Sino-EU Academic Collaborations

Identifying Risks & Challenges

datenna®

datenna.com

/ About Datenna

Datenna is the global provider of techno-economic intelligence on China, with unmatched depth of coverage of Chinese entities, and identification of hidden connections to the Chinese state and military.

To deliver these insights, our in-house team of China experts uses open-source intelligence (OSINT) to curate publicly available Chinese-language information and provide it to clients through a proprietary software platform. Decision-makers worldwide rely on Datenna's platform for extensive mapping of over 45 million Chinese companies, more than 70 million individuals, 27,000+ research institutes, over CNY 600 billion in research funding, 42+ million patents, and 850,000+ PLA military and government procurements.

By offering a comprehensive view of China's economic and academic landscape, we equip our clients with the tools necessary to accurately assess national-, economic-, and knowledge-security risks.

Datenna's intelligence platform supports a wide range of use cases, including inbound and outbound investment screening, export control of dual use technologies, due diligence on individuals and companies, as well as evaluations of China's technological advancements and research collaborations.

For more information, visit *datenna.com*.

/ Table of Contents

/ 1. Introduction: China as an Academic Power

Concerns about the security risks of Sino-European academic collaborations have increased during the Xi Jinping era as China has raised the level and volume of its research output and emerged as a geopolitical competitor. Growing awareness of the connections between technological, economic, and national security has increased the need for identifying risks – such as those related to unwanted knowledge and technology transfer – and safeguarding strategic technologies.

At the same time, the attraction for foreign universities brought by the expansion of Chinese academic research is clear. The growing numbers of leading researchers and well-resourced research units and facilities in China have created a significant pull factor for foreign universities to pursue research collaboration with Chinese institutions. China has become a global leading producer of research in many academic disciplines, especially those in natural science and technology fields. China's research output has not only significantly expanded in volume but also in quality, as shown by indices tracking discipline-leading journals such as the Nature Index, where China is now the highest contributor to publications in top journals.[1] This has been accompanied by significant increases in international linkages such as joint research centers, programs and co-authored papers.

This report will introduce **a toolbox for addressing some of the major risks associated with academic collaborations** and conducting due diligence on collaboration partners in China. For this process, a specially compiled OSINT dataset including various Sino-European academic collaborations has been cross-referenced with the Datenna platform. This process enabled the identification of institutional connections to government and military entities, as well as dual-use technology development within the Chinese academic entity involved in the collaborations.

Datenna's data is well-suited to addressing several interrelated types of risk within the knowledge security space. These risks fall broadly under the umbrella of unwanted technology transfer in strategically critical fields where European institutions are world-leading, or in technologies with dual-use potential. These can in turn:

- **Harm the competitiveness of European industries in emerging technology fields** and consequently damage Europe's long-term prosperity.
- **Inadvertently support military actors in China** through the partner organization's links to the military sector: this applies in cases in which a partner university is conducting research that is directly military-applicable or dual-use, or that same partner has links to the defense industry through procurements and other commercial activities that are commonplace in the Chinese university system.

[1] "What China's leading position in natural sciences means for global research," Nature, accessed august 7 2024, https://www.nature.com/articles/d41586-023-02159-7

/ 2. The Emergent Knowledge Security Debate

Various policy responses have been developed to address the potential risks in academic collaborations – both at the European and national level – with the concept of knowledge security gaining currency in the European Union (EU) and the United States (U.S.). There is growing recognition that academic collaborations facilitating technology and knowledge transfer may give third countries an advantage in leveraging key technologies for commercial or military purposes, diminishing Europe's technological edge in the process. This can in turn **threaten Europe's broader military or economic security.** The conversation around knowledge security can be seen as one part in a more comprehensive discussion around security and the 'de-risking' paradigm in a context of increased geopolitical competition.

One manifestation of this is the EU's recent series of policies informed by the concept of de-risking. These include the June 2023 economic security strategy by the European Commission (updated in January 2024),[2] the October 2023 recommendation on critical technology areas for the EU's economic security,[3] and the European Commission proposal for a Council recommendation on enhancing research security, adopted by the Council in May 2024.[4]

The latter document gives recommendations for European practices on **balancing academic freedom and international openness with security priorities**. Emphasizing the crucial role of exchanges for scientific progress but simultaneously recognizing the presence of geopolitical risks and hybrid threats, it names "the undesirable transfer of critical knowledge, know-how and technology that may affect the security of the EU and its Member States."[5] This broadly characterizes knowledge security risk with the working assumption that it can expose Europe to foreign competitors and military actors. The academic sector, open and without a strong tradition of establishing geopolitical safeguards, can be particularly vulnerable. The EU recommendations also emphasize the principle of proportionality: "not go[ing] beyond what is strictly necessary to mitigate the risks at stake and avoid unnecessary administrative burden". They equally caution against "protectionism and unjustified political instrumentalization of research and innovation."[6]

[2] "Commission proposes new initiatives to strengthen economic security," European Commission, accessed 7 august 2024, https://ec.europa.eu/commission/presscorner/detail/en/IP_24_363

