•	•		•		•	•	0	•	•	•	•	•	•	•	•	•		۰	•	•	•	•	•		•	•	•	•	•
•	۰		٠	٠	•	۰	0	٠	•	٠	۰	•	٠	٠	٠	•	•	0	0	0	0	٠	•	•	•		•	•	•
٠	•	٠	•	•	•	٠	٠	•	•	•	•	•	•	•	•	•	٠	٠	•	•	٠	•	•	•	•	٠	•	٠	٠
	•		•	•	•	٠	٠	•	•	•	•	•	•	•	•	•	٠	٠		•	0	•	•	•	٠	٠	•	٠	0
•	•	٠	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	٠	٠	•	•	•	•	•	•	•	
•	•	٠	•	•	•	•	•	•	•	•	٠	•	•	٠	•	٠	•	٠	۰	٠	٠	٠	•	•	٠	•	•	•	•
٠	٠	٠	٠	•	٠	٠	٠	٠	٠	٠	٠	•	٠	٠	٠	٠	٠	٠	0	0	٠	٠	0	•	٠	٠	0	٠	0
•	•		•	٠	•	٠	•	•	٠	•	٠	•	•	•	٠	•	•	٠	•	٠	•	•	•	•	٠	•	•	•	٠
•	٠	•	٠	۰	•	٠	0	۰	•	٠	•	•	۰	•	۰	۰	۰	0	•	•	•	•	0	0	0	٠	0	٥	0
٠	•	٠	•	٠	٠	٠	٠	•	٠	٠	٠	•	٠	٠	٠	٠	٠	٠	•	•	•	•	•	•	٠	•	•	•	0
•	•		۰	•	•	•		٠	٠	٠	•	•	٠	•	٠	٠	٠	0	٠	•	•	•	•	•	•	•	0	0	٠
•	•	۰	٠	•	٠	٠	٠	•	•	•	•	•	•	•	•	•	٠	•	•	•	•	•	•	•	٠	•	•	۰	0
•	•	۰	٠	•	٠	٠	٠	٠	•	•	•	•	٠	•	•	•	٠	•	•	•	•	•	0	٠	٠	•	0	٠	۰
•	•		۰	•	•	•	٠	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	0	•
•	۰	٠	•	•	•	٠		۰	•	٠	•	•	•	•	•	•	•	•	•	•	•	•	•	•	0	•	0	•	•
•	•	۰	٠	•	•	٠	0	•	•	٠	۰	•	•	•	•	•	٠	•	•	•	•	•	•	•	٠	•	0	۰	۰
•	•	۰	•	•	•	٠	٠	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	۰	0
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	0	•	•	•	0	•	0
			•				•																		•			•	
•		•	•		•	٠	0			•	•	•	•	•	•			٥	0	0	0	•	0	•	•		0	•	0
	•	•	۰	•		•	•	•		•			•	•		•	•	•	•	•	•		•		•	•		٠	0
	•	•	•	•		٠	•	•		•		•	•			•	•	•	•	•	•	•	•		•	•	•	٥	0
•	•	•	•	•		٠	•	•		•		•	•			•	•	•	•	٠	•	•	•		•	•	•	•	0
•	•	٠	٠	•	•	•		31		à	.	ti	'n	Ċ	ſ	'h	5	ŀ	N I		*) C				•	٠	٠	0
0	•	٠	٠	٠		•		a		ŏ	đ	ĻI		ŏ			Ģ		ÇI	įŞ	55	5	Q		ų	•	•	٠	0
•	•	•	•	•					•		•		•	•		•	•	•	•	•	•	•	٠	•	•	•	٠	•	٠
•	•	۰	۰	•	•		S	K	5	In		51	n	0		U	r	0	De	22	r	•	٠	•	٠	•	•	۰	٠
٠	•	۰	٠	٠	0	•	•		0	•	•		•	•	•	0		•			•		٠	•	٠	•	٠	۰	0
•	•		٥	٠	•	4	Ca	3 C	le	n	ni	Ċ	C	0		a	b	Ö	r'a	t	Ó	n	Ŝ	•	٠	•	•	۰	0
•	•	۰	•	•	. –	•	-			•	•	•		Ŭ	•							•	•	•	٠	•	•	۰	0
•	•	٠	•	•	•	٠	•	•	•	٠	۰	•	٠	٠	۰	•	٠	٠	0	•	۰	٠	•	•	۰	•	0	•	0
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	0
		•	•							•								•			•				•			•	
•	•		•	•		•	•	•		•			•	•			•	•			•	0			•	•		•	
	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	0
•	•	•										•	•			•	•	•	•	•	•		•		•	•	•	•	0
•	•	0	٠	4		1	n			R	٠	•	•	٠	٠	•	٠	٠	0	٠	٠		•	•	٠	•	•	٠	0
•	•	•	•	U	d	Lt			d		•	•	•	•	•	•	•	•	0	0	0	•	0	•	•	•	0	•	•
•			•	•	•	٠	•	•	•	•		•	•	•		•	•	٠	•	•	٠	•	•		•	•		٠	•

