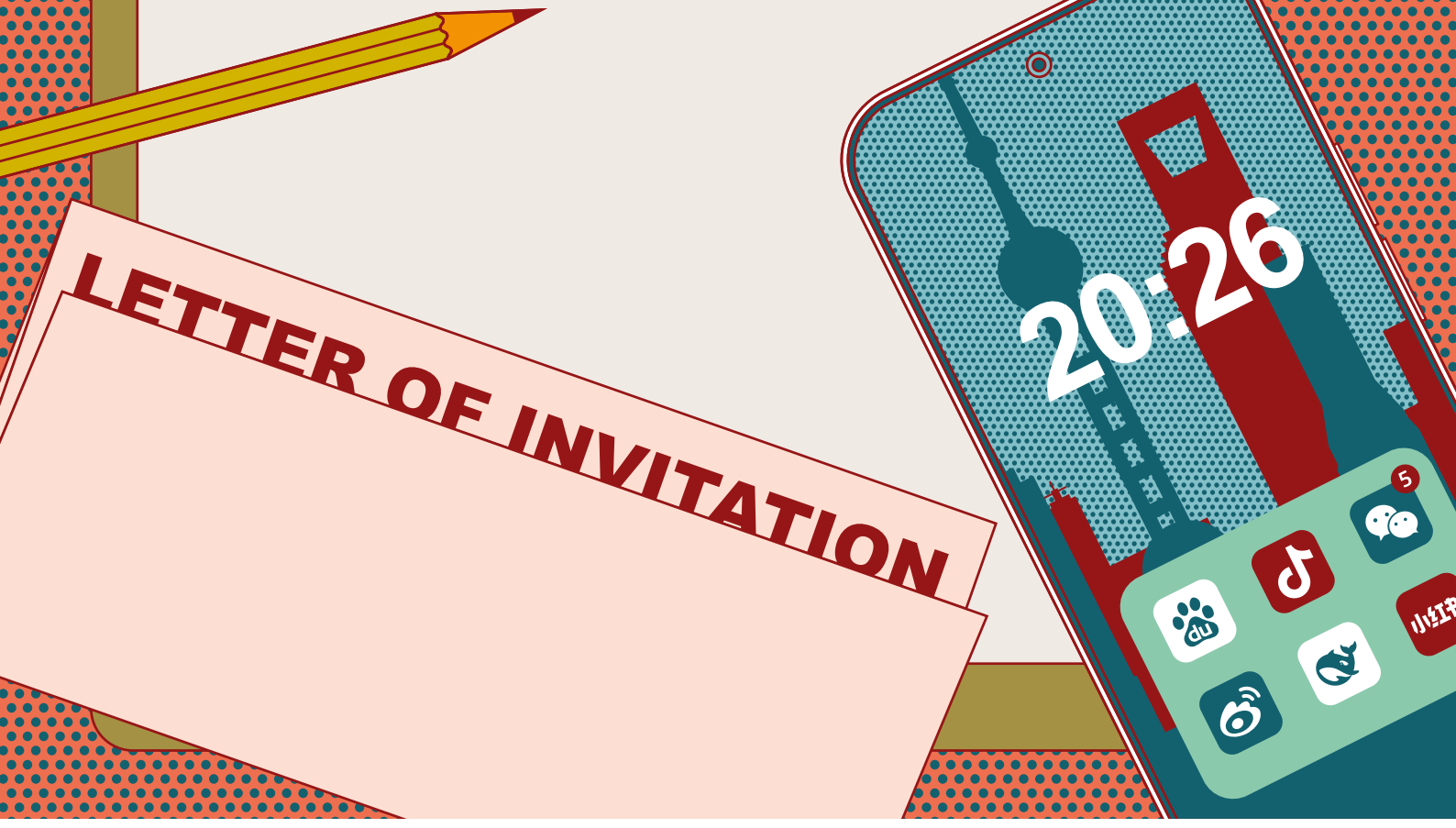
MERICS
REPORT



SECURE RESEARCH ON AND IN CHINA

Lessons from community experiences

Jessica Batke, Daria Impiombato, Katja Drinhausen



MERICS
Mercator Institute for China Studies

ABOUT THE AUTHORS

Jessica Batke is a Non-Resident Fellow at the Global Public Policy Institute (GPPi) and a Senior Fellow at ChinaFile, where she researches China's internet censorship system and its wider impacts on the world. She is also a Senior European Fellow at Cybersecurity for Democracy and a Senior Associate Fellow at MERICS.

Daria Impiombato is a Senior Analyst at MERICS, where she researches elite politics and party-state structures, domestic security, societal resilience and human rights in China, as well as the PRC's communication strategies and global information and influence operations.

Katja Drinhausen is Head of Program of "Politics & Society" at MERICS. Her research focuses on the development of China's legal and governance system, including digital governance and the social credit system, as well as human rights in China and state policies towards minorities.

ABOUT MERICS

The Mercator Institute for China Studies (MERICS) is a Berlin-based, independent think tank and leading European provider of policy-oriented research on contemporary China.

This project was supported in part by ChinaFile, an online magazine published by Asia Society, with funding from the Andrew Carnegie Foundation.

Contents

Acknowledgments 4

Key takeaways 5

Introduction: Shifting political environment requires proactive measures and new strategies 6

General guidelines: Research on China requires attentiveness and preparation 9

Working with counterparts based in China requires a case-by-case approach 15

Traveling to China for research poses new challenges 18

Conducting work solely outside of China doesn't mitigate all risk 21

Annex 24

Endnotes 28

Acknowledgments

The authors would like to thank the experts listed below and other anonymous contributors for providing individual consultations, participating in the workshop that informed the recommendations in this report, and/or for their thorough peer review and substantive feedback. Any inaccuracies are a responsibility of the authors alone.

Contributing experts:

Vincent Brussee, PhD Candidate at Leiden University
Lily Grumbach, Research Analyst at Datenna
David Levin, Associate Professor of Computer Science at the University of Maryland
Rosie Levine, Executive Director of the US-China Education Trust (USCET)
Ludovica Meacci, PhD Candidate at the Brussels School of Governance
Laura Murphy, Professor at Sheffield Hallam University
Theo Storella, China Economic Security Consultant at Bruegel
Miriam Tardell, Head of Economic Section at the Swedish National China Centre
Erik Mo Welin, Analyst at the Swedish National China Centre

KEY TAKEAWAYS

- **Research in and on China is increasingly risky.** This research is now more important than ever, but the current international geopolitical environment and national security considerations in China add a growing array of risks.

- **Risks arise across a wide array of research fields.** Those who conduct research on China in fields such as political science, international relations, history, economics, and culture encounter many barriers to carrying out meaningful exchanges or field work.

- **It can be difficult to see the risks.** China produces world-class talent and innovation, especially in science, technology, engineering, and mathematics (STEM) fields. Given heightened attention to scholarly exchange with China in these fields, individuals and institutions whose work is not China-focused, but who work in China, on China, or with Chinese counterparts, need to nurture China literacy and consider the potential consequences of their interactions.

- **Institutions should provide support and resources to their staff and to counterparts based in China.** Rather than leaving individuals with the burden of navigating research safety and ethics questions, institutional policies should remain flexible and responsive to individual cases, helping researchers manage situations in which there are no optimal solutions.