[3] "Commission recommends carrying out risk assessments on four critical technology areas: advanced semiconductors, artificial intelligence, quantum, biotechnologies," European Commission, accessed 7 august 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4735

[4] "Council adopts a recommendation to enhance research security," European Council, published 24 May 2024, [accessed 19 November 2024], https://www.consilium.europa.eu/en/press/press-releases/2024/05/23/council-adopts-a-recommendation-to-enhance-research-security/ , full text: https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf

[5] "Council recommendation on enhancing research security," European Commission, p. 4, 13

[6] "Council recommendation on enhancing research security," European Commission, p. 12-14

The recommendation on enhancing research security formulates a four-stage risk appraisal framework, including:

1) the risk profile of the EU-based organization,
2) the particular research domain and risks specific to it,
3) the risk profile of the third country, and
4) the risk profile of the partner institution.

In connection with partners in third countries, the fourth point can present challenges due to issues like access to information, language barriers and a lack of awareness of possible institutional links to state and military actors.

The challenges of implementing a necessary degree of de-risking and protecting knowledge security are real, considering the limited resources universities often have in this field and a lack of established practices for assessing security considerations related to academic collaborations. The Council recommendations advise public authorities to offer resources and assistance to better conduct due diligence in universities. Shared capabilities, when developed collaboratively, can be a helpful way to advance knowledge security goals. One of the objectives of this report is to showcase the types of tools and data necessary for thoroughly analyzing potential academic partners and making well-informed assessments of associated risks.

Various National Approaches and Challenges

The potential risks of collaboration with China have prompted varied discussions in different European countries around practical ways to mitigate risks. The Netherlands released their National Guidelines for Knowledge Security for knowledge sector organizations in 2022. Using a similar definition of knowledge security risk to the EU, they focus on identifying the domains of knowledge that may be vulnerable to being targeted for knowledge transfer – especially focusing on institutional "crown jewels". They recommend conducting due diligence on the home country and institutional characteristics of potential partners. At an institutional level, the guidelines offer several points for consideration, including potential governmental or military/defense affiliation, as well as whether it is a sanctioned entity, the general reputation of the institution, and the other activities of the researchers involved.[7]

The 2023 German Federal China Strategy expresses support for increasing student and researcher exchanges with China.[8] The German Rectors' Conference has also released their own statement that expresses broad support for continued engagement but encourages establishing practices and structures for mitigating risks in sensitive research.[9] Other countries like the United Kingdom (UK) and Sweden have

[7] "Knowledge Security," NWO, accessed 7 august 2024, https://www.nwo.nl/en/knowledge-security

[8] The Government of the Federal Republic of Germany, "Strategy on China", Auswärtiges Amt, published 2023, https://www.auswaertiges-amt.de/blob/2608580/49d50fecc479304c3da2e2079c55e106/china-strategie-en-data.pdf

[9] "Guiding questions on university cooperation with the People's Republic of China", HRK, accessed 7 august 2024, https://www.hrk.de/resolutions-publications/resolutions/beschluss/detail/guiding-questions-on-university-cooperation-with-the-peoples-republic-of-china/

released guidelines that have similar foci but do not specifically address China, instead emphasizing greater awareness of Europe's principles of research and ethics.[10]

Outside of Europe, both state entities and individual institutions have released China-specific as well as general guidelines on the security of academic collaborations. For example, the MIT China Strategy Group, a group of experts on U.S.-China relations from the Massachusetts Institute of Technology, has issued a recommendation that the institute should not engage in research cooperation with universities that have ties to the PLA, national defense universities, or designated national defense laboratories in China.[11]

There is an **emerging consensus among players in Europe on the main priorities and red lines in academic collaboration**. Key among these is preventing transfer of sensitive technologies and inadvertent support for Chinese military actors. However, despite the shared understanding expressed in the different policy documents on identifying high-risk academic institutions in third countries, conducting due diligence on academic institutions may be harder than it seems.

One reason for this is the **general opacity of many institutions in China** and the difficulty of ascertaining their possible military connections and defense-related work. Another is the inherent resource and knowledge constraints limiting the ability to conduct due diligence on Chinese institutions. There is, therefore, a clear need to develop practices and resources for mitigating risks in research collaboration while avoiding undue restraints on international research and the benefits it can bring.

/ 3. The Dataset

This paper offers several contributions to the developing debate and practices around identifying and managing risks in collaborating with Chinese institutions. The focus will be on a dataset compiled by Datenna on past and current **European academic collaborations with 20 leading Chinese universities** established before 2022, comprising the top 13 universities in academic rankings and the Seven Sons of National Defense (7S) – universities known for their established position in China's military development ecosystem. These universities were chosen for their size and importance within China's academic ecosystem. In the case of the 7S, their inclusion is due to known links to military research. The dataset was collected manually through online research from English and Chinese-language sources.

With this large-scale dataset, we can identify various trends on the types of academic collaborations, as well as how many concern potential strategic risks. Unlike some of the studies cited below, this paper focuses on established institutional mechanisms between universities and not on individual collaborations between academics.