Introduction: China as an Academic Power - the Pros and Cons of Collaboration

Concerns about the security risks of Sino-European academic collaborations have increased during the Xi Jinping era as China has, on the one hand, raised the level and volume of its research output and emerged as a geopolitical competitor on the other. Growing awareness of the connections between technological, economic and national security has increased the need for identifying risks 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. This has been accompanied by significant increases in international linkages such as joint research centres, 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, military entities, and dual-use technology development in the Chinese academic party involved in the collaborations.

Datenna's data is particularly suited to addressing several interrelated forms of risk that have been identified in discussions around knowledge security and that will be the focus of this report. They all 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 organisation'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 defence industry through procurements and other commercial activities that are commonplace in the Chinese university sector.¹

¹ Nature: What China's leading position in natural sciences means for global research. <u>https://doi.org/10.1038/</u> <u>d41586-023-02159-7</u>

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 EU and the 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 purpose - diminishing Europe's technological edge in the process. This can in turn **threaten Europe's broader security, whether militarily or economically**. 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), the October 2023 recommendation on critical technology areas for the EU's economic security, and the January 2024 European Commission proposal for a Council recommendation on enhancing research security.²

The latter document gives recommendations for European practices on **balancing academic freedom and international openness with security priorities**. Emphasising the crucial role of exchanges for scientific progress but simultaneously recognising 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". This broadly characterises 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 emphasise 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 instrumentalisation of research and innovation."3

The recommendation on enhancing research security formulates a four-stage risk appraisal framework, considering: 1) the risk profile of the EU-based organisation, 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 in particular 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.

² <u>https://research-and-innovation.ec.europa.eu/document/download/e82a2fd9-ac12-488a-a948-87639eef1od4_en</u>, <u>https://</u> defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economicsecurity-further_en

³ Commission proposal on enhancing research security, p. 12-13

The challenges of implementing a necessary degree of de-risking and protecting knowledge security are real, considering the often-limited resources universities 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 in order to better conduct due diligence in universities. Shared capabilities, when developed collaboratively, can be a very 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 analysing potential academic partners and making well-informed assessments of associated risks.

Various national approaches and the challenges in accessing information

The potential risks of collaboration with China have prompted varied discussions in different European countries around practical ways to mitigate risk. The Netherlands released their National Guidelines for Knowledge Security for knowledge sector organisations 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. On the institutional level, the guidelines offer a number of points for consideration, including potential governmental or military/defence affiliation: whether it is a sanctioned entity, the general reputation of the institution and the other activities of the researchers involved.⁴

The 2023 German Federal China Strategy expresses support for increasing student and researcher exchanges with China.⁵ The German Rectors' Conference has also released their own statement that also expresses broad support for continued engagement but encourages establishing practises and structures for mitigating risks in sensitive research.⁶ Other countries like the UK and Sweden have also released guidelines with broadly similar foci but not specifically addressing China - emphasising greater awareness and holding on to European principles of research and ethics.⁷

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 recommendations according to which the institute should not engage in research cooperation

^{4 &}lt;u>https://www.nwo.nl/en/knowledge-security</u>

⁵ https://www.auswaertiges-amt.de/blob/2608580/49d5ofecc479304c3da2e2079c55e106/china-strategie-en-data.pdf

⁶ <u>https://www.hrk.de/resolutions-publications/resolutions/beschluss/detail/guiding-questions-on-university-cooperation-with-the-peoples-republic-of-china/</u>

⁷ Overview of different national guidelines in: <u>https://www.amo.cz/wp-content/uploads/2022/09/HTDTR_report_how-to-do-</u> <u>trusted-research_A4_18_web.pdf</u>

with universities with ties to the PLA, national defence universities or designated national defence laboratories in China.⁸

In general then, 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 defence-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 practises and resources for mitigating risks in research collaboration while avoiding undue restraints on international research and the benefits it can bring.