- **Individuals should take a pragmatic yet principled approach to research and exchanges.** They should ensure they have the backing of their institutions but also take individual steps to further enhance their safety and the quality of their work.

- **Conducting work solely outside of China doesn't mitigate all risk.** Evaluate changing Chinese regulations, degraded access to data, and cybersecurity practices as you conduct open-source research work.

INTRODUCTION: SHIFTING POLITICAL ENVIRONMENT REQUIRES PROACTIVE MEASURES AND NEW STRATEGIES

The need to study China and engage with its research and innovation system has never been greater. Given China's importance on the global stage, its political system, society and culture, economy, and foreign policy all demand greater attention from international observers. In a wide range of fields, including science, technology, engineering, and mathematics (STEM), the People's Republic of China (PRC) produces world-class talent and innovation.[1] Individuals and institutions interested in collaborating with such talent must nurture China literacy and build expertise.

At the same time, however, institutions are increasingly likely to experience political blowback stemming from China-related work. Such blowback can come from Beijing[2] or from an institution's domestic government.[3] Even as China research becomes more necessary, those who conduct it must overcome many barriers to carrying out meaningful exchanges or field work.[4]

China continues to expand its definition of national security threats

The PRC continues to expand its definition of national security threats, making topics such as political science, international relations, history, economics, and culture harder to study. A growing suite of Chinese laws (e.g. the National Security Law,[5] the Foreign NGO Law,[6] and the updated Counterespionage Law[7]) restrict cross-border exchanges as well as foreign access to certain archives and materials. Universities, think tanks, and media conducting research in China must obtain prior approval and are subject to a surveillance apparatus spanning the online and offline worlds. Detentions of foreign scholars,[8] non-profit employees,[9] and journalists[10] have further raised practitioners' security concerns.

Yet, Beijing's political pressure is not confined to China's borders. In response to research and reporting deemed hostile, Chinese authorities have enacted travel bans, used the threat of financial repercussions, and harassed people living abroad to deter work on such issues.[11] Chinese officials have also limited foreign access to even nominally public online information.[12]

Some research domains, such as STEM fields, may, at first blush, seem outside these political developments, but unseen faultlines remain. Individuals and institutions whose primary work is not China-focused, but who occasionally work in China, on China, or with Chinese counterparts, must consider how even simple interactions may have unintended consequences. While Beijing proactively promotes foreign research cooperation, especially when it aligns with its national interests,[13] recent cyber and data security regulations limit what information can be transferred abroad.[14] Beijing's mutable definition of "state secrets" also means that it's not just human rights researchers who should be wary.[15] Economists, computer scientists, geographers, or seismologists may become targets of suspicion as well.

Rather than allowing these risks to impinge on academic inquiry and freedom, institutions should take proactive steps to strive for balance between stated principles, financial or practical considerations, and specific safety concerns. Such preparation will allow them to better navigate security requirements at home, conflicting interests within their own organization, political pressure relayed through Chinese counterparts, as well as potential reputational risks.

Similarly, practitioners should prepare themselves in advance for potentially difficult decisions down the road. Even individuals working fully outside China's borders should be aware of Beijing's ever-shifting sensitivities and its long reach.[16] Funders working in this space should recognize that conducting secure research in this environment requires additional resources.

Yet, it's not just Beijing erecting barriers. Throughout Europe, the United States and other countries, governments and other institutions have implemented a range of security measures that impact research.[17] Such measures, including internal evaluation processes and restrictions on working with or transferring knowledge to high-risk counterparts, aim to safeguard national security and research security.

It's not just Beijing erecting barriers

According to practitioners, in some cases, the resulting requirements (such as requiring practitioners to abide by two sets of mutually contradictory national laws) are impossible to implement in practice. In other cases, individuals are left alone to figure out how to enact them without any institutional support.

Given such challenges, practitioners have adopted a range of approaches to China-related work. Some individuals strive to maintain their physical access to China, even if that means forgoing certain research topics. Indeed, on-the-ground experience in China remains critical to our collective efforts in research, reporting, diplomacy, and general cross-cultural understanding. For others, reporting and research restrictions, visa barriers, and sometimes even sanctions limit field research. Some individuals are unable or unwilling to return for safety concerns, meaning they conduct their work outside China, often using open-source intelligence (OSINT) methodologies. All approaches are valuable and necessary in the current environment.

For a number of practitioners, the shifting political environment both inside and outside China has induced uncertainty and even fear. Among their questions: *How can I conduct research or interviews responsibly? How can I collect and transfer data without creating risks for myself or my counterparts? What personal safety protocols should I implement when visiting the PRC? How should I research subjects Beijing considers "sensitive"?*

The recommendations below attempt to answer some of these questions. During a purpose-held workshop organized by ChinaFile and MERICS in June 2026, individuals from think tanks, industry, journalism, and the academy offered their perspectives and best practices developed over years of first-hand experience. Their recommendations are not a comprehensive list of dos and don'ts, nor a unified response to a specific set of national standards for research security. Instead, they represent a snapshot of a particular community's own hands-on practices and a starting point for further discussion. In general, the recommendations seek to strike a balance between open inquiry and personal safety, and between intellectual integrity and a duty of care.

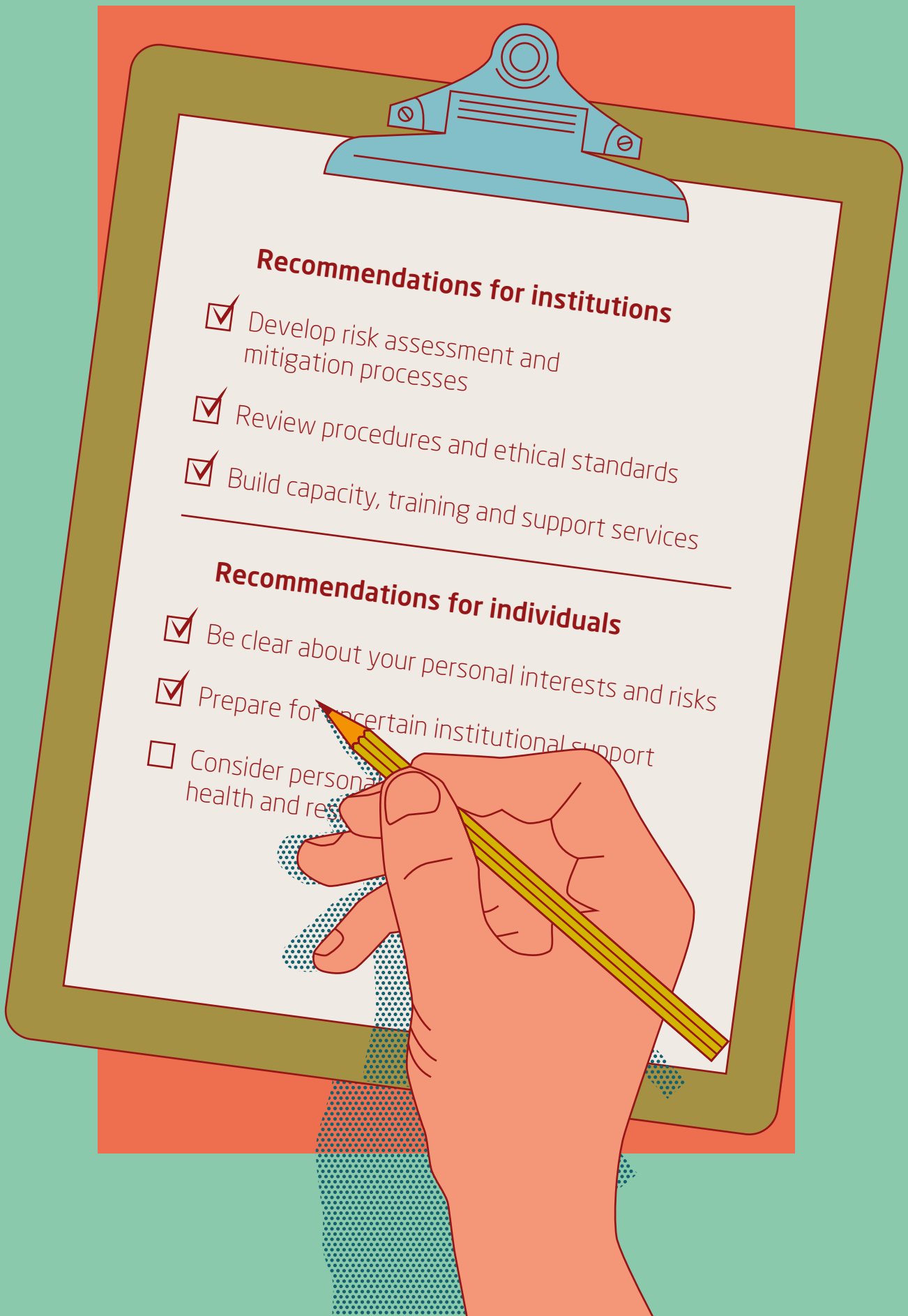
These recommendations are aimed at any institution or individual working in China, on China, or with Chinese counterparts—not just China specialists who may already be familiar with some of its recommendations. Though not every recommendation will apply to every situation (national regulations, institutional conventions, research practices, and individual circumstances vary greatly), the report offers readers tools to identify potential risks and see how others have chosen to manage them.

