CSET CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

China's STI Operations

MONITORING FOREIGN SCIENCE AND TECHNOLOGY THROUGH OPEN SOURCES

AUTHORS
Wm. C. Hannas
Huey-Meei Chang

科技情报

JANUARY 2021

CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

Established in January 2019, the Center for Security and Emerging Technology (CSET) at Georgetown's Walsh School of Foreign Service is a research organization focused on studying the security impacts of emerging technologies, supporting academic work in security and technology studies, and delivering nonpartisan analysis to the policy community. CSET aims to prepare a generation of policymakers, analysts, and diplomats to address the challenges and opportunities of emerging technologies. CSET focuses on the effects of progress in artificial intelligence, advanced computing, and biotechnology.

CSET.GEORGETOWN.EDU | CSET@GEORGETOWN.EDU

JANUARY 2021

China's STI Operations

MONITORING FOREIGN SCIENCE AND TECHNOLOGY THROUGH OPEN SOURCES

AUTHORS
Wm. C. Hannas
Huey-Meei Chang

PRINT AND ELECTRONIC DISTRIBUTION RIGHTS

Cover illustration: "S&T Intelligence" in Chinese.

Document Identifier: doi: 10.51593/20200049

Contents

Executive Summary

The United States is no longer the hegemon in worldwide research and development (R&D) and is vulnerable to technical surprise. This country's fragmentary, secrets-based monitoring of foreign science and technology will not protect it in an era of rapid global development. Can open source intelligence lead the way?

- China and the United States hold opposing views of "open source" and its role in the intelligence process. In the United States, Open Source Intelligence (OSINT) "enables" classified reporting, while in China it is the "INT" of first resort.
- The contrast extends to "science and technology intelligence," which has a lower priority in the U.S. system, whereas China and its top leaders personally lavish great attention on STI and rely on it for national decisions.
- Chinese monitoring through open sources of foreign science and technology (S&T) is based on statutes dating to 1958. The system supported China's development of nuclear and other strategic weapons, and its paramount role persists today.
- While centrally directed, China's STI apparatus is distributed and functions at all levels in separate but interlocking organizations. Some 100,000 S&T intelligence workers—open source collectors, analysts, and field operatives—make up its ranks.
- Accessible Chinese documents provide ample evidence of the system's design and operations. An astonishing amount of thought goes into its makeup and daily execution, with a premium on metrics and "customer" interaction.

- Chinese authorities do not naturally distinguish "intelligence" from "information." A byproduct of the language, the two ideas are a fused concept expressed by one word: *qingbao*. This feature may account for different attitudes toward the role of open source in the intelligence process.
- More than a dozen journals support China's STI enterprise, as do social organizations at the national and local levels. The apparatus is staffed by experts in all relevant disciplines, attesting to its thorough professionalization.
- The roles of the Chinese system and its much smaller U.S. counterpart differ: China tracks—and transfers—foreign S&T. An effective American STI program must monitor these transfers for an accurate picture of China's S&T profile, which in balance narrows the difference in workloads.
- We recommend creating a "National S&T Analysis Center" within the U.S. government to address its vulnerability to technical surprise. China's success at STI is evidence that a viable monitoring system can be built and offers examples of how to do so.

Introduction

For six decades, China has operated a state-of-the-art science and technology intelligence (STI) network to speed national development and give the country a leg up on global science and technology (S&T) competition. The system is staffed by some 100,000 trained "STI workers" at all levels and is based on open sources. No other country has anything remotely comparable.

Our interest in China's STI system began with a study of its role in technology transfer,[1] but the mechanism itself—its philosophy, design, and functioning—draws our attention, inasmuch as an understanding of Chinese STI could help guide U.S. efforts to monitor emerging technologies.[2] Are there lessons here for the United States?

This study begins with an overview of "open source intelligence" (OSINT) and "science and technology intelligence" in the abstract and as understood in the United States. We then examine the growth of China's STI system, its structure, operation, and conceptual foundations. A final section explores factors contributing to its professionalization.

The paper concludes with recommendations for an open source-based STI program within the U.S. government, but outside the U.S. intelligence community, to secure for the United States a similar ability to identify, track, and learn from emerging technologies. U.S. dominance of global science is an anachronism; we must acknowledge that reality and adapt.

The authors thank CSET's Tarun Chhabra for nominating the topic and, with Dewey Murdick and Anna Puglisi, helping craft the study's recommendations. Thanks are also due to Sue Gordon and James Mulvenon for serving as external readers, and CSET's Igor Mikolic-Torreira for oversight.

We acknowledge with gratitude the support of Anastasya Lloyd-Damnjanovic and Alexander Bowe of the U.S.-China Economic and Security Review Commission, CSET's Remco Zwetsloot and Emily Weinstein for comments on the draft, and Maura McCarthy, Shelton Fitch, and Lynne Weil for editorial guidance.

WM. C. HANNAS
HUEY-MEEI CHANG

1 What is open source STI?

Open source intelligence and science and technology intelligence are realized differently in the United States and China, with China putting greater value on both. The two fields are examined here from the U.S. perspective as preamble to a full treatment of China's system, which has features that the United States may wish to emulate.

A. OSINT VERSUS THE OTHER INTS

In the United States, the phrase "open source intelligence" and its acronym OSINT depict not what open source is but what it is not. Conceptually, they beg the question: "open" in opposition to what? Operationally, the field is an adjunct to its classified counterparts. Definitions typically turn on this distinction:

- "In the intelligence community, the term 'open' refers to overt, publicly available sources (as opposed to covert or clandestine sources)."[3]
- "Open Source involves no information that is: classified at its origin; is subject to proprietary constraints (other than copyright); is the product of sensitive contacts with U.S. or foreign persons; or is acquired through clandestine or covert means."[4]
- "The main qualifiers to open-source information are that it does not require any type of clandestine collection techniques to obtain it and that it must be obtained through means that entirely meet the copyright and commercial requirements of the vendors where applicable."[5]

This reverse characterization of "open source intelligence," a reflection of its status in the U.S. intelligence community (USIC), is also evidenced

in the term's etymology. While the emergence of "OSINT" as a term of reference cannot be dated precisely,[6] its use postdates acronyms used for other "INTs" and was created *by analogy* with these recognized disciplines.

HUMINT	human intelligence (typically clandestinely acquired)
COMINT	communications intelligence (radio intercepts, etc.)
ELINT	electronic intelligence (radar signatures, satellite telemetry, etc.)
SIGINT	signals intelligence (cover term for COMINT and ELINT)
GEOINT	geospatial intelligence (satellite imagery)
MASINT	measurement and signature intelligence[7]

As recently as 2010, a former director of the Open Source Center (now Open Source Enterprise, the U.S. government's flagship OSINT operation[8]) discouraged use of the term "OSINT" partly for aesthetic reasons—the term does not roll off one's tongue—but chiefly out of concern the acronym might be perceived as an attempt to assert its value equivalence in a hierarchy where open source is regarded as a poor cousin to "real" (classified) intelligence by those funding it.[9]

One can define "open source" positively, citing venues and acquisition methods, although the USIC's bias to interpret OSINT in a restricted, secrets-based framework remains.[10] Open source includes mass and digital media, parts of the internet, social media, public government data, professional journals, academic theses, conference proceedings, think tank studies, commercial data and databases, and even patents and technical reports.[11] Acquisition focuses on permissions: its availability to public audiences in general, by request, or through subscription.[12]

In reality, the "openness" of open source is compromised by practices such as:

- covert assets reporting information from press accounts or radio broadcasts inaccessible to their (non-linguist) case officers;
- circuitous acquisition of open information to avoid betraying interests, leaving a trail, or to circumvent restrictions, for example, on open-but-protected "grey" literature;
- satellite photos purchased or obtained freely online to supplement classified overhead imagery;
- use of open sources to nominate targets for clandestine and technical collection or to validate classified reporting;
- proactive disclosure of open source intelligence to affect policy goals, communicate sensitive information to allies by proxy, or provide them plausible deniability.[13]

The second element of the phrase—"intelligence"—is less problematic and is typically viewed as a category of "information" distinguished by its military or political value. It is information that addresses an "intelligence requirement." That is, something is "intelligence" if it responds to the informational needs of an intelligence agency.

While the use of openly available materials to inform military and political decisions has existed for centuries, and within the U.S. intelligence community since at least 1942, its acceptance by the USIC as an intelligence pursuit is strained. Moreover, its value is not fully embraced—at the institutional or analyst levels—by those using it, who tend to regard open source as a supplement to the intelligence disciplines they are chartered to exploit.[14] As Florian Schaurer and Jan Storger point out in their study of open source intelligence:

> "(1) Intelligence agencies seek an informational advantage through covertly dealing with secrets. Relying on open information and its respective copyright restrictions runs counter to that idea. (2) In most cases it is more difficult, risky and expensive to apply clandestine methods in order to acquire secret sources, thus giving the impression that those sources must be of higher value than open sources, confusing the method with the product or mistaking secrecy for knowledge."[15]

The public history of OSINT within the Central Intelligence Agency, its parent organization, supports this characterization. The passage of the National Security Act of 1947 put the Foreign Broadcast Information Service—the major U.S. OSINT provider under various names since 1941[16]—under the CIA's auspices. Essentially, CIA leadership could not determine where FBIS fit in its organizational hierarchy and assigned the Directorate of Science and Technology to manage it.[17] The mismatch between monitoring foreign media (FBIS's forte) and creating, adapting, developing, and operating technical collection systems[18] for clandestine operations (the DST's *raison d'être*) was apparent from the beginning and resulted in a lack of vigorous "top cover" for open source at the directorate level.