[10] Ivana Karaskova, Filip Sebok, Veronika Blablova, "How to Do Trusted Research: China-Specific Guidelines for European Stakeholders," AMO, published December 2022, p. 28-29: https://www.amo.cz/wp-content/uploads/2022/09/HTDTR_report_how-to-do-trusted-research_A4_18_web.pdf

[11] Richard Lester, Lily Tsai, Suzanne Berger, Peter M Fisher, Taylor Fravel, David Goldston, Yasheng Huang, Daniela Rus, "University engagement with China: an MIT approach," MIT, published in October 2022, p.4-7, https://orgchart.mit.edu/system/files/reports/20221007-AssociateProvost-University-Engagement-with-China.pdf

The report also presents **case studies on individual collaborations of interest,** using Datenna's broader database that contains information on the institutional and commercial links of Chinese institutions, as well as data on their operations, such as patents and research projects. These data allow us to zoom in on certain institutions of interest once these are identified through the macro-level dataset.[12]

Sino-European Academic Collaborations through the Numbers

We divided the programs discovered during our research into two categories**: joint study programs and joint research centers** between European and Chinese universities. Of the 20 Chinese universities we tracked, 379 collaborations fall under these broad categories.

Out of the 379 collaborations, 267 fall under joint study programs and 112 under research centers (see Figure 1). While it may be difficult to make a clear distinction between the two categories, our analysis attempted to identify the primary purpose of a collaboration and categorize it accordingly. For example, a joint undergraduate or master's level program will usually be relatively easy to categories under "study programs" but joint PhD programs inherently also involve research. However, we established that a categorization under "research centers" should involve dedicated staff, a research agenda, and a stable institutionalized structure with the primary purpose of conducting research even though postgraduate training may also be organized. Therefore, we found that in most cases the collaborations clearly fell in one or the other category.

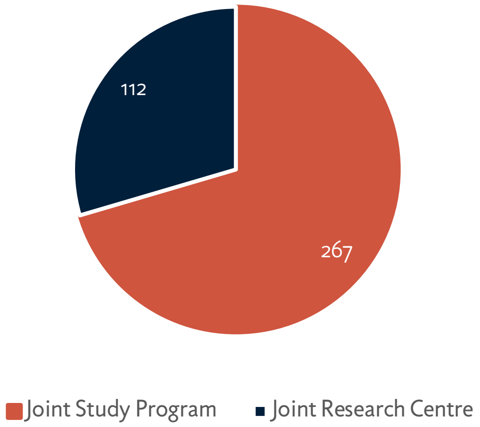

Figure 1: collaborations by type

[12] For this study, it should be noted that certain potentially important categories were left out. These include Confucius Institutes which, while often integrating into the academic life of the university, primarily focus on individual courses and general outreach activities. It is also important to note that individual research collaborations between academics or teams in Europe and China were also not included in our dataset. This is because the aim is to track long-standing and institutionalized forms of collaboration aiming to create more durable links between institutions and creating more lasting sets of commitments.

Collaborations with 20 key Chinese Universities

Among the 20 universities we tracked, our data reveals certain standout institutions that have a **large number of cooperation projects,** with a fairly high level of disparity between the most and the least popular universities (see Figure 2):

1) Zhejiang University;
2) Fudan University;
3) Tsinghua University;
4) Shanghai Jiaotong University;
5) Northwestern Polytechnical University;
6) Peking University.

Except for Northwestern Polytechnical University, the top five universities are all high-profile, large generalist universities and part of the so-called C9 group, which includes China's highest-ranking universities. It therefore stands to reason that these universities are attractive cooperation partners and have a desire to pursue international research and education projects.