The four sections below cover both institutional and individual recommendations for:

- China-related work generally (Section 1, a baseline for all readers),
- working with counterparts based in China (Section 2),
- traveling to China for research purposes (Section 3),
- conducting China-focused research from abroad (Section 4).

Finally, an annex lists and links external resources relevant to these recommendations, including sources that provide more detailed guidance on specific issues.

General guidelines: Research on China requires attentiveness and preparation



General guidelines: Research on China requires attentiveness and preparation

Given the shifting circumstances both inside and outside of the PRC, institutions and their employees must proactively plan for China-related work. This includes, but is not limited to, the following cases:

- An institution that hosts research on China as a major focus area
- An institution that hosts research and/or events on topics that sometimes feature China-related work (for example, human rights or sustainable development)
- An academic institution whose scholars conduct individual research projects on China
- An academic institution with a large population of Chinese national students, and/or that hosts a Chinese Students Association[18]
- Individuals involved in the work listed above



RECOMMENDATIONS FOR INSTITUTIONS

When designing and implementing guidelines, institutions should remain flexible. What is necessary in one case may be counterproductive in another. The goal should be to help researchers navigate situations in which there may be no optimal solutions. To this end, blanket bans should be reserved for the most severe risks, such as cooperation on projects with military applications.

Beyond such cases, a graded approach may be more appropriate, e.g., allowing WeChat on specific devices for certain types of fieldwork but denying its use for other purposes. Institutions should recognize that employees may disregard data and cybersecurity rules if they become so stringent as to prevent basic information-sharing or on-the-ground access, especially when institutions do not themselves assist with compliance (such as providing separate travel devices).

Institutions should also consider the specific context for guideline exceptions. For example, informed consent documentation is critical when conducting medical research. However, in other cases, such documentation poses risks to Chinese nationals by creating a permanent record of research participation, which may outweigh default ethics assumptions.

Institutions need to be sensitive to the unique challenges that confront Chinese nationals working abroad. These researchers are frequently at high risk of transnational repression,[19] with family members still inside China facing pressure from local authorities. They are often dependent on their international employers for their visas, and they may fear that their institution won't come to their aid if Beijing interferes with their work. Any institutional guidelines should account for the full range of these unique circumstances.

The following are suggested steps institutions can take to support their researchers:

Develop risk assessment and mitigation processes

- Consult existing China-specific research security guidelines published by relevant governments or research institutions (see Annex for examples from various countries).
- When assessing the risks tied to a particular project, seek out advice from China specialists, both those on your staff (if available) as well as external experts.
- Establish a firewall between risk assessments and ethics determinations. Do not block ethically sound initiatives solely based on perceived risk or threat of retaliation from the PRC.
- Consider reputational risks in addition to legal or financial risks; blocking China-related work can be seen as self-censorship and may hurt funding opportunities and employee retention.
- Identify potential risks (e.g., online- or offline employee harassment, the forced closure of offices in China, the detention of employees) and create action plans outlining the steps to take should these risks materialize.
- Make sure your employees know whom in your institution to contact should they be individually targeted.
- To fend off potential accusations of bias or defamation from Beijing, always clearly document research processes and standards in writing and help employees obtain factchecking and subject-matter expert reviews for their written publications.

Review procedures and ethical standards

- Analyze where local laws conflict with China's and develop specific guidance. For example, certain provisions of China's Personal Information Protection Law contradict the EU's General Data Protection Regulation and leave researchers in a bind regarding data sharing and transport.
- Consider revising your ethics requirements for China work. Practitioners advise the following:
  - Not requiring real-name or written consent forms if this could put interviewees or sources at risk.
  - Not assuming that data provided by Chinese institutions was obtained with full participant consent.
  - Not requiring interview recordings and accepting meeting notes instead.
  - Developing source anonymization protocols.
  - Consulting outside experts and advisory institutions if you do not feel equipped to undertake a China-specific ethics review (see Annex for country-specific resources).
  - Publicly assuring employees working on China (and other authoritarian countries) that the institution will support and defend their work should they be subject to intimidation or retaliation (see principles and pledges institutions can adopt in the Annex).
- Develop AI usage standards that account for the data, privacy, and censorship concerns associated with Chinese models, while permitting specific uses of these models where warranted.

Build capacity, training and support services

- Provide preparatory training and ongoing support services to help mitigate both institutional risk and practitioner burnout, including through external providers. Such services may include:
  - Workshops on conducting fieldwork in restrictive political environments and with open-source intelligence techniques.
  - Training for employees who are not experienced China specialists (such as STEM researchers or early-career practitioners) to familiarize them with China-specific political contexts, ethical concerns, and safety risks.
  - Training in data security, especially related to data sharing and transfer, travel (data minimization, network exposure, account synchronization, device compromise), and research infrastructure.
  - Cybersecurity and doxxing prevention training.
  - Access to mental health support or therapy services for employees dealing with challenging research content or harassment.
- Consider the differing safety needs of individuals, which vary by research topic, working conditions, nationality and visa status (Chinese nationals with family in China face additional risks).
  - Create policies on allowing anonymous contributions and use of pseudonyms when needed.
  - Ensure that freelance or subcontracted workers have adequate institutional protection for especially risky work.
  - Provide support for visa and citizenship applications when possible.
  - For universities, be aware that the Chinese government may co-opt Chinese Student Associations. CSA members may then partake in activities such as participating in counterprotests or monitoring other students.