The DST's take on open source was expressed, for example, in 1995, when its deputy director proposed massive reductions in FBIS's mission and workforce to free up funding for new offices better aligned with the DST's mission.[19] Open source's subsidiary role in the USIC was further evidenced in a description of the open source "mission" by Eliot Jardines, Assistant Deputy Director of National Intelligence for Open Source, in 2006, namely that it is:

> "... to *enable all intelligence disciplines* to provide timely, relevant and value-added insight to consumers via the National Open Source Enterprise." (Our emphasis added.)[20]

Meanwhile, statements of open source's value as an intelligence provider in *its own right* are conspicuously absent. More recently, the establishment of "mission centers" within the CIA in 2015 ensured that whatever autonomy OSINT providers had over their products and tradecraft would serve the hosting agency's parochial goals.[21]

Taking these caveats and institutional priorities into account,* we summarize the intelligence community's and, by extension, the USG's attitude toward open source as follows:

"Open source" is the information that remains after other intelligence disciplines define the landscape and stake their proprietary claims. Its value to the U.S. intelligence community lies chiefly in its ability to support classified reporting.

This philosophy contrasts sharply with China's OSINT thinking and practices, which place open source collection and analysis at the forefront of the country's intelligence effort.

B. SCIENCE AND TECHNOLOGY INTELLIGENCE

STI is not a collection methodology like SIGINT (e.g., intercepting radio signals to reconstruct an adversary's order-of-battle), OSINT (e.g., comparing current and former speeches to divine leadership intent), or other INTs. Rather "STI" refers to an intelligence *target* or goal serviced by multiple collection venues.

A 2013 U.S. Senate commission on intelligence defined it this way:

> "STI is the systematic study and analysis of foreign capabilities in basic and applied research and applied engineering. STI products are used to warn of foreign technical developments and capabilities and to guide the development of future capabilities, which are often provided through R&D."[22]

Note this definition is not limited to military technology[23] but also covers civilian technologies that affect a country's economic competitiveness, including those that *lead* to military threats ("dual-use" technology). A second definition, from the National Defense Intelligence College (now the National Intelligence University), also looks beyond military technology at the bigger picture, stating that STI aims to: "address threats to national security arising from globalization of science and technology; identify disruptive consequences of adversarial technology adaptations; and provide a framework for effective collection and warning."[24]

*Confidential disclosure agreements limit our ability to address some particulars.

The justification for pursuing STI—if any were needed—is outlined in a National Academies of Sciences, Engineering, and Medicine review of NDI's graduate program for aspiring government STI analysts, which states:

> "As the world becomes more technologically advanced, the need for intelligence officers and analysts skilled in science and technology intelligence (STI) increases .... (There are reasons) why the United States needs analysts and intelligence officers with STI skills:
>
> - The increased speed of science and technology breakthroughs;
> - The globalization of science and technology (S&T);
> - The convergence of various S&T disciplines (computer science, biology, physics, neuroscience, nanotechnology, chemistry);
> - The impact of commercial technology and its speed of dissemination; and
> - The increased capabilities of potential adversaries, including both non-state and state actors and the willingness of these parties to share with or sell to one another."[25]

A list of duties in a job announcement for the Office of the Director of National Intelligence's (ODNI) Deputy National Intelligence Officer for Science and Technology sheds more light on the nature of STI. They include:

- Provide expert assessments on collection and analysis regarding global science and technology issues.
- Lead the IC's production and coordination of strategic analysis ... on issues of importance to United States interests in global science and technology with particular focus on advanced asymmetric and military S&T threats.
- Develop and sustain a professional network with IC analysts, analytic managers, and collection managers on advanced asymmetric and military S&T threats and S&T community management and outreach issues.
- Establish and foster liaison relationships with academia, the business community, and other non-government subject matter experts to ensure the IC has a comprehensive understanding of advanced asymmetric and military S&T threats.[26]

Lacking in most such accounts are two key insights captured in the U.S. commission's 2013 review meant to put the enterprise on a practical footing, namely that

STI should be understood more broadly, with "aspects of counterintelligence and open-source intelligence used to provide a comprehensive picture of global scientific and technological advancements."[27]

The first of these insights—the need to treat counterintelligence as part of S&T threat awareness and mitigation—applies to China especially, whose technology depends heavily on foreign access and whose own collection posture reflects this dependency.[28] The commission's findings cited the U.S. government's less-than-stellar record addressing the issue of technology transfer:

> "Finding 1: The Commission found a limited effort by the IC to discern and exploit the strategic R&D—especially non-military R&D—intentions and capabilities of our adversaries, and *to counter our adversaries' theft or purchase of U.S. technology.*"[29]

The second insight highlighted in the commission's report is the need for OSINT to contribute more substantially to the national STI effort:

> "Finding 2: The Commission found that while the traditional ways and means of collecting and analyzing intelligence remain useful and necessary, emerging and future threats cannot be addressed without Enhanced Integrated Intelligence capabilities that enable shared, discoverable data for analysis and shared, discoverable information for decisionmakers."

These "enhanced" capabilities are defined as "collection and analysis processes enabled by automated collection, analysis, integration, and discovery of relevant intelligence data and information from classified *and open sources.*"[30]

The commission's recommendations, made in 2013, coincide point for point with China's STI operation that its chief architects described some three decades ago.[31] Both establish key roles for OSINT in the STI process, the difference being that while the USIC has at times entertained the idea that OSINT has a major place in STI production, in China open sources have long been its mainstay. The preference for secrets-based sourcing in the U.S. intelligence community extends even to topic selection, the assumption being if it is secret, it must be important. Or put another way, if it's not secret, why should the IC do it?

A final statement by the commission speaks to the role STI *should* play in U.S. intelligence, namely, a key initiative resourced on a par, at least, with counter-narcotics, counter-terrorism, and country-specific military/economic assessments, given S&T's potential to shape national strength and define military readiness:

> "Failure to properly resource and use our own R&D to appraise, exploit, and counter the scientific and technical developments of our adversaries—including both state and non-state actors— may have more immediate and catastrophic consequences than failure in any other field of intelligence."[32]

The commission's need to argue for STI demonstrates its relative neglect in the post-Cold War era,* when novel threats and short-term political concerns absorb most IC resources. STI is de-prioritized relative to other requirements not only within today's U.S. intelligence establishment, it is largely neglected within that part of the USIC responsible for OSINT, where a concentrated effort on STI is most needed and most likely to be effective.

In the United States, STI has the same standing within the USIC's open source community that OSINT has in the broader intelligence community, namely, last at the budgetary trough.

This neglect is troubling given STI's importance to national security and the need to monitor—ideally, forecast—technological threats from foreign adversaries.† Notably, these U.S. priorities are the inverse of China's, as characterized in Table 1 and described in the remainder of this paper.

TABLE 1

China vs. U.S. intelligence priorities

	OSINT	STI
CHINA	INT of first resort[33]	top intelligence priority
UNITED STATES	enabler of other INTs	second or third tier priority

*The U.S. intelligence community's STI work against the Soviet target was an effective undertaking for which it can be justly proud. Its success was owed both to a shared view of the existential threat and to the USIC's classified mandate aligning with the types of materials available to inspect. The paucity of open STI sources from the pre-1991 Soviet bloc hardly compares with today's circumstances, where openly available S&T information carries most of the potential intelligence.

† The authors acknowledge pockets of STI excellence within the USIC and Department of Defense—dedicated professionals with whom we had the pleasure of working. That said, adequate resources to service the classified record, not to mention the larger challenges of open source, are not provided.

2 China's STI posture

China's government has highly valued open source intelligence since the nation's founding and continues to depend on it as the primary source of information on foreign scientific developments. These sections describe the growth and structure of STI in China, which is light-years ahead of the world in this area. Understanding their approach offers insights into how the United States could proceed.

C. EARLY DEVELOPMENT OF STI IN CHINA

China's commitment to STI dates from the country's first "Long-Term S&T Plan" issued in August 1956.[34] According to multiple sources,[35] Chinese Premier Zhou Enlai (周恩来) in January of that year was shown an early draft of the plan, which lacked a mechanism to monitor foreign S&T developments. He reacted with a martial metaphor:

> "Doing science is like fighting a war. You've been working all these years, and you haven't even set up an intelligence agency. How can you fight this war?"[36]

At Zhou's insistence, the following Article 57 was added to the plan:

> "The foundation of our country's scientific and technological information work is very weak. The main task of intelligence work is to quickly establish institutions, train experts in intelligence work, comprehensively and on a timely basis collect, research and report on the development and new achievements of science and technology at home and abroad, especially in advanced scientific coun-

> tries, so that national scientific work can understand these developments and achievements promptly.* The specific method is to prepare for the establishment of specialized institutions, organize forces, engage in extracting papers from scientific and technological journals around the world, and compile, print and publish [this information] in the form of newsletters and abstracts."[37]

Subsequently, in May 1958 China's State Council approved a "Plan for the Development of Science and Technology Intelligence Work" (关于开展科学技术情报工作的方案), which named the scope and goals of Chinese STI as follows:

> "The responsibility of S&T intelligence work is to report the most recent accomplishments and trends in domestic and foreign science in all types of important scientific and technological fields so that scientific, technological, economic and higher education departments get timely access to the information and materials needed to facilitate the absorption of modern scientific and technological accomplishments, reduce time and manpower, avoid duplication of work, and promote the development of science and technology in China."[38]

An ideological justification for China's STI program was thereby established. As Wu Heng (武衡), deputy secretary of the State Council's Science Planning Committee,[39] described it: the plan "determined the tasks, management system, institutional setting and principles of establishing a domestic science and technology intelligence network."[40]

While formulating the plan, China was also building an infrastructure for its realization. In October 1956, an "Institute of Scientific Information" under CAS was established, later renamed the "Institute of Scientific and Technical Information of China" (see "ISTIC," Section E) to oversee STI work. Some months later, a Chinese University of Science and Technology Information (中国科学技术情报大学) was stood up—the world's first known example—with departments of S&T information, translation, and library science focused on foreign materials. In 1959 it became part of the University of Science and Technology of China (中国科学技术大学).[41]

In November 1958, China's first National STI Work Conference (全国科技情报工作会议) was convened. Delegates produced five documents defining the goals and methods of China's S&T open source system, including instructions on strengthening S&T intelligence work, a list of principles and techniques, a proposed structure for a national STI network, "secrecy rules," and training requirements for intelligence workers.[42]

*及时, also: "in time" or, in this context, "early enough to matter."

