Eyes Wide Open

ETHICAL RISKS IN RESEARCH COLLABORATION WITH CHINA

Jeffrey Stoff and Glenn Tiffert

A PUBLICATION OF THE HOOVER INSTITUTION

A HOOVER INSTITUTION REPORT

Eyes Wide Open

ETHICAL RISKS IN RESEARCH COLLABORATION WITH CHINA

JEFFREY STOFF AND GLENN TIFFERT

December 2021

This report presents a case study of the Chinese Academy of Sciences Institute of Automation (CASIA), a global leader in education and research on artificial intelligence, biometrics, and neuroscience. CASIA exemplifies a class of entities—common to authoritarian nations—that simultaneously pursue beneficial and reprehensible lines of research. While its subdivisions and commercial affiliates undertake projects that advance human welfare and the frontiers of knowledge in areas such as medicine, they also partner with public security organs on mass surveillance technologies associated with human rights violations, particularly in the Xinjiang region.

US research institutions and companies collaborate extensively with CASIA. Yet the ethical and integrity risks of those collaborations receive insufficient scrutiny and may compromise democratic values as well as sanctions, export controls, and other policy measures adopted by the US government in response to repression by authoritarian regimes. The US research enterprise must develop nuanced knowledge and procedures for grappling with the dilemmas that collaboration with Janus-faced entities such as CASIA entails.

The report makes the following recommendations:

- Research institutions and governments should revise existing concepts of research integrity to ensure consistency with democratic values, and define a common standard or set of conditions for ethical reviews of research that considers legal and political context and ethical and human rights risks. These reviews must include, for example, protocols for affirmatively validating the provenance of personally identifiable information and biometric and genetic datasets, and their compliance with standards of ethics and informed consent; planning for scenarios such as the diversion of research and data to organs of China's party-state; and concrete deliberation over the potential for lines of research that seem comparatively benign in a democratic polity to serve abhorrent ends in an authoritarian one.

- Federal agencies should deny or remove funding for research projects that involve collaboration with entities, based in authoritarian nations, that support mass surveillance and human rights abuses.

- The US Department of Commerce should place CASIA and the affiliated businesses discussed in this report on the Entity List for export controls.

- Academic and private sector organizations should review their partnerships with CASIA and its affiliates for risks to human rights, and to research ethics and integrity.

- Civil society institutions should work together to develop knowledge and promote robust due diligence and information sharing on suspect entities based in authoritarian nations in order to uphold ethical standards and protect human rights.

EXECUTIVE SUMMARY

US research collaboration with entities based in authoritarian states presents unique ethical and national security challenges because those entities may "be indifferent or hostile to [US] values and exempt from comparable standards of transparency or accountability."[1] This is particularly true for the People's Republic of China (PRC), where state-controlled research institutions have obfuscated their activities and associations, incentivized unauthorized transfers of intellectual property or know-how, and engaged in other questionable practices that undermine human rights and the integrity of scientific research. Potential research partners from China and other authoritarian states therefore warrant more intensive vetting than those from democratic nations.

China's public security and mass surveillance apparatuses play a central role in the human rights abuses perpetrated by the Chinese Communist Party (CCP) and PRC government ("party-state"). These abuses affect all of China's civil society but are most conspicuous in the Xinjiang region, where the party-state oppresses Muslim minorities. They include unprecedented mass racial and "pre-criminal" profiling; coerced mass collection of biometric and genetic data; ethnic oppression; arbitrary detention and mass internment of at least one million Uighurs in concentration camps; family separation; and allegations of forced sterilization of women, rape, torture, and forced labor. China's public security and mass surveillance apparatuses are arguably the most technologically sophisticated in the world.[2]

The US government has sought to restrict trade with PRC entities that supply, support, or are part of those apparatuses.[3] However, the research ecosystem foundational to this supply chain has received insufficient attention. This is particularly the case for PRC research institutions that drive the commercialization and weaponization of surveillance applications for public security and mass surveillance purposes. Compounding this knowledge gap is the fact that it can be difficult to separate public security applications from commercial and defense applications of a given technology, and a prospective research partner may support all three. Given the authoritarian context, we must consider these intersecting applications together when vetting potential partners regardless of a project's stated aims. Yet firms and universities outside of China routinely fall short of that standard and have established research collaborations and partnerships without adequate awareness of the potential harms, ethical considerations, and reputational risks at stake in those relationships.

This report addresses some of these deficiencies with a case study of a PRC institution that boasts prestigious international partners despite its key supporting role in China's public security and surveillance apparatuses: the Chinese Academy of Sciences Institute of Automation (CASIA). The report supplies a framework for conducting due diligence that examines not only CASIA's mission and organizational elements but also its research activities, published research output, and commercial spin-offs and partnerships. This degree of scrutiny is essential to effectively evaluate the risks and implications of partnering with CASIA and PRC organizations like it.

Like many PRC research institutions, CASIA has a dual identity. On the one hand, it confers academic degrees and is an important contributor to global R&D in areas such as neuroscience and artificial intelligence (AI). On the other hand, it also serves the missions and mandates of an increasingly repressive and ambitious party-state, including developing ethically troubling mass surveillance applications for public security organs and technologies designed to supplant the economic and military supremacy of the United States. International entities that collaborate with CASIA on joint research must therefore weigh the strong possibility that CASIA, as an organ of the central government, will divert, direct, or attempt to commercialize or weaponize its research for public security and national defense purposes.

Research Design and Limitations

This report examines CASIA's research and commercial activities and domestic and foreign collaborations through in-depth research on CASIA's structure, programs, and affiliated business entities and investments, and through surveys of scientific and engineering literature published in both Chinese and English between 2014 and 2020. This dataset includes a corpus of more than 1,200 bibliographic metadata records[4] enhanced by supplemental research.

This report focuses on CASIA's activities concerning mass surveillance, public security, and defense applications. Although the report identifies research topics such as facial, iris, or gait recognition, it does not offer technical assessments or gauge the maturity or applicability of that research to surveillance or defense programs. Likewise, the report highlights examples of research collaboration between CASIA and the People's Liberation Army (PLA), major PRC defense conglomerates, and defense research institutions, but it does not comprehensively catalogue CASIA's projects or partnerships with every PRC institution that is known to support China's defense industry and research. Expanding the report's scope to encompass those entities, projects, and programs could reveal additional ethical or national security concerns.

Key Findings

CASIA, established in 1956, originally focused on space technologies for the PRC military. Since its absorption by the Chinese Academy of Sciences in 1970, CASIA's research

has focused on "intelligent technology" disciplines: intelligent processing of large data, intelligent control of complex systems, and "integrated intelligent systems."[5] CASIA plays a significant role within China's research pipeline on AI and related disciplines, which enable or enhance the capabilities of the nation's public security and mass surveillance apparatuses and their corresponding human rights abuses. CASIA's research also supports China's defense R&D and industrial base.

There are notable discrepancies between the English- and Chinese-language information that CASIA supplies about itself. Activities and partnerships of concern were usually found in Chinese-language sources. Given CASIA's extensive engagements with foreign research institutions and industry, these discrepancies suggest attempts to obfuscate CASIA's more sensitive programs or associations and underscore the necessity of conducting due diligence in native language sources.

1. Many of CASIA's research centers, laboratories, and other divisions declare partnerships with or conduct research in support of public security or surveillance projects.

    - CASIA's National Laboratory of Pattern Recognition plays a key role in China's surveillance-related technology development, and one of its subordinate divisions claims to be China's largest research institute specializing in biometric identification.

    - Other CASIA divisions conduct research on human gait and facial recognition, suspect targeting and tracking, and video analysis on object recognition and analysis of human actions for "abnormal behavior detection to serve the needs of public security."[6]

    - CASIA-affiliated researchers have coauthored or worked on projects funded by entities subordinate to the Ministry of Public Security and the People's Armed Police (PAP).

2. Tan Tieniu, a senior CASIA leader and renowned expert on computer vision and biometric recognition, collaborates on research internationally while overseeing domestic public security and surveillance projects. Tan concurrently serves as a deputy director of the PRC's government liaison office in Hong Kong. The US Treasury Department recently added Tan to its "specially designated nationals list" as part of the US government's sanctions on Hong Kong officials for their responsibility for a human rights crackdown in the city.[7]

    Tan has led numerous CASIA labs, research centers, and international collaboration projects focusing on biometric recognition, intelligent video surveillance, and network security for public security purposes. Tan's online biographies omit his associations with several CASIA-affiliated companies that produce surveillance technologies for PRC public security organs. Tan took up his post as deputy director of the central government's

liaison office in Hong Kong in 2016, not long after a cycle of pro-democracy protests began that culminated in the dismantling of the city's political autonomy and the detention and imprisonment of political dissidents.

3. CASIA's international collaboration is extensive. It includes foreign academia; companies such as GE, Dell, IBM, Microsoft, Intel, the European Aeronautic Defence and Space Company, and Nokia; US government partners; and projects funded by the US government.

4. At least five companies spun directly off CASIA's research programs provide surveillance products and services to China's public security organs and other companies supporting public security operations.

5. In addition to its research and partnerships supporting surveillance and public security, CASIA has partnered with the PLA; all of the "Seven Sons of National Defense" (国防七子) universities, which support defense programs as their primary mission; five of China's state-owned defense conglomerates; and a division of China's nuclear weapons complex. (This report catalogues CASIA's ties to China's defense R&D in appendix C).

Conclusion and Recommendations

The research in this report belies the scale and scope of CASIA's collaborations, partnerships, international engagements, and commercial spin-offs and investments that support public security and defense missions. CASIA's Janus-faced pursuit of both beneficial and reprehensible research should be a wake-up call to public and private sectors; state-run research institutions in the PRC may observe values that are deeply at odds with or even antithetical to those of their partners in liberal democracies. Adequately assessing the ethical dilemmas, risks, and challenges of engaging with PRC organizations like CASIA requires an extraordinary degree of due diligence. Therefore, this report offers the following recommendations:

1. CASIA, its subordinate research centers and laboratories, and the associated commercial enterprises identified in this report should be added to the Department of Commerce's Entity List. Private sector firms should terminate any relationships with CASIA or its associated businesses to avoid possible future regulatory compliance problems and reputational harm.

2. Research institutions based in the US and other democracies should review their collaboration (formal or informal), research partnerships, and related agreements with CASIA for risks to human rights, and to research ethics and integrity. Federal agencies should place restrictions that would deny or remove funding to principal investigators who collaborate with organizations such as CASIA that support mass surveillance and human rights abuses.

Research institutions in liberal democracies champion values such as freedom of expression and inquiry, transparency, and universal human rights. By contrast, many of those in the PRC commonly contravene these values. The extensive international collaboration that PRC research institutions like CASIA enjoy in spite of divergent values must not continue. Upholding ethical standards and protecting human rights should be a condition for collaborations with partners based in liberal democracies. As the National Security Commission on Artificial Intelligence stated with respect to dangerous and unethical uses of AI, "[US] government and research institutions share responsibility for protecting core values and countering malicious activities."[8]

3. Research institutions and governments in democratic nations must revise existing concepts of research integrity and expand the use of ethical review processes when the research involves collaboration with partners in China and other authoritarian nations. These reviews must include, for example, protocols for affirmatively validating the provenance of personally identifiable information and biometric and genetic datasets, and their compliance with standards of ethics and informed consent; planning for scenarios such as the diversion of research and data to organs of China's party-state; and concrete deliberation over the potential for lines of research that seem comparatively benign in a democratic polity to serve abhorrent ends in an authoritarian one.

   Existing approaches to scientific research integrity focus mostly on the research process; research misconduct is typically understood as fabrication, falsification, plagiarism, or undue influence from financial interests. Ethical reviews of research are typically limited to research involving human subjects and fail to adequately address privacy protections and data governance controls when collaborating with China. Collaborations with CASIA may not trigger any of these tripwires because the ethical concerns raised in this report lie instead with the research partners themselves and the end-uses of the research. Consequently, institutional or ethical review boards should be revised to include two additional procedures that would close gaps in oversight:

   - Research institutions should define a common standard or set of conditions for ethical reviews of research that does not involve direct participation of human subjects. For instance, any research conducted in collaboration with partners in authoritarian nations that has surveillance applications (e.g., facial, iris, or gait recognition, or other areas that seek to identify specific individuals) should be included.

   - Due diligence on potential partners based in authoritarian nations and the relevant political impositions and legal requirements that they are subject to must be conducted and incorporated into ethical risk evaluations.

   The effectiveness of these additional ethical review procedures will depend on robust due diligence research on foreign entities. Given the scale and complexity of such a task, this report offers a fourth recommendation to address this challenge:

4. Civil society institutions, such as think tanks, NGOs, private sector firms, government, academia, and the media should apply and expand upon the due diligence methodologies described in this report to identify and share information on other PRC-based entities that support or partner with China's public security apparatus.

   Academic institutions and businesses typically lack the resources or subject matter knowledge to conduct the type of in-depth due diligence applied in this report. A coalition of public and private partners within civil society, such as think tanks, NGOs, and the media, is needed to help identify and share information on other PRC institutions that, like CASIA, engage in reprehensible behaviors and undermine democratic values. Such efforts are intended to assist universities, researchers, and governments in upholding their values by making better, more informed risk assessment and mitigation decisions.

I: INTRODUCTION

As Glenn Tiffert explains, research organizations in authoritarian nations may "be indifferent or hostile to [US] values and exempt from comparable standards of transparency or accountability."[9] Academic institutions in China warrant particular scrutiny given that nearly all of them are overseen and funded by the PRC government and subject to the dictates of the Chinese Communist Party (CCP). These institutions can lack transparency, deliberately obfuscate their activities and associations, incentivize unauthorized intellectual property or intellectual capital transfers, and engage in other questionable practices that undermine human rights and the integrity of scientific research.

A recent Hoover Institution report, *Global Engagement: Rethinking Risk in the Research Enterprise*, examined China's exploitation of open academic research in the United States, much of which is lightly regulated and not subject to export or classification controls. That report focused on risks to US national security and to the US research and innovation ecosystem from collaborations between US institutions and PRC entities that directly support the PRC's defense R&D and industrial base. It argued that threat assessments need to look beyond the commonly used binary standard of (il)legality.[10]

This report exposes ethical risks—in addition to national security concerns—from research collaboration with PRC entities that support China's public security and mass surveillance apparatuses. These apparatuses are arguably the most technologically sophisticated in the world and play a key role in the human rights abuses that the CCP and PRC government carry out against China's population. These abuses affect all corners of China's civil society, but they are most conspicuous in the Xinjiang region, where the party-state targets Muslim minorities, particularly the ethnic Uighur population. The US Secretary of State has described China's actions in Xinjiang as "genocide" and "crimes against humanity."[11] These actions include unprecedented mass racial and "pre-criminal" profiling; coerced mass collection of biometric and genetic data; ethnic oppression; arbitrary detention and

mass internment of at least one million Uighurs in concentration camps; family separation; and allegations of forced sterilization of women, rape, torture, and forced labor.[12] The US Congress is also seeking to bolster enforcement of sanctions, export controls, and other policy measures to punish PRC entities engaged in such abuses.[13]

Scholarship and monitoring of China's surveillance and public security apparatuses has mainly focused on identifying supply chains and methods of oppression. These efforts must continue in earnest. At the same time, the foundations of these supply chains—the research ecosystem and infrastructure that form the basis of China's technical capabilities in this area, especially the PRC institutions and foreign collaborations that enable current and future commercialization and weaponization of mass surveillance applications for public security and defense purposes—have received insufficient attention and are not ordinarily examined as part of the due diligence that US research institutions conduct on their PRC partners.

Purpose of Report

This report addresses some of these deficiencies through a detailed case study of the Chinese Academy of Sciences Institute of Automation (CASIA, 中国科学院自动化研究所). It supplies a framework for rigorous examination of CASIA's organizational structure, mission, and research programs, published research output, and commercial spin-offs and partnerships that support China's public security and mass surveillance apparatuses. In authoritarian nations such as the PRC, it is difficult to separate public security applications from commercial and defense applications of a given technology. CASIA's related support to China's defense research and industrial base is therefore catalogued in appendix C.

This in-depth approach is vital to effectively evaluating the risks and implications of research collaboration between CASIA and institutions in the United States and other democratic nations. If this approach is extended to other PRC institutions, it can comprehensively map the R&D ecosystem that enables China's public security and mass surveillance apparatuses and their corresponding human rights abuses.

Making changes to formal or informal research collaboration can involve difficult or uncomfortable decisions. Indeed, PRC research institutions in many areas are important and substantial contributors to global scientific R&D. However, these institutions do not operate in the same way as institutions in liberal democracies do. This is particularly true with regard to organizations under the Chinese Academy of Sciences (CAS). While CASIA and other CAS institutes and laboratories contain academic components that confer degrees, CAS is a central government organ under the PRC State Council; it is run by and for the PRC government and the CCP. CAS missions and priorities are based on party-state objectives. This includes developing and utilizing advanced technologies to ensure political and social controls over China's population, and within economic and national defense

realms, dominating and displacing US technical and military supremacy and reshaping the world order—goals that do not align with US or allied nations' interests.