RECOMMENDATIONS FOR INDIVIDUALS

Be clear about your personal interests and risks

- Pursue topics and research that interest you; don't pre-emptively forgo certain "sensitive" subjects without actively considering the benefits and risks. Keep in mind that Beijing's shifting red lines can suddenly make a "safe" topic less so, and pursuing your genuine interests may be easier than trying to predict the political winds.
- When considering how authorities might respond to your work, consider factors other than content. This might include your nationality, personal relationships, or institutional affiliations, as well as what kind of media or policy impact your work might have.
- Remain vigilant against unintentional self-censorship (censoring yourself before you even know you've done it). Nearly everyone in the community has experienced situations in which the unvarnished truth was at odds with other goals, such as protecting sources' safety or maintaining a low profile. The goal is to make any such trade-offs intentionally, rather than letting the pressure to censor alter how you conceive your work at the onset. One strategy: keep the first draft of your work as frank and truthful as you can make it, knowing that you can later decide to use a pseudonym, pause publication, or re-frame the work.

- Don't hesitate to reach out to peers, mentors or senior experts to ask for advice regarding risk and mitigation, especially as it relates to potential career opportunities. This is a fast-changing field, and practitioners are generally happy to share information, even with people they don't know (see Annex for research associations and mentorship networks).
- To make informed choices about projects or job opportunities, take stock of your personal goals, circumstances, and values. Consider potential risks and whether you can realistically manage them:
  - Enumerate your top four or five personal values and determine whether the opportunity at hand fulfills enough of these to merit taking it. When possible, say "yes" when offered the opportunity to do meaningful, fulfilling work.
  - Weigh the value proposition of the expected output (e.g. highly visible or impactful publication) against the likely risks. Higher-impact outputs may warrant taking on more risk, and vice versa.
- Consider the pros (e.g., increased personal security) and cons (e.g., hindering career advancement) of working anonymously or with a pseudonym.
- Consider how you would respond were you to lose the ability to travel to China.

Prepare for uncertain institutional support

- Assess the baseline support your institution offers, so that you have a clear sense of what kind of assistance you can reasonably expect.
  - Determine whether your work directly aligns with the organization's mission and broader goals, or if it is more tangential. In the latter case, be aware that your organization may be more likely to withdraw its support when under pressure.
  - Determine whether your institution has procedures in place to support you in certain worst-case scenarios; if not, consider helping to establish some.
- Be proactively transparent with your institution about your work and work processes. If you are in an institution that conducts ethics reviews and/or risk assessments before you begin a project, take time to engage with the people in charge of these tasks.
- Document everything, from communication with your institution to your research processes and evidence. Consult with others in your field about best practices before you begin a new project, then clearly define your research processes and standards in writing. If possible, include funding for fact-checking and legal review in your grant applications.
- Know the legal risks that apply in the jurisdiction where your publication is based. For example, risks and conditions for defamation suits may vary substantially between countries or regions. Individuals should also check contracts (especially US contracts) for indemnification clauses, which may leave researchers personally liable for any legal action taken as the result of their work.

Consider personal security, mental health and resilience

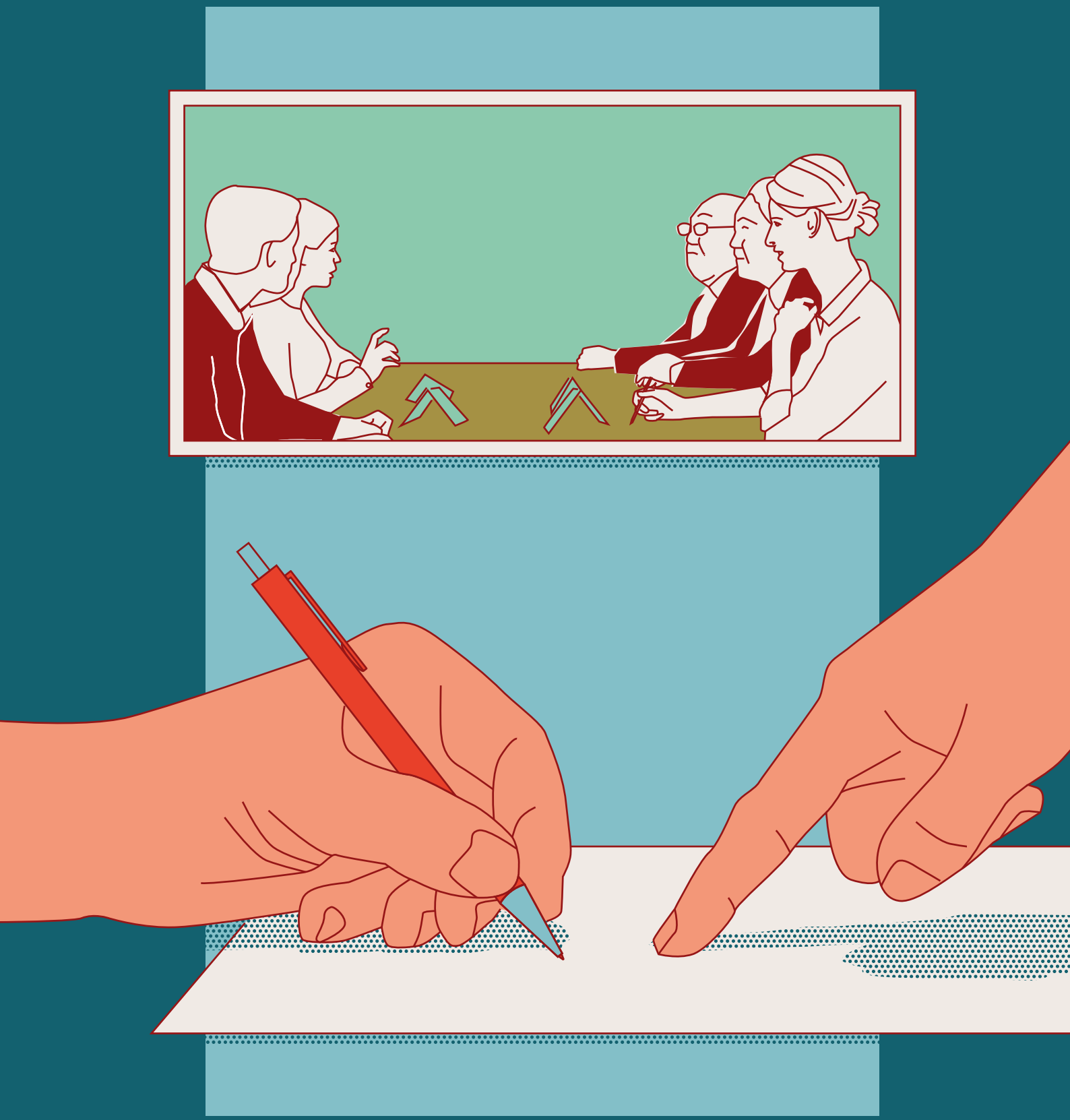
- You can prepare yourself to better manage critical reactions to your work.
  - Establish strong data and cybersecurity practices early in your career (see Annex for a sample of resources). Where possible, talk to more experienced colleagues to learn their best practices.
  - Use social media thoughtfully. Allow yourself time away and deploy blocking as needed. Be aware that Chinese authorities or their proxies may approach you through such accounts. (In some cases, authorities may also try to reach you via your personal phone number or email).