The conference left no doubt about the direction China would follow. STI would be the "ears and eyes, vanguard, and staff officers" (耳目、尖兵、参谋) of the nation.[43] "Vanguard" implies substituting, where possible, STI for indigenous R&D. Staff officers were to "engage in intelligence work that assists and supports decision-making" (从事辅助并支撑决策的情报工作).[44] To serve China's needs, STI must be "broad, fast, precise and accurate" (广、快、精、准).[45] The conference also identified "three categories and nine sub-categories" of open sources from "catalogs, abstracts, indices, and reports through newsletters, translations, and research trends.[46]

The mandate to monitor foreign S&T was supported by instructional fora on where to find the necessary information and what to do with it. In December 1957, China published its first STI professional journal "Science Information (or Intelligence) Work" (科学情报工作).[47] The periodical underwent several name changes[48] on its way to becoming the present "China Science & Technology Resources Review" (中国科技资源导刊). Two years later, in December 1959 the Institute of Scientific Information published "Lecture Notes on STI Work" (科技情报工作讲义) and "China Science Abstracts" (中国科学文摘) on methods for searching periodicals. Wu Heng noted that in little more than a year since the release of China's STI plan in May 1958, some 457 "types" (种) of how-to publications were issued, along with a host of abstracts and bulletins.[49]

According to Chen Zeqian (陈则谦) and Bai Xianyang (白献阳), who studied the STI system's evolution, the goal in this early period was to "reflect comprehensively, accurately, and in a timely manner" the trends and developments in foreign S&T.[50] This "intelligence work" was limited at first to translating foreign publications into Chinese but developed quickly into an end-to-end system with multiple layers of redundancy, graded by feedback loops and metrics.[51]

By the mid-1960s, China's STI system was supporting nuclear weapons research, satellite development, and computing.[52] Even during the Cultural Revolution (1966-76), when all government institutions were under attack in China,[53] STI had its defenders, including Zhou Enlai and, famously, PLA Marshall Nie Rongzhen (聂荣臻), who urged that the system—a "national treasure" (国宝)—be strengthened.[54]

From about 1980 on, STI was providing "integrated research and policy support" to key national projects, with an emphasis on solving difficult problems in research and production.[55] By 1985, there were 412 major S&T intelligence institutes nationwide, including 35 attached to the State Council's technical ministries, 33 at the provincial and municipal levels, and 344 local institutes employing more than 25,000 people.[56] Miao Qihao (缪其浩), the Shanghai ISTIC director at that time, adds to the figure 3,000 "basic cells" in grassroots units such as companies and labs for a total of 60,000 workers engaged fulltime by 1985 in one or more aspects of the STI enterprise.[57]

A detailed chronology of the early growth of China's STI system is available in ISTIC's 2016 compendium *60 Years of Glory—The 60th Anniversary of the Founding of the Institute of Science and Technical Information of China* (in Chinese)[58] and in "China's Use of Open Sources"—chapter two of the 2013 book *Chinese Industrial Espionage* (in English).[59] We highlight a few such developments here:

- **1959:** The State Science and Technology Commission (SSTC), predecessor to China's Ministry of Science and Technology (MOST), created an S&T Intelligence Office (科技情报局) to coordinate STI nationally.
- **1963:** The third "National STI Work Conference" defined the duties of STI organizations within the State Council's technical ministries, and provided rules for information units at the provincial and local levels.*
- **1975:** Hu Yaobang (胡耀邦), who became Party Chairman in 1981, during his brief tenure at CAS "personally inspected and guided" China's STI work and ordered regular reports be given to China's leaders.[60]
- **1977:** The SSTC released an S&T development plan with updated responsibilities for the STI system.[61] This plan mandated the use of advanced technology for the acquisition and distribution of STI materials.
- **1979:** An agreement brokered by Deng Xiaoping (邓小平) for S&T cooperation with the United States gave China access to "four major sets" (四大套) of USG technology compendia.[62] The reports became mainstays of China STI exploitation.[63]
- **1980:** The fifth "National STI Work Conference" committed to linking "intelligence work" closely to S&T development, and to "broadly exploit" (广辟) novel information sources.
- **1983:** Qian Xuesen (钱学森) delivered his speech "The Science and Technology of STI Work."[64] Qian is remembered for founding China's missile program; in our view his work to put STI on a logical footing had equal impact.
- **1984:** China's State Council and the Central Military Commission promulgated the "Regulations on National Defense Science and Technology Intelligence Work,"[65] complementing the "civilian" structure (ISTIC) laid down in 1956.

*This predates—and validates—a suggestion by Dr. Dewey Murdick, Director of Data Science for Georgetown University's Center for Security and Emerging Technology (CSET), to the U.S. Senate Committee on Homeland Security and Governmental Affairs in December 2019 for regional, semi-autonomous units in a national STI construct.

Meanwhile, we note that none of the Chinese documents we have examined—those cited here or others—suggests that OSINT plays a subsidiary role in a broader (classified) collection program. Rather, the emphasis in China has always been on expediting the delivery of open source S&T intelligence directly to decisionmakers.

D. STRUCTURE AND LAYOUT OF CHINESE STI[66]

China's present STI system was laid down in 1989, four decades after the People's Republic of China was founded and some 33 years after the system was first conceived. In January of that year, the State Science and Technology Commission issued "Opinions on Restructuring and Strengthening the Document Work of the National STI System" aimed at rationalizing the STI workflow and delineating responsibilities.[67] The document defined five main national organizations:

- **Institute of Scientific and Technical Information of China** (中国科技情报研究所)

  The national comprehensive S&T information center primarily responsible for collecting and storing documents on engineering technology, management science, and high technology. This is today's ISTIC, descendent of the Institute of Scientific Information and the primary "civilian" component (see Section E below).

- **COSTIND S&T Intelligence Bureau** (国防科委科技情报研究所)[68]

  The national military S&T information center primarily responsible for collecting and storing documents on military technology, engineering, weapons, and equipment. It is now the Military Science Information Research Center (军事科学信息研究中心) or MSIRC, China's main military STI component (see Section F below).[69]

- **CAS National Science Library** (中国科学院文献情报中心)*

  The national natural sciences information center primarily responsible for collecting and storing documents on mathematics, physics, chemistry, astronomy, geography, biology, cutting-edge science, and high technology. This library, along with ISTIC itself, was later subsumed into a National Science and Technology Library.

*Also known in English as the "CAS Documentation and Information Center."

- **China Patent Office Patent Documentation Library** (中国专利局专利文献馆)

  The national patents document center for collecting and storing documents such as patent manuals, patent announcements, and patent category indices. Now the Patent Documentation Library (专利文献馆) and the China Patent Information Center (中国专利信息中心), both part of the State Intellectual Property Office (国家知识产权局).

- **State Bureau of Technical Supervision Standards Information Center** (国家技术监督局标准情报中心).

  The national standards document center for collecting and storing documents on international standards, regional standards, national standards, professional standards, and corporate standards. Now the China National Institute of Standardization, National Library of Standards (中国标准化研究院国家标准馆).

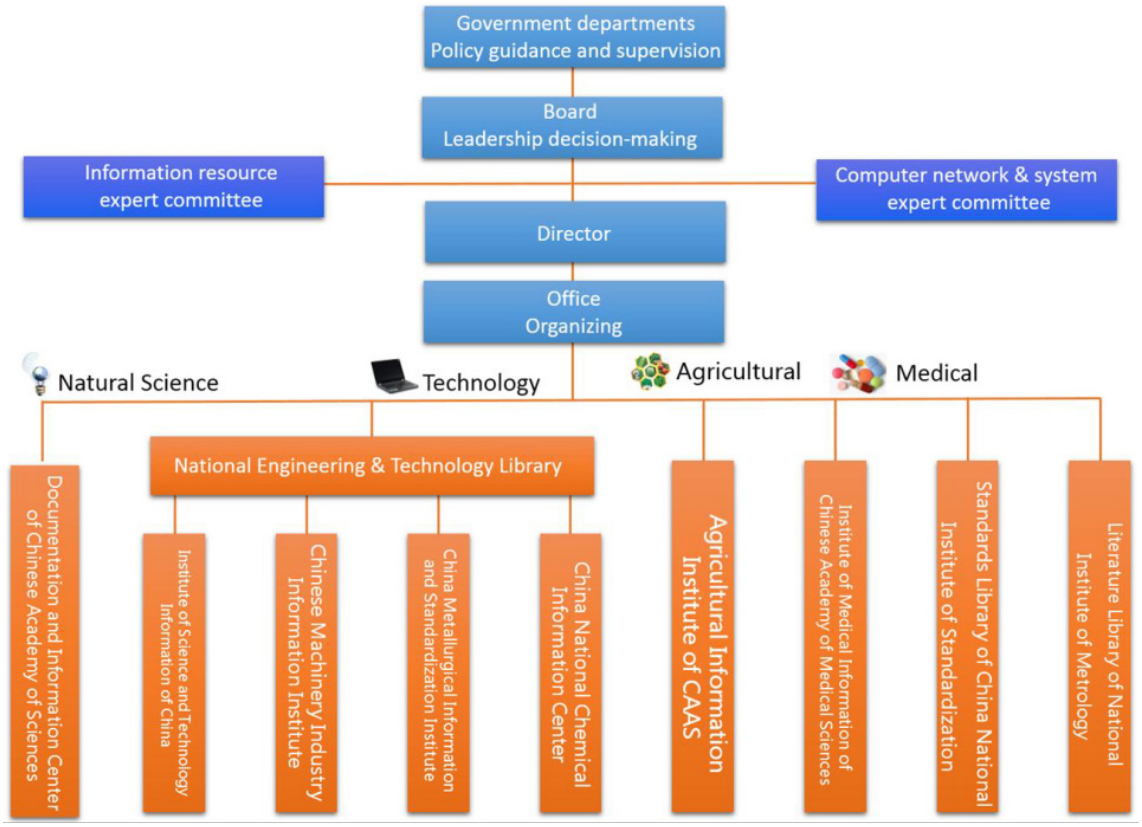
These five organizations made up the system's top (national) tier, according to the SSTC schema. A second tier consisted of STI centers attached to technical ministries. Facilities at the provincial, municipal, and county levels formed a third tier.[70]

This basic structure was tweaked in June 2000, when the State Council established a National Science and Technology Library (国家科技图书文献中心), "a virtual S&T document information service organization"[71] run by MOST, with no holdings of its own. Its mission was to oversee member libraries, which manage their own operations according to NSTL guidelines.[72]

A recent Chinese source outlines the civilian STI structure:[73]

FIGURE 1

Civilian STI structure



The military component is missing in the diagram. Former ISTIC director He Defang (贺德方) explains: "Collection and processing of foreign S&T documents are mainly undertaken by the central ministries' STI agencies, such as ISTIC and the NSTL's six other member units, and the seven member units of the National Defense S&T Industry Digital Library System."[74] So there is a built-in bifurcation of civil and military tasking. We treat these military units in Section F.