This last point is at the heart of the challenge facing liberal democracies when collaborating with partners in authoritarian nations. CASIA's mission and research programs themselves present a dilemma. On the one hand, CASIA undertakes important medical and neuroscience research and is involved in international collaboration that undoubtedly can benefit humanity, such as its brain mapping projects and brain-inspired AI research. On the other hand, CASIA simultaneously conducts research in areas such as human gait and facial recognition and suspect targeting and tracking, which have serious ethical implications and directly support China's mass surveillance apparatus and human rights abuses. International entities that collaborate with CASIA on joint research must therefore weigh the strong possibility that CASIA, as a government organ, will divert, direct, or attempt to commercialize or weaponize that research for public security and national defense purposes.

Research Design

This report investigated CASIA's academic research and commercial activities by the following methods:

- Retrieving information on CASIA's Chinese- and English-language websites that describe its organizational structure, research programs and activities, and stated domestic and international partnerships.

- Collecting and analyzing a corpus of bibliographic metadata[14] representing research published between 2014 and 2020 that includes: (a) 493 domestic science and technology (S&T) publications hosted on China National Knowledge Infrastructure (CNKI),[15] a major PRC online repository, to identify additional activities, funding sources, and collaborations (coauthorship) between researchers affiliated with CASIA and other PRC entities; and (b) searching English-language S&T publication aggregator *Dimensions* to collect and analyze a second corpus of bibliographic data on 744 articles that name a CASIA-affiliated coauthor and a coauthor affiliated with a US institution.

- Conducting supplemental research on select institutions collaborating with CASIA based on information derived from the corpora of bibliographic metadata to identify their organizational hierarchies (i.e., parent entities and subdivisions) and activities of potential concern. Additional research was conducted on some of the periodicals that published the articles as well as on sources of funding.

- Surveying CASIA's commercial endeavors such as CASIA-affiliated companies and their customers or partners.

Appendix D discusses methodologies and sources in greater detail to encourage others to replicate these processes. While this report identifies many of CASIA's activities of concern, it is by no means exhaustive, and its findings are subject to limitations.

Research Limitations

This report focuses on CASIA's research efforts involving topics that have clear surveillance applications, such as facial recognition, or involving collaborations with China's public security elements. It did not conduct technical assessments to determine the level of maturity of that research or assessments of its capabilities.

Due to scoping limitations, the report does not comprehensively survey all of the subdivisions, research groups, collaborative programs, and research projects described on CASIA's main website or the webpages of its subordinate entities. Further research may reveal additional areas and activities of ethical or national security concern.

The English-language portion of the collected corpus, which totaled 744 publication records, was too large to individually assess the risks of US collaboration with CASIA. The records were screened to identify surveillance-related articles, and a sample of those articles was read closely. The collected corpus focuses on US entities, but entities in many other nations appear to partner with CASIA, and they are encouraged to examine those partnerships carefully.

Also, CASIA's commercial spin-offs and investments are too extensive to adequately survey here for ethical or national security concerns. This report profiles five such businesses; yet CASIA has invested in about forty companies, most of which warrant similar scrutiny.

Appendix C reviews the S&T literature in the PRC to identify CASIA's connections to defense programs. However, that effort focuses on a subset of institutions whose primary mission is to support the PLA and the PRC's defense R&D and industrial base. It likely understates the extent of CASIA's broader involvement in or support to defense R&D. Furthermore, many of CASIA's publications and projects may have public security, national defense, and commercial applications, including reconnaissance drones, autonomous vehicles, and object detection, targeting, and tracking. This report refrains from arbitrarily distinguishing them, even when no partner is specified.

II: OVERVIEW OF CAS INSTITUTE OF AUTOMATION

CASIA was established in 1956 as the Institute of Automation. In 1968, it was transferred to the China Academy of Space Technology and renamed the Institute of Space Control Technology, also known as the 502 Institute of the PLA. In 1970, it was re-established under its current name. CASIA claims to have "pioneered" control science and engineering in China and contributed to the country's development of the "two bombs and one satellite."[16]

CASIA states that its research focuses on "intelligent processing of massive information, intelligent control of complex systems, and integrated intelligent systems." At the end of 2020, the institute had 1062 full-time staff, of whom 113 were professors; 663 graduate students; and 59 post-doctoral researchers. In 2017, it also helped establish the first school in China devoted exclusively to artificial intelligence (AI), the School of Artificial Intelligence at the University of the Chinese Academy of Sciences.[17]

This report examines research activities, including international partnerships and collaboration, by CASIA subdivisions and commercial endeavors that engage in AI, machine learning, computer vision, and related disciplines that raise serious ethical and national security concerns owing to their support to China's public security and mass surveillance apparatuses as well as its defense research and industrial base.

This section focuses primarily on CASIA's National Laboratory of Pattern Recognition (NLPR, 模式识别国家重点实验室), a state key laboratory that houses numerous divisions and centers that conduct research related to mass surveillance for public security applications. NLPR also collaborates with other CASIA divisions that have overlapping missions related to hardware (such as imaging equipment and microelectronics research), neuroscience, and AI and machine learning systems for public security, defense, and other commercial applications. A complete list of CASIA divisions and examples of other divisions supporting defense research appears in appendix A. Many of these divisions, such as the Aerospace Information Research Center, warrant further scrutiny but are beyond the scope of this report.

CASIA Divisions Supporting Surveillance, Public Security, and Defense Missions

This report identifies fourteen CASIA research centers, laboratories, and departments, not including international collaboration centers or programs. One of these divisions is not listed in the organization chart on the English-language version of CASIA's website. CASIA also "incubates" at least four commercial firms and owns or invests in dozens of other companies, many of which develop or produce surveillance equipment, software, analytic tools, and other services for public security and defense entities in China.[18]

CASIA's Chinese-language website lists dozens of research projects conducted over the past decade. The following sample demonstrates the R&D support that CASIA supplies to China's public security and surveillance apparatuses:

- In December 2019, CASIA's "iris recognition technology team" won an award at the Ministry of Public Security's first "Criminal Technology 'Double Ten Plan' Tackling Innovation Contest." CASIA's project involved collaboration with the Beijing Public Security Bureau and the Jilin Provincial Public Security Department. The award describes CASIA's development of a lightweight and compact "mobile intelligent

multi-dimensional handheld police terminal" that can perform second-generation ID, iris, facial, and fingerprint biometric identification functions.[19]

- CASIA and Lenovo, a PRC technology firm, established a joint laboratory in 2016 to develop a "biometric identification cloud service platform" that allows for "autonomous and controllable identity authentication cloud services in finance, *government*, *public security*, social security, transportation, education, and medical fields" (emphasis added). It aims to integrate Lenovo's industrial resources in cloud services with CASIA's iris, facial, fingerprint, and voice recognition capabilities. Tan Tieniu (profiled below) is the director of the management committee of the joint laboratory.[20]

- In September 2015, CASIA convened a seminar on facial recognition technology. Noteworthy participants included Wang Rong, who leads "video image detection technology" research at the People's Public Security University of China, and representatives from Samsung Electronics, KDDI, Lenovo, Huawei, Datang Telecom, Hikvision, and Tencent's YouTu Lab. The seminar discussed China's "urgent need for facial recognition technology and applications" for "rail transportation, public security, civil airports, national defense, and military industries."[21]

In addition to surveillance-related projects listed on CASIA's website, a review of S&T publications reveals collaboration on mass surveillance R&D between CASIA researchers and organizations directly subordinate to the Ministry of Public Security and the People's Armed Police. Section IV details these partnerships and provides a sample of that literature.

National Laboratory of Pattern Recognition

The National Laboratory of Pattern Recognition was established in 1984 as one of China's first designated state key laboratories. NLPR claims to have undertaken over four hundred research projects as well as various international cooperation and industry projects. NLPR's main research areas are pattern recognition, computer vision, image processing and graphics, speech and language processing, and natural language processing.[22] Within CASIA, NLPR appears to play a key role in mass surveillance–related R&D.

NLPR's website lists awards from national and local government offices. A selection of projects that received such recognition and that raise ethical concerns appears below. This information was accessible only in Chinese, which may suggest an intention to conceal it from foreign eyes.

- A 2016 National Technology Invention Award for a project entitled "** Processing and Application Technologies" (**处理与应用技术). The asterisks (**) denote redactions, typically because the PRC government considers the information sensitive or classified.

- A 2013 Beijing Municipal Invention Patent Award for a project entitled "A Method and System for Filtering Sensitive Web Pages Based on Multi-classifier Fusion." This project could support the party-state's vast Internet censorship system.

- A 2011 National S&T Progress Award entitled "Video Content Understanding Technology and Application for Security Surveillance Purposes."[23] The award suggests that the central government considered this project a national development priority.

NLPR also collaborates on research internationally and claims that its staff "publish hundreds of papers in leading national and international journals and conferences" annually. NLPR organizes and hosts national and international conferences and workshops. Its main webpage claims that "dozens of notable scholars from Canada, France, Japan, and the US routinely visit NLPR to give lectures." NLPR has also partnered with France's Institut National de Recherche en Informatique et en Automatique (INRIA) to establish the Sino-French Laboratory for Computer Science, Automation and Applied Mathematics.[24] Additional research institutions based in EU countries subsequently partnered with this lab.[25]

NLPR houses several centers and research groups, and it closely collaborates with other CASIA divisions. A few of these entities are discussed below, including NLPR's Biometric and Security Research Group, the Visual Information Processing Group, and the Computational Medicine Group, which partners with CASIA's Brainnetome Center and the Research Center for Brain-inspired Intelligence.

Biometric and Security Research Group NLPR's Biometric and Security Research Group consists of the Center for Biometrics and Security Research (生物识别与安全技术研究中心) and the Center for Research on Intelligent Perception and Computing (CRIPAC, 智能感知与计算研究中心). The latter is of particular interest.

According to its Chinese-language website, CRIPAC addresses the "major strategic needs of national public security and intelligent industrial development." Its research focuses on multimodal intelligent computing, bio-inspired intelligent computing, intelligent perception theory, and "intelligent surveillance technologies and applications," which include pattern recognition and biometric recognition such as facial, iris, fingerprint, and palm print identification, "network content understanding and information security," and intelligent video processing and understanding.[26] It claims to have produced more than nine hundred journal and conference papers, and more than two hundred patents.[27]

CRIPAC bills itself as the largest research institute specializing in biometric identification in China. It oversees four research groups, two institutes, four start-up companies that it describes as "industry incubators," and two "industrial technology innovation strategic alliances." These research elements include the following:

- CAS—Artificial Intelligence Research[28] (中科人工智能创新技术研究院)*
- Tianjin Academy for Intelligent Recognition [Industrial] Technologies (天津中科智能识别产业技术研究院)
- Intelligent Perception Fundamental Theory Research Group (智能感知基础理论研究组)*
- Bio-inspired Intelligent Computing Research Group (生物启发的智能计算研究组)*
- Biometrics and Security Research Group (生物识别与安全研究组)
- Multimodal Intelligent Computing Research Group (多模态智能计算研究组)[29]

Those marked with asterisks do not appear on CRIPAC's English-language webpages. As to the others, their webpages describe research in support of China's public security and mass surveillance apparatuses, including the following examples:

- Maintenance of a "pedestrian attribute database" and separate gait, facial image, fingerprint image, iris image, palm print image, multispectral palm print, and handwriting databases.[30]
- Research on iris and facial recognition from controlled to complex scenes and "high-level identification technology for public safety."
- Studies of semantic information of human actions and behaviors in visual surveillance for abnormal behavior detection and analysis "to serve the needs of public security."
- Research on pedestrian attribute analysis and "re-identification in non-overlapping camera networks by exploiting relationships across cameras."
- Development of object recognition, object detection, video segmentation, and video analysis for "public security and business intelligence," and large-scale social network data mining to "adapt to the needs of public and content security."[31]

CRIPAC's "industry incubators" are Vistek, IrisKing, IriStar, and Watrix. Section III and appendix B discuss these firms and CASIA's other commercial operations and investments in detail. However, several points are relevant here:

- Vistek deploys its video surveillance tools in Xinjiang for public security purposes. In the course of writing this report, the company's website became inaccessible from US points of presence. That website consisted solely of Chinese-language screenshots (images), which impeded indexing and retrieval by search engines.[32]

- IrisKing specializes in machine vision, biometric recognition, and AI technology research, with a primary focus on iris recognition technology. It serves China's public security bureaus at the national and local levels.[33]

- IriStar provides iris and facial recognition for "public security and justice, counterterrorism, border inspection, security, finance, and education" customers.[34]

- Watrix claims to have the world's most advanced human gait recognition and visual detection technology geared to public security departments.[35]

Visual Information Processing Group NLPR's Visual Information Processing Group focuses on research relating to modeling human perception and cognition, algorithms for extracting 3D shapes from images, image/video analysis, and computer vision prototype systems.[36] This group consists of two research teams: the Robot Vision Group and the Image and Video Analysis Group. Projects undertaken by the Robot Vision Group have supported defense programs and are listed in appendix C.

The Image and Video Analysis Group's research areas include web multimedia content search, multimedia semantic analysis and understanding, and visual and video surveillance. The group conducts research for industry and claims to have "in-depth cooperation with many well-known companies such as Microsoft, Nokia, Intel, Huawei, and JD."[37]

Research Center for Brain-inspired Intelligence and Brainnetome Center

The Research Center for Brain-inspired Intelligence (类脑智能研究中心) and the Brainnetome Center (脑网络组研究中心) are closely linked to and collaborate on research with NLPR, but both are listed as independent CASIA divisions on CASIA's homepage.[38] Nevertheless, many researchers are affiliated with both NLPR and one (or both) of these two centers. The Research Center for Brain-inspired Intelligence focuses on neural computation and cognitive brain modeling, neuromorphic computing systems, brain-inspired information processing, and neural robotics.[39] A sample of articles published by researchers affiliated with this center and their biographies indicate that some research conducted there has surveillance and defense applications, such as pose estimation, feature extraction, image motion analysis, image matching and reconstruction, object detection and tracking, and autonomous and uncrewed aerial vehicles.[40]

The Brainnetome Center seeks to map the human brain at macroscopic, mesoscopic, and microscopic scales to identify brain functions and malfunctions to understand and treat neurological and psychiatric disorders and to model or simulate the brain's neural networks and organizing principles to derive cognition and behaviors.[41] This report did not find any direct evidence of the Brainnetome Center's involvement in surveillance-related research. At the same time, it did not evaluate much of the surveyed corpus of published

literature that names authors affiliated with this center. Scientists affiliated with the Brainnetome Center frequently also list NLPR affiliations on scientific publications, and the Brainnetome Center publishes research with scientists affiliated with the Research Center for Brain-inspired Intelligence.

These two centers epitomize CASIA's dual identity. On the one hand, they conduct research with the potential to treat or cure neurological disorders, and it is therefore understandable that international partners might seek to collaborate with them. The Brainnetome Center has an international advisory committee made up of neuroscience researchers from Australia, Cuba, France, Germany, Switzerland, the UK, and the US.[42]

On the other hand, these centers are well integrated with NLPR and their research may advance NLPR's documented contributions to the party-state's mass surveillance and public security apparatuses. As a report by the human rights group Article 19 attests, surveillance technologies are already in use in "emotion recognition" for predictive policing, racial profiling, and other human rights abuses.[43]

Intelligent Manufacturing Technology and System Research Center

Other CASIA divisions also support China's public security and defense missions, such as the Intelligent Manufacturing Technology and System Research Center (智能制造技术与系统研究中心), which focuses on intelligent control and intelligent information processing research. One of its projects was awarded a second prize Ministry of Public Security S&T Progress Award.[44]

Profile of CASIA Executive Tan Tieniu

Dr. Tan Tieniu (谭铁牛) is a recognized expert in computer vision and pattern recognition and has authored many domestic and international publications. After receiving a bachelor's degree in China and a PhD and fellowships in the UK, in 1998 he returned to China, where he has held leadership roles within CASIA and the Chinese Academy of Sciences and several prestigious political appointments in the CCP and PRC government.