Mentorship and community-building are key

Mentorship and community-building are critical to ensuring that up-and-coming researchers have the means, know-how, and support to conduct safe, high-quality work—and to prevent potential risks from driving them away from the field.

- Proactively inform junior practitioners about potential risks from day one. Don't assume they already know, even if they are Chinese nationals.
- Help younger researchers develop risk mitigation plans, procedures, and skills that will support their resilience in the face of future challenges.
- Help junior practitioners develop their own networks of fellow practitioners.
- Build a community based on shared work challenges, rather than solely based on work topics. For example, exchange best practices and documentation with practitioners working in other authoritarian environments.
- Be generous but cautious when making introductions and sharing information. Seek consent and consider the potential impact of security breaches.
- Even if you experience no issues with your work, have empathy for others who have come under scrutiny or pressure from Chinese authorities.

Working with counterparts based in China requires a case-by-case approach



Working with counterparts based in China requires a case-by-case approach

Working with Chinese counterparts often entails murky or ambiguous safety or ethical situations. To avoid endangering individual or institutional counterparts based in China, precise, China-specific guidelines are essential for the following cases:

- Institutions with formal exchange or research arrangements with Chinese counterparts
- Institutions with occasional exchanges or research projects that involve Chinese institutions or individual researchers, regardless of the subject matter
- Individuals involved in the above exchanges or research projects



RECOMMENDATIONS FOR INSTITUTIONS

Establish procedures for employees and their counterparts

- Institutions have a duty of care towards their employees' counterparts in China. Understand that guidelines and protocols developed in different contexts may be harmful in the China context. Assess whether your policies require your employees to take steps that are either impracticable or actively harmful to interlocutors in China and consider updating them (See Section 1 for suggested changes to institutional ethics requirements).
- When they are working outside China, provide private, secure spaces for your employees to conduct interviews with Chinese counterparts.
- Develop specific policies for data transfer/sharing with China-based counterparts. Specifically, provide guidance on how and where to store data, with an eye to retaining copies and access even if the partnership ends or access to storage in China is cut off.

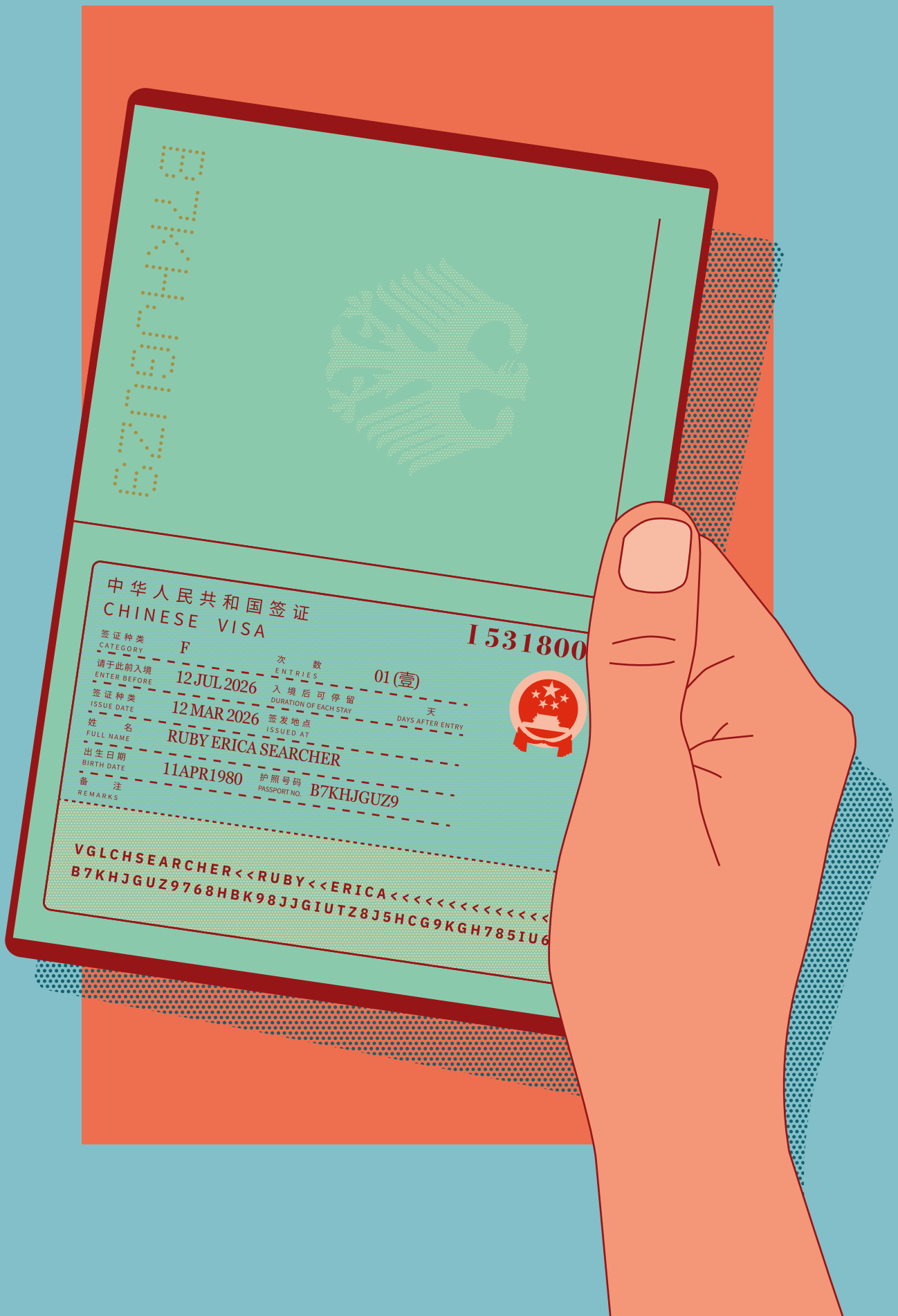
Manage collaboration requests and exchanges

- Review proposed participants' backgrounds, including their institutional affiliations and the topics on which they have previously worked. At the same time, do not pre-emptively exclude participants solely based on nationality or affiliation with the Chinese Communist Party. Make decisions on a case-by-case basis.
- Ensure you actively shape the agenda and exchange format (smaller group sizes tend to enable more open, unscripted dialogue).
- Provide non-China-focused staff and junior researchers with relevant background knowledge on China's political and education system and (where applicable) institutional guidance for contact with Chinese counterparts, particularly with Chinese government officials and institutions.
- Review joint statements, memoranda of understanding, and other agreements to ensure they do not contain language and expectations that conflict with your institution's mission, principles, and interests.