He Defang's count of seven NSTL member units excludes the National Library of Standards (second from right) and the Metrology Institute's (中国计量科学研究院) library—shown in the diagram but administratively independent. He also leaves out the Patent Library, included in the 1989 construct but not part of NSTL's design despite its vigorous exploitation of foreign patent information.[75] Operationally these distinctions are irrelevant, since NSTL has resource sharing agreements with each of these outliers—the military, patents, and standards libraries—and with major PRC libraries outside the STI system.[76]

These exceptions aside, NSTL itself has four divisions for basic science (理), engineering (工), agriculture (农), and medicine (医)—the four traditional Chinese categories. They are:

- Chinese Academy of Sciences' National Science Library (中国科学院文献情报中心).
- National Engineering and Technology Library (国家工程技术(数字)图书馆, NETL).
- Library of the Chinese Academy of Agriculture Science (中国农业科学院图书馆).
- Library of the Chinese Academy of Medical Sciences (中国医学科学院图书馆).

The CAS National Science Library (NSL), also called the CAS "Document and Information Center" (中国科学院文献情报中心), has its main library in Beijing with branches in Shanghai,* Wuhan, Lanzhou, and Chengdu; some 120 document information offices at R&D institutes throughout China; smaller collections at factories, schools and publishing houses; and some two dozen "specialized information networks."[77] Its holdings, a mix of Chinese and foreign books, journals, academic theses, proceedings, and reference works—print and digital—are also accessible from more than 100 CAS institutes in cities throughout China. The system services demand for information in natural sciences and high-technology, with holdings in all the hard sciences. Chen Jiugeng in his 2006 study called NSL and its branches China's "basic science information resources system."[78]

One aspect of its mission is apparent in the workings of the library's Lanzhou branch, notable for its proximity to China's nuclear weapons industry. The facility collects "special document information" and does deep studies for local institutes, with specialties in chemistry, chemical engineering, nuclear science, applied mathematics and computing. Unspecified "strategic intelligence research" (战略情报研究) is done on demand.[79]

Second on the list is the National Engineering and Technology Library, the engineering counterpart to CAS's science library. Like NSTL, NETL is a virtual organization, an umbrella for the "T" and "E" components of "STEM,"† and comprising four institutes: the China Machine Industry Information Institute (机械工业信息研究院), China Metallurgical Information and Standardization Research Institute (冶金工业信息标准研究院), China National Chemical Information Center (中国化工信息中心),

*The Shanghai branch is now called the Shanghai Information Center for Life Sciences (生命科学图书馆).

† Science, technology, engineering, mathematics.

and those offices in ISTIC concerned with engineering. While ISTIC is treated as a component of NETL, it is clearly first among equals (see Section E).[80]

Some statistics point to the magnitude of the overall operation. According to NSTL director Peng Yiqi (彭以祺) writing in 2020:[81]

> Each year, we order more than 17,000 printed foreign language periodicals, including more than 6,000 that are unique domestically, and more than 8,000 foreign language conference proceedings and other documents. The number of printed copies collected ranks first in China and in the forefront of the world.... Currently, NSTL provides access to 127 databases, covering more than 20,000 online foreign-language current journals, and more than 3,000 retrospective journals.

Bear in mind these figures refer to S&T literature, not generic holdings. In terms of employees, the most recent figure we have for the system as a whole is "more than 100,000 S&T intelligence workers" (科技情报工作人员) by the first decade of the 21st century,[82] up from the 60,000 figure given by ISTIC's Miao Qihao in 1985.

And while budget figures are elusive, we note Chen Jiugeng's (陈久庚) claim in 2006 that the annual funding increase for STI institutes from 1997 to 2005, when the system was put into final form, exceeded growth of state expenditures on R&D, absolutely and per capita.[83]

As these data and citations indicate, China's STI system is library-based. The construct sounds and is benign. While not the architecture foreign observers with intelligence backgrounds expect, the material after all is "open source," the provenance of library scientists.*

A Chinese analyst's reading of the June 2000 State Council memo observes that:[84]

- Aggregation and analysis of intelligence and information (情报信息综合分析) became part of the STI analyst's tasks, along with timely customer service and an emphasis on user consultation.
- An earlier requirement for entry into the "intelligence corps" (情报队伍) to be "good in one area" (一技之长) was no longer adequate. The modern open source worker had to bring to the job IT skills, management savvy, and an academic background.

*One of this paper's authors spent several years proselytizing in the USG for an open source database of foreign S&T. Among some 200-plus briefings to respectful but inert audiences, the author had the pleasure once of briefing a group of IC librarians, who immediately and enthusiastically grasped the proposition's import and within three minutes had taken over the briefing. Little to tell them. By the same token, the author's most valuable colleague at the time was a Ph.D. linguist with a post-doc M.S. *in library science*.

- **Open source workers were also asked to play a larger part in the intelligence process, provide top leaders with information, and perform a direct role in policymaking** (出谋划策).

China's STI cadre are expected to join in national S&T planning. The leaders of the Chinese Academy of Sciences require that "all major scientific and technological plans must have STI personnel participating and serving."[85]

If China's open source STI workers ever played second string to an access-privileged *qingbao* cadre, or their efforts to support China's development were less important than other intelligence needs, it is not evident in the materials we have examined. Indeed, it is impossible to study this system without sensing the pride its practitioners take in their work and its value to China.

3 Main organizations*

Among China's open source STI organizations, two stand out as core units for civilian and military data exploitation. The Institute of Scientific and Technical Information of China is the premier civilian organization for gathering and disseminating foreign technical intelligence. Its counterpart is the Military Science Information Research Center, which services China's defense industry. The two are examined in detail.

E. INSTITUTE OF SCIENTIFIC AND TECHNICAL INFORMATION OF CHINA (ISTIC)

ISTIC (中国科学技术信息研究所), with headquarters in Beijing and branches throughout China, began life in 1956 as the "Institute of Scientific Information" under an initiative sponsored by China's senior leaders. The institute acquired its present English name during a reorganization in 1958, when it also assumed a new Chinese name: 中国科学技术情报研究所, literally "Institute of Scientific and Technical Intelligence of China," i.e., the equivalent to the United States' "STI." In 1992, the seventh and eighth characters were changed from 情报 (intelligence) to 信息 (information) to avoid the stigma attached by laypersons to the former term, with no change in the English.[86]

Nuance aside, ISTIC's subordination to NETL (described above) is only nominal. A modern expression of Taoist dualism, ISTIC is treated as both part of the National Engineering and Technology Library—along with three other technical institutes—as shown in NSTL's table of organization (Section D), and paradoxically as NETL's *parent organization*, as depicted in ISTIC's own org chart, where NETL appears in a subordinate slot as the

* Parts of these segments are adapted from *CIE*, chapter two.

"Information Resource Center (NETL)" (信息资源中心 (国家工程技术图书馆))[87] with eight other ISTIC departments.[88]

ISTIC views itself as the national center for managing and providing S&T information services, as exercising leadership over and serving as a model for the entire country's STI system, and as positioned to "offer decision-making support" to MOST and other government offices.[89] ISTIC has some 850 staffers in seven functional divisions and nine public-good departments (公益部门). It owns three corporations including the digital S&T document provider Wanfangdata.* Its business areas are data research and analysis in support of government decision-making; S&T information services; research, development, and propagation of new technologies and service platforms; fostering talent in the field of S&T information; and media publication services."[90]

More specifically, ISTIC:

> "processes and reports on domestic and foreign S&T publications including documents, translations, reference works, reports, and research; builds domestic and foreign document databases that conform to China's needs and circumstances; does research and analysis on domestic and foreign S&T sources that pertain to China's national economic and S&T issues; reports on domestic and foreign S&T achievements and trends; performs strategic information services for policy making departments; provides in a planned fashion specialized information services for the nation's many priority science research programs; does research on information science, policy, management, service, methods and research; and develops international cooperation and exchange in S&T information work."[91]

*Wanfangdata (万方数据, http://www.wanfangdata.com.cn/index.html) is the major domestic competitor of Tsinghua University's China National Knowledge Infrastructure (CNKI). Holdings are similar but not identical due to agreements upstream providers have with one organization or the other. A third Chinese aggregator CQVIP (重庆维普网, http://www.cqvip.com/) is managed by ISTIC's Chongqing branch—now the Chongqing Southwest Information Digital Co., Ltd. (重庆西南信息有限公司)—and also provides unique content.