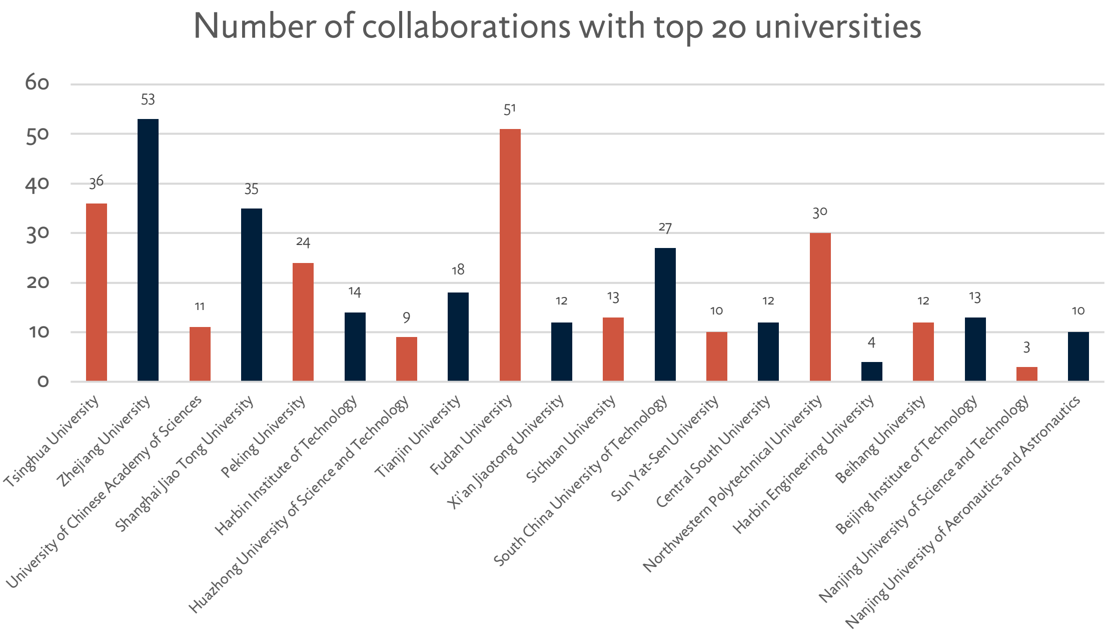

Figure 2: Number of collaborations with top 20 universities

Northwestern Polytechnical University, on the other hand, is part of the 7S grouping as well as the E9 group of engineering universities. The 7S stands for a group of seven Chinese universities that are currently under the management of the Ministry of Industry and Information Technology. The focus of these universities revolves around research and development (R&D) in a variety of technological and scientific areas, of which a significant proportion have dual-use applications. They receive funding from the Chinese Ministry of State and Security to conduct this research. They also play an important part in the Chinese defense industry with their research contributions as well as industry connections. It can, therefore, be particularly interesting to focus on these institutes and their collaborations with European universities.

While **screening these 20 universities using Datenna's platform**, we found that **all of them had been flagged as defense-related** by the platform's algorithm. The algorithm uses various criteria to determine this classification, including patent data, military procurements, and possible sanctions by foreign governments. This is significant since it shows that in addition to the known defense links of the 7S, activities of potential military significance are present in practically all the institutions included here. While this finding does not necessarily mean that the same is true of China's broader academic landscape, it does point to the need for vigilance and accounting for a broad variety of data points. Information like this can be key when addressing institutional risk, as identified in the European and national-level policy documents.

Figure 2 also shows that, generally speaking, high-profile generalist institutions like Zhejiang University tend to have more collaborations but specialized technical institutions – often with an engineering focus – are also involved in many international collaborations. Among these are Northwestern Polytechnical University and Beihang University: two high-profile institutions that are part of the Seven Sons of National Defense. We find that a total of 84 collaborations have one of the 7S as the Chinese partner or slightly more than one-fifth of the total in our dataset. This highlights that established collaborations exist even in cases where there is a known connection to dual-use research and thus a heightened need for conducting due diligence.