RECOMMENDATIONS FOR INDIVIDUALS

- Practitioners have a duty of care towards their China-based counterparts, particularly current or former Chinese passport holders. Clearly tell your interlocutors who you are and why you wish to speak with them, allowing them to make an informed choice about interacting with you.
- Beijing's red lines will likely shift, meaning that even innocuous-seeming interactions with interlocutors may become harmful for them down the line. Be prepared to take steps that may not match the best practices in your field, such as:
  - Anonymizing your sources.
  - Forgoing interview recordings (and, if in person, removing phones from the room).
  - When possible, relying less on interviews and instead scaffolding your work using several different methodologies.
  - Leaving space for your interviewees to direct the conversation away from issues they feel uncomfortable discussing.
- Perceived surveillance and/or pressure may induce counterparts to change their behavior towards you. Be prepared for last-minute meetings or interview cancellations. Be aware that, even at events or spaces outside China, interlocutors may feel the need to self-censor or even proactively support party-state narratives.
- Assume authorities are monitoring or can retroactively investigate any digital interaction (text, voice, or video) with interlocutors in China, including Hong Kong and Macau.
  - Choose online platforms that are appropriate to the level of risk involved. For example, for interviewing participants whose identity must be protected, it is best to err on the side of caution and use foreign platforms to which the Chinese government has no direct access. In cases where transparency is the priority, or when it's a preference expressed by participants, platforms such as WeChat (which should be considered actively monitored[20]) may be the best option.
  - When conducting exchanges with counterparts in China, be aware that use of foreign platforms or tools blocked in the PRC also comes with risk, as access to blocked sites via censorship circumvention tools may result in fines and even criminal penalties.[21]

Traveling to China for research poses new challenges



Traveling to China for research poses new challenges

Despite the increasing headwinds against travel and exchange, many projects still benefit from researchers' conducting on-the-ground work. Such trips, however, should be planned with care, and with host institutions' active assistance. This reduces the travelers' personal safety risks and mitigates institutional risk in case of emergencies. This is particularly important for:

- Institutions that have employees or students traveling to China for research, conferences, or educational exchanges
- Individuals traveling to China for research, conferences, or educational exchanges



RECOMMENDATIONS FOR INSTITUTIONS

China-specific policies

- Develop policies for data collection, storage, and transfer, including how to transmit or carry data out of China. Ensure these policies do not put researchers in an impossible bind (e.g., requiring them to abide by two mutually contradictory sets of national laws). Include AI and other emerging technologies in your planning.
- Communicate requirements related to Chinese partners. Employees of institutions such as non-profits and universities, for example, require a Chinese partner to officially support/sponsor the trip.[22] Ensure that employees have formalized such a partner relationship and have obtained an invitation letter, if necessary.
- Establish norms for travel risk assessment. Consult China specialists as well as your relevant guidelines (see e.g., Annex) and familiarize yourselves with established practices by international organizations.[23]
- Create an emergency action plan. Document the steps you will take in a variety of scenarios, such as an employee being followed, threatened, or detained. Make sure your plan accounts for the enhanced risks faced by current/former Chinese nationals, and that it also includes separate steps for employees who may be citizens of a third country (i.e., neither China nor your institution's own country). Communicate this plan clearly to employees so they know what they can (or cannot) expect from you.
- Ensure your employees have the resources to implement your China-specific policies. For example, if you mandate that employees must take "burner" devices to China, you should either provide them with such devices or rescind the requirement. Similarly, provide IT support to set up (including travel-specific accounts or platforms) and clean up such devices.

RECOMMENDATIONS FOR INDIVIDUALS

Take online precautions

- Consider your digital device usage strategy. For example, having WeChat on your device is a must if you plan to contact Chinese counterparts, but it is also a security risk.
- If you travel to China regularly, maintain separate devices for Chinese and non-Chinese apps/contacts.
- If you travel to China infrequently, use a "burner" device that can be wiped clean upon your return. This device should not contain any login or data beyond what is strictly necessary for the trip. Though carrying an empty device may raise suspicions should Chinese authorities check it, the more travelers who regularly use burner devices, the less "suspicious" such behavior may appear over time.
- Consider your online profile. Determine whether "cleaning up" certain posts or links to publications or institutions might allow you to stay below authorities' notice—or if such a "clean up" would be too harmful to your long-term career.

Take offline precautions

- Be cautious about mixing business and pleasure. Be transparent about why you're traveling. If you are asked, be up front with authorities about what you plan to do while in China.
  - If you are in China on a tourist visa, do not attempt to work.
  - If you are from a country that enjoys visa-free travel, be cautious about conducting work without a visa. Get an official invitation from your Chinese partner institution before traveling and keep your activities to those outlined in your host institution's agenda.
  - If you are in China for work, you would ideally travel under an appropriate visa obtained with support from your home institution and/or your Chinese partner institution. When contacting local friends/family, consider the likelihood of your current work having unintended consequences for them, such as questioning by the authorities. Keep your personal activities visible to authorities, i.e., visiting public museums or bookshops.
- Develop a travel safety plan before departing. This may include:
  - Creating a set travel itinerary and sharing it with others before you leave; having said itinerary readily available should authorities question you during your stay.
  - Always carrying your embassy's contact details with you.
  - Designating a trusted contact outside China to communicate with at set intervals during your stay.
- Do not assume the worst-case travel scenario but be aware of the risks.
  - The widespread deployment of surveillance technologies[24] means that you may be monitored at any time, even if it is not obvious to you.
  - If authorities "invite you to tea" (ask to speak with you at their offices, without officially detaining you), you may be able to politely decline, but if you simply ignore them, authorities may begin contacting other acquaintances to pressure you indirectly.
  - Be aware that authorities may ask you about your activities outside China, such as travel to Taiwan.
  - Be aware that under Chinese law, authorities can detain you for lengthy periods without informing your embassy.[25] This almost never happens, but it is technically possible.

Conducting work solely outside of China doesn't mitigate all risk



Conducting work solely outside of China doesn't mitigate all risk

As field research and travel have become more restrictive, OSINT research has gained prominence especially during and after the Covid-19 pandemic. OSINT is particularly especially important for areas of research that the Chinese government proactively obstructs, such as human rights and/or research in geographically restricted areas of Xinjiang and Tibet.

While conducting research from a distance is seen as generally safer, Chinese authorities make use of transnational repression and other tactics that should prompt institutions and individuals to build additional guardrails.

This is particularly important for:

- Institutions hosting OSINT research projects on China, especially if they involve large data collection
- Individuals conducting the research



RECOMMENDATIONS FOR INSTITUTIONS

- Know the relevant portions of Chinese data laws and of your local laws.
- Create technical guidelines for web-scraping, including storage and usage of the resulting data.
- If applicable, create ethical guidelines for collecting online content in China (such as public-facing social media posts), including your rules about user expectations of privacy, anonymization procedures, and citation standards.



RECOMMENDATIONS FOR INDIVIDUALS

- Several practitioners are successfully deploying OSINT data collection methods like web scraping to conduct research. However, be aware that though this approach mitigates in-country fieldwork risks, it, too, will never be fully risk-free. Chinese authorities can opt to more aggressively (or arbitrarily) enforce data security laws at any time.
- Follow established practices such as archiving sources and ensuring you have locally backed-up copies of key information.
- Reach out directly to others doing OSINT work to learn their best practices; some practices cannot be shared publicly without reducing their efficacy.
- Consider whether your work might cause cybersecurity issues for your device or your network, and, if feasible, use a separate machine for such work. Make sure you deploy additional tools such as trusted VPNs, virtual machines and sandboxes as needed.
- To reach Chinese sites and services that try to limit access from abroad (geo-blocking),

practitioners advise frequently switching proxy servers or configuring a separate virtual environment on your computer from which to visit target sites. When you encounter Domain Name System (DNS) blocks, proxies will not be helpful, but you can try configuring your browser/PC to use a China-based DNS server.[26]