- (Current) Director of CRIPAC
- (Former) Director of CASIA
- (Former) Director of NLPR
- (Former) Deputy Secretary and Vice Dean of the Chinese Academy of Sciences
- Member of the Standing Committee of the 13th National Committee of the Chinese People's Political Consultative Conference

- Vice Chairman (since 2008) of the Western Returned Scholars Association (WRSA), an organization subordinate to the CCP's United Front Work Department that carries out global influence operations and technology transfer[45]

- Positions in international academic bodies such as president of the IEEE Biometrics Council, fellow of the World Academy of Sciences (TWAS), and International Fellow of the UK's Royal Academy of Engineering

- Chair or committee member of international conferences and editorial board member of international journals, such as founding chair of the International Association of Pattern Recognition's Technical Committee on Biometrics, editor-in-chief of the *International Journal of Automation and Computing*, and editorial board member of the *IEEE Transactions on Pattern Analysis and Machine Intelligence* and *IEEE Transactions on Information Forensics and Security*[46]

Biographies or CVs posted on Chinese-language CASIA websites detail Tan's leadership of projects related to biometric recognition, intelligent video surveillance, and network data understanding and security. Examples include a 2012–16 project entitled "National-level Social Perception Data Management for Public Security Purposes,"[47] and the previously mentioned "Video Content Understanding Technology and Application for Security Surveillance Purposes" that received a 2011 National S&T Progress Award.[48]

Notably, none of the CVs, faculty pages, or biographical descriptions surveyed for this report list Tan's affiliations as inventor, scientist, chairman, or shareholder of at least four companies, among them the aforementioned "incubator" firms tied to CRIPAC, which provide mass surveillance technologies to China's public security organs.[49]

In December 2016, Tan was named deputy director of the PRC Central Government Liaison Office in Hong Kong while retaining his CASIA affiliation. It is telling that the PRC government selected an expert in public security and surveillance R&D for that position in the interlude between two waves of mass pro-democracy demonstrations. In 2021, the US Treasury Department added Tan to its "specially designated nationals list" of sanctioned officials for his role in presiding over the dismantling of the city's autonomy and freedoms and its crackdown on dissent.

CASIA's Partnerships with Foreign Industry and Research Institutions

CASIA's own website describes extensive partnerships with foreign companies and research institutions. Section V examines some of these collaborations with US partners in detail. Other examples include the following:

- CASIA and Intel Corporation jointly established in 2012 the China Intel Internet of Things Technology Institute[50] in Beijing as part of an "industry-academia-research-government

collaborative innovation" to help develop China's Internet of Things industry. The institute has a steering committee composed of Beijing municipal government organs, Intel Corporation, and CASIA. The president of the Intel China Research Institute and CASIA's Tan Tieniu were selected as co-directors.[51]

- CASIA hosts the Sino-European Laboratory in Computer Science, Automation and Applied Mathematics, or LIAMA. Originally a partnership with the French National Institute for Research in Computer Science and Control (INRIA), LIAMA has since expanded to include other EU nations. Projects involve cooperation between European and PRC researchers and are hosted by a partnering institution in China.[52] EU members include Centrum Wiskunde & Informatica of the Netherlands, European Aeronautic Defence and Space Company, and other French, Belgian, and Dutch research institutions.[53] LIAMA's director on the PRC side is Tao Jianhua, who concurrently serves as deputy director of CASIA's NLPR and specializes in speech and signal processing, emotion recognition, and human-computer interaction. Additionally, one of LIAMA's projects in 2016 involved "multi-modal sensing and scene understanding" based on data from sound, image, video, infrared, or radar.[54]

- NLPR's Speech and Language Information Processing Group claims to have "good ties" with industry, naming Google, Baidu, Tencent, and Huawei as partners. The research group focuses on natural language processing related to machine translation, information extraction, text mining, speech recognition, and computational auditory scene analysis.[55]

- CASIA claims to host over seven hundred "overseas guests" for scientific visits and chairs more than ten international conferences each year. CASIA partners with "internationally well-known research organizations and worldwide companies" from the US, the UK, Australia, New Zealand, Belgium, France, Germany, Italy, Spain, Japan, Korea, and Singapore.[56]

III: CASIA-LINKED ENTERPRISES SUPPORTING SURVEILLANCE, PUBLIC SECURITY OPERATIONS

CASIA's contributions to China's public security and mass surveillance apparatuses extend beyond fundamental research. For instance, CASIA has an investment arm, the Beijing CASIA Investment Management Co. Ltd. (北京中自投资管理有限公司), that promotes the commercialization of its research. Appendix B lists thirty-eight companies in which that entity holds a stake.

This section examines five such companies with clear ties to CASIA's NLPR, all of which offer products and services in the fields of computer vision and biometric

recognition that directly support China's mass surveillance and public security operations. Four of the companies are listed as "industry incubators" on CRIPAC's organization chart: Vistek, IrisKing, IriStar, and Watrix. Key findings on the companies include the following:

- Three of the firms describe "anti-terrorism" as a core application; one of the firms (Vistek) explicitly states that it deploys its surveillance tools in Xinjiang.

- Tan Tieniu, one of CASIA's key leaders, is a chairman, inventor, scientist, and/or shareholder in four of these five companies.

- Four of the firms partner with other enterprises that are on the US Department of Commerce's Entity List due to human rights concerns or for participation in China's defense apparatus. Huawei partners with three of these firms, demonstrating its ties to China's surveillance operations and public security organs.

- These firms claim US companies such as Intel and Qualcomm as partners. This report did not attempt to verify those claims.

Vistek

(Beijing) Vistek Co. Ltd. (中科唯实科技 [北京] 有限公司) provides China's public security apparatus with surveillance technologies born out of research from CASIA's CRIPAC and Tan Tieniu's work specifically. Tan appears on the company's website as one of the firm's key inventors.[57] These surveillance technologies center around "intelligent video big data analysis," and the company claims that its video content understanding for security and surveillance applications has been "widely used in state security affairs." It also declares that its "safe city" products are used for anti-terrorism efforts in Xinjiang.

One suggestion of the sensitivity of Vistek's operations is that the company's website offered no English-language content, and its Chinese-language content—while detailed in its descriptions of products and services—appeared to consist solely of screenshots. The absence of text not only impeded machine translation or copying by visitors but also indexing by search engines.[58] In the course of writing this report, Vistek's website became inaccessible from US points of presence.

Nevertheless, Vistek explicitly states that its products and services are used by public security personnel and organizations. For example, the company claims that its facial recognition technologies include the following:

- Dynamic face capture storage, which can be transferred to central facial management platforms for storage and comparison

- Real-time facial comparisons
- Pedestrian monitoring that can recognize and capture in real time an individual's gender, age range, hair length, clothing color, and specific clothing accessories (such as hats or bags)
- Prison monitoring systems and services[59]

The company also offers "smart zone intelligent surveillance cloud platform systems," which include video surveillance, video analysis, facial recognition, vehicle management, access controls, alarm systems, and "deep integration of GIS and 3D mapping."[60]

Lastly, the company lists "cooperative partners" on its website. These partners include the China Intel Internet of Things Technology Institute,[61] other CASIA-affiliated companies ViSystem and IrisKing (also discussed in this section), major surveillance technology provider Hikvision, and state-owned defense conglomerates China Electronics Technology Group Corporation (CETC) and China Aerospace Science and Technology Corporation. The latter three firms are on the US Department of Commerce's Entity List.[62]

IrisKing

Beijing IrisKing Co. Ltd. (北京中科虹霸科技有限公司) was established by CASIA and received investments from Legend Holdings, a conglomerate that holds a controlling stake in Lenovo, as well as Linzhou Heavy Machinery Group and CASIA's investment management firm. The company states that its "core technologies" come from twenty years of R&D conducted at CASIA's NLPR led by Tan Tieniu, who serves as IrisKing's chairman.[63] The Chinese-language version of its website states that the company specializes in machine vision, biometric recognition, and other AI technology, with a primary focus on iris recognition technology. It boasts that its technologies are "widely used in public security."[64]

For instance, a news item on the company's website notes that a project on iris data building and application service for the Beijing Public Security Bureau and the Ministry of Public Security (MPS) First Institute won third prize in an MPS-issued S&T award.[65] The company also claims to be building a "super scale authentication system" using its technologies. A possible example of this was described in a press release, which states that the Zhengzhou (Municipality) Public Security Bureau completed construction of a "10 million capacity iris verification system" in partnership with IrisKing.[66]

The company claims that it exports its products to India, the Philippines, and the Middle East, Africa, and Europe. Its website lists cooperative partners, including Ant Financial Services, Huawei, Lenovo, Spreadtrum Communications, China Mobile, and Qualcomm.[67]

IriStar Technology

IriStar Technology Co. Ltd. (中科虹星科技有限公司) claims to have the largest R&D team focusing on long-distance iris recognition in the world and states that its key personnel came from CASIA's NLPR. IriStar's products and services relate to "high-performance imaging and intelligent visual data analysis" specifically for iris and facial recognition in public security and the financial and information technology industries. The company works with Tan Tieniu's research group at CASIA on long-distance biometrics, and Tan is listed as an inventor and scientist for IriStar. The company's founder-CEO and another listed inventor concurrently hold professor positions at NLPR. Its biometric recognition technologies include object detection, facial detection, keypoint localization, depth estimation, 3D reconstruction, iris recognition, and "liveness detection" (referring to an ability to differentiate between a live person vs. an image).[68]

IriStar claims to be the first PRC company to launch a domestically produced long-distance iris recognition product that can perform "high precision identity authentication" in large crowds, serving "public security and justice, counterterrorism, border inspection, security, finance, and education" customers. The company claims that its products can also combine body temperature detection with iris recognition that can identify people wearing masks.[69]

In addition to its iris recognition technologies, IriStar also develops technologies that can aid in "multi-person detection, big action recognition, and other complex scene applications" by "accurately locating" facial and body features and positioning, including head, neck, shoulder, elbow, hand, hip, knee, and foot.[70]

IriStar's iris and facial recognition machine received operational and quality certifications by the MPS First Institute.[71] The company also received certification by "national authorities" for meeting the registration requirements of "biometric identification agencies."[72]

Lastly, the company's website lists partnerships with other companies but does not detail the nature of those relationships. In addition to the aforementioned IrisKing, IriStar partners with firms on the Department of Commerce's Entity List for defense-use or human rights reasons, such as the state-owned China Electronics Technology Group Corporation, Beijing Institute of Technology (a "Seven Sons of National Defense" university), Megvii, and Huawei.[73]

Watrix

Watrix.ai (银河水滴科技 [北京] 有限公司; hereafter, Watrix) was founded in 2016 and claims to have the world's most advanced gait recognition and visual detection technology. Watrix is listed as one of the companies that CASIA "incubated" out of its CRIPAC division. The

CEO and founder Huang Yongzhen (黄永祯) graduated from CASIA's NLPR and studied under Tan Tieniu. Prior to founding Watrix, Huang worked as an associate researcher at CRIPAC.[74] According to an online business research and investment information portal, Huang owns 20.6 percent of Watrix. Other notable shareholders include Lenovo (16.5 percent stake), Tan Tieniu (6.6 percent stake), and CASIA through its investment holding arm (3.8 percent stake).[75] While Watrix serves the "smart city, safe community, intelligent transportation," medical, and recreation industries, its touted surveillance capabilities for public security are the most alarming.

For instance, Watrix explains on its website that human gait is the only biometric feature that can be recognized in complex scenes from long distances and is unaffected by camouflage, which makes "gait recognition a unique advantage in public security areas."[76] In October 2018, Watrix announced the launch of a new product for public security departments named "shui di shen jian" (水滴神鉴), which may be translated as "waterdrop omniscient surveillance." The product can target and identify suspects by monitoring their posture and gait up to fifty meters away from any angle day or night, regardless of what the individual is wearing or whether his or her face is covered "without the suspect being aware." The company also claims that its gait recognition has a world-leading accuracy rate of 94 percent.[77]

According to a *Global Times*[78] article, Watrix's tracking system "can mobilize tens of thousands of real-time cameras to recognize a person's gait and help police nab criminal suspects." The article states that the system can locate and track targets by monitoring their postures from tens of thousands of either real-time or offline videos and issue an alarm if it spots "someone doing something suspicious or illegal."[79] The article also quoted an unnamed Beijing-based professor that Watrix's technology will enhance China's Sharp Eyes and Safe City projects, which include mass surveillance systems deployed to rural and urban areas that Western human rights groups have raised concerns about.

Watrix is also building gait databases to establish "personnel gait big data platforms."[80] In addition to its gait recognition–related products, the company develops industrial inspection technologies for various industries and manufacturers of military equipment.[81]

ViSystem

Beijing ViSystem Corporation Ltd. (北京多维视通技术有限公司; hereafter, ViSystem) is a subsidiary of Beijing Hisign Technology Co. Ltd. (北京海鑫科金高科技股份有限公司). It claims to be one of the largest biometric identification companies in China to handle facial recognition, fingerprint identification, palm print matching, and handwriting and vehicle license plate recognition. Hisign states that it primarily serves "public security, antiterrorism, and procuratorial" applications.[82] ViSystem also appears to serve almost

exclusively public security and regional and local police and criminal justice organs through its video surveillance products and services. CASIA is a shareholder of ViSystem[83] and co-founded a joint laboratory with the company described below.[84]

ViSystem's products and services revolve around video big data analysis and forensics for China's law enforcement and public security purposes, and further the goal of "strengthening the police through S&T" (为科技强警).[85] The company offers human and facial image identification and analysis at different resolutions and postures of individuals, 3D portrait scanning technology, 3D portrait reconstruction and comparison technology, and other video forensics for evidence processing in criminal investigations. ViSystem describes one of these products as a "Police Vision Human Image Intelligent Reconstruction System." This product compares collected video with the "suspect target for analysis . . . based on a library of suspect targets to determine the identity of the suspect."[86]

ViSystem also offers a "mobile video reconnaissance vehicle solution" for individual public security officers that includes mobile video investigation studio equipment, crime scene and tracking routes for video capture, and rapid screening, processing, storage, and transmission functions.[87]

According to an article on China Police Net, a web portal run by MPS, in 2013 ViSystem, CASIA, the MPS Physical Evidence Identification Center, and the Beijing Public Security Forensic Identification Center formed the Joint Laboratory of Video Investigation Technology (视频侦查技术联合实验室). This was the first professional laboratory of video investigation technology in China and specifically focuses on technologies for the public security industry. The article also noted how this laboratory can aid in the development of China's "Safe City" and "Skynet" projects "to promote video surveillance for public security organs."[88] China's "Skynet" is a mass surveillance system cited by Amnesty International as raising serious human rights concerns.[89]

Unsurprisingly, ViSystem partners with many universities and academies that fall directly under the supervision of MPS. For example, the company

- jointly established the Institute of Video Investigation Technology with the Shandong Police College's Department of Criminal Science and Technology in 2014;

- signed a strategic cooperation agreement with the Criminal Investigation Police University of China in 2017; and

- lists as "cooperative partners" the People's Public Security University and numerous provincial and municipal police academies in Jiangsu, Sichuan, Guangdong, Hangzhou, Liaoning, Chongqing, Shandong, and Guizhou.[90]

Lastly, the company identified Huawei as an "ecological partner" (生态合作伙伴) and was invited to participate in a "National Safe City Video Cloud Partner Open Alliance Signing Ceremony" with Huawei. The news item posted on ViSystem's website noted that the company partners with Huawei specifically to promote the development and application of video technologies for "public security, prosecution, anti-terrorism and security" purposes.[91] Huawei has been sanctioned by the US government for violations of Iran sanctions and allegations of intellectual property theft.[92] This report also provides examples of Huawei's activities supporting public security and anti-terrorism operations.

IV: SURVEY OF CASIA'S RESEARCH PUBLISHED IN CHINA

The previous sections examined some of CASIA's divisions, programs, and commercial operations, which support mass surveillance R&D and China's public security apparatuses. This section examines CASIA's domestic research activities by way of bibliographic records from a corpus of 493 publications that name at least one CASIA-affiliated author, were published between 2014 and 2020, and are hosted on CNKI, one of China's major research publication aggregators. This domestic corpus of scientific literature was screened for research that supports China's public security and national defense missions.[93] A catalog of defense-related R&D appears in appendix C, which documents CASIA's partnerships with the PLA, China's nuclear weapons complex, and several state-owned defense conglomerates.

Publications Revealing CASIA's Contributions to Public Security and Surveillance Research

A survey of this corpus identified nineteen articles that were published with CASIA-affiliated authors whose research clearly supports China's public security and surveillance apparatuses. Owing to limitations in this report's research design, this sample may understate the true extent of CASIA's R&D contributions to public security purposes. Nevertheless, the corpus contains the following:

- Eleven articles that either (a) name coauthors affiliated with MPS organs, including the Institute of Forensic Science and two universities directly subordinate to MPS: the People's Public Security University of China (中国人民公安大学) and the Criminal Investigation Police University of China (中国刑事警察学院); (b) credit research funding from MPS; and/or (c) are published in an MPS-run journal.

- One article that names coauthor(s) from the People's Armed Police (PAP).

- One article published in a journal run by the CCP Central Committee Secrecy Office and the National Administration of State Secrets Protection.

Many of these research partners prompt ethical and national security concerns. The MPS Institute of Forensic Science was added to the Department of Commerce's Entity List in 2020 for engaging in human rights violations and abuses.[94] The PAP is a paramilitary police force under the direct authority of the Communist Party Central Committee and its Military Affairs Commission. The PAP performs domestic security and surveillance functions to support the party-state's authoritarian control over the PRC population.