⁸ <u>https://orgchart.mit.edu/system/files/reports/20221007-AssociateProvost-University-Engagement-with-China.pdf</u>

The Dataset: the European Collaborations of 20 Chinese Universities

This paper can offer several contributions to the developing debate and practises 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**, comprising the top 13 universities in academic rankings, and the Seven Sons of National Defence (7S) - universities known for their established position in China's military development ecosystem. These were chosen for their size and importance within the Chinese 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 data, 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.

In addition, the report presents **case studies on individual collaborations of interest** that we identified. Here we used Datenna's broader database as it contains information on the institutional and commercial links of Chinese institutions as well as data on their operations, such as patents and research projects. This data makes it possible to zoom in on certain institutions of interest once these are identified through the macro-level dataset.

Sino-European academic collaboration through the numbers

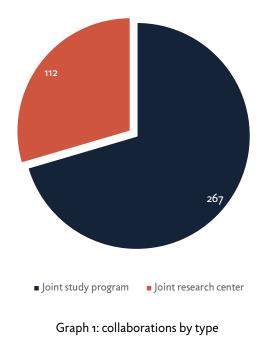
We divided the programs discovered during our research into two categories: **joint study programs** and **joint research centres** between European and Chinese universities. Of the 20 Chinese universities we tracked 379 collaborations falling under these broad categories were found.⁹

Out of the 379 collaborations, 267 fall under joint study programs and 112 under research centres (graph 1 on the next page). While it may sometimes be difficult to make a clear distinction between the two categories, our analysis attempted to identify the primary purpose of a collaboration and categorise it accordingly. For example, a joint undergraduate or master's level program will usually be relatively easy

⁹ 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 institutionalised forms of collaboration aiming to create more durable links between institutions and creating more lasting sets of commitments.



to categorise under "study programs" but joint PhD programs inherently also involve research. However, we established that a categorisation under "research centres" should involve a permanent staff, a research agenda, and a stable institutionalised structure with the primary purpose of conducting research even though postgraduate training may also be organised. Therefore, we found that in the majority of cases the categorisations were fairly clear.



A macro-level look: Collaborations in the 20 key universities

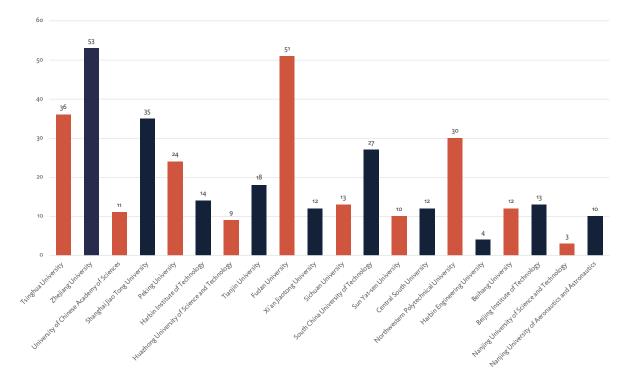
Among the 20 universities we tracked, our data reveals certain standout institutions that have a **large number of cooperation projects** with a fairly high level of disparity between the most and the least popular universities (graph 2):

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

With the exception of Northwestern Polytechnical University, all of the top five universities are highprofile, 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.



Graph 2: number of collaborations by university

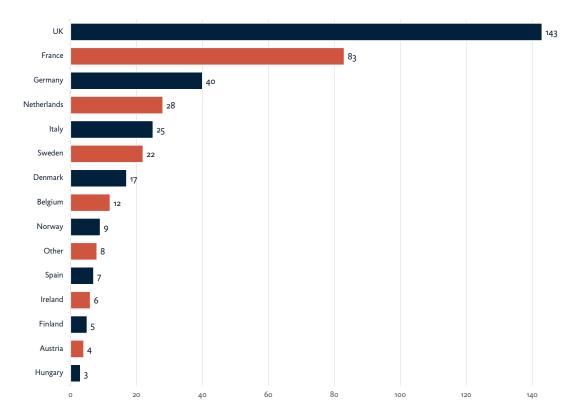
Northwestern Polytechnical University, on the other hand, is part of the 7S grouping as well as the E9 group of engineering universities. The 7S stand for a group of seven Chinese universities that are currently under the management of the Ministry of Industry and Information Technology. The focus of these universities revolves around R&D in various technologies and science of which a significant proportion have dual-use applications. In order to do this, they receive funding from the Chinese Ministry of State and Security. They also play an important part in the Chinese defence 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.