- At the outset of your research planning, account for questions of data availability and data reliability on the subject matter. Be aware of the political constraints that affect what you're able to see or gather online (the changing nature of what information can be published in China, how the data is presented, what has been censored).[27] You may not know when something is missing, which can skew your observations or analysis. Consider mixing or complementing quantitative data with qualitative data where possible to offset this concern. Reflect on what incentives for disclosure or nondisclosure/censorship exist for Chinese counterparts and weave this knowledge into your research process.[28]

Government-issued guidelines on research security, academic collaboration and academic freedom

	RESOURCE	PROVIDER	YEAR
EU	Research Security Guidelines for Ireland	Irish Department of Further and Higher Education, Research, Innovation and Science	2026
EU	Methodological recommendation: Defining the minimum scope of due diligence and risk management in cooperation with third parties within the context of strengthening the resilience of the higher education and research environment against illegitimate interference	Czech Ministry of the Interior and Ministry of Education, Youth, and Sports	2025
EU	EU Council Recommendation on Enhancing Research Security	EU Council	2024
EU	National Knowledge Security Guidelines – Secure International Collaboration	Government of the Netherlands	2022
EU	Committee on Guidelines for International Research and Innovation Cooperation	Danish Ministry of Higher Education and Science	2022
EU	★ Recommendations for academic cooperation with China	Ministry of Education and Culture of Finland	2022
EU	Academic freedom of expression	Norwegian Ministry of Education and Research	2022
	RESOURCE	**PROVIDER**	**YEAR**
NON-EU	★ China Resources	Australian Government Department of Education	2026
NON-EU	National Security Guidelines for Research Partnerships	Government of Canada	2026
NON-EU	Safeguarding Academia	US National Counterintelligence and Security Center	2025
NON-EU	Conducting Open Source Due Diligence for Safeguarding Research Partnerships	Government of Canada	2025
NON-EU	Guidelines to Counter Foreign Interference in the Australian University Sector	Australian Government Department of Education	2025
NON-EU	Trusted Research: Guidance for Institutions and Researchers	Government of New Zealand	2025
NON-EU	G7 Best Practices for Secure and Open Research	G7	2024
NON-EU	Named Research Organizations	Government of Canada	2024
NON-EU	★ China: The Risk to Academia	U.S. Federal Bureau of Investigation	2019
NON-EU	Trusted Research Guidance for Academia	UK National Protective Security Authority	2019

Source: MERICS ★ China-specific resources

© MERICS

Academic institutions' and sector associations' own resources

	RESOURCE	PROVIDER	YEAR
★	Resource Hub for U.S. Academic Travel to China	US-China Education Trust	2026
	How universities can protect and promote academic freedom: EUA principles and guidelines	European University Association	2025
	Risk and opportunity assessment for international collaboration and activities	The Swedish Foundation for International Cooperation in Research and Higher Education	2025
★	The KoWinChi Project (Training program for cooperation with Chinese counterparts)	Würzburg University, University of Erlangen–Nuremberg	2024
★	Cooperation Guidelines	The China Competence Centre at the Julius Maximilians University	2024
	Managing risks in Internationalisation: Security related issues	Universities UK	2022
★	Guiding Questions on University Cooperation with the People's Republic of China	German Rectors' Conference	2020
	Responsible internationalisation: Guidelines for reflection on international academic collaboration	The Swedish Foundation for International Cooperation in Research and Higher Education	2020
PLEDGES AND PRINCIPLES	Primary Representative AgreementForm	Scholars at Risk	2026
	G7 Common Values and Principles on Research Security and Research Integrity	G7	2022
	Magna Charta Universitatum	European University Association; Alma Mater Studiorum University of Bologna	2020

Source: MERICS ★ China-specific resources

© MERICS

General resources

RESOURCE	PROVIDER	YEAR
★ Chinese Academy of Sciences Directory	RAND	2026
★ China Defence Universities Tracker	Australian Strategic Policy Institute (ASPI)	2026
★ Chinese students & scholars associations in Europe, and long-distance authoritarian engagement	Sciences Po Center for International Studies	2026
Investigative policy analysis: Leveraging ethnography's postures to research secretive state policies in access-restricted authoritarian contexts	Sage Journals	2026
★ Swedish research collaborations with China still increasing, but politically more difficult	The Swedish National China Centre	2025
★ Managing the Risks of China's Access to U.S. Data and Control of Software and Connected Technology	Carnegie Endowment for International Peace	2025
Regulatory advice 24: Guidance related to freedom of speech	Office for Students (UK)	2024
★ People's Republic of China Legal Research: Introduction to China's Legal System	Harvard Law School	2024
Measures for the Management of Scientific Data	Center for Security and Emerging Technology (CSET)	2023
Model code of conduct: protection of academic freedom and the academic community in the context of the internationalisation of the UK HE sector	Academic Freedom and Internationalisation Working Group	2022
★ How to do Trusted Research: China-Specific Guidelines for European Stakeholders	Association for International Affairs	2022
★ Checklist for Collaboration with Chinese Universities and Other Research Institutions	The Hague Centre for Strategic Studies	2019
★ Resisting Chinese Government Efforts to Undermine Academic Freedom Abroad A Code of Conduct for Colleges, Universities, and Academic Institutions Worldwide	Human Rights Watch	2019
Academic Freedom and Internationalisation Working Group at Human Rights Consortium	Human Rights Consortium, Institute of Commonwealth Studies, School of Advanced Study, University of London	2019
Research, Ethics and Risk in the Authoritarian Field	Palgrave Macmillan	2018

Source: MERICS ★ China-specific resources

© MERICS

Annex 4

Cyber and OSINT resources

RESOURCE	PROVIDER	YEAR
Online Open Source Investigation Toolkit	Bellingcat	N/A
Digital Security Resource Hub for Civil Society	Amnesty International	N/A
Open-source intelligence (OSINT) self-audit for researchers	University of Toronto	2026
John Scott-Railton Shares Tips and Tools to Protect Yourself Digitally	Global Investigative Journalism Network	2026
★ Mining China's 'Little Red Book' for Open Source Gold	Bellingcat	2026
Practical Advice to Avoid Getting Pwned by AI	American Enterprise Institute	2026
★ The Locknet: How China Controls Its Internet and Why It Matters	ChinaFile	2025
★ The Challenges of Conducting Open Source Research on China	Bellingcat	2023
Into the Jungle: Best Practices for Open-Source Researchers	Georgetown Center for Security and Emerging Technologies (CSET)	2022

Source: MERICS ★ China-specific resources

© MERICS

Annex 5

Associations and mentorship resources

RESOURCE	TYPE
★ European Association for Chinese Studies	International organisation representing China scholars from all over Europe
★ EURAXESS China	Community of researchers
★ Global China Studies Early Career Researcher Network	Community of researchers
★ British Association for Chinese Studies	Community of students and researchers
★ Berlin Contemporary China Network	Community of researchers and scholars
★ Young China Watchers	Community of professionals

Source: MERICS ★ China-specific resources

© MERICS

Endnotes

1 | MERICS, UC Institute on Global Conflict and Cooperation. “Re-engineering China’s innovation machine”. Accessed 25 September 2026. https://merics.org/en/re-engineering-chinas-innovation-machine.

2 | Damian Grammaticas. “China intimidated UK university to ditch human rights research, documents show”. BBC. 3 November 2025. https://www.bbc.com/news/articles/cq50j5vwny6o.