ISTIC's S&T document holdings

By the end of 2015, ISTIC's Information Resource Center had more than 3.11 million domestic and 500,000 foreign theses and dissertations; more than 270,000 foreign-language conference documents; 2.4 million US government S&T [AD, etc.] reports; more than 4,300 foreign journals; 260,000 foreign search and reference books; and had opened 22 abstracts databases and 27 full-text databases. Its digital resources reached 104 million Chinese and foreign abstracts and 163 million citations, and the total number of digital full texts has reached 60 million.[92]

ISTIC offers a full range of data services, including access to the world's major S&T journals (via worldwide aggregators such as LexisNexis, ProQuest, Lawrence Erlbaum Online Journals, and the ISI Derwent Innovations Index). Print media offerings include "western language conference proceedings, western language periodicals, foreign language S&T reports, Chinese language conference proceedings, and a Chinese language academic theses database."[93] Among other services, ISTIC:

> "obtains and delivers for registered clients original documents from its own and outside (馆外) holdings; verifies the originality of S&T content for customers setting up research programs; appraises S&T achievements, does evaluations, and applies for patents; offers document research services and advice to central Party, government, and military leadership organizations, to state key lab production units, and to clients at large; verifies the recorded content and citations of papers and works publicly available through Chinese and foreign search engines; arranges proxy searches and loans of resources in domestic and foreign libraries and information organizations; and performs other personalized services."[94]

As MOST, which oversees the ensemble, describes it, ISTIC is "the largest and most authoritative professional library in the field of engineering technology in China."[95] ISTIC, however, does more than collect and provide S&T materials to domestic customers. It provides "fact-and-data-based decision-making support to government agencies, research institutions, and industry."[96] It actively supports state R&D projects through "comprehensive, policy-driven strategic research" on the latest worldwide S&T achievements and trends for leading government departments.[97]

FIGURE 2

ISTIC headquarters at 15 Fuxing Road, Beijing

ISTIC's National Science and Technology Management Information System offers "one-stop" (一站式) support for five types of state-level science and technology plans, including those of the National Natural Science Foundation of China (国家自然科学基金), National Science and Technology Major Projects (国家科技重大专项), National Key R&D Programs (国家重点研发计划), Technical Innovation Guidance Special Projects (技术创新引导专项), and China's "Bases and Talent Special Projects" (基地和人才专项).[98] The organization is involved in state-level S&T planning, providing decision-making support to the Ministry of Science and Technology, and helping form the country's five-year plans, the "National Medium and Long-term Science and Technology Development Plan," and a host of government-directed special studies, such as China's "New Generation Artificial Intelligence Development Plan."[99]

ISTIC's scope extends to "the formulation, revision and promotion of core standards related to science and technology reports," making "policies and regulations for science and technology reports" including the submission and review process (presumably for grant applications and papers in domestic journals), researching the ownership of intellectual property rights, and the "setting and declassification of confidentiality levels" (密级设置和解降密), which suggests that ISTIC—like OSINT operations in other nations—has "low-" and "high-side" dimensions.[100]

Other duties include supporting technology transfer from foreign sources to national industries. ISTIC achieves this, in part, through its engineering center's (工程中心) patent database, "high-level scientific and technological talent database" (高层次科技人才数据库), a "scientific and technological project information database" (科技项目信息数据库)[101] and, since 2008, an "Overseas High-level Talent Database—Thousand Talents Plan (海外高层次人才数据库 - 千人计划).[102] ISTIC provides

input to China's "global science and technology talent policy" and, through its business unit (业务部门), "conducts competitive intelligence research via tracking and analysis of key industries and S&T fields, providing information for industrial development and corporate decision-making."[103]

ISTIC trains its cadre and staff in the skills needed for open source STI. In 1978, it began recruiting postgraduate students in information science. The institute offers Masters degrees in library, information, and archive management, and collaborates with Beijing University and its military counterpart to train PhDs in information science. It also accepts post-doctoral researchers and trains professionals deployed elsewhere in the STI system.[104]

FIGURE 3

State Council's "National S&T Advancement Award"

ISTIC has sent its reports to China's State Council, General Office of the Communist Party of China, National People's Congress, Chinese People's Political Consultative Conference, and to Party and state leaders.[105] It has received the State Council's "National S&T Advancement Award" (above) around nine times and has been commended for its work by leaders from provincial through national levels.[106]

It also plays a direct role in selecting and training "intelligence personnel" for overseas postings, including "S&T counselors at embassies abroad."[107]

ISTIC is more than an STI aggregator. Its work affects Chinese government policy on all levels, with reach down to state-owned and private businesses. **Its services depend wholly on open source exploitation and the skills of its open source analysts.**

F. MILITARY SCIENCE INFORMATION RESEARCH CENTER (MSIRC)

ISTIC's open source operations are complemented on the military side by the Military Science Information Research Center (军事科学信息研究中心), an appendage of the PLA's Academy of Military Sciences (军事科学院) since 2017, and successor to the long-serving China Defense Science and Technology Information Center (中国国防科技信息中心, CDSTIC). The evolution of CDSTIC and the system that

revolves around it is as convoluted as its civilian counterpart, a function of its age, number of units involved, and the attention China has given it.

CDSTIC grew out of the Commission on Science and Technology Industry for National Defense's (国防科工委, COSTIND) S&T Intelligence Bureau (科技情报研究所) established in March 1959, which was a culmination of developments that began in early 1956.[108] It is unclear when the "STI Bureau" formally became the "China Defense Science and Technology Information Center" and knowledgeable insiders use the two names interchangeably.* Over its six decades of service the Center underwent seven major adjustments[109] and is best known in its "CDSTIC" iteration, a practice we follow here.

CDSTIC's role is analogous to ISTIC's in two ways: it (1) services the defense establishment's needs for open source intelligence on military S&T worldwide, and (2) is a hub for an expanded network of STI facilities. The identities of these other facilities were named in a 1984 State Council directive that defined China's "national defense S&T intelligence system" as follows:

> "COSTIND, each defense industry ministry (including the Ministry of Electronics Industry, the China State Shipbuilding Corporation); the PLA's General Staff Department and General Logistics Department; related departments from each branch of the military services; organizations responsible for S&T intelligence work within the national defense S&T industry offices of each province, autonomous region, and municipality directly under the central government; national defense S&T intelligence professional working units at each level; local national defense S&T intelligence service centers; and the defense S&T intelligence network."[110]

Their duties as outlined in the directive are to collect and make available foreign and domestic S&T materials, manage the systems' intelligence reports, organize S&T intelligence exchanges, perform analysis and provide intelligence needed for policymaking, research, and production.[111]

*Multiple sources date "CDSTIC's" emergence from March 14, 1959, i.e., the founding date of its progenitor, although Huo and Wang, and various state documents, referred to it by its older name as late as 1991. Similarly, the U.S. Open Source Enterprise, so named as of 2015, traces its legacy to the founding of FBIS in 1941. Its staff regarded FBIS, OSE, and its intermediate organization, the "Open Source Center" (2005-2015), as synonyms and continued to use the old labels months and even years later, orally and in some cases on written products.

CDSTIC's role as the "main unit" in the network was defined as follows:

> "COSTIND's S&T Intelligence Bureau *is the integrated center* for national defense S&T intelligence. Each of the national defense industry departments' S&T intelligence bureaus is an S&T intelligence center within the system. The S&T intelligence offices directly subordinate to related departments and bureaus in the General Staff Dept., General Logistics Dept., and each branch of military service *should gradually develop into S&T intelligence centers within the system.*"[112] (Our italics.)

That is, the new structure under CDSTIC's tutelage as defined in 1984 was mostly aspirational. Huo and Wang noted in 1991 that actual implementation did not begin until 1986 and only later spread to "each respective intelligence organization."[113]

Qian Xuesen, early STI pioneer

Qian Xuesen (钱学森), scientist, former U.S. defense contractor, prominent returnee, and revered founder of China's strategic missile program, played an early and decisive role in the evolution of China's STI system that is little known outside China. His contributions as the "mentor and leader of China's S&T information (信息) industry, especially the national defense S&T information industry" were acknowledged by CDSTIC Director Yan Wei (闫巍) on the anniversary of his 100th birthday.[114] Qian's achievements include early recognition of the potential impact of AI on intelligence (in both senses of the term). His thinking on STI is discussed in Section G on the theoretical foundations of China's open source operations.

In December 2003, some two decades after the State Council's edict and three years after the creation of the seven-unit NSTL on the civilian side (see Section E), a National Defense S&T Industry Digital Library System (国防科技工业数字图书馆系统) was formally organized under CDSTIC's purview.[115] Like NSTL, it had seven members:

- China Nuclear S&T Information and Economic Research (中国核科技信息与经济研究院)
- China Aerospace Engineering Consulting Center (中国航天工程咨询中心)

- China Aviation Industry Development Research Center (中国航空工业发展研究中心)
- China Shipbuilding Industry Research Institute (中国船舶工业综合技术经济研究院)
- China Ship Information Center (中国船舶信息中心)
- Northern S&T Information Research Center (北方科技信息研究所)
- MIIT, Institute of Electronic STI (信息产业部电子科学技术情报研究所)

The list does not include some national-level organizations named in the 1984 State Council STI directive or other units doing related work that are known to exist, for example, the Beijing Document Center (北京文献服务处) founded in 1978 and a key provider of foreign military S&T information;[116] COSTIND's China Engineering and Technology Information Network (中国工程技术信息网, CETIN), an online repository of foreign military equipment and specifications;[117] the Military Library of the Chinese Academy of Military Sciences (中国人民解放军军事科学院, 军事图书资料馆) operating under various names since 1958; and its affiliated China National Digital Library Military Science Branch Library (中国国家数字图书馆军事科学院分馆). In 2005, China's Central Military Commission issued "Regulations on the Chinese People's Liberation Army General Armaments Department S&T Information Work," which set guidelines for the military services' STI units beyond those laid down in 2003 and the State Council directive.[118]

FIGURE 4

CDSTIC office and data buildings at 26 Fucheng Road, Beijing

Focusing on CDSTIC itself, Chinese accounts of its accomplishments are almost hagiographic. A typical example posted to the PLA's China Military Network (中国军网) in 2016, the year before it re-emerged as MSIRC noted:

> "Nuclear bombs, ballistic missiles, and earth satellites (两弹一星),* the Shenzhou spacecraft ... Behind our country's many world-renowned high-tech achievements there is the same organization—the China National Defense Science and Technology Information Center. The center is hailed as an 'innovation brain trust' by researchers."[119]

The same article summarized CDSTIC's three "secrets" of success, namely that:

- The center "collaborates with many large domestic S&T documentation centers, and carries out document sharing, resource exchange, personnel exchanges and training." (CDSTIC, like ISTIC, is first among equals.)
- It focuses on breakthroughs in key technologies such as "network information source discovery" and "knowledge graph construction," effectively enhancing core scientific research capabilities. (Data science is used to good effect.)
- The system houses millions of paper documents, "some ten thousand hours of audio-visual materials, and more than ten million electronic documents for use by scientific research personnel." (Collection, not only analysis, is valued.)