One notable finding is that in screening these 20 universities using Datenna's platform, we found that all of them had been flagged as defence-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 defence links of the 7S, activities of potential military significance are present in practically all of the institutions included here. While this does not necessarily tell us that the same is true of the wider Chinese university landscape outside of our sample, 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 risk at the level of institutions as identified in the European and national-level policy documents.



Graph 2 also shows that, generally speaking, high-profile generalist institutions like Zhejiang University tend to have more collaborations but specialised 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 Defence. 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.

The countries included in the dataset are European countries that are members in the EU and/or NATO (graph 3). We find that the UK has, by some margin, the most individual collaborations with 143, followed by France with 83. In third and fourth 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



Graph 3: collaborations by European country



countries such as Portugal, Romania, Lithuania and Bulgaria only appear in the dataset once, and some European countries were not found to have any collaborations.¹⁰

The high proportion of UK and French universities is not surprising considering their overall high number of universities and level of internationalisation. These countries also rank among the top in Europe when it comes to the number of international students from China. Nordic countries also feature fairly 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.

Collaboration fields

We also analysed the fields of collaboration with a particular interest in tracking how many of these potentially fall within a **strategic or dual-use category**. Graph 4, on the next page, shows the overall number of collaborations in different academic fields.¹¹

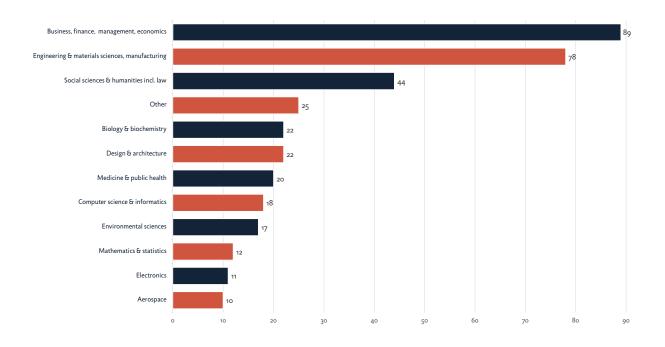
We see that the major fields in which collaborations take place are related to **business**, **finance**, **management and economics alongside engineering and materials science fields**. Together they account for almost half of all collaborations. Other more minor but still interesting groups include aerospace with 10 collaborations an AI & automation with five. Other fields are more evenly divided, with the social sciences, environmental sciences and architectural and design fields having a relatively large number of collaborations.

In graph 5, we see that a total of **81 of the 379 collaborations** can be determined to fall under 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 the EU's economic security strategy.¹² Lists of priority technologies released by other organisations such as NATO, while not fully overlapping, share a similar focus on areas such as AI, quantum, advanced materials and biotechnology. We can thus assume that these fields represent a broad consensus of what research areas are considered to fall under the scope of protecting knowledge security.

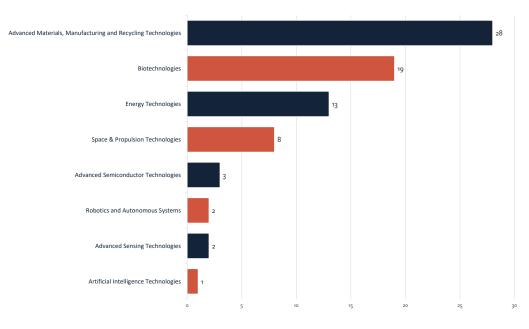
¹⁰ While interpreting this numerical data on collaborations between institutes in different countries, it is important to keep in mind the limitations of this targeted dataset. First, only focusing on a select group of 20 Chinese universities doubtlessly leaves out many interesting collaborations between 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 can not always be completely verified.