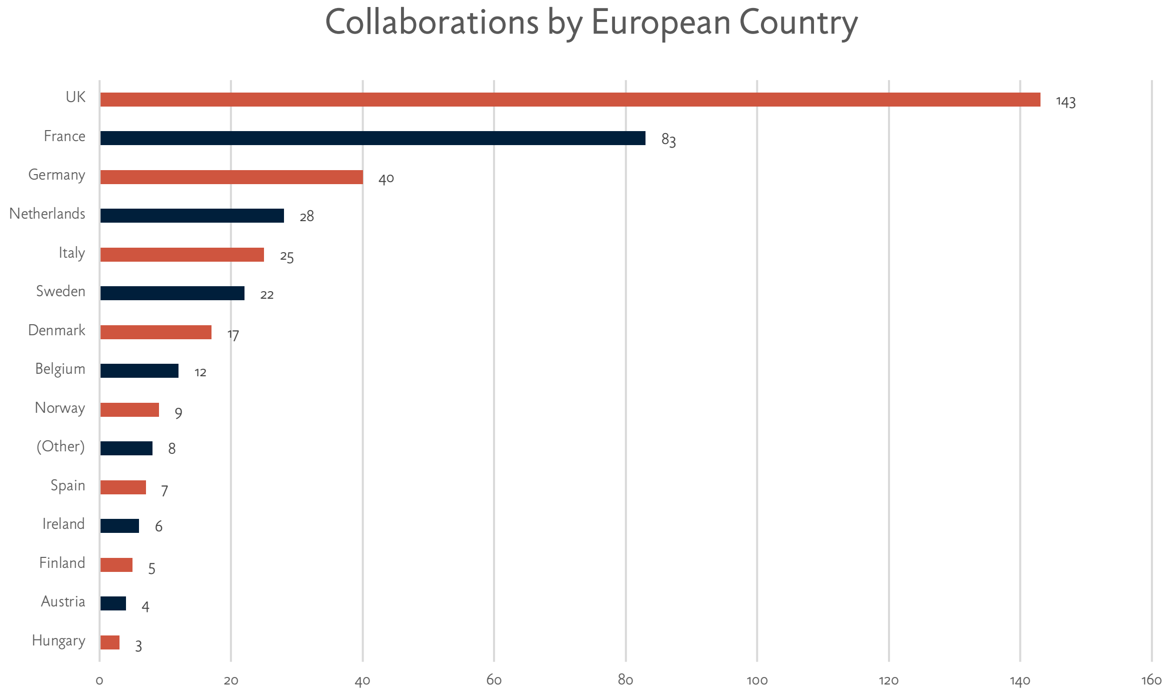

Figure 3: Collaborations by European Country

The countries included in the dataset are European countries that are members of the EU and/or NATO (see Figure 3). We find that the UK has, by some margin, the most individual collaborations with 143, followed by France with 83. In third, fourth and fifth place are Germany, the Netherlands, and Italy, with 40, 28, and 25 respectively. Together, these account for around three-quarters of all the collaborations in our dataset. A total of 22 eligible countries have collaborations with the 20 universities we tracked. Some countries such as Portugal, Romania, Lithuania, and Bulgaria appear in the dataset only once, and some European countries were not found to have any collaborations.[13]

The high proportion of UK and French universities is not surprising considering their overall high number of universities and level of internationalization. These countries also rank among the top in Europe when it comes to the number of international students from China. Nordic countries also feature prominently relative to their size. Overall, we find that collaborations with top Chinese universities are heavily concentrated in Northern and Western Europe, with newer EU member countries in Eastern Europe as well as many Southern European countries only having collaborations in the low single digits or none at all.

Fields of Collaboration

We also analyzed the fields of collaboration, with a particular interest in tracking how many of these potentially fall within **a strategic or dual-use category**. Figure 4 shows the overall number of collaborations in different academic fields.[14]

We see that the major fields in which collaborations take place are related to **business, finance, management and economics (89 collaborations), as well as engineering, and materials science fields (78)**. Together they account for almost half of all collaborations. Other groups include aerospace with 10 collaborations and artificial intelligence (AI) & automation with five. Other fields are more evenly divided, with the social sciences (44), environmental sciences (17), and design and architecture (22) fields also having a relatively large number of collaborations.

In Figure 5, we see that a total of **81 of the 379 collaborations** fall within a field of **potential strategic importance**. We based this classification on the EU's list of critical technologies for economic security, released in 2023 in connection with its economic security strategy.[15] Lists of priority technologies released by other organizations such as NATO, while not fully overlapping, share a similar focus on areas such as AI, quantum, advanced materials, and biotechnology. We can assume that these fields represent a broad consensus of what research areas are considered to fall within the scope of prioritizing knowledge security.

[13] While interpreting this numerical data on collaborations between institutes in different countries, it is important to keep in mind the limitations of this targeted dataset. First, only focusing on a select group of 20 Chinese universities doubtlessly leaves out many interesting collaborations between other European countries and universities that may or may not be represented here. In addition, a manual and targeted approach relying on open-source data like the one used here, despite identifying several hundred collaborations can also not guarantee complete coverage. This may be due to short-term or person-to-person collaborations that are not the focus of the present report, or more established links that were simply not captured through open-source research despite making every effort for data completeness. In addition, data found in open-source desk research cannot always be completely verified.

[14] The classification is based on the list of academic disciplines found on the Web of Science, adapted for brevity and clarity.

[15] "Annex to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States," European Commission, published 3 October 2023, https://defence-industry-space.ec.europa.eu/document/download/d2649f7e-44c4-49a9-a59d-bffd298f8fa7_en?filename=C_2023_6689_1_EN_annexe_acte_autonome_part1_v9.pdf