Although this report did not undertake technical assessments of the research in this corpus, the titles, keywords, and abstracts of publications in it were screened for relevance. Examples of topics covered in relevant articles include facial and iris recognition, biometric identification, 3D human posture estimation, and head pose estimation. Table 1 lists these articles and the basis for their inclusion. Two examples taken from this table are discussed.

Example 1: CASIA Collaboration with People's Public Security University

CASIA's involvement in computer vision research that directly supports China's public security organs is evident in the article entitled "A Survey on Head Pose Estimation," which names at least one coauthor affiliated with the People's Public Security University of China School of Criminal Science and Technology (中国人民公安大学刑事科学技术学院).[95] This university is directly subordinate to MPS, serving as the ministry's primary higher education institution and police academy after the People's Police Academy University merged with the similarly named Public Security University in 1998.[96] Keywords provided in the metadata include *head pose estimation*, *pattern recognition*, *computer vision*, and *facial recognition*. Also worth noting is that one of the CASIA coauthors is senior CASIA leader and computer vision expert Tan Tieniu.

Example 2: CASIA Research Funded by the Ministry of Public Security

A 2020 article entitled "Real-Time Crowd Counting for Embedded Systems with High Accuracy" credits funding from the MPS. The keywords include *crowd-counting*, *head-shoulder detection*, and *multi-target tracking*.[97] Additionally, the journal that published the article, *High Technology Letters*, was founded by the Ministry of Science and Technology's "High Technology Research Program (863 Plan) Joint Office."[98] China's 863 Plan primarily focuses on national defense research, which may indicate China's interest in both public security and defense applications of the research discussed in this article.

Table 1. Articles published by CASIA-affiliated authors supporting China's public security and surveillance apparatuses

Article title	*Apparent ties to public security*
"A Benchmark for Iris Segmentation"[99]	Keywords include biometric identification, iris recognition, iris segmentation
"Three-Dimensional Human Pose Estimation Based on Video"[100]	Title and keywords include 3D human posture, convolutional neural network, video sequence
"Research on Biometrics Technology Development Applications and Security Issues"*[101]	Keywords include biometrics, facial recognition, fingerprint identification Published in *Secrecy Science & Technology* (保密科学技术), which is run by the National Secrecy Science and Technology Evaluation Center (中国保密科技测评中心), an organization subordinate to the CCP Central Committee Secrecy Office and the National Administration of State Secrets Protection (国家保密局)[102]
"Facial Recognition Combined with Video Surveillance, Examining Public Security and Financial Market Applications"*[103]	Title reveals surveillance applications Published in *China Security & Protection* (中国安防), a journal produced by the MPS Scientific and Technical Information Research Institute (公安部科学技术信息研究所) and the China Security & Protection Industry Association (中国安全防范产品行业协会)[104]
"Attempt to Denoise into 3D-point Cloud of Linear Trace"[105]	Coauthor(s) affiliated with MPS Institute of Forensic Science (公安部物证鉴定中心) Published in *Forensic Science & Technology* (刑事技术), a journal produced by the China Institute of Forensic Science and supervised by MPS[106]
"Detection of Birds' Nest in Catenary Based on Improved RetinaNet Model"[107]	Coauthor(s) affiliated with Guangdong Province Smart City Infrastructure Health Monitoring and Evaluation Engineering Technology Research Center (广东省智慧城市基础设施健康监测与评估工程技术研究中心) Abstract reveals potential surveillance applications by discussing how "deep learning–based object detection algorithms are trained and tested using data sets collected by on-board equipment of high-speed railways"
"Real-Time Crowd Counting for Embedded Systems with High Accuracy"[108]	Keywords include crowd-counting, head-shoulder detection, multi-target tracking Funding source includes MPS
"Simulation of Deep Residual Network Detection in Fingerprint Triangle Region"[109]	Coauthor(s) affiliated with People's Public Security University of China School of Criminal Science and Technology (中国人民公安大学刑事科学技术学院)
"Study of Brain-Like Mechanisms of Deep Learning Based on Visual Information Encoding and Decoding"*[110]	Coauthor(s) affiliated with Huawei Corporation Keywords and abstract include vision-based multi-view, deep learning neural network, machine intelligence simulation of human visual perception

Continued

Table 1. (*Continued*)

Article title	*Apparent ties to public security*
"Detection of Image Splicing Manipulation by Automated Classification of Color Temperature Distance"[111]	Coauthor(s) affiliated with Criminal Investigation Police University of China (中国刑事警察学院) and National Engineering Laboratory of Evidence Traceability Technology (现场物证溯源技术国家工程实验室), a lab whose formation was overseen by the MPS Institute of Forensic Science and jointly established by several organizations including CAS Beijing Institute of Genomics[112]
"Exploration of Research Progress on Portrait Attribute Recognition Key Technologies and Applications"*[113]	Published in *Police Technology* (警察技术), a journal run by the MPS First Institute Keywords include pedestrian re-identification, video surveillance
"Key Technology and Research Status of Registration Methods for Pulmonary Image"[114]	Coauthor(s) affiliated with Beijing Zhongdun Security Technology Development Co. Ltd. (北京中盾安全技术开发公司), a commercial spin-off of the MPS First Institute[115] and PLA General Hospital (国人民解放军总医院)
"Research on Application of Pulmonary Non-rigid Registration Method with 3D-SIFT Features"[116]	Coauthor(s) affiliated with Beijing Zhongdun Security Technology Development Co. Ltd. (北京中盾安全技术开发公司), and PLA General Hospital
"Hot Areas and New Directions in Fingerprint Identification Technology Research"*[117]	Published in *Police Technology* (警察技术)
"A Survey of Video Forensic Technology"[118]	Coauthor(s) affiliated with the MPS Institute of Forensic Science and Beijing ViSystem Co. Ltd. (北京多维视通技术有限公司)[119]
"Application of Fluoroescein Sodium on Cerenkov Radiation Energy Transfer"[120]	Coauthor(s) affiliated with People's Armed Police General Hospital (武警总医院) and PLA General Hospital
"Smart City PK Safe City"*[121]	Keywords include pixel level, safe city, intelligent video analysis system, HD network camera, smart city, HD monitoring, active defense
"A Survey on Head Pose Estimation"[122]	Coauthor(s) affiliated with People's Public Security University of China School of Criminal Science and Technology (中国人民公安大学刑事科学技术学院) Keywords include head pose estimation, pattern recognition, computer vision, facial recognition
"Research and Applications of Forensic DNA Fragment Analysis Software"*[123]	Coauthor(s) affiliated with the MPS Institute of Forensic Science Published in *Police Technology* (警察技术)

**Indicates an approximate translation by the authors of this report as no English title was provided by the publication.*

V: CASIA'S RESEARCH COLLABORATION WITH US ENTITIES

US research institutions and companies collaborate extensively with CASIA. Using the methodologies outlined in appendix D and the international publications aggregator *Dimensions*, this report analyzed metadata from a corpus of English-language publications issued between 2014 and 2020 that have at least one US-based coauthor or funding source and at least one CASIA-affiliated coauthor. That corpus yields the following findings:

- Seven hundred forty-four publications (journal articles and conference proceedings) list coauthors from CASIA and US institutions.

- The US-based coauthors are affiliated with 224 US research institutions, among them elite US universities and government facilities. The corpus also contains twenty-five articles that name researchers from ten US technology companies, typically in collaboration with US university researchers.

- Tan Tieniu appears as a coauthor in ten of the articles.

CASIA's dual identity runs through the collected corpus. On the one hand, 289 articles credit funding from the US National Institutes of Health and involve medical or neuroscience research, often with CASIA's Brainnetome Center or the Center for Excellence in Brain Science and Intelligence Technology. On the other hand, forty-eight articles in the collected corpus concern surveillance and biometrics. Because CASIA conducts most of its work in the Chinese language and serves sensitive party-state organs, the English-language open-source record may underrepresent the share of those topics in its full research portfolio.

A sample of the surveillance-related articles in the corpus was selected for close reading. To cite a few examples, a 2019 article lists as coauthors Tan Tieniu, colleagues from CRIPAC, CASIA's Center for Research on Intelligent System and Engineering, and a US university.[124] It describes the architecture for an intelligent video surveillance platform that can alleviate the labor-intensive task of monitoring surveillance regions by evaluating big surveillance data from large-scale camera networks. It performs "pedestrian detection with tracking, attribute recognition, and re-identification" and can algorithmically annotate video samples with seventy-two visual attributes.[125]

A second 2019 article proposes computational methods for distinguishing and tracking multiple targets, such as vehicles or persons, with similar appearances through collisions, crowded scenes, and rapid motion.[126] It states that such multiple target tracking solutions are "crucial for visual surveillance and human-computer interaction."[127] Another article, from 2018, compares different approaches to using convolutional neural networks and structured ordinal measures for detection of pedestrians, vehicles, and faces via biometric recognition,

large-scale image retrieval, and facial recognition from video sources.[128] Several of the NLPR coauthors on this article and the last, including Tan, cite joint affiliation with the CAS Center for Excellence in Brain Science and Intelligence Technology, a clear indication that even the CAS components that ostensibly focus on medical science share both a mission to advance surveillance and key personnel with CASIA's public security projects.

Finally, a second 2018 article proposes a two-stage neural network that "achieves state-of-the-art detection accuracy and high efficiency" on standardized visual object datasets.[129] Apart from two coauthors from a major US corporation, all of the PRC-based authors share affiliations with NLPR and its subordinate Center for Biometrics and Security Research, which aspires to be a world leader in facial, iris, fingerprint, and palm print recognition "to ensure the safety of the country, society and individuals in the information age."[130]

Stripped of their context, none of these articles raise red flags; they all take up standard problems in artificial intelligence and computer vision in ways that are conventional to the field. But to end the analysis there would be premature. Just as citizens and institutions in democratic societies are critically interrogating the ramifications of these technologies at home, these citizens and institutions must reflect no less on the potential consequences when they have a hand in developing and refining the same technologies abroad.

The specific CASIA units and personnel involved in the examples cited above (and many others like them) serve diverse clients in the PRC's party-state, and in this way their research cross-pollinates and circulates among China's commercial, public security, and defense establishments. Applications optimized to automatically track, characterize, and identify vehicles or people in a crowd, or acquire biometric information such as iris, facial, and gait attributes at a distance without consent are inherently neither benign nor malignant. That determination depends on the people who wield them and the end-uses to which they are put. In contemporary China, beneficial uses of these technologies coexist alongside rampant abuses by the party-state, and particularly when the same institutions and researchers straddle both domains the two cannot be reliably separated or compartmentalized. This is the dilemma that our research enterprise must forthrightly acknowledge and reckon with when it partners with entities such as CASIA.

VI: CONCLUSION AND RECOMMENDATIONS

CASIA occupies an important role in the R&D pipeline that enables and enhances China's mass surveillance and public security apparatuses and their corresponding human rights abuses. This report focuses primarily on the activities and partnerships of a CASIA division, NLPR, and may understate the scale of the CASIA partnerships, international engagements, and commercial spin-offs that support mass surveillance and public security missions. Additionally, NLPR-affiliated researchers collaborate extensively with US institutions. Scrutiny of other CASIA divisions (described in appendix A) may reveal similar findings.

This report establishes that such scrutiny is necessary to adequately assess the risks and challenges of engaging with PRC organizations like CASIA, and it provides a framework for doing so. It also shows how state-run research institutions, such as those under the umbrella of the Chinese Academy of Sciences, have a well-developed system for integrating research, international collaboration, and industrial development into an innovation ecosystem that in its subservience to the PRC party-state deviates significantly from liberal democratic notions of research ethics and human rights. Traditional due diligence on prospective partners and their technologies does not reliably account for that; it is essential to also examine the R&D ecosystems and networks that those partners participate in.

US research institutions that espouse values of integrity and transparency at home may be receiving less when they collaborate with entities like CASIA in authoritarian nations. Notable discrepancies between English- and Chinese-language information on CASIA's websites suggest intentional obfuscation of sensitive programs or associations, or at minimum a selective lack of openness. None of the US-based entities identified in this report may have violated any laws or regulations. US legal and regulatory frameworks generally overlook the ethical concerns this report raises and should be revised to address that deficiency.

The cognitive dissonance of CASIA simultaneously pursuing both beneficial and reprehensible applications of research should be a wake-up call; PRC research institutions operate in a political order inimical to liberal democratic values, and as instrumentalities of the party-state they serve a regime fiercely committed to the maintenance of that order. This report therefore offers the following recommendations:

1. CASIA, its subordinate research centers and laboratories, and all associated commercial enterprises should be added to the Department of Commerce's Entity List with a presumption of denial designation. The following affiliated companies should also be added to that list:

    - Beijing Vistek Co. Ltd.
    - Beijing IrisKing Co. Ltd.
    - IriStar Technology Co. Ltd.
    - Watrix.ai
    - Beijing ViSystem Corp. and its parent company Beijing Hisign Technology Co. Ltd.

Section III examined five companies that develop surveillance technologies that enable serious human rights abuses. Yet CASIA partially owns at least thirty-three other companies

that warrant similar scrutiny to determine whether those firms should also be subject to export controls. A list of those companies is provided in appendix B.

Foreign firms, particularly from the US and other democracies, should not facilitate human rights abuses associated with China's mass surveillance operations by selling hardware components that may be used in the products of these CASIA-affiliated companies, such as sensors, microprocessors, system-on-chip designs, and other computer vision and communication components. This comports with a recommendation by the National Security Commission on Artificial Intelligence, which states that the Department of Commerce should implement end-use controls on high-end US-designated or US-manufactured AI chips for use in mass surveillance applications.[131] Similarly, US firms should not import any of the CASIA-affiliated or invested companies' products or services to ensure they do not end up in our supply chains. Private sector firms should terminate their relationships with CASIA or its associated businesses on ethical grounds and to avoid possible government sanctions, future regulatory compliance problems, and reputational harm.

2. Research institutions based in the US and other democracies should review their formal and informal collaborations, research partnerships, and related agreements with CASIA for risks to human rights, and to research ethics and integrity.

Academia in liberal democracies champions free expression, research integrity, transparency, and universal human rights, yet expends insufficient effort to understand who its partners in authoritarian nations are. It must uphold those values by not permitting CASIA and its subordinate entities to take for granted and benefit from international collaboration. Federal agencies should incentivize such measures by putting restrictions in place that would deny or remove funding to principal investigators that collaborate with organizations such as CASIA that support surveillance and human rights abuses. Concerted scrutiny of CASIA in democratic nations would send a message to the PRC that upholding ethical standards and human rights are prerequisites for international collaboration in scientific research.

This report acknowledges that at least some of the research that CASIA conducts may be beneficial to humanity and that restrictions on collaborations with CASIA or its affiliates might impede global science. Nevertheless, irrespective of their personal rectitude, CASIA employees are all subject to demands by the PRC party-state for their research and data. Moreover, this report has documented the intimate institutional and individual connections that they maintain with public security organs in particular. No safe zones exist where beneficial research pursuits could be unequivocally preserved from unethical (mis)use.

3. Research institutions and governments in democratic nations must revise existing concepts of research integrity and expand the use of ethical review processes when the research involves collaboration with partners in China and other authoritarian

nations. These reviews must include, for example, protocols for affirmatively validating the provenance of personally identifiable information and biometric and genetic datasets, and their compliance with standards of ethics and informed consent; planning for scenarios such as the diversion of research and data to organs of China's party-state; and concrete deliberation over the potential for lines of research that seem comparatively benign in a democratic polity to serve abhorrent ends in an authoritarian one.

Existing approaches to scientific research integrity focus mostly on the research process; research misconduct is typically understood as fabrication, falsification, or plagiarism. Other concepts used by US agencies such as the National Science Foundation relate to objectivity: not being biased or influenced by financial interests or affiliations, or preventing suppression or manipulation of findings for political reasons.[132] Regarding ethical considerations, universities and the US government provide guidelines for institutional or ethical review boards (often referred to as IRBs) to ensure that research involving human subjects adheres to common standards. Collaborations with CASIA may not trigger any of these tripwires, and indeed the ethical concerns raised in this report lie elsewhere, with the research partners themselves and the end-uses of the research.

Current IRB mechanisms fail to address the realities of operating in or with authoritarian nations. Some of the gaps in IRB or ethical review board processes include the following:

- The onus is on individual researchers to seek IRB approvals when research involves human subjects. However, neither the researchers nor the IRBs may understand the nature, mission, political context, or research environment of the relevant foreign partners.

- US institutions lack effective data governance controls when collaborating with China. If data or research outputs—such as biometric signatures, images or videos of human subjects—are shared with entities in the PRC, then that data is subject to PRC law and party-state controls. Experience shows that the US side cannot reliably monitor or prevent unethical use or manipulation of that research.[133]

- Privacy protection considerations in IRBs have not kept pace with increasingly sophisticated AI, machine learning, and big data analysis capabilities that can de-anonymize individuals at scale.