CDSTIC, like its civilian counterpart, has conferred graduate degrees in related disciplines since 1986 and sponsors "post-doctoral research stations" in military STI.[120] **Six decades of experience have taught China that open source intelligence is not picked gratis from an open source tree but depends on the quality of its OSINT professionals (see Section H).**

On September 29, 2017, CDSTIC was officially reborn as the Military Science Information Research Center under a reorganized Academy of Military Sciences. An "Introduction to the Center" states that the organization, successor to CDSTIC and other military STI units, is mainly responsible for building and servicing information resources, "dynamic tracking and analysis," strategic intelligence research,

*A canonical reference to China's development of three classes of weapons. The two *dan* (弹) are commonly misconstrued as "atomic and hydrogen bombs" (原子弹、氢弹). The second *dan* actually is part of the word for "ballistic missile" (导弹). See http://discovery.cctv.com/special/C19607/20071018/104899.shtml.

policy research, and "big data intelligence technology" in the field of worldwide military technology and armaments.[121]

The announcement—preface to a hiring advertisement for technicians and other professionals—noted that the "center's real-time (实时) interconnected data analysis environment provides the scientific means to support the Central Military Commission's decision-making and consultation requirements."[122]

Key takeaways here are (1) the center relies on open sources to follow foreign defense S&T projects on a continuing basis (动态跟踪, "dynamic tracking")[123] and (2) is able to impart this information directly to decision-makers. The next sections examine the concepts that underpin China's STI system.

4 Chinese STI in theory and practice

China's use of open source as the basis of its S&T intelligence program has its psychological roots in the Chinese language, whose term "*qingbao*" encompasses simultaneously both "information" and "intelligence." This conceptual overlap paves the way for acceptance of open source as a fully-fledged intelligence discipline. China's embrace of OSINT and its role in STI gave rise to a network of social organizations and journals that support professionalization.

G. CHINESE WRITERS ON "*QINGBAO*" AND STI

A key to understanding Chinese STI is the fact that "information" and "intelligence" are not distinguished by many Chinese speakers and are used interchangeably by "STI workers" (科技情报工作人员). Huo and Wang wrote in 1991:

> "Unanimity has yet to be reached in different quarters as to the semantic difference between intelligence and information. If, during the historical stage characterized by intelligence activities, we certainly could mix up information and intelligence; and if, during the historical stage characterized by intelligence work, we still could get away with mixing up information and intelligence; then, in the historical stage characterized by intelligence as a science and a technology, we certainly must clearly differentiate information and intelligence, both from a theoretical standpoint and from the standpoint of practical experience."[124]

Here is a more recent (2017) testimonial:

> "Information science is a concept with Chinese characteristics. In Chinese characters, *qingbao* [情报] has two meanings: one refers to information [信息], the corresponding word in English is 'information;' the other refers to our spying and military intelligence, and the corresponding word in English is 'intelligence.' *Qingbao* science in my country also has two meanings: 'information science;' and 'intelligence services'."[125]

The first rigorous attempts to separate the two concepts were Qian Xuesen's seminal paper "The Science and Technology of STI Work"[126] in 1983 and his 1984 speech to a National Symposium on Thinking Science.[128] Unlike many of his countrymen, Qian, a returned overseas scholar, treated "intelligence" as unique: as knowledge extracted ("activated") from information to solve particular problems. In his own comprehensive epistemology, "information science" (信息学) is one branch of a "theory of knowledge" (认知论)—the other being "noetics" (思维学, the "study of thought).* "Intelligence science" (情报学) occupies a subordinate level in the schema—it is a *subset* of information science, and the two have entirely different referents.

This distinction is relevant and—in context—revolutionary, inasmuch as Chinese thought bundles the two concepts under a single lexical item *qingbao* (情报, literally "a report on the circumstances"). Qian's need to separate "information" from "intelligence" speaks to this cultural difference, which we believe has genuine ramifications. While it is risky to assert that languages differentially affect cognition,† the merger of these two concepts in a single lemma is consistent with observable Chinese attitudes toward "intelligence." Like "information," it is not something nefarious to be hidden, stolen, or embarrassed by, but a normal and reasonable goal.

Indeed, as intimated earlier in this study, the SSTC's formal decision in 1992 to rename China's open source "intelligence" (情报) organizations "information" (信息) organizations—a decision that has still not filtered down to some grassroots bodies—was done out of concern with *foreign perceptions* of China's intelligence mission, not by intrinsic distrust of "intelligence" on the part of its mainland Chinese users.[128] The tendency in some other countries to think of STI in terms of secrets had to be learned.

---

*Made up of "enlightenment" (灵感思维), "image cognition" (形象思维), and "abstract thinking" (抽象思维), i.e., direct apprehension, pictorial/iconic thought, and symbolic thought.

† The Whorf-Sapir hypothesis. This once "discredited" theory is enjoying a rebirth. Its weaker version—that the structure of language *influences* (but does not determine) thought—is hard to refute but equally hard to prove.

China's tendency to rely more than its non-Asian counterparts on open source (or not to classify it out of existence, which is the same thing) may also, in part, have roots in the psycholinguistics of the language: it is all "intelligence" and thus equally able to serve the needs of the nation.

Huo and Wang, who acknowledge Qian's mentorship, also call for an end to the "ambiguity" of the earlier stages of China's STI development in favor of an open source *intelligence* discipline.

> "People are gradually coming to appreciate the need to make a conceptual distinction between intelligence and information, reflecting the fact that the social function of intelligence is now undergoing a transformation, that intelligence science is maturing with each passing day, and that development of the intelligence cause is just now undergoing a transition from the stage characterized by intelligence work to the stage characterized by intelligence as a science and a technology."[129]

The two authors go on to define classes of "information" based on where and how it is used, following theoretical work by Claude Shannon, founder of information theory,[130] and expand the distinctions into an eight--point list of characteristics "needed for macro-management of national defense technology." Table 2 is a direct translation, offered as a demonstration of the extent to which China was enmeshed in the relationship between OSINT and policymaking three decades ago, while the United States was schooling its open source officers on the need to support "all-source analysts" with translations of foreign press articles.

TABLE 2

Policymaking and categories of information

INFORMATION CHARACTERISTIC	CATEGORY OF POLICYMAKING	
	TACTICAL	STRATEGIC
TIME	historical	predictive
EXPECTATION	predictable	unpredictable
SOURCE	internal	external
CONTENT	specialized	synthesized
ORGANIZATION	highly organized	diffuse
COMPRESSION	detailed	summarized
RATE OF PRODUCTION	high	low
ACCURACY	high accuracy	fairly high accuracy

Huo and Wang lay the groundwork for open source as the "first stage" of the intelligence process, a viewpoint opposite to that taken in the United States.

> "As we know, collection is the first of the three links in intelligence work .... In view of the fact that "intelligence" and "information" are different in their natures, attributes and functions, then information, not intelligence, should be the target of collection work, even though the ultimate goal of intelligence work is to obtain intelligence. *The work should be information collection, not intelligence collection.*"[131] (Our italics.)

They then drive a stake into the notion that open source is an adjunct to (classified) intelligence: "(F)or various reasons related to perceptions and policies, people are ever wanting to obtain intelligence directly, and moreover are sometimes successful at doing it. However, this course of action is really very inefficient."[132]

The authors, part of CDSTIC's top cadre, propose a collection taxonomy based on media type, the level of processing, technical nature of the content, its field of application, transmission means, user demands, time constraints, level of expectation, whether the sources are "internal" or "external," specialized or synthesized, organized or diffuse, the level of compression, accuracy, and its probability of existing.[133]

Sources are categorized by how they are obtained, each type described in terms of its own search theory. Source evaluation is done through an indexing scheme based on reliability, suitability, timeliness, availability, cost, and ease of decoding. Formulas are proposed to quantify these evaluations.[134] Everything gets tagged and binned. The efficiency of collection is assessed then by "numerical probability values," such as "the probability of collecting the needed information within the period of time stipulated by the consumer, and the mathematical expectation of the amount of the needed information that will be collected within the stipulated time period."[135]

An entire chapter (6) is given to explaining transmission channels—to whom and where do you send the information—e.g., serial, centralized, ring, bilateral, and mutual, each having its own advantages or drawbacks. The authors also discuss other characteristics such as time, capacity, susceptibility to interference, and security.

TABLE 3

Huo and Wang on the old and new STI[136]

	TRADITIONAL	MODERN
COLLECTION	Build complete collections; wait for consumers to come.	Target real needs; actively contact consumers.
ASSESSMENT	Gauge quality on basis of amount collected.	Is the material scientific, targeted, prompt and useful?
SOURCING	Written (published) materials only.	All media types, broadly defined.
STORAGE	Databanks.	Databases.
METHODS	Routine work, dependent on collector's preferences.	A scientific endeavor that is demand driven.
SKILLS	Collector knows a foreign language "and can type."	Contingent of professionals with distributed skills.
EXPENDITURES	Spend first, plan later; neglect development and management.	Plan first, spend later; value efficiency and management.