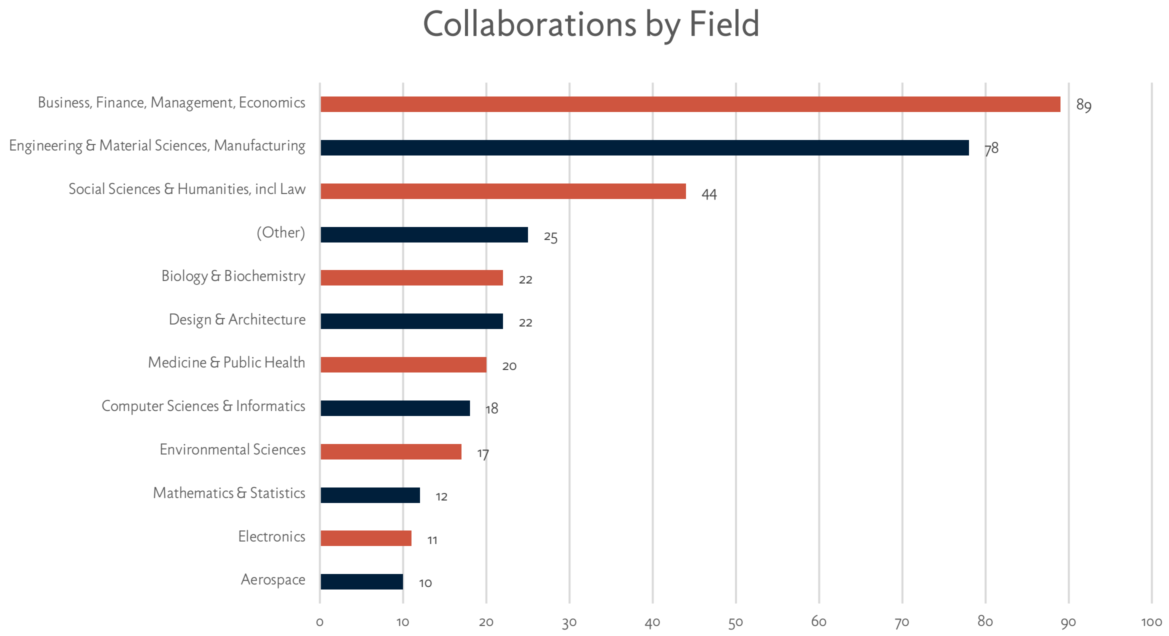

Figure 4: Collaborations by academic field

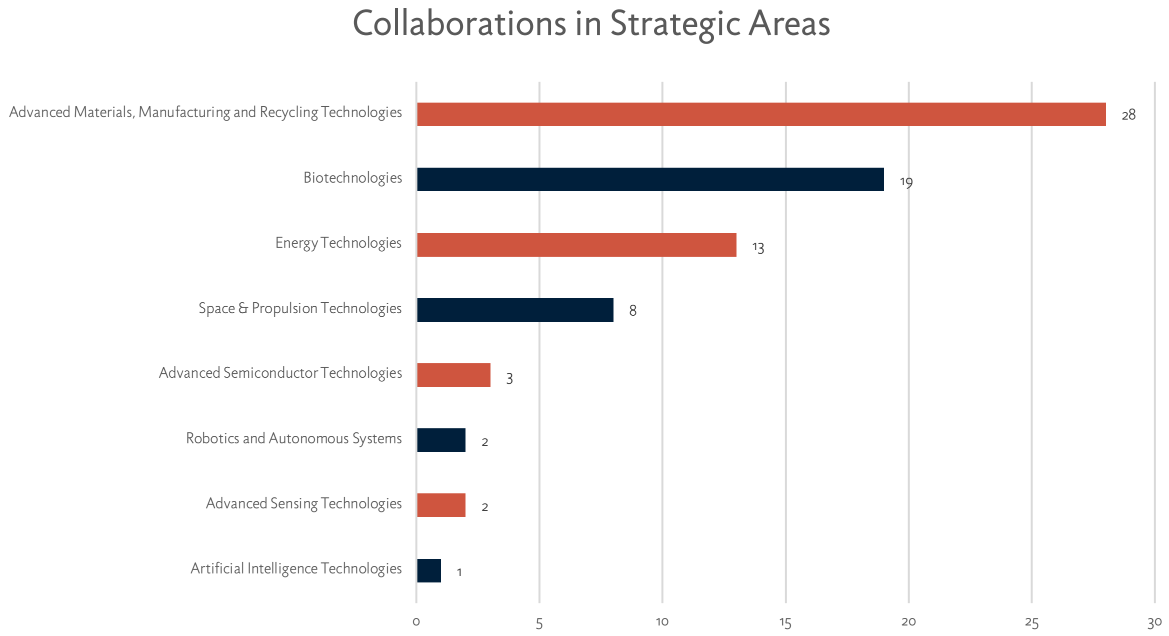

Figure 5: Collaborations in strategic areas

Since the goal of this analysis is to identify cases with potential technology transfer risks, a further criterion was included where we excluded joint undergraduate-level study programs from this list, since such programs do not generally aim to generate or share groundbreaking technological inventions. The numbers in Figure 5 reflect either joint research projects or joint postgraduate study programs, which are more likely to include the types of technologies policymakers and universities should scrutinize more closely.

The three areas of potential strategic interest with the most collaborations are **Advanced Materials (Manufacturing and Recycling Technologies), Biotechnologies, and Energy Technologies**, accounting for around two-thirds of the total number. A closer look at a country breakdown for some of the major critical technology areas reveals that they tend to reflect the broader spread of academic collaborations. The **United Kingdom** has the largest number of collaborations in these fields, followed by Germany and France. All these technology areas can be considered highly pertinent to the EU's goals of strategic autonomy and various areas of security. They also have considerable dual-use potential, especially within the advanced materials and biotechnology fields.

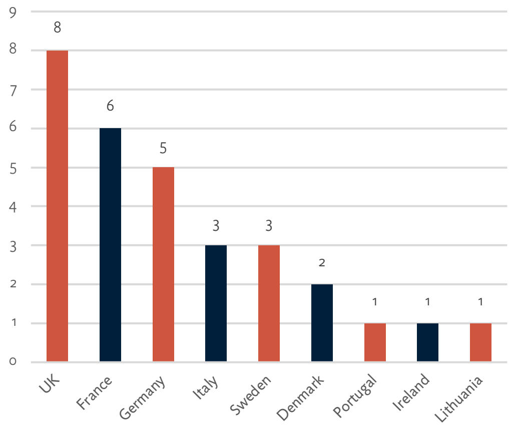

Figure 6: Advanced Materials

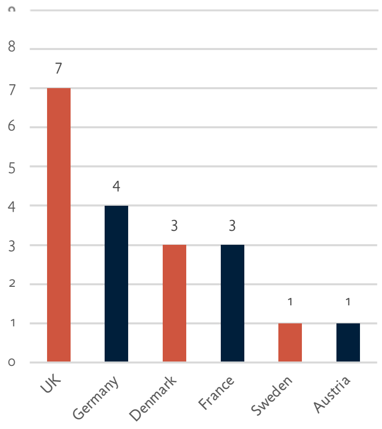

Figure 7: Biotechnology

For example, within Advanced Materials, the Chinese universities with the most collaborations are:

1) Zhejiang University (7 collaborations);
2) Sichuan University (3);
3) Tsinghua University (2).

While the critical field of AI has fewer overall collaborations, there are some notable examples. For instance, there is an active joint PhD program on AI and Bioscience between Leiden University in the Netherlands and Xi'an Jiaotong University, which has recruited 30 students since starting in 2020, and was jointly funded with the Chinese Scholarship Council.

Datenna's platform data shows that all the four Chinese universities, Zhejiang, Sichuan, Tsinghua and Xi'an Jiaotong, are labeled as Defense-related institutions with many dual-use patents and, with some institutions, a history of participating in defense procurements.

/ 4. Case Study: Beihang University

In this next section, we will zoom in on an individual Chinese institution to showcase how the risk factors discussed above can appear in practice. Using Datenna's platform, **we can demonstrate how to utilize data to offer deeper insights on a company's linkages and activities that can potentially give cause for concern**. Beihang University can serve as an example of a high-profile university with known defense links, is one of the 7S universities, is particularly prominent in aerospace research, and is also engaged in multiple collaborations with European institutions. Beihang is known to conduct a large amount of research related to aerospace and rocketry, among other fields that the EU and NATO have named as "strategic." It hosts various national-level laboratories, including two State Key Laboratories: one on software development environments and one on virtual reality technology as well as national research centers on satellites, big data, and materials manufacturing-related fields. These are research centers considered critical and receive support from the central government.

However, simply stating that a university is known for its defense-related research and military links does not necessarily provide enough insight to determine the viability and potential risks of a particular collaboration. For this, we need more granular and specific data on a university's activities.

Beihang has, or has had, collaborations with multiple European universities in fields identified as "strategic" in the European Commission's 2023 recommendations on strategic technology risk assessment. These include space & propulsion technologies and advanced materials.[16]

Multiple European universities in five different countries have established collaborations, both research institutes and joint study programs, with Beihang University during the last 20 years.[17] High-profile cooperations include universities in France (Paris-Saclay and Lorraine with joint PhD programs, as well as the Sino-French Engineering School of the Ecole Centrale established in 2005). Other collaborations include a Dual Master Degree Program in Economics and Management with Vrije Universiteit Brussel, a double PhD program with Eindhoven University of Technology, and a joint education and research center with the Technical University of Madrid. An international group of several UK institutions such as the Universities of Edinburgh and Leeds established the International Research Center of Big Data Science and Engineering. RAL Space in the UK and Beihang established the UK-China Virtual Joint Space Laboratory. In addition, the IMDEA Materials Research Institute founded by Madrid's central government established the Spain-China joint research center of advanced materials (JRCAM), with Beihang as well as several Spanish universities including the Technical University of Madrid as partners.

[16] While this report does not make claims as to any particular collaboration or project conflicting with the EU guidelines, we aim to draw attention to the presence of potentially risky research and present ways to conduct due diligence using granular institute-level data. The purpose of this section is not to make judgements on the appropriateness or the precise level of security risk in any of the individual collaborations mentioned. Instead, it serves as a showcase on how different institute-level data can aid in conducting due diligence and deciding the appropriate scope for a collaboration.

[17] The majority of the programs are still active with two having been removed from the websites of their respective universities, indicating they may have been discontinued. As for research centers, confirming their current status is at times more difficult due to their smaller public profile. However, we found most of them to continue to be in operation. Regardless of their current status, the past establishment of these programs speaks to a mutual interest between universities and can still act as a demonstration case on mitigating risk.

Patents as Indicator for Military and Dual-Use Research

A general look at Beihang University through Datenna's databases shows several indicators of activities that may be of concern to academic collaborators. It holds several hundred patents that have been given a defense label according to our methodology, indicating that potential military or dual-use technologies are involved. A search of patents with the keyword "aerospace" yields 460 results, and several dozen defense-labeled patents including rocket engine and wing technologies, and various advanced material-related patents.

While the overall number and variety of patents are significant, the general trend shows that many of them are related to **missile and aerospace applications**. They range from materials-related, such as flight device materials, reinforced frame structures and engine technologies to launching devices, remote sensing and guidance applications for missiles, as well as software technologies and applied semiconductor technology. For example, Beihang University possesses a patent on a Field Programmable Gate Array (FPGA, a type of integrated circuit that allows users to reconfigure the hardware to meet specific requirements after manufacturing) -based ground launching control device for small and medium-sized rockets.

In addition, a search with the keyword "frame" yields multiple **defense-labeled patents**, including an "integrated platform for missile assembly and transportation" and applications related to materials manufacturing such as a frame-covering missile wing structure. In total, there are hundreds of patents of potential dual-use or military interest, and these are just some that have been picked for potential connections to areas considered strategic by the EU.

The presence of these patents is an indication that a large volume of military and dual use-related research is taking place at Beihang. While it is not in itself proof that technology transfer or military technology development is taking place in the context of academic collaborations with European universities, this information can help determine whether the particular research projects being pursued are a cause for concern in each university's individual context. Datenna's patent data also shows the names of the relevant inventors, allowing users to screen for potential risks.

Military Procurements & Foreign Sanctions as Risk Indicators

Our data also shows **around 200 procurement calls in which Beihang participated**. Some of these are for military actors such as the Central Military Commission, Academy of Military Sciences, the PLA, and the China Aerospace Science and Technology Corporation (an SOE with an important role in China's space program). The broad range of different military-affiliated organizations that Beihang has submitted bids for indicates that many of its research areas and technologies are of interest to China's military ecosystem. Beihang evidently possesses considerable readiness to supply these organizations.

The procurements themselves involve various fields, many of them related to engine technology, launchers, aerospace materials, as well as related computer systems. There are also some that concern fields as specialized as psychological evaluation systems for the People's Liberation Army. These are all bids in which Beihang participated and won. This shows that it can be very difficult to determine in advance which academic fields potentially run the risk of contributing to military organizations in China, without first conducting a detailed data-based evaluation.

We can also see that Beihang was included in two different **sanctions lists** by the **U.S. and Japanese governments**. It has been listed since 2005 in the U.S. Bureau of Industry and Security Entity List and the Japanese Ministry of Economy, Trade and Industry's End User List. The Japanese list mentions "potential involvement in development of weapons of mass destruction (missile)" as the cause for being included in its list.

Varied and Complex Avenues for Military Collaboration

This information shows that an institution's links to the military-industrial complex in China can be wide-ranging and that gathering the relevant information can be a laborious process and hindered by a lack of transparency. Nevertheless, **being able to determine as accurately as possible the risks involved in a given collaboration is crucial while conducting due diligence**, and this is often difficult to do accurately without specialized resources. Identifying areas where a lot of procurements take place, or many defense-related patents are issued, can constitute an important step in the process.

Considering the large volumes of research related to aerospace and projectiles on the one hand and software-related research on the other, as well as the close military links of the university, **universities should consider the history of particular research projects and whether these have resulted in dual use patents**. Universities should carefully consider collaboration especially when it concerns fields or researchers with a history of producing such research work. It is important for universities to build capabilities for screening potential partner institutions. This can become especially pertinent in case new legal obligations are placed upon universities to screen against technology transfer and related risks on the national or EU level. In such instances, having access to detailed data on the institutional level in China can become a valuable tool in conducting due diligence.

/ 5. Conclusion

This report has presented a method for conducting due diligence on Chinese entities. This method can be used for due diligence on potential or current collaboration partners of European universities. In this report, we first conducted large-scale online research to identify a list of collaboration partners and then combined these findings with Datenna's platform containing data on institutional links, sanctions notices, procurements, research projects, and patents. In this way we were able to first gain a broad look at the most common collaboration partners and then demonstrate the insights that using Datenna's OSINT-based platform can provide in support of doing research on potential collaboration partners. This demonstrates the kinds of data that can help fill knowledge gaps that exist in dealing with Chinese universities.

Of course, access to data needs to be combined with interpretative capabilities that include a familiarity with the Chinese academic landscape and a well-developed understanding of the home university's values, policies, and priorities to know what factors should be considered "red flags" in Chinese universities. There is no universal answer to these questions, and they should be answered based on national, institutional and disciplinary circumstances and guidelines and can also change with time. **The toolbox needed for the screening and de-risking of academic collaborations consists of many parts but the access that large,**

data-driven service provides proves to be crucial in gaining a vantage point toward the Chinese academic landscape.

Lastly, it is important to remain aware of the **large scale of defense-related activities of Chinese universities** beyond the 20 that we have looked at in this paper. A characteristic of the interaction between the academic landscape and the national defense fields in China is the large number of links and interactions that are present at various levels. **Datenna's platform has data on thousands of academic institutes, of which over 2,000 have been flagged as being involved in defense-related activities**. While the 20 in this report constitute some of the most important of these, an awareness of this larger landscape remains essential. Only by accurately identifying the breadth and depth of the defense links of universities can we effectively manage the risks involved in collaborations.

This report was compiled with care by Datenna B.V. (Datenna). While Datenna has made every effort to ensure the accuracy and completeness of the data presented, we acknowledge that inaccuracies may exist. At the time you read this report, the information might not be up-to-date. If the reader notices any inconsistencies or errors, please contact the Datenna team. Datenna assumes no responsibility or liability for any loss or damage resulting from the use of or reliance on this information.