- Surveillance research disciplines, such as those that CASIA specializes in, often seek to identify individuals by overcoming such privacy protections and data access controls and are therefore fundamentally at odds with the goals of the conventional IRB process.

IRBs could be revised to include additional procedures that would close these gaps in oversight and ensure that the ethical risks described in this report are fully assessed. Expanding existing IRBs may entail lesser administrative burdens than creating a new process. This report recommends the incorporation of two additional processes into ethical reviews by research institutions:

- Universities and other research institutions define a common standard or set of conditions for ethical reviews of research not involving direct participation of human subjects. For instance, any research conducted in collaboration with partners in authoritarian nations that has surveillance applications (e.g., facial, iris, or gait recognition, or other areas that seek to identify specific individuals) should be included.

- Due diligence on potential partners based in authoritarian nations and the relevant political impositions and legal requirements to which they are subject must be conducted and incorporated into ethical risk evaluations.

The effectiveness of these additional ethical review procedures will depend on robust due diligence research on foreign entities similar to this report's examination of CASIA. Given the scale and complexity of such a task, this report offers a fourth recommendation to address this challenge:

4. Civil society institutions, such as think tanks, human rights NGOs, private sector firms, government, academia, and media organizations, should assist in applying the research methodologies in this report to other PRC-based entities that support or partner with China's mass surveillance and public security apparatuses.

Institutions in democratic societies need not shoulder the burden singly of applying the methodologies in this report to their international engagements. A coalition of public and private partners from civil society, including universities, think tanks, and NGOs, could collectively train their resources and subject matter knowledge on the challenge and share findings on entities like CASIA that engage in ethically reprehensible behaviors and undermine democratic values. The US government could also provide funding support for such research efforts and expand existing programs that already oversee research security and technology protection missions.

The purpose of such an effort would be to aggregate detailed information on key organizations in authoritarian countries, their subdivisions, research programs, personnel, and partnerships. This effort need not create a new type of denied entity list. Rather, it is intended to assist universities, researchers, and governments in upholding their values by making better, more informed risk assessment and mitigation decisions.

APPENDIX A: LIST OF IDENTIFIED CASIA SUBDIVISIONS

CASIA's English-language website lists twelve research departments or divisions:

- National Laboratory of Pattern Recognition (模式识别国家重点实验室)
- State Key Laboratory of Management and Control for Complex Systems (复杂系统管理与控制国家重点实验室)
- National Engineering and Technology Research Center for ASIC Design (国家专用集成电路设计工程技术研究中心)
- Key Laboratory of Molecular Imaging (分子影像重点实验室)
- Intelligent Manufacturing Technology and System Research Center (智能制造技术与系统研究中心)
- Integrated Information System Research Center (综合信息系统研究中心)
- Digital Content Technology and Media Service Research Center (数字内容技术与服务研究中心)
- Precise Perception and Control Research Center (精密感知与控制中心)
- Aerospace Information Research Center (空天信息研究中心)
- Brainnetome Center (脑网络组研究中心)
- Center for Research on Intelligent Perception and Computing (智能感知与计算研究中心)
- Research Center for Brain-inspired Intelligence (类脑智能研究中心)

Center for Research on Intelligent System and Engineering

At least one other division (the CAS Center for Excellence in Brain Science and Intelligence Technology) and several international collaboration centers do not appear on this website, such as the Center for Research on Intelligent System [sic] and Engineering (智能系统与工程研究中心, also known as CRISE). Furthermore, CRISE does not mention support for national defense or public security in the self-introduction posted on its Chinese-language website, but its research areas have clear defense-use potential. Examples include research on "man vs. machine/adversarial machine intelligence and intelligent decision theory and technologies," and "game adversarial mechanisms, game dynamics, and intelligent game confrontation and applications."[134]

Scrutiny of other divisions, such as the State Key Laboratory of Management and Control for Complex Systems and the Aerospace Information Research Center, is warranted on ethical and national security grounds but lies beyond the scope of this report.

APPENDIX B: CASIA INVESTMENTS IN DOMESTIC COMPANIES

Beijing CASIA Investment Management Co. Ltd. (北京中自投资管理有限公司) is owned by CASIA and invests in companies, some of which are outgrowths of the institute's research. The company's website lists companies in which it has invested but does not disclose the percentage stake or amount invested.[135] The list below was taken from the company's Chinese-language website. Many of these firms use the characters "中科" in their names, which refers to the Chinese Academy of Sciences (abbreviated in Chinese as 中科院). Further research is recommended on these companies to determine if they also partner with or provide products or services to China's public security and surveillance apparatuses.

Company name, official English name (if provided)	*Approximate English name (when no official name found)*
北京吉信气弹簧制品有限公司 (Beijing CITI BEN GS Product Co. Ltd.)	
北京嘉恒中自图像技术有限公司 (Beijing JoinHope Image Technology Ltd.)	
北京锐音恒讯科技有限公司	Beijing Ruiyin Hengxun Technology Co. Ltd.
北京三博中自科技有限公司 (Beijing Sciample Technology Co. Ltd.)	
北京数字精准医疗科技有限公司 (Beijing Digital Precision Medicine Co. Ltd.)	
北京中科贝银科技有限公司 (Beijing Zhongke Bei Silver Technology Co. Ltd.)	
北京中科富斯信息科技有限公司 (Beijing Zhongke Foursis Information Technology Co. Ltd.—aka Foursis)	
北京中科虹霸科技有限公司 (Beijing IrisKing Co. Ltd.)	
北京中科喀斯玛科技孵化器有限公司	Beijing Zhongke Kasima Technology Incubator Co. Ltd.
北京中科模识科技有限公司 (Beijing Pattek Co. Ltd.)	
北京中科融盛海洋科技有限公司	Beijing Zhongke Rongsheng Marine Technology Co. Ltd.
北京中科锐思科技有限公司	Beijing Zhongke Ruisi Technology Co. Ltd.
北京中科神探科技有限公司 (Beijing Shentan Tech Co. Ltd.)	

Continued

(*Continued*)

Company name, official English name (if provided)	*Approximate English name (when no official name found)*
北京中科闻歌科技股份有限公司 (Wenge Group)	
北京中科宇天科技发展有限公司 (Beijing CAS-SKY Technology Development Co. Ltd.)	
北京中科智加科技有限公司 (Beijing Iplustek Co. Ltd.)	
北京中科智控科技有限公司 (Beijing Zhongke Zhikong Control Technology Co. Ltd.)	
北京中科智源科技有限公司	Beijing Zhongke Zhiyuan Technology Co. Ltd.
北京中自百佳技术服务有限公司	Beijing Zhongzi Baijia Technology Service Co. Ltd.
广州中科恺盛医疗科技有限公司 (Guangzhou Zhongke Kaisheng Medical Technology Co. Ltd.)	
汉王科技股份有限公司 (Hanwang Technology Co. Ltd.—aka Hanvon)	
惠州先进制造产业技术研究中心有限公司 (Huizhou Zhongke Advanced Manufacturing Research Center Co. Ltd.)	
青岛中科慧聚文化创意有限公司 (Qingdao Zhongke Huiju)	
深圳慈航无人机自主系统技术有限公司 (Shenzhen Cihang Unmanned Intelligent Systems Tech Co. Ltd.)	
天津开发区中自长庆科技有限公司	Tianjin Development District Zhongzi Changqing Technology Co. Ltd.
天津中科智能技术研究院有限公司 (Tianjin Intelligent Tech Institute of CASIA Co. Ltd.)	
天津中科智能识别产业技术研究院有限公司 (Tianjin Academy for Intelligent Recognition Technologies Co. Ltd.)	
银河水滴科技 (北京) 有限公司 (Watrix [Beijing] Technology Co. Ltd.—aka Watrix.ai)	
浙江数容智能技术开发有限公司	Zhejiang Digital Intelligence Technology Development Co. Ltd.
中科佰能科技股份有限公司 (Bluenergy Technology Co. Ltd.)	
中科搏锐 (北京) 科技有限公司 (Casibrain Technology)	
中科步思德 (洛阳) 智控科技有限公司 (Zhongke Buside [Luoyang] Intelligent Control Technology Co. Ltd.—aka ZKBoost)	

Continued

(*Continued*)

Company name, official English name (if provided)	*Approximate English name (when no official name found)*
中科慧远视觉技术 (洛阳) 有限公司 (CASI Vision Technology [Luoyang] Co. Ltd.)	
中科建昊 (洛阳) 自动化科技有限公司 (Janho Tech [Luoyang] Automation Technology Co. Ltd.)	
中科锐智 (洛阳) 数码科技有限公司	Zhongke Ruizhi (Luoyang) Digital Technology Co. Ltd.
中科唯实科技 (北京) 有限公司 ([Beijing] Vistek Co. Ltd.)	
中科智能 (北京) 投资管理有限公司	Zhongke Smart (Beijing) Investment Management Co. Ltd.
中滦科技股份有限公司 (Zhongluan Technology Co. Ltd.)	

APPENDIX C: SURVEY OF CASIA'S CONTRIBUTIONS TO OR COLLABORATION WITH CHINA'S DEFENSE R&D AND INDUSTRIAL BASE

In the course of probing CASIA and its contributions to China's public security and surveillance apparatuses, evidence of its support for China's defense R&D and industrial base accumulated. With the understanding that separating those streams can be difficult because the relevant research and technologies may be dual-use, this appendix catalogues areas where CASIA is directly involved in defense programs or where it partners with entities such as the PLA and China's nuclear weapons complex.

CASIA Divisions and Research Programs Supporting National Defense

CASIA'S Robot Vision Group (机器视觉课题组) conducts research on areas that can support both surveillance and military purposes, and it claims collaboration with Finland's Nokia Research Institute to "promote practical applications of computer vision research results."[136] The group's English- and Chinese-language websites list completed projects including nine projects funded by the National 863 Program that likely have defense applications.[137] Two additional projects involving the PLA are conspicuously absent from the English-language webpage:

- A 2010–12 project entitled "Optical Image Sequence-Based 3D Model Reconstruction of a Target" in partnership with a PLA unit with a redacted name (中国人民解放军 XXXX 部).
- A 2010–11 project entitled "Multi-view Image-Based 3D Fast Reconstruction System" in collaboration with the PLA's Information Engineering University Institute of Surveying and Mapping (解放军信息工程大学测绘学院).[138]

CASIA's Chinese-language website also lists research projects conducted over the past decade that clearly support China's military, including the following:

- A research project on image processing from synthetic aperture radar (SAR), which discussed how to "extract 3D structure information from SAR images" by utilizing "3D perception mechanisms of human visual systems and methods of computer vision," "generalized learning of 3D target recognition of SAR images under small samples, and 3D visual verification and fast processing of SAR images of typical targets and scenes."[139]

- A project on uncrewed aerial vehicles (UAV) and crewed aircraft gaming theories and technologies, which described "rapid and intelligent attack in the face of rapidly changing enemy aircraft in the co-integration of UAV and crewed aircraft," and "UAV cognitive intelligence and human-machine cognitive co-integration and decision making."[140]

- The creation of a "Joint Innovation Center of Smart Logistics and Intelligent Equipment" between CASIA and the Hangtian Xinguang Group (航天新光集团) in 2014.[141] Hangtian Xinguang, officially known as the Shenyang Hangtian Xinguang Group Co. Ltd. (沈阳航天新光集团有限公司), is a subsidiary of state-owned defense conglomerate China Aerospace Science & Industry Corporation.[142]

Domestic Publications Revealing CASIA Collaboration with PRC Defense Entities

This report identifies seventy-two articles in the domestic publication corpus in which CASIA researchers coauthored publications with entities that clearly support China's defense R&D and industrial base. Many Chinese-language articles list only the divisions or laboratories that the coauthors are affiliated with. Supplemental research identified the parent organizations and their ties to defense entities or programs. The following sample of articles likely underestimates CASIA's contributions to defense research as there are many other civilian institutions that support defense research not included here due to scoping limitations. That said, this survey identified the following:

- Twenty-one articles naming coauthors affiliated with the PLA

- Fifteen articles naming coauthors from one or more of the "Seven Sons of National Defense" universities, which have primary missions to conduct defense research

- Fourteen articles that credit a funding source tied to PRC defense research

- Nine articles involving five of China's major defense state-owned enterprises

- Four articles with coauthors from Nanchang Hangkong University, an aerospace university that conducts defense research

- Three articles with coauthors from the China Academy of Engineering Physics, which hosts China's nuclear weapons R&D and production complex

CASIA's Collaboration with PLA

Table C-1 lists articles in the corpus that show CASIA's research collaboration with entities directly subordinate to the PLA. Additional information on some of these entities and the divisions named in the publications is included below.

The National University of Defense Technology is the PLA's premier scientific and technical R&D institution that focuses on research in computer science, optical engineering, communications engineering, and aerospace sciences.[143]

Another article names coauthor(s) affiliated with the National Nuclear, Biological, and Chemical Disaster Prevention State Key Laboratory (国民核生化灾害防护国家重点实验室) but did not mention the laboratory's parent organization.[144] According to a *Sina* news article on its establishment that cites the state-run China News Service (中国新闻社), this laboratory was subordinate to the Institute of Chemical Defense of the PLA's General Armament Department[145] (总装备部防化研究院)[146] but later transferred to the Academy of Military Sciences

Table C-1. Number of articles published in S&T journals (2014–20) with PLA entities and CASIA coauthorship[147]

PLA institutions	*Articles with CASIA coauthorship*
National University of Defense Technology (国防科技大学)	8
PLA General Hospital (解放军总医院)	2
Fourth Military Medical University (第四军医大学)	2
PLA Unit 91917 (中国人民解放军 91917 部队)	1
PLA Unit 63961 (中国人民解放军 63961 部队)	1
PLA Navy Armament Department Project Management Center (海装装备项目管理中心)	1
PLA Information Engineering University (解放军信息工程大学)	1
PLA Army Officer Academy (解放军陆军军官学院)	1
PLA Army Medical University Chongqing Xinan Hospital Information Section (陆军军医大学重庆西南医院信息科)	1
Naval Research Academy (海军研究院)	1
Institute of Chemical Defense (总装备部防化研究院)	1
Army Research Institute S&T Innovation Research Center (陆军研究院科技创新研究中心)	1
Academy of Military Sciences (军事科学院)	1
2nd Military Medical University (第二军医大学)	1

(军事科学院). The institute has a stated purpose of conducting chemical weapons defense and chemical, biological, and nuclear safety research.[148] It is not known if the institute's mission is strictly defensive in nature given its sensitivity; China claims to adhere to the international Chemical Weapons Convention, which bans the development of offensive chemical weapons.

CASIA's Collaboration with China's "Seven Sons of National Defense" Universities

CASIA has collaborated on research with all of China's "Seven Sons of National Defense" universities. These ostensibly civilian schools have a primary mission of supporting the PRC's military and defense industrial base. These institutions were examined extensively in a previous Hoover Institution report, *Global Engagement: Rethinking Risk in the Research Enterprise*.[149] These seven schools partner with the PLA and state-owned defense enterprises and implement state-directed military-civil fusion efforts (see Table C-2). All seven universities are on the Department of Commerce's Entity List for export control purposes.

Table C-2. Number of articles published in S&T journals (2014–20) with "Seven Sons of National Defense" universities and CASIA coauthorship

Seven Sons university and subdivisions named	*Articles with CASIA coauthorship*
Beihang University (北京航空航天大学) School of Software (软件学院), School of Computer Science (计算机学院), Robotics Institute (机器人研究所)	5
Beijing Institute of Technology (北京理工大学) Chongqing Innovation Center (重庆创新中心), School of Mechatronical [sic] Engineering (机电学院), School of Computer Science (计算机学院)	4
Nanjing University of Science and Technology (第四军医大学) School of Computer Science and Engineering (计算机科学与工程学院)	4
Northwest Polytechnical University (西北工业大学) School of Computer Science (计算机学院), School of Astronautics (航天学院), Key Laboratory of Science and Technology on Aerospace Flight Dynamics (航天飞行动力学技术重点实验室)	4
Harbin Engineering University (哈尔滨工程大学) School of Electro-mechanical Engineering (机电工程学院), Engineering Training National Experimental Teaching and Demonstration Center (工程训练国家级试验教学示范中心)	2
Harbin Institute of Technology (哈尔滨工业大学) School of Computer Science and Technology (计算机科学与技术学院)	2
Nanjing University of Aeronautics and Astronautics (南京航空航天大学) School of Automation (自动化学院), School of Computer Science and Technology (计算机科学与技术学院)	1

Two articles in this corpus have coauthors affiliated with the Key Laboratory of Science and Technology on Aerospace Flight Dynamics (航天飞行动力学技术重点实验室). These articles do not disclose the parent organization of that laboratory. Supplemental research indicates that the laboratory was established jointly by the Beijing Aerospace Control Center (北京航天飞行控制中心) and Northwest Polytechnical University, the latter of which is a "Seven Sons of National Defense" university.[150]

CASIA's Collaboration with PRC Defense Industry

The domestic publication corpus includes ten articles with CASIA-affiliated authors and researchers from five of China's state-owned defense conglomerates: Aviation Industry Corporation of China, China Aerospace Science & Technology Corporation, COMAC Shanghai Aircraft Manufacturing Co. Ltd., China Shipbuilding Industry Corporation, and China Electronics Technology Group Corporation. Bibliographic metadata often provided only the name of the research institute or subsidiary, but supplemental research identified the parent organizations in over half of the articles.