3 | Olivia Mapes, Skyler Mofle. “Purdue reportedly directs admissions to reject students from list of ‘dangerous countries’”. The Exponent. 5 December 2025. https://www.purdueexponent.org/campus/features/purdue-university-admissions-chinese-students-security-concerns-admissions-discrimination/article_baf8f46c-a7ad-4d6b-98e1-60b42a6cbb47.html.

4 | Throughout this report, we use the terms “researcher” and “practitioner” interchangeably to refer to anyone in any field who studies China, conducts research in China, writes about or reports on China, or works with Chinese counterparts.

5 | Rogier Creemers. “National Security Law of the People’s Republic of China”. DigiChina. 1 July 2015. https://digichina.stanford.edu/work/national-security-law-of-the-peoples-republic-of-china/.

6 | The China NGO Project. “Law of the People’s Republic of China on Administration of Activities of Overseas Nongovernmental Organizations in the Mainland of China”. China File. 28 April 2016. https://www.chinafile.com/ngo/laws-regulations/law-of-peoples-republic-of-china-administration-of-activities-of-overseas.

7 | Yuechao Nie. “China: Counterespionage Law Revised”. Library of Congress. 22 September 2033. https://www.loc.gov/item/global-legal-monitor/2023-09-21/china-counterespionage-law-revised/

8 | Yvette Tan. “China arrests US scholar suspected of spying”. BBC. 12 June 2026. https://www.bbc.com/news/articles/c8728lv910po.

9 | Peter Xavier Rossetti. “The Detention of the Two Michaels: A Story on China’s Human Rights Abuses”. Amnesty International. 5 January 2022. https://amnesty.sa.utoronto.ca/2022/01/05/the-detention-of-the-two-michaels-a-story-on-chinas-human-rights-abuses/.

10 | Emily Feng, John Ruwitch. “Cheng Lei, detained Australian journalist, is freed by China”. NPR. 11 October 2023. https://www.npr.org/2023/10/11/1205145233/china-cheng-lei-freed.

11 | Yojana Sharma. “Academics continue China research – while targeted by China sanctions”. University World News. 2 June 2021. https://www.universityworldnews.com/post.php?story=20210602152426562; Albert Zhang, Danielle Cave. “Smart Asian women are the new targets of CCP global online repression”. ASPI Strategist. 3 June 2022. https://www.aspistrategist.org.au/smart-asian-women-are-the-new-targets-of-ccp-global-online-repression/.

12 | OpenTech Fund. “Blocked by Numbers: The Impact of Real-Name Registration Policies on Transnational Access to Chinese Social Media Apps”. Accessed on 25 September 2026. https://blocked-by-numbers.opentech.fund/en/; Vincent Brussee. “Conceptualizing the reverse great firewall: cybersecurity and the logics of government geo-blocking in China”. Journal of Cybersecurity. Volume 12, Issue 1, 2026, tyag005. https://doi.org/10.1093/cybsec/tyag005.

13 | Jeroen Groenewegen-Lau, Michael Laha. “Controlling the innovation chain: China’s strategy to become a science & technology superpower”. MERICS. 2 February 2023. https://merics.org/en/report/controlling-innovation-chain.

14 | Kai von Carnap. “The increasing challenge of obtaining information from Xi’s China”. MERICS. 14 February 2024. https://merics.org/en/report/increasing-challenge-obtaining-information-xis-china

15 | Carolyn Braun. “Beijing expands state secrets law”. Table Briefings. 27 February 2024. https://table.media/en/china/news/beijing-expands-state-secrets-law.

16 | International Consortium of Investigative Journalists. “Transnational Repression”. Accessed on 25 September 2026. https://www.icij.org/tags/transnational-repression/.

17 | OECD. “OECD Science, Technology and Innovation Outlook 2025”. 28 October 2025. https://www.oecd.org/en/publications/oecd-science-technology-and-innovation-outlook-2025_5fe57b90-en.html.

18 | Jérôme Doyon. “Chinese Students and Scholars Associations in Europe, and long-distance authoritarian engagement”. Sciences Po Center for International Studies. 2 February 2026. https://www.sciencespo.fr/ceri/en/news/chinese-students-and-scholars-associations-in-europe-and-long-distance-authoritarian-engagement/.

19 | Amnesty International. “China: ‘On my campus, I am afraid’: China’s targeting of overseas students stifles rights”. 13 May 2024. https://www.amnesty.org/en/documents/asa17/8006/2024/en/

20 | NetAskari. “Does the Chinese police eavesdrop via ZOOM calls?”. Substack. 14 August 2026. https://netaskari.substack.com/p/does-the-chinese-police-eavesdrop.

21 | China does not categorically ban virtual private networks (VPNs), though mainland-based VPN services must obtain governmental approval and cooperate with security agencies where requested. Overseas services, in contrast, operate in a legal grey zone: While Chinese authorities generally tolerate the use of proprietary VPN systems to access foreign companies’ or universities’ own networks, individuals using commercial VPN services to circumvent China’s internet restrictions—as well as the service providers themselves—have faced fines and even criminal prosecutions.

22 | The China NGO Project. “Law of the People’s Republic of China on Administration of Activities of Overseas Nongovernmental Organizations in the Mainland of China”. ChinaFile. 28 April 2016. https://www.chinafile.com/ngo/laws-regulations/law-of-peoples-republic-of-china-administration-of-activities-of-overseas.

23 | US-China Education Trust. “Resource Hub for U.S. Academic Travel to China”. Accessed on 25 September 2026. https://uscet.org/resource-hub/.

24 | NetAskari. “Sharp Eyes: Mass surveillance of foreigners in China - Part 1”. Substack. 19 May 2026. https://netaskari.substack.com/p/sharp-eyes-how-to-track-a-foreigner.

25 | Safeguard Defenders. “RSDL: A factsheet on China’s system of Black Jails”. Accessed on 25 September 2026. https://safeguarddefenders.com/sites/default/files/pdf/FACTSHEET RSDL.pdf.
26 | Vincent Brussee. “Conceptualizing the reverse great firewall: cybersecurity and the logics of government geo-blocking in China”. Journal of Cybersecurity. Volume 12, Issue 1, 2026, tyag005. https://doi.org/10.1093/cybsec/tyag005.
27 | Glenn Tiffert. “Peering down the Memory Hole: Censorship, Digitization, and the Fragility of Our Knowledge Base”. The American Historical Review. 2019; 124: https://doi.org/10.1093/ahr/rhz286.
28 | Vincent Brussee. “Mitigating Missingness in Analysing Chinese Policy and Implications for the Fragility of Our Knowledge Base”. The China Quarterly. 2025; 261:234-248. https://doi.org/10.1017/S0305741024000948.

IMPRINT

CONTACT
Daria Impiombato
Senior Analyst, MERICS
daria.impiombato@merics.de

EDITORIAL TEAM
Claudia Wessling
Director Communications and Publications, MERICS

GRAPHICS AND LAYOUT
Studio FÖRM
www.foerm.net

PUBLISHER
MERICS | Mercator Institute for China Studies
Alte Jakobstraße 85–86 | 10179 Berlin
Tel.: +49 30 3440 999 0
Mail: info@merics.de
www.merics.org

Copyright © 2026
Mercator Institute for China Studies (MERICS)

Printed in Berlin, Germany

ISSN (Print): 2941-5799
ISSN (Online): 2941-5608

Read online:



www.merics.org