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

¹² <u>https://defence-industry-space.ec.europa.eu/document/download/d2649f7e-44c4-49a9-a59d-bffd298f8fa7_en?</u> <u>filename=C_2023_6689_1_EN_annexe_acte_autonome_part1_v9.pdf</u>



Graph 4: collaborations by field

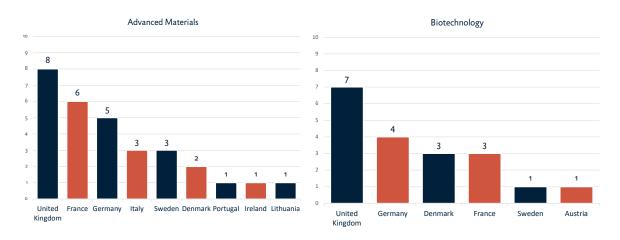


Graph 5: collaborations in strategic areas

Since the goal of this analysis is to identify cases with potential technology transfer risks, a further criterion was included in the analysis 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 graph 5 thus reflect either joint research projects or joint postgraduate study programs, more likely to include the types of technologies policymakers and universities should scrutinise 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** having the largest number of collaborations in these fields, followed by Germany and France. All of 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 with advanced materials and biotechnology.



Graph 6: amount of projects in selected strategic technology areas. Right: advanced materials; Left: biotechnology

For example, considering Materials Science, the Chinese universities with the most collaborations are:

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

For an important field like AI with fewer overall collaborations but clear strategic significance, a joint PhD program on AI and Bioscience between Leiden University in the Netherlands and Xi'an Jiaotong University has been active, recruiting 30 students starting in 2020 and was jointly funded with the Chinese Scholarship Council. This collaboration touches upon two potentially strategic areas. Importantly, Datenna's platform data shows that all of the four Chinese universities, Zhejiang, Sichuan, Tsinghua and Xi'an Jiaotong, are labelled as Defence-related institutions with many dual-use patents and, with some institutions, a history of participating in defence procurements.

Case Study: European Collaborations with Beihang University

Above, we have looked at macro-level data on Sino-European university collaborations. Next, we will zoom in on an individual institution to showcase how the risk factors discussed above can appear in practise. Using Datenna's platform, we can demonstrate how to utilise 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 defence links, being one of the 7S universities and having a particularly prominent role in aerospace research, that 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 centres on satellites, big data and materials manufacturing related fields. These are research centres considered critical and receive support from the central government.

However, simply stating that a university is known for its defence-related research and military links does not in itself necessarily provide enough detail 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. While this report does not make claims as to any particular collaboration or project being in conflict 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.

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.¹³ 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). Vrije Universiteit

¹³ 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 centres, 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.



Brussel established a Dual Master Degree Program in Economics and Management. Eindhoven University of Technology a double PhD program, and the Technical University of Madrid a joint education and research centre. An international group including several UK such as the Universities of Edinburgh and Leeds (International Research Center of Big Data Science and Engineering), as well as RAL Space in the UK (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 centre of advanced materials (JRCAM), with Beihang as well as a number of Spanish universities including the Technical University of Madrid as partners.

Patents as an indicator of 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 Defence 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 Defence-labelled 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. To give an example, Beihang University possesses a patent on an 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 **Defence-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. Patent data also shows the names of the relevant inventors, allowing users to screen for potential risks.

Military procurements and foreign sanctions are additional 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 organisations 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 organisations.

The procurements themselves involve various different 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 specialised 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 organisations in China, without first conducting a detailed data-based evaluation.

We can also see that Beihang has been 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 Japan 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 the 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 wideranging 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 specialised resources. Identifying areas where a lot of procurements take place or many defence-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 institution level in China can become a valuable tool in conducting due diligence.



Conclusion

This report has presented a method for conducting due diligence on Chinese entities that can be used on 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 on the most common collaboration partners and then demonstrate the insights that using an 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 decided 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 defence-related activities of Chinese universities** beyond the 20 that we have looked at here. A characteristic of the interaction between the academic landscape and the national defence 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 defence-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 defence links of universities can we effectively manage the risks involved in collaborations.

/ About Datenna

Datenna is an open-source intelligence (OSINT) software company and the leading data provider of techno-economic intelligence on China. Our proprietary intelligence platform is built entirely on publicly available information that is translated into actionable open-source intelligence. This information is delivered exclusively to allied governments to empower them in their mission to safeguard economic and national security. For more information, visit our website at <u>www.datenna.com</u>.