Aviation Industry Corporation of China (AVIC) Three articles named coauthors from AVIC subsidiaries. Two of the articles involved the "China Aero-Polytechnology Establishment [sic] (中国航空综合技术研究所)." The company's website has the AVIC logo adjacent to it and states that it is directly subordinate to AVIC.[151]

One article lists coauthor(s) from AVIC Chengdu Aircraft Industrial Group Co. Ltd. (航空工业成都飞机工业 [集团] 有限责任公司). This company uses the AVIC logo and website domain, confirming AVIC as the parent entity.[152] The company was added to the Department of Commerce Bureau of Industry and Security's "Military End User" list via the amended Export Administration Regulations in 2020.[153]

In light of AVIC Chengdu Aircraft Industrial Group's orientation toward defense, it is interesting to note that this article[154] also names coauthors from COMAC Shanghai Aircraft Manufacturing Co. Ltd. (上海飞机制造有限公司), which claims to focus on commercial aviation (COMAC is short for Commercial Aircraft Corporation of China). In January 2021, the Department of Defense added COMAC to a list of PRC entities that US organizations are barred from conducting business with because it supports China's military modernization efforts.[155]

China Aerospace Science & Technology Corporation (CASC) Two articles list coauthors from the Beijing Institute of Space Control Equipment (北京航天控制仪器研究所). Supplemental research reveals that this organization is a subordinate division of major aerospace defense conglomerate CASC, also referred to as the CASC 13th Institute (航天十三所) under its 9th Academy (中国航天科技集团公司第九研究院第十三研究所). A 2017 job openings announcement described the institute and indicated its relationship to CASC.[156]

Another article listed coauthors from the National Key Laboratory for Aerospace Intelligent Control Technologies (宇航智能控制技术国家级重点实验室) and the Beijing Aerospace Institute of Automation Control (北京航天自动控制研究所).[157] The former entity (the laboratory) is subordinate to the latter institute, which is a research element of the China Academy of Launch Vehicle Technology (CALT).[158] CALT itself is subordinate to CASC and is China's "largest, most important organization for the research, development and production of space launch vehicles, liquid-fueled surface-to-surface missiles, and solid-fueled surface-to-surface and submarine-launched ballistic missiles."[159]

China Shipbuilding Industry Corporation (CSIC) One article names coauthors from the China Ship Research and Development Academy (中国舰船研究院) and discusses AI and maritime warfare.[160] This institute is also known as the 7th Academy of the China Shipbuilding Industry Corporation (中国船舶重工集团公司第七研究院),[161] one of China's state-owned defense conglomerates supporting the PLA Navy.

CASIA's Collaboration with Other Defense Research Entities

The collected corpus includes three articles naming coauthors from CASIA and the China Academy of Engineering Physics (CAEP) Research Center of Laser Fusion (中国工程物理研究院激光聚变研究中心). CAEP is China's primary nuclear weapons R&D and production complex. Additionally, there are four articles with coauthors from Nanchang Hangkong University Ministry of Education Key Laboratory of Nondestructive Testing (南昌航空大学无损检测技术教育部重点实验室). According to the Australian Strategic Policy Institute, this laboratory "engages in high levels of defense research," though it is unclear if the laboratory is designated by the PRC government as a defense key laboratory.[162]

Publications Funded by PRC Defense Programs

In addition to coauthor affiliations, the collected corpus of domestic publications contains fourteen articles that credit a funding source that supports PRC defense research and at least one CASIA-affiliated author. An example is an article entitled "Lightweight Issues of Swarm Intelligence Based Multi-Agent Game Strategy," which credits funding from the National Defense Basic Research Plan Project (国防基础科研计划项目 [JCKY2019203C029] 资助).[163] All of the coauthors are affiliated with CASIA, suggesting that the funding went directly to CASIA. The abstract discusses "intelligent technologies in future warfare," such as autonomous systems used for "intelligent missile swarms and uncrewed aerial vehicle swarms."[164] The article was published in the *Journal of Command and Control*, a periodical jointly run by the Chinese Institute of Command and Control and NORINCO Group's Northern Automatic Control Technology Institute (中国兵器工业集团北方自动控制技术研究所).[165] NORINCO is one of China's key state-owned defense conglomerates.

Table C-3. Number of articles (2014–20) with PRC defense-affiliated entities having US and CASIA coauthorship

Entities supporting PRC defense	*Articles with US and CASIA coauthorship*
Xidian University	38
Beihang University (Seven Sons of National Defense)	33
National University of Defense Technology (subordinate to PLA)	23
Beijing Institute of Technology (Seven Sons of National Defense)	21
University of Electronic Science and Technology of China	21
Northwestern Polytechnical University (Seven Sons of National Defense)	13
Harbin Institute of Technology (Seven Sons of National Defense)	11
(PLA) Air Force Medical University	9
PLA General Hospital	7
Nanjing University of Aeronautics and Astronautics (Seven Sons of National Defense)	3
Nanjing University of Science and Technology (Seven Sons of National Defense)	3
Harbin Engineering University (Seven Sons of National Defense)	3
Southern Medical University (aka PLA First Military Medical University)	3
Academy of Military Medical Sciences	2
China Electronics Technology Group Corporation (CETC)	1
Beijing Computational Science Research Center (subordinate to CAEP)[166]	1
Total	**192**

CASIA Collaboration with PRC Defense Entities and US Institutions

This report's survey of English-language publications identified PRC defense-linked entities whose researchers coauthored articles with CASIA and US institutions. These entities include PLA research institutes and medical facilities, civilian universities that partner with defense entities such as all of the "Seven Sons of National Defense" universities, defense conglomerate China Electronics Technology Group Corporation, which provides surveillance technologies, and a subdivision of China's nuclear weapons complex. Table C-3 lists these entities and the number of articles in which they appear. There are some articles that name more than one entity supporting defense, hence the totals in this table exceed the number of unique articles.

APPENDIX D: SOURCES AND METHODOLOGIES

Generally speaking, Chinese-language sources provide fuller and more current details on CASIA's research programs, partnering entities, and activities. However, English-language

material from both CASIA-run websites and from the collected corpus of international publications described below also proved useful.

Review of CASIA Websites

This report reviews CASIA's main website and the official webpages associated with many of its research divisions and subordinate components. Both English- and Chinese-language versions were studied to compile information on organizational structure, research priorities, major projects, key partners, and international collaboration. This report focuses only on CASIA's associations with public security, surveillance, or national defense activities. Even within that narrow scope, the report could not catalogue all activities of potential ethical or national security concern, and its findings are therefore not exhaustive.

This report centers predominantly on CASIA's National Laboratory of Pattern Recognition and a few of its key partners because of their focus on surveillance-related technologies and research. CASIA's other research centers and divisions and their partnerships and activities warrant similar scrutiny.

Collected Sources of Bibliographic Metadata

Domestic Chinese Publication Sources

The survey of S&T literature involved two sets of extracted bibliographic metadata. The first dataset was derived using the search facilities of major PRC online publication repository China National Knowledge Infrastructure (CNKI) and contains Chinese- and English-language journal articles published in scientific and engineering sources. A total of 493 bibliographic records were retrieved representing articles published from 2014 through the end of 2020 (data was extracted in January 2021) in order to spotlight recent activity and provide a sufficiently large sample. The metadata records had to contain at least one author affiliated with CASIA.

Once the bibliographic metadata was collected and placed into a spreadsheet, the authors conditioned the data to standardize institution names. Data analysis focused on funding sources (when provided), collaborating institutions, and periodical names to identify research that supports China's public security and surveillance operations or national defense. Supplemental internet research in Chinese filled many gaps.

No technical assessments were made on the research in the collected corpus to determine level of maturity or applicability; however, articles were screened for terms in the titles, keywords, or abstracts that clearly focus on surveillance methods, such as video surveillance and facial and iris recognition. A sample of articles was chosen from the collected corpus for further scrutiny and discussion.

The corpus of S&T literature was also screened for CASIA's connections to defense programs, but this effort was limited to identifying institutions that have a *primary* mission to support China's defense R&D. Collaboration between CASIA and other universities that have subdivisions known to support China's military-civil fusion efforts, such as universities co-managed by the State Administration for Science, Technology, and Industry for National Defense, were not included due to scoping limitations. Consequently, this report likely understates the extent of CASIA's involvement in, or support to, defense R&D.

International (English-Language) Publication Sources

Texas A&M University provided a second set of bibliographic data that surveyed international, English-language S&T literature retrieved from *Dimensions* (by Digital Science & Research Solutions, Inc.) via Google BigQuery. The searches involved the following criteria:

- Published year = 2014–20; *and*
- one of the research organizations is CASIA; *and*
- one of the research organizations is a US institution.

This search yielded 744 publication records, which were exported into Excel files. Publication types included journal articles and conference papers or proceedings. A secondary search was conducted on abstracts of articles in the collected corpus using a limited set of keyword terms that relate to surveillance applications:

- Facial recognition
- Target tracking
- Surveillance
- Pose estimation
- Localization
- Gait recognition
- Iris recognition
- Biometrics
- Person detection
- Place recognition
- Landmark
- Location awareness
- Video surveillance or intelligent video surveillance

Other research areas related to computer vision, AI, genetics, and other disciplines were excluded from these searches, though they may support surveillance applications. A

sample of articles from the collected corpus was then selected for close reading. Technical evaluations of articles in that corpus were beyond the scope of this report. Thus, this report may understate the number of publications that involve surveillance research or that present CASIA with opportunities to divert that research to surveillance applications.

Supplemental Internet Research

All aspects of this report required supplemental research. For example, supplemental research identified parent and partnering institutions, ownership of select PRC journal sources, and built profiles of companies and research institutions. In general, Chinese-language searches yielded more fruitful results because many entities had little to no English-language presence online.

ACKNOWLEDGMENTS

The authors wish to thank Kevin Gamache and Andrew Stokes at Texas A&M University for their assistance with data collection and analysis efforts. Special thanks go to Larry Diamond, Jacquelyn Johnstone, and the Hoover Institution for their support.

NOTES

1 Glenn Tiffert, "Compromising the Knowledge Economy: Authoritarian Challenges to Independent Intellectual Inquiry," National Endowment for Democracy, May 2020.

2 See, for example, Ross Andersen, "The Panopticon Is Already Here," *The Atlantic*, September 2020, https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197.

3 For example, in 2020, the US Bureau of Industry & Security added companies and government organs to the Entity List for export controls for engaging in human rights violations and abuses in Xinjiang. ["Commerce Department to Add Nine Chinese Entities Related to Human Rights Abuses in the Xinjiang Uighur Autonomous Region to the Entity List," US Department of Commerce, May 22, 2020, https://www.commerce.gov/news/press-releases/2020/05/commerce-department-add-nine-chinese-entities-related-human-rights.]

4 Metadata compiled included article title, authors and their affiliations, publication source and date, abstract, and funding sources when provided.

5 "Profile," Institute of Automation, Chinese Academy of Sciences, accessed February 3, 2021, http://english.ia.cas.cn/au/bi.

6 "Research Focus," Center for Research on Intelligent Perception and Computing, accessed March 21, 2021, http://cripac.ia.ac.cn/en/EN/column/column36.shtml.

7 "Publication of Hong Kong Business Advisory; Hong Kong-related Designations," US Department of the Treasury, July 16, 2021, https://home.treasury.gov/system/files/126/20210716_hong_kong_advisory.pdf.

8 "Final Report," *National Security Commission on Artificial Intelligence*, 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

9 Tiffert, "Compromising the Knowledge Economy."

10 Glenn Tiffert, Jeffrey Stoff, and Kevin Gamache, *Global Engagement: Rethinking Risks in the Research Enterprise*, (Stanford: Hoover Institution Press, 2020), https://www.hoover.org/sites/default/files/research/docs/tiffert_globalengagement_full_0818.pdf.

11 "Promoting Accountability for Human Rights Abuse with Our Partners," Press Statement by Antony J. Blinken, March 22, 2021, https://www.state.gov/promoting-accountability-for-human-rights-abuse-with-our-partners.

12 A suggested sample of materials that examine these issues includes: (a) James Millward and Dahlia Peterson, "China's System of Oppression in Xinjiang: How It Developed and How to Curb It," (Washington: Brookings Institution, September 2020); (b) Ross Andersen, "The Panopticon Is Already Here"; (c) UYGHUR HUMAN RIGHTS POLICY ACT OF 2020, PUBLIC LAW 116–145, June 17, 2020; (d) Robin Emmott and David Brunnstrom, "West Sanctions China over Xinjiang Abuses, Beijing Hits Back at EU," *Reuters*, March 22, 2021, https://www.reuters.com/article/uk-usa-china-eu-sanctions/west-sanctions-china-over-xinjiang-abuses-beijing-hits-back-at-eu-idUSKBN2BE2LF; (e) Emile Dirks and James Leibold, "Genomic Surveillance: Inside China's DNA Dragnet," Australian Strategic Policy Institute no. 34 (2020); (f) "China: Big Data Program Targets Xinjiang's Muslims," *Human Rights Watch*, December 9, 2020, https://www.hrw.org/news/2020/12/09/china-big-data-program-targets-xinjiangs-muslims; (g) Maya Wang, "China's Techno-Authoritarianism Has Gone Global," Human Rights Watch, April 8, 2021, https://www.hrw.org/news/2021/04/08/chinas-techno-authoritarianism-has-gone-global.

13 For example, see draft bill introduced by the Senate, "United States Innovation and Competition Act of 2021," https://www.democrats.senate.gov/imo/media/doc/DAV21A48.pdf.

14 Metadata compiled included article title, authors and their organizational affiliations, publication name and date, keywords, abstract, and funding sources when provided.

15 This process utilized data collection and conditioning methodologies described in section 1 and accompanying appendix of a previous Hoover Institution report, *Global Engagement: Rethinking Risk in the Research Enterprise* (Stanford: Hoover Institution Press, 2020). A fuller discussion of CNKI as a Chinese domestic source is provided in that report and is not duplicated here.

16 "Profile," Institute of Automation, Chinese Academy of Sciences, date accessed February 3, 2021, http://english.ia.cas.cn/au/bi. The "two bombs" refers to China's development of its first atomic bomb and later the hydrogen bomb and an intercontinental ballistic missile; the "one satellite" refers to China's first artificial satellite.

17 "Profile," Institute of Automation, Chinese Academy of Sciences.

18 CASIA's commercial spin-offs and investments are discussed in depth in section III.

19 "自动化所生物特征识别技术助力首届刑事技术 '双十计划' 攻关创新大赛 [CASIA's Biometric Identification Technology Helps the First Criminal Technology 'Double Ten Plan' Tackling Key Problems Innovation Contest]," December 20, 2019, http://www.ia.cas.cn/xwzx/cyhdt/201912/t20191220_5461809.html.

20 "自动化所与联想集团共建身份认证云服务联合实验室 [CASIA and Lenovo Establish an Authentication Cloud Service Joint Laboratory]," February 3, 2016, http://www.ia.cas.cn/kygz/ydhz/hzdt/201602/t20160203_4530405.html.

21 "2015 人脸识别技术与行业应用研讨会在自动化所召开 [CASIA Convenes 2015 Seminar on Facial Recognition Technology and Industry Applications]," September 14, 2015, www.ia.cas.cn/kygz/ydhz/hzdt/201509/t20150914_4424570.html.

22 "实验室简介 [Lab Overview]," 模式识别国家重点实验室 [National Laboratory of Pattern Recognition], accessed March 26, 2021, www.nlpr.ia.ac.cn/cn/column/22.html.

23 "2012–2016 年度国家科技奖列表 [List of 2012–2016 National S&T Awards]," National Laboratory of Pattern Recognition, accessed March 4, 2021, http://www.nlpr.ia.ac.cn/cn/item/259.html.

24 “Overview,” National Laboratory of Pattern Recognition, accessed March 26, 2021, http://www.nlpr.ia.ac.cn/en/column/122.html.

25 See “CASIA’s Partnerships with Foreign Industry and Research Institutions” in this section for more details on this NLPR-EU partnership.

26 “中心简介 [Center Overview],” 生物识别与安全技术研究中心 [Center for Biometrics and Security Research], accessed March 3, 2021, www.cbsr.ia.ac.cn.

27 “中心简介 [Center Overview],” 智能感知与计算研究中心 [Center for Research on Intelligent Perception and Computing], accessed March 23, 2021, http://www.cripac.ia.ac.cn/CN/column/column143.shtml.

28 Official English titles of organizations are used if provided. In this case, a more direct translation is the CAS Institute of AI Innovation Technology.