These are the system's visible traces, available to researchers who read Chinese; we have no window into the private deliberations of China's STI workers and leaders. By contrast, our grasp of U.S.—and to some extent allied—STI operations is based on first-hand experience over decades. **Yet we struggle to identify anything comparable to the minute disquisitions China affords this enterprise.** The odd occasional article in CIA's *Studies in Intelligence*[137] on OSINT—usually an historical vignette—cannot begin to compare.

H. CHINA AND THE PROFESSIONALIZATION OF STI

How does the Chinese STI system play out in practice? It is one thing to create agencies and networks, quite another thing to ensure they are staffed with qualified personnel and that these staffers* have opportunities for discourse relevant to their professions, socially and through publishing. While neither of these venues is available to their U.S. counterparts,† open dialog and a sense of inclusion are part of the Chinese system and play major roles in its success.

The STI system's professionalization is also evident in its hiring practices. What types of people fill China's STI ranks? A list of job vacancies issued by MSIRC in 2019 shows the breadth of talent. Vacancies per slot range from one to three. Only the first 10 of 26 line entries are shown.

*We have not observed references to the use of contractors in the Chinese STI system.

† The work is classified by default, cannot be discussed in open fora, and "outside" publishing on work-related topics is almost nil.

TABLE 4

2019 AMS/MSIRC military-civilian recruitment form[138]

JOB CATEGORY	POSITION TITLE	TYPE OF WORK	EDUCATION	PROFESSION
engineer	assistant engineer	software development	Masters or above	computer science and technology, software engineering
science rsch	research intern	comprehensive research on national defense tech	Masters or above	chemical engineering and technology, engineering
science rsch	assistant researcher	big data knowledge mining research	Ph.D.	computer science and technology, software engineering
science rsch	research intern	academic journal editor	Masters or above	design, translation
engineer	assistant engineer	computer network and equipment management	Masters or above	computer science and technology
engineer	assistant engineer	multimedia, animation, film and TV production	undergrad or above	postgraduate: drama and film studies, design
librarian	assistant librarian	website programming and network DB management	full-time undergrad	computer science and technology
science rsch	research intern	data analysis	Masters or above	control science and engineering, computer S&T
engineer	assistant engineer	project management	Masters or above	management science and engineering
librarian	librarian	library file management	Masters or above	management science and engineering

Other vacancies are for digital processing and database construction; digital library application technology development and maintenance; intelligence research; electronics research, system demonstration and evaluation; computer network security; software and network engineering; database construction and maintenance; translation and management of foreign language library materials; more "comprehensive research on national defense technology;" and file management.

Another job announcement issued by the same organization in 2020 lists skill categories sought, underscoring the quality of China's STI cadre:

TABLE 5

2020 AMS/MSIRC recruitment announcement[139]

	Civilian staff sought in 2020 mainly are in big data mining, data analysis, intelligence research, software development, information construction, and journal editing.
LITERATURE	journalism and communications
MANAGEMENT	information science, management science and engineering, administrative management
SCIENCE	mathematics, computational mathematics, applied mathematics, statistics, probability statistics, applied statistics, probability theory, mathematical statistics
ENGINEERING	computer software and theory, computer technology, computer application technology, communication and information systems, computer systems structure, cyberspace security, information security, signal and information processing, software engineering, optical engineering, electronic science and technology, biomedical engineering
	Double degree students with both a science and engineering background and a literary background are preferred.

Another measure of a mature discipline, and a key element in its development, is the number of journals that grow up around it. Here are some samples—print and digital periodicals, all peer-reviewed—that promote open source S&T intelligence in China. Titles and metadata from recent papers are included to demonstrate the nature and sophistication of the discourse.

1. 情报学报 (*Journal of the China Society for Scientific and Technical Information*). Since 1982, sponsored by the Chinese Society for Science and Technology Information (中国科学技术情报学会) and ISTIC, Beijing. Has published 2,883 articles.[140]

- Dai Guoqiang (戴国强), "推进竞跑阶段的创新情报研究 (Intelligence Studies for Innovation in the New Era)," 2019: 38 (8).

2. 中国科技资源导刊 (*China Science & Technology Resources Review*). Since 1957, sponsored by ISTIC and Nanjing University. Originally *Science Intelligence Work* (科学情报工作). Has published 4,009 documents.[141]

- Hu Yingjun et al. (胡寅骏等), "利用人工智能技术挖掘高层次创新人才 ——以专利数据为例 (Mining High-level Innovation Talent with Artificial Intelligence Technology —A Case Study of Patent Data)," 2020: 52(3).

3. 情报工程 (*Technology Intelligence Engineering*). Since 2015, sponsored by the Chinese Society for Science and Technology Information and ISTIC, Beijing.[142]

- Qian Hong et al. (钱虹等), "基于SCI论文的无人机领域技术发展态势分析 (Analysis of Development of Technological Situation of UAVs Based on SCI Database)," 2020: 6 (4).

4. 情报理论与实践 (*Information Studies: Theory & Application*). Since 1964, formerly *Ordnance Intelligence Work* (兵工情报工作), sponsored by the China National Defense Science and Technology Information Society (中国国防科学技术信息学会) and the 210th Research Institute of China North Industries Group (中国兵器工业集团第二一〇研究所). Published 7,502 articles.[143]

- Zhou Jingyan et al. (周京艳等), "混合战争背景下科技情报工作的战略定位 (The Strategic Orientation of S&T Intelligence Work under the Hybrid War)," 2020: 43 (10).

5. 情报杂志 (*Journal of Intelligence*). Since 1982, sponsored by Shaanxi Institute of Science and Technology Information (陕西省科学技术情报研究院), Shaanxi. Published 13,043 articles.[144]

- Ma Shuhui et al. (马曙辉等), "基于美国解密发明信息的国防专利转移效果特征研究(Research on the Transfer Effect Characteristics of National Defense Patents Based on American Decryption Invention Information)," 2020: 39 (9).

6. 现代情报 (*Journal of Modern Information*). Since 1980, formerly *Information Knowledge* (情报知识), sponsored by the Jilin Institute of STI (吉林省科学技术情报研究院) and the Chinese Society for Science and Technology, Jilin. Published 14,951 articles.[145]

- Wu Lin et al. (吴林等), "大数据时代安全情报人才培养的思考 (Reflections on the Cultivation of Security Intelligence Talent in the Era of Big Data)," 2020: 40 (10).

7. 情报资料工作 (*Information and Documentation Services*). Since 1980, sponsored by Renmin University of China (中国人民大学) and the Chinese Society of Social Sciences and Information (中国社会科学情报学会), Beijing. Published 4,727 articles.[146]

- Li Lin (栗琳), "情报机构视域下情报、智库与战略决策关系透析 (Analysis of the Relationship between Intelligence, Think Tanks and Strategic Decisions from the Perspective of Intelligence Organizations)," 2020: 41 (5).

8. 科技情报研究 (*Scientific Information Research*). Founded in 2019, sponsored by the Hunan Institute of Science and Technology Information (湖南省科学技术情报研究院), Hunan.[147]

- Miao Qihao (缪其浩), "组织决策中的情报与循证决策中的证据 (*Qingbao* in Organizational Decision-making and Evidence in Evidence-based Policy)," 2020: 2 (3).

9. 图书情报工作 (*Library and Information Service*). Since 1980, sponsored by the CAS National Science Library (中国科学院文献情报中心), Beijing.[148]

- Yu Houqiang et al. (余厚强等), "人工智能领域科研团队识别与领军团队提取 (Identification and Extraction of Research Teams in the Artificial Intelligence Field)," 2020: 64 (20).

FIGURE 5

Selected Chinese periodicals covering open source S&T intelligence

These journals are a small sample of the inventory. Each of China's 31 provinces, special municipalities, and autonomous regions is host to one or more journals, including the present authors' two personal favorites.[149] A recent Chinese bibliometric study of these provincial STI journals concludes that "provincial STI institutions are the backbone and supporting force of China's scientific and technological intelligence industry."[150] The study named ten provincial STI organizations, whose journal content ranked in a top 20 list of frequently cited articles.[151] They included STI "institutes" (研究所) or "academies" (研究院) in Beijing, Guangdong, Hebei, Hubei, Jiangsu, Jiangxi, Shaanxi, Shanxi, Shanghai, and Sichuan.*

Information on STI operations is also shared through the National Science and Technology Library system—the civilian S&T OSINT authority—which operates 40 "service stations" (服务站) throughout China and another 30 local management

*Three of the ten have switched to "S&T information" (信息), while the remaining seven continue to use "S&T intelligence" (情报) in their names.

platforms (管理平台) for universities[152] linked to the center by a broadband network meant to bridge a "digital divide" between the "information wealthy" and "information poor."[153]

China also supports its open source cadre with professional groups, so-called mass organizations (群众组织) that translate requirements from the leadership to workers and communicate upward input from these grassroots elements. Chief among them are the China Society for Science and Technology Information (中国科学技术情报学会) on the civilian side, and its defense counterpart, the China National Defense Science and Technology Information Society (中国国防科学技术信息学会).

The former was founded in 1964. Its activities include academic exchanges on STI theory and practice, disseminating STI knowledge and technology, commissioned research and project development, liaison between central and local STI institutions, academic publication and member recognition, and serving as a "home" (家) for STI workers.[154]

The China National Defense Science and Technology Information Society was established in 1988 for the same purposes. According to information posted on the China Military Network (中国军网), the organization's goal is to "unite the broad masses of national defense STI workers," conduct training, cultivate talent, and "promote the development of national defense STI."[155]

At the risk of dwelling on a theme that by now should be well-established, **we know of nothing comparable to these professional organizations outside China.** Although SCIP[156] comes to mind, its focus is business intelligence, it is international in scope, and has no S&T monitoring mission. Efforts by SCIP's leaders some years ago to cast China's STI program, and the broader network within which it operates, as a run-of-the-mill business competitive intelligence (BCI) enterprise, gained no traction within the USIC.[157]

Recommendations

If we were invited to manage—all things being equal—the United States' open source intelligence system or China's, we would choose the latter without hesitation. Since that option is not on the table, we propose the creation of an open source STI organization, provisionally called the "National S&T Analysis Center" (NSTAC), within the U.S. government, designed without dependencies on prior art, structure, budgets, or assumptions, but with cues from the Chinese model.

A *minimum layout* would consist of a hub in the Washington Metropolitan Area staffed with 350 full-time employees and four regional outstations (Atlanta, Boston, Houston, Silicon Valley) with staffs of 25-30 each, including administrators, linguists, analysts, data scientists, subject matter experts, IT personnel, and support staff, at an estimated cost of $125M-150M *per annum* plus facilities. Other important considerations are:

- During startup, the targeted staffing numbers should be approached in increments over three years. Year 1 = hub only; Year 2 = hub + two outstations; Year 3 = hub + four outstations.
- Significant investment in the licensing, creation, and aggregation of relevant scientific and technical information is essential for the effective operation of NSTAC.
- NSTAC collaboration with allied/friendly foreign STI organizations and with civil society actors should be encouraged, potentially through public-private partnerships.
- No more than 5-10 percent of NSTAC personnel should have IC clearances (TS/SCI) to avoid mission creep and absorption by IC elements.

- That said, measures are needed to protect the security of information generated, used, and shared by NSTAC. We recommend all employees have Secret-level clearances.*

NSTAC should support U.S. counterintelligence agencies with open source analysis programs that highlight and vigorously pursue illegal and extralegal technology transfers, as per the U.S. Senate commission's 2013 recommendation. This is needed especially for China, where grey zone transfers account for much of its S&T profile.

The proposed body, like those in China, should have a role in technology policymaking and programmatic planning at the national level. Contextual insight provided by NSTAC should be available at the federal as well as state and local levels. Furthermore, relevant discoveries should be made publicly available, where consistent with national security, while others can be shared within public-private partnerships.

The IC should interact with NSTAC but not define its priorities or methods, to avoid co-option and the "secrecy trap" that accords priority to classified programs. The IC may retain its marquee OSINT enterprises: there is a legitimate need for open source to "enable" classified intelligence, although that is hardly the whole of it or even its most important part. Locating NSTAC outside the IC also eliminates the "U.S. Persons" issue that prohibits collecting and holding information on U.S. companies and individuals, which given the global nature of S&T would make tracking developments nearly impossible.

These recommendations apply to STI only. We are agnostic about an *overall* OSINT solution, other than to insist NSTAC be fenced off from it entirely, given the inclination of open source managers to appropriate STI budgets for projects directed at "current intelligence."

This proposal is consistent with that of the U.S. House of Representatives Permanent Select Committee on Intelligence, stated in its September 29, 2020 study "The China Deep Dive: A *Report on the Intelligence Community's Capabilities and Competencies with Respect to the People's Republic of China*." In particular:

> "(U) The Committee's central finding of this report is that the United States' intelligence community has not sufficiently adapted to a changing geopolitical and technological environment increasingly shaped by a rising China and the growing importance of interlocking non-military transnational threats, such as

*This recommendation follows the Chinese model, which pairs its collecting, cataloguing, and disseminating of open source information with adequate security to protect the sensitive nature of its work.

> global health, economic security, and climate change. **Absent a significant realignment of resources, the U.S. government and intelligence community will fail to achieve the outcomes required to enable continued U.S. competition with China on the global stage for decades to come, and to protect the U.S. health and security.**" (emphasis in the original)[158]

As analysts who have tracked China's borrowing of ideas for decades, we find it ironic that the model for our proposal is China's own pioneering intelligence work. One might object that comparisons with China are unrealistic because the two countries' goals differ. It is true that China's STI mission does not match that of the United States. China tracks *and transfers* foreign technology whereas the U.S. goal, in principle, is to monitor security threats. Hence, China's needs are greater. *But a thousand times greater?** It is obvious one side is failing.

Moreover, since Chinese S&T leverages foreign invention,[159] a U.S. STI program, beyond keeping an eye on China's indigenous innovations, must employ mechanisms to gather relevant data and perform in-depth analysis to track these accesses across the entire spectrum of actors and actions. It is likely that this analysis will uncover legal, illegal, and extralegal attempts at transfers, which could be referred to the appropriate local or federal agencies for investigation under their authorities. In other words, China's unique mission requires a tailored response, as noted by the 2013 U.S. Senate commission (Section B).

A second objection is more fundamental. U.S. national decisionmakers and Americans in general coast on the assumption that the United States and its allies are so far ahead of China in science and technology that a U.S. monitoring system would provide little more than an aperture into our own past. That is, we can skip the scrutiny because the gap is so wide. Regrettably, while this thesis may have been plausible decades ago, the United States is no longer the global S&T hegemon.† Whereas U.S. R&D in 1960 was more than two-thirds of global R&D, today it is less than one-third.[160]

China's work in artificial intelligence[161] and biotechnology,[162] to cite just two areas, suggests any "gap" between U.S. and Chinese performance is transient. Past successes can no longer safely guide the United States through an era of accelerat-

---

*Authors' observation of the maximum number of USG persons and contractors who attend IC-wide China S&T conferences, i.e., fewer than 100 focused American analysts, compared to 100,000 Chinese "STI workers."

† An exception is fundamental research, where China agrees that the United States maintains an enviable lead. Ironically, it is the one area of science the USG has been reluctant to protect (see Hannas and Chang, "China's 'New Generation' AI-Brain Project," National Defense University Press / *PRISM* (forthcoming).

ed S&T development, in which security is as likely to be defined by "products" as by "weapons." Given the globalization of scientific innovation and the central role of technology in U.S. prosperity, effective policy requires timely monitoring of worldwide S&T developments. We consider this point indisputable.

Endnotes

1. Hannas, Mulvenon and Puglisi, *Chinese Industrial Espionage*, 2013, chapter 2 "China's Use of Open Sources."
2. Critiqued most recently by U.S. Representative Adam Schiff, "The U.S. Intelligence Community Is Not Prepared for the China Threat," *Foreign Affairs*, September 30, 2020.
3. https://en.wikipedia.org/wiki/Open-source_intelligence.
4. OSS Notices, 2.9 (30 November 1994) cited in Robert D. Steele, "Open Source Intelligence: What Is It?," archived on 28 March 2018. https://en.wikipedia.org/wiki/Open-source_intelligence.
5. Mark M. Lowenthal, "Open-Source Intelligence: New Myths, New Realities," in Roger Z. George and Robert D. Kline, *Intelligence and the National Security Strategist*, Rowen and Littlefield (Lanham, MD), 2006, p. 273.
6. "There is no specific date on when the term OSINT was first proposed." (Nihad Hassan, "An Introduction to Open Source Intelligence (OSINT) Gathering," August 12, 2018, https://www.secjuice.com/introduction-to-open-source-intelligence-osint/) "The US military first coined the term OSINT in the late 1980s, arguing that a reform of intelligence was necessary to cope with the dynamic nature of informational requirements, especially at the tactical level on the battlefield." (Florian Schaurer and Jan Storger, "The Evolution of Open Source Intelligence (OSINT)," *The Intelligencer: Journal of U.S. Intelligence Studies*, 19.3, 2013.)
7. See Federation of American Scientists' definition (https://fas.org/irp/program/masint.htm).
8. https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html.
9. Authors' personal recollection.
10. In the last two years the USIC has bifurcated the open source domain into two elements: OSINT, which requires official Title 50 authorities for collection, analysis, and operations; and the phrase "Publicly Available Information (PAI)" which does not require those authorities. We thank Dr. James Mulvenon for pointing this out.
11. https://en.wikipedia.org/wiki/Open-source_intelligence. and https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html.
12. https://www.recordedfuture.com/open-source-intelligence-definition/.
13. "Open source materials can protect sources and methods. Sometimes an intelligence judgment that is actually informed with sensitive, classified information can be defended on the basis of open-source reporting. This can prove useful when policy-makers need to explain policy decisions or communicate with foreign officials without compromising classified sources." https://en.wikipedia.org/wiki/Open-source_intelligence.
14. https://en.wikipedia.org/wiki/Open-source_intelligence. By 1942, William J. Donovan's Office of Strategic Services (OSS), precursor to the CIA, had a Research and Analysis Branch of some 900 scholars across multiple disciplines analyzing newspapers, library holdings, and other openly available sources for information on the Axis Powers of intelligence value. (https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/oss-research-and-analysis.html).
15. Florian Schaurer and Jan Storger, "The Evolution of Open Source Intelligence (OSINT)," *The Intelligencer: Journal of U.S. Intelligence Studies*, 19.3, 2013.)
16. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/foreign-broadcast-information-service/.
17. Oral history conveyed to author circa 2005.
18. https://www.cia.gov/offices-of-cia/science-technology.

19. https://en.wikipedia.org/wiki/Ruth_A._David.
20. Eliot A. Jardines, National Open Source Enterprise," April 2006. https://web.archive.org/web/20070928150640/http://upload.wikimedia.org/wikipedia/en/b/b4/NationalOpenSourceEnterprise.pdf.
21. https://www.cia.gov/news-information/press-releases-statements/2015-press-releases-statements/cia-achieves-key-milestone-in-agency-wide-modernization-initiative.html.
22. "Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community (unclassified version)," 2013. https://www.intelligence.senate.gov/sites/default/files/commission_report.pdf.
23. For example, "STI examines foreign developments in basic and applied sciences and technologies with warfare potential, particularly enhancements to weapon systems." https://warontherocks.com/2018/04/an-inflection-point-for-scientific-and-technical-intelligence/.
24. Studds, Susan, et al., "National Defense Intelligence College – School of S&T Intelligence." Presentation to the committee, May 13, 2011.
25. National Research Council, *Review of the National Defense Intelligence College's Master's Degree in Science and Technology Intelligence*, The National Academies