29 “中心简介 [Center Overview],” 智能感知与计算研究中心 [Center for Research on Intelligent Perception and Computing].

30 “Databases,” Center for Research on Intelligent Perception and Computing, accessed March 21, 2021, http://cripac.ia.ac.cn/en/EN/folder/folder6.shtml.

31 “Research Focus,” Center for Research on Intelligent Perception and Computing, accessed March 21, 2021, http://cripac.ia.ac.cn/en/EN/column/column36.shtml.

32 中科唯实科技(北京)有限公司 [Beijing Vistek Co. Ltd.], accessed May 9, 2021, http://vistek.cn.

33 “关于我们 [About Us],” 北京中科虹霸科技有限公司 [Beijing IrisKing Co. Ltd.], accessed May 1, 2021, http://www.irisking.com/about.php.

34 “产品系列 [Product Series],” 中科虹星科技有限公司 [IriStar Technology Co. Ltd.], accessed May 2, 2021, http://www.iristar.com.cn/iristar-product.

35 “Gait Recognition” (English page), 银河水滴科技(北京)有限公司 [Watrix Technologies (Beijing) Co. Ltd.], accessed May 13, 2021, http://www.watrix.ai/en/gait-recognition.

36 “Visual Information Processing Group,” National Laboratory of Pattern Recognition, accessed March 21, 2021, http://www.nlpr.ia.ac.cn/en/news/1394.html.

37 “Visual Information Processing Group,” National Laboratory of Pattern Recognition.

38 “研究所简介 [Research Center Overview],” CASIA, accessed August 1, 2021, http://www.ia.cas.cn/gkjj/yjsjj.

39 “About the Research Center for Brain-inspired Intelligence,” Research Center for Brain-inspired Intelligence, accessed March 23, 2021, https://bii.ia.ac.cn/about.htm.

40 Examples of articles that have surveillance and defense applications include: (a) Tielin Zhang et al., “Cognitive Template-Clustering Improved LineMod for Efficient Multi-object Pose Estimation,” *Cognitive Computation* 12, 834–43 (2020), https://doi.org/10.1007/s12559-020-09717-5; (b) Dongcheng Zhao and Yi Zeng, “Dynamic Fusion of Convolutional Features Based on Spatial and Temporal Attention for Visual Tracking,” 2019 International Joint Conference on Neural Networks (IJCNN), 14–19 July 2019, *IEEE*, https://doi.org/10.1109/IJCNN.2019.8852301; and (c) Y. Zeng, G. Wang, and B. Xu, “A Basal Ganglia Network Centric Reinforcement Learning Model and Its Application in Unmanned Aerial Vehicle,” *IEEE Transactions on Cognitive and Developmental Systems*, vol. 10, no. 2 (June 2018): 290–303, doi: 10.1109/TCDS.2017.2649564.

41 “About Us,” Brainnetome Center, accessed March 20, 2021, http://www.brainnetome.org/au; and http://www.brainnetome.org/cn/nwlzbjszdsys/gjgwwyh.

42 “About Us,” Brainnetome Center.

43 Vidushi Marda et al., "Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights," *Article 19*, January 2021.

44 "智能制造技术与系统研究中心 [Intelligent Manufacturing Technology and System Research Center]," CAS Institute of Automation, accessed March 23, 2021, http://www.ia.cas.cn/jgsz/kyxt/bm3.

45 For a detailed discussion on the WRSA's role in facilitating technology transfers, see William Hannas and Didi Kirsten Tatlow, eds., *China's Quest for Foreign Technology: Beyond Espionage* (Abingdon, UK: Routledge 2021), 263–67.

46 "Congratulations on Professor Tieniu Tan successfully elected as a standing committee member of the 13th CPPCC National Committee," CRIPAC, accessed April 1, 2021, http://cripac.ia.ac.cn/en/EN/news/news81.shtml; and "Tieniu Tan," CRIPAC, accessed April 1, 2021, http://cripac.ia.ac.cn/en/EN/column/item80.shtml.

47 This is a translation of the Chinese project name appearing on Tan's CV; original Chinese is "面向公共安全的社会感知数据处理."

48 "谭铁牛 [Tan Tieniu]," CAS Institute of Automation, August 2009, http://www.ia.cas.cn/sourcedb_ia_cas/cn/iaexpert/200908/t20090804_2310461.html; and "谭铁牛 [Tan Tieniu]," CRIPAC, accessed April 1, 2021, http://cripac.ia.ac.cn/CN/column/item83.shtml.

49 See section III for details on these identified companies with which Tan affiliates.

50 Intel Corporation provided its own news release on this partnership, calling it the China Intel Internet of Things Joint Labs (https://newsroom.intel.com/news-releases/intel-beijing-municipal-government-and-chinese-academy-of-sciences-establish-internet-of-things-joint-research/#gs.102fo3d).

51 "中国英特尔物联技术研究院正式挂牌投入运营 [China Intel Internet of Things Technology Institute Officially Begins Operations]," CAS Institute of Automation, December 9, 2012, http://www.ia.cas.cn/kygz/ydhz/hzdt/201310/t20131011_3948581.html.

52 Several of the participating institutions in China are also extensively engaged in defense research, such as Northwestern Polytechnical University, CAS Institute of Remote Sensing and Digital Earth, and the University of Electronic Science and Technology of China.

53 "The Sino-French Laboratory in Computer Science, Automation and Applied Mathematics," CAS Institute of Automation, August 7, 2009, http://english.ia.cas.cn/rd/200908/t20090807_27606.html; and "About Us," LIAMA, accessed March 22, 2021, http://liama.ia.ac.cn/about-about.html.

54 "Research—Multi Modal Sensing and Scene Understanding," LIAMA, November 10, 2016, http://liama.ia.ac.cn/research-researchd-cid-4-dataId-14.html.

55 "Speech and Language Information Processing Group," National Laboratory of Pattern Recognition, accessed March 3, 2021, http://www.nlpr.ia.ac.cn/en/news/1396.html.

56 "Introduction," CAS Institute of Automation, accessed March 3, 2021, http://english.ia.cas.cn/ic/introduction/.

57 "核心技术发明人 [Core Technology Inventors]," 中科唯实科技(北京)有限公司 [Beijing Vistek Co. Ltd.], accessed May 9, 2021, http://vistek.cn/pro.html.

58 中科唯实科技(北京)有限公司 [Beijing Vistek Co. Ltd.].

59 "监狱监控解决方案 [Prison Monitoring Solutions]," 中科唯实科技(北京)有限公司 [Beijing Vistek Co. Ltd.], accessed May 9, 2021, http://vistek.cn/jail.html; and "公共安全领域人员监控解决方案 [Solutions in Public Security Fields and Monitoring Personnel]," Beijing Vistek Co. Ltd., accessed May 9, 2021, http://vistek.cn/sub.html.

60 "智慧园区解决方案 [Smart Zone Solutions]," Beijing Vistek Co. Ltd., accessed May 9, 2021, http://vistek.cn/garden.html.

61 This partnership between CASIA and Intel Corp is briefly described in section II.

62 “合作伙伴 [Cooperative Partners],” Beijing Vistek Co. Ltd., accessed May 9, 2021, http://vistek.cn/cooperation.html.

63 “About IrisKing,” Beijing IrisKing Co. Ltd., accessed May 1, 2021, http://en.irisking.com.

64 “关于我们 [About Us],” 北京中科虹霸科技有限公司 [Beijing IrisKing Co. Ltd.], accessed May 1, 2021, http://www.irisking.com/about.php.

65 “中科虹霸虹膜数据建库及应用服务技术荣获公安部科学技术三等奖 [Iris Database Building and Application Services Wins Third Prize for S&T by Ministry of Public Security],” November 12, 2020, http://www.irisking.com/newsn.php?id=660.

66 “河南省委书记王国生率河南党政代表团莅临参观指导 [Henan Provincial Party Secretary Wang Guosheng Leads Party and Government Delegation for a Visit and Guidance],” December 21, 2020, http://www.irisking.com/newsn.php?id=656.

67 “关于我们 [About Us],” 北京中科虹霸科技有限公司 [Beijing IrisKing Co. Ltd.], accessed May 1, 2021, http://www.irisking.com/about.php.

68 “关于我们 [About Us],” 中科虹星科技有限公司 [IriStar Technology Co. Ltd.], accessed May 2, 2021, http://www.iristar.com.cn/iristar-about.

69 “产品系列 [Product Series],” 中科虹星科技有限公司 [IriStar Technology Co. Ltd.], accessed May 2, 2021, http://www.iristar.com.cn/iristar-product.

70 产品系列 [Product Series],” 中科虹星科技有限公司 [IriStar Technology Co. Ltd.].

71 “虹星科技虹膜人脸识别一体机通过公安部一所检测认证 [IriStar’s Integrated Iris and Facial Recognition Machine Passes Ministry of Public Security First Institute Testing Certification],” August 20, 2020, http://www.iristar.com.cn/news-details/37.

72 “虹星科技喜获生物特征识别机构注册证书 面部多模态融合识别发展迈入快车道 [IriStar Is Happy to Be Awarded a Registration Certificate from Biometric Identification Organs and the Development of Facial Multimodal Fusion Recognition Is on the Fast Track],” June 23, 2020, http://www.iristar.com.cn/news-details/33.

73 “合作伙伴 [Cooperative Partners],” 中科虹星科技有限公司 [IriStar Technology Co. Ltd.], accessed May 2, 2021, http://www.iristar.com.cn/index.

74 “公司简介 [Company Profile],” 银河水滴科技(北京)有限公司 [Watrix Technologies (Beijing) Co. Ltd.], accessed May 12, 2021, http://www.watrix.ai/company-profile/.

75 “Watrix Technologies (Beijing) Co. Ltd. [银河水滴科技 (北京) 有限公司],” 企查查 [QCC.com], accessed May 14, 2021, https://www.qcc.com/firm/2ced25f6fcb1da7f3658d2621f78b842.html.

76 “步态识别 [Gait Recognition],” 银河水滴科技(北京)有限公司 [Watrix Technologies (Beijing) Co. Ltd.], accessed May 12, 2021, http://www.watrix.ai/anfang.

77 “Gait Recognition” (English page), 银河水滴科技(北京)有限公司 [Watrix Technologies (Beijing) Co. Ltd.], accessed May 13, 2021, http://www.watrix.ai/en/gait-recognition.

78 *Global Times* is a nationalistic English daily overseen by the official CCP daily *Renmin Ribao*. It is curious that the CCP chose to detail Watrix’s capabilities in a paper that is intended for foreign audiences.

79 Liu Caiyu, “Chinese Cities Pilot Gait Recognition System,” *Global Times*, July 4, 2019, http://www.globaltimes.cn/content/1156769.shtml.

80 “步态数据库建设 [Gait Database Construction], 银河水滴科技(北京)有限公司 [Watrix Technologies (Beijing) Co. Ltd.], accessed May 13, 2021, http://www.watrix.ai/portfolio-item/ebutaishujuku.

81 “工业视觉 [Industrial Vision],” 银河水滴科技(北京)有限公司 [Watrix Technologies (Beijing) Co. Ltd.], accessed May 14, 2021, http://www.watrix.ai/jiance.

82 “About Us,” Beijing Hisign Technology Co. Ltd., accessed May 12, 2021, http://en.hisign.com.cn/About.asp.

83 CASIA’s ownership stake in ViSystem is unknown.

84 “公司简介 [Company Profile],” 北京多维视通技术有限公司 [Beijing ViSystem Corporation Ltd.], accessed May 13, 2021, https://www.visystem.cn/company-profile.

85 “公司简介 [Company Profile],” 北京多维视通技术有限公司 [Beijing ViSystem Corporation Ltd.].

86 “产品 [Products],” 北京多维视通技术有限公司 [Beijing ViSystem Corporation Ltd.], accessed May 13, 2021, https://www.visystem.cn/product?filter=1&f=product_line&k=2.

87 “产品 [Products],” 北京多维视通技术有限公司 [Beijing ViSystem Corporation Ltd.].

88 “视频侦查技术联合实验室挂牌仪式在京举行 [Joint Laboratory of Video Investigation Technology Launch Ceremony Held in Beijing],” 中国警察网 [China Police Net], March 1, 2013, http://www.cpd.com.cn/n10216060/n10216148/c15961657/content.html.

89 For example, Amnesty International urged EU nations to stop exporting technologies to China that enable this Skynet program. See the September 21, 2020, article, “EU Companies Selling Surveillance Tools to China’s Human Rights Abusers,” (https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers).

90 “院校合作 [College Cooperation],” 北京多维视通技术有限公司 [Beijing ViSystem Corporation Ltd.], accessed May 13, 2021, https://www.visystem.cn/college-cooperation.

91 “生态合作伙伴 [Ecological Partners],” 北京多维视通技术有限公司 [Beijing ViSystem], accessed May 11, 2021, https://www.visystem.cn/eco-partners.

92 US Department of Justice, Office of Public Affairs, “Chinese Telecommunications Device Manufacturer and Its US Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction of Justice,” January 28, 2019, https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade.

93 See appendix D for details on collection methodology and sourcing.

94 “Commerce Department to Add Nine Chinese Entities Related to Human Rights Abuses in the Xinjiang Uighur Autonomous Region to the Entity List,” May 22, 2020, https://www.commerce.gov/news/press-releases/2020/05/commerce-department-add-nine-chinese-entities-related-human-rights.

95 唐云祁 [Tang Yunqi], 孙哲南 [Sun Zhenan], and 谭铁牛 [Tan Tieniu], “头部姿势估计研究综述 [A Survey on Head Pose Estimation],” 模式识别与人工智能 [*Pattern Recognition and Artificial Intelligence*] 3 (March 2014): 213–-25.

96 “学校简介 [School Overview],” 中国人民公安大学 [People’s Public Security University], accessed March 14, 2021, www.ppsuc.edu.cn/xxgk/xxjj.htm.

97 金鑫 [Jin Xin] et al., “面向嵌入式系统的高精度实时人群计数算法研究 [Real-Time Crowd Counting for Embedded Systems with High Accuracy],” 高技术通讯 [*High Technology Letters*] 30 (2020): 32–40, http://dx.doi.org/doi%EF%BC%9A10.3772/j.issn.1002-0470.2020.01.004.

98 “《高技术通讯》简介 [‘High Technology Letters’ Overview],” accessed March 15, 2021, http://www.hitech863.com/gjstxcn/ch/first_menu.aspx?parent_id=20121106055516001.

99 王财勇 [Wang Caiyong] and 孙哲南 [Sun Zhenan], “虹膜分割算法评价基准 [A Benchmark for Iris Segmentation],” 计算机研究与发展 [*Journal of Computer Research and Development*] 57, no. 2 (2020): 395–412, doi: 10.7544/issn1000-1239.2020.20190092.

100 杨彬 [Yang Bin] et al., “基于视频的三维人体姿态估计 [Three-Dimensional Human Pose Estimation Based on Video],” 北京航空航天大学学报 [*Journal of Beijing University of Aeronautics and Astronautics*] 45, no.12 (2019): 2463–69, https://doi.org/10.13700/j.bh.1001-5965.2019.0384.

101 于成丽 [Yu Chengli] and 刘浩 [Liu Hao], “生物识别技术的发展应用及安全问题研究 [Research on Biometrics Technology Development Applications and Security Issues],” 保密科学技术 [*Secrecy Science & Technology*] 5 (2018): 28–31.

102 “所属单位 [Subordinate Units],” 国家保密局 [National Administration of State Secrets Protection], accessed March 25, 2021, http://www.gjbmj.gov.cn/n1/2017/0309/c409087-29134356.html.

103 李子青 [Li Ziqing], “人脸识别结合视频监控 看公安与金融市场应用 [Facial Recognition Combined with Video Surveillance, Examining Public Security and Financial Market Applications],” 中国安防 [*China Security & Protection*] 15 (2015): 35–38.

104 “中国安防杂志 [China Security & Protection Magazine],” 公务员期刊网 [Civil Service Journal Network], accessed May 30, 2021, https://www.21ks.net/gzqk/gzqk_15058.html.

105 朱志华 [Zhu Zhihua], “线形痕迹三维点云去噪技术研究 [Attempt to Denoise into 3D-point Cloud of Linear Trace],” 刑事技术 [*Forensic Science & Technology*] 45, no. 6 (2020): 556–61, doi:10.16467/j.1008-3650.2020.06.002.

106 “刑事技术杂志 [Forensic Science & Technology Magazine],” 公务员期刊网 [Civil Service Journal Network], accessed May 30, 2021, https://www.21ks.net/shkx/shkx_18672.html.

107 刘国文 [Liu Guowen] et al., “基于改进 RetinaNet 模型的接触网鸟巢检测 [Detection of Birds’ Nest in Catenary Based on Improved RetinaNet Model],” 数据采集与处理 [*Journal of Data Acquisition & Process*] 35, no. 3 (2020): 563–71: doi:10.16337/j.1004-9037.2020.03.018.

108 金鑫 [Jin Xin] et al., “面向嵌入式系统的高精度实时人群计数算法研究 [Real-Time Crowd Counting for Embedded Systems with High Accuracy],” 高技术通讯 [*Chinese High Technology Letters*] 1 (2020): 32–40, DOI:10.3772/j.issn .1002-0470.2020.01.004.

109 艾乐 [Ai Le] and 张志忠 [Zhang Zhizhong], “关于指纹三角区域的深度残差网络检测仿真 [Simulation of Deep Residual Network Detection in Fingerprint Triangle Region],” 计算机仿真 [*Computer Simulation*] 12 (2019): 455–58, 467.

110 杜长德 [Du Changde] and 何晖光 [He Huiguang], “基于视觉信息编解码的深度学习类脑机制研究 [Study of Brain-Like Mechanisms of Deep Learning Based on Visual Information Encoding and Decoding],” 张江科技评论 [*Zhangjiang Technology Review*] 4 (2019): 25–27.

111 孙鹏 [Sun Peng] et al., “图像拼接篡改的自动色温距离分类检验方法 [Detection of Image Splicing Manipulation by Automated Classification of Color Temperature Distance],” 自动化学报 [*Acta Automatica Sinica*] 44, no.7 (2018): 1321–32, doi:10.16383/j.aas.2017.c170267.

112 “现场物证溯源技术国家工程实验室启动仪式, 理事会暨技术委员会会议在京召开” [National Engineering Laboratory of Evidence Traceability Technology Launch Ceremony, Council and Technical Committee Convenes in Beijing],” CAS Beijing Institute of Genomics/China National Center for Bioinformation, September 14, 2017, http://www.big .cas.cn/xwdt/kyjz/201709/t20170918_5747709.html.

113 康运锋 [Kang Yunfeng] et al., “人像属性识别关键技术研究进展及应用探索 [Exploration of Research Progress on Portrait Attribute Recognition Key Technologies and Applications],” 警察技术 [*Police Technology*] 12 (2018): 12–16.

114 史明霞 [Shi Mingxia] et al., “肺部图像配准关键技术及研究现状 [Key Technology and Research Status of Registration Methods for Pulmonary Image],” 北京生物医学工程 [*Beijing Biomedical Engineering*] 4 (2017): 427–32.

115 “中盾介绍 [About Zhongdun],” 北京中盾安全技术开发公司 [Beijing Zhongdun Security Technology Development Co.], accessed June 1, 2021, http://www.zhongdun.com.cn/about/introduction.

116 史明霞 [Shi Mingxia] et al., “基于 SIFT 特征的肺部非刚性配准应用研究 [Research on Application of Pulmonary Non-rigid Registration Method with 3 D-SIFT Features],” 计算机技术与发展 [*Computer Technology and Development*] 27, no. 11 (2017): 181–86, doi:10.3969/j.issn.1673-629X.2017.11.039.

117 臧亚丽 [Zang Yali] and 杨鑫 [Yang Xin], “指纹识别技术研究热点与新方向 [Hot Areas and New Directions in Fingerprint Identification Technology Research],” 警察技术 [*Police Technology*] 5 (2015): 3–7.

118 张旭 [Zhang Xu] et al., “视频取证技术研究进展 [A Survey of Video Forensic Technology],” 刑事技术 [*Forensic Science and Technology*] 2 (2015): 87–93, doi: 10.16467/j.1008-3650.2015.02.001.

119 See section III for a profile of ViSystem and its support to public security and surveillance.

120 何耘 [He Wei], “荧光素钠在切伦科夫能量转移中的应用 [Application of Fluoroescein Sodium on Cerenkov Radiation Energy Transfer],” 中华核医学与分子影像杂志 [*Chinese Journal of Nuclear Medicine and Molecular Imaging*] 35, no. 1 (2015): 59–62, doi: 10.3760/cma.j.issn.2095-2848.2015.01.014.

121 陈龙 [Chen Long], “智慧城市 PK 平安城市 [Smart City PK Safe City],” 智能建筑与城市信息 [*Intelligent Building and City Information*] 5 (2014): 9–14, doi:10.13655/j.cnki.ibci.2014.05.003.

122 唐云祁 [Tang Yunqi] et al., “头部姿势估计研究综述 [A Survey on Head Pose Estimation],” 模式识别与人工智能 [*Pattern Recognition and Artificial Intelligence*] 27, no. 3 (2014): 213–25.

123 孙辉 [Sun Hui] et al., “法医 DNA 片段分析软件的研究与应用 [Research and Applications of Forensic DNA Fragment Analysis Software],” 警察技术 [*Police Technology*] 1 (2014): 15–17, doi:10.3969/j.issn.1009-9875.2014.01.004.

124 Dai Li et al., “ISEE: An Intelligent Scene Exploration and Evaluation Platform for Large-Scale Visual Surveillance,” *IEEE Transactions on Parallel and Distributed Systems* 30 no. 12 (2019): 2743–58, doi: 10.1109/TPDS.2019.2921956.

125 Li et al., “ISEE,” 2744.

126 Xinchu Shu et al., “Rank-1 Tensor Approximation for High-Order Association in Multi-Target Tracking,” *International Journal of Computer Vision* 127 (2019) 1063–83, doi: 10.1007/s11263-018-01147-z.

127 Shu et al., “Rank-1 Tensor Approximation,” 1063.

128 Ran He et al., “Learning Structured Ordinal Measures for Video Based Face Recognition,” *Pattern Recognition* 75 (2018): 4–14, doi: 10.1016/j.patcog.2017.02.005.

129 Shifeng Zhang et al., “Single-Shot Refinement Neural Network for Object Detection,” *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition* (2018): 4203–12, doi: 10.1109/CVPR.2018.00442.

130 “中心简介 [Center Overview],” 生物识别与安全技术研究中心 [Center for Biometrics and Security Research], http://www.cbsr.ia.ac.cn.

131 “Final Report,” *National Security Commission on Artificial Intelligence*, 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

132 “NSF Scientific Integrity Policy,” *National Science Foundation*, revised October 29, 2019, https://www.nsf.gov/bfa/dias/policy/si/sipolicy.pdf.

133 For instance, a Yale geneticist collaborated with China, which enabled the PRC to carry out mass genetic surveillance of Uighurs in Xinjiang. The geneticist assumed his PRC partners were acting within scientific norms that require informed consent by DNA donors. See Sui-Lee Wee, “China Uses DNA to Track Its People, with the Help of American Expertise,” *New York Times*, February 21, 2019, https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html.

134 “中心简介 [Center Introduction],” 智能系统与工程研究中心 [Center for Research on Intelligent System and Engineering], accessed March 15, 2021, http://www.crise.ia.ac.cn/about.aspx?TypeId=1&FId=t1:1:1.

135 “持股企业 [Shareholding Enterprises],” 北京中自投资管理有限公司 [Beijing CASIA Investment Management Co. Ltd.], accessed May 5, 2021, http://www.caspark.com.cn/page94.

136 “机器视觉课题组 [Robot Vision Group],” National Laboratory of Pattern Recognition, accessed March 3, 2021, http://vision.ia.ac.cn/zh/index_cn.html.

137 A few examples include: “3D Terrain Reconstruction Based on Stereo Images,” “Active Vision Based Robot Navigation System,” and “Panoramic Map Real-Time Generation and Rapid Updating.”

138 “机器视觉课题组承担的科研项目 [Scientific Research Projects Undertaken by Robot Vision Group],” accessed March 3, 2021, http://vision.ia.ac.cn/zh/projects/index.html.

139 “SAR 图像视觉三维认知理论与方法 [SAR (Synthetic Aperture Radar) Image Visual 3D Cognition Theory and Methods],” September 11, 2020, http://www.ia.cas.cn/kygz/zdxm/202009/t20200911_5695665.html.

140 “无人机与有人机共融博弈的基础理论与关键技术研究 [Research on Basic Theory and Key Technologies of Integrated Uncrewed Aerial Vehicles and Crewed Aircraft Games],” September 11, 2020, http://www.ia.cas.cn/kygz/zdxm/202009/t20200911_5695696.html.

141 “自动化所与航天新光集团共建智慧物流与智能装备联合创新中心 [CAS Institute of Automation and Hangtian Xinguang Group Establish the Joint Innovation Center of Smart Logistics and Intelligent Equipment],” April 28, 2014, http://www.ia.cas.cn/kygz/ydhz/hzdt/201501/t20150112_4297149.html.

142 “公司简介: 沈阳航天新光集团有限公司 [Company Overview—Shenyang Hangtian Xinguang Group Co. Ltd.],” accessed March 27, 2021, http://htxg.chinaepu.com; and “沈阳航天新光集团有限公司,” 百度百科 [Baidu Baike], accessed March 27, 2021, https://baike.baidu.com/item/%E6%B2%88%E9%98%B3%E8%88%AA%E5%A4%A9%E6%96%B0%E5%85%89%E9%9B%86%E5%9B%A2%E6%9C%89%E9%99%90%E5%85%AC%E5%8F%B8/10206449?fr=aladdin.

143 “学校概况 [School Overview],” National University of Defense Technology [国防科技大学], accessed March 16, 2021, https://web.archive.org/web/20170602170852/http://www.nudt.edu.cn/introduce.asp?classid=4.

144 张根伟 [Zhang Genwei] et al., “一种离子迁移谱谱图重构及特征峰提取算法 [Ion Mobility Spectrometry Spectrum Reconstruction and Characteristic Peaks Extraction Algorithm Research],” 光谱学与光谱分析 [*Spectroscopy and Spectral Analysis*] 40, no. 9 (2020): 2681–85, doi:10.3964/j.issn.1000-0593(2020)09-2681-05.

145 PLA’s General Armament Department is now known as the Equipment Development Department.

146 “中国国民核生化灾害防护国家重点实验室揭牌 [China National Nuclear, Biological, and Chemical Disaster Prevention State Key Laboratory Unveiled],” 中国新闻网 [China News Service], December 18, 2012, http://news.sina.com.cn/o/2012-12-18/161825840018.shtml.

147 There are several articles in this corpus that named coauthors from CASIA and more than one entity supporting China’s defense research base in the same article; thus the totals tallied in the tables exceed the seventy-two unique articles in the corpus.

148 “中国人民解放军军事科学院防化研究院–2020 年人才招聘 [PLA Academy of Military Sciences Institute of Chemical Defense – 2020 Recruitment],” accessed March 16, 2021, http://www.sciencehr.net/uploads/fhyjy.

149 Specifically, see chapter 1: “Under the Radar: National Security Risk in US-China Scientific Collaboration,” in Tiffert et al., *Global Engagement: Rethinking Risk in the Research Enterprise* (Stanford: Hoover Institution Press, 2020).

150 “航天飞行动力学技术重点实验室 [Key Laboratory of Science and Technology on Aerospace Flight Dynamics],” accessed March 9, 2021, https://hangkong.nwpu.edu.cn/info/1204/2622.htm.

151 “About the Enterprise [企业简介],” 中国航空综合技术研究所 [China Aero-Polytechnology Establishment], accessed March 9, 2021, http://www.airyc.cn/Com/Cominfo/6515847/index.html.

152 “航空工业成都飞机工业(集团) 有限责任公司 [AVIC Chengdu Aircraft Industrial Group Co. Ltd.],” accessed March 18, 2021, http://cac.avic.com/web=.

153 “Addition of ‘Military End User’ (MEU) List to the Export Administration Regulations and Addition of Entities to the MEU List,” Bureau of Industry and Security, 12/23/2020, Docket No. 201215-0344, https://www.federalregister.gov/documents/2020/12/23/2020-28052/addition-of-military-end-user-meu-list-to-the-export-administration-regulations-and-addition-of.

154 周良明 [Zhou Liangming] et al., “飞机结构件内腔机器人自动打磨工艺 [Technology of Robotic Automatic Grinding Internal Surface in Aircraft Structural Parts],” 科学技术与工程 [*Science Technology and Engineering*] 36 (2019): 128–33.

155 Mike Stone, “Exclusive: Trump Administration Adds China’s Comac, Xiaomi to Chinese Military Blacklist,” *Reuters*, January 14, 2021, https://www.reuters.com/article/us-usa-china-comac-military-exclusive-idUSKBN29J2HK.

156 “航天十三所 2017 年校园招聘启事 [CASC 13th Institute’s 2017 Campus Recruitment],” October 15, 2016, https://webcache.googleusercontent.com/search?q=cache:HbnX2yyxTSsJ:https://ee.seu.edu.cn/2016/1015/c25267a171889/page.htm+&cd=5&hl=en&ct=clnk&gl=us.

157 张伯川 [Zhang Bochuan] et al., “一种新的基于目标区域知识的地面复杂场景目标显著性计算方法 [A New Method for Calculating the Saliency of Target of Complicated Ground Background Based on the Target’s Regional Knowledge],” 自动化与仪器仪表 [*Automation & Instrumentation*] 10 (2019): 98–100, 105.

158 “北京航天自动控制研究所在集团公司重点实验室考核评比中获第一名 [Beijing Institute of Space Flight Automation and Control Receives First Place in Industry Group Key Laboratories Assessment],” 中国运载火箭技术研究院新闻中心 [CALT News Center], April 20, 2020, www.calt.com/n481/n497/n855/c17574/content.html.

159 “China Academy of Launch Vehicle Technology (CALT),” Nuclear Threat Initiative, February 1, 1994, www.nti.org/learn/facilities/59.

160 蹇成刚 [Jian Chenggang] et al., “人工智能应用于海战场网络信息体系总体设计的关键问题 [The Key Problems of AI Applied to the System Design of the Network Information System in the Sea Battlefield],” 舰船科学技术 [*Ship Science and Technology*] 41, no. 11 (2019): 180–83.

161 “中国舰船研究院 [China Ship Research and Development Academy],” March 5, 2019, webcache.googleusercontent.com/search?q=cache:qItgZw5paFgJ:www.cansi.org.cn/xievip/shownews.php%3Flang%3Dcn%26id%3D10589+&cd=5&hl=en&ct=clnk&gl=us; and “中国舰船研究院 [China Ship Research and Development Academy],” 百度百科 [Baidu Baike], accessed March 9, 2021, baike.baidu.com/item/%E4%B8%AD%E5%9B%BD%E8%88%B0%E8%88%B9%E7%A0%94%E7%A9%B6%E9%99%A2.

162 Alex Joske, The China Defence Universities Tracker, Report No. 23 (Canberra: Australian Strategic Policy Institute, 2019), accessed March 9, 2021, https://unitracker.aspi.org.au/universities/nanchang-hangkong-university.

163 曾隽芳 [Zeng Junfang] et al., “多智能体群智博弈策略轻量化问题 [Lightweight Issues of Swarm Intelligence Based Multi-Agent Game Strategy],” 指挥与控制学报 [*Journal of Command and Control*] 4 (2020): 381–87.

164 曾隽芳 [Zeng Junfang] et al., “多智能体群智博弈策略轻量化问题 [Lightweight Issues of Swarm Intelligence Based Multi-Agent Game Strategy].

165 “指挥与控制学报 [About the Journal of Command and Control],” website of *Journal of Command and Control*, accessed March 8, 2020, www.jc2.org.cn/CN/column/column105.shtml.

166 “Addition of Entities to the Entity List, Revision of Certain Entries on the Entity List,” June 5, 2020, https://www.federalregister.gov/documents/2020/06/05/2020-10869/addition-of-entities-to-the-entity-list-revision-of-certain-entries-on-the-entity-list.

hoover.org

27 26 25 24 23 22 21 7 6 5 4 3 2 1

About the Authors

JEFFREY STOFF

Jeffrey Stoff is the founder of Redcliff Enterprises, a start-up that seeks to build public-private partnerships dedicated to protecting research and intellectual capital. Stoff spent eighteen years in the US government as a senior analyst focused on critical technology protection issues. He has advised the White House, departments of Defense and State, and the Office of the Director of National Intelligence.

GLENN TIFFERT

Glenn Tiffert is a research fellow at the Hoover Institution and a historian of modern China. He manages the Hoover project on China's Global Sharp Power and works closely with government and civil society partners to document and build resilience against authoritarian interference with democratic institutions. He coauthored and edited the Hoover report *Global Engagement: Rethinking Risk in the Research Enterprise* (2020).

China's Global Sharp Power

A Hoover Institution Project

The Hoover Institution's project on China's Global Sharp Power (CGSP) tracks, documents, and analyzes how China's Communist party-state operates in the shadows to shape and control information flows, coerce governments and corporations, infiltrate and corrupt political systems, and exploit, disrupt, and debase civic institutions, particularly in open and democratic societies. Through its research and global partnerships, CGSP produces papers, lectures, conferences, workshops, publications, and web-accessible resources to educate opinion leaders and policy makers so that they may pursue diverse, balanced, and vigilant relationships with China, tailored to their circumstances.

For more information about this Hoover Institution project, visit us online at www.hoover.org/research-teams/chinas-global-sharp-power-project.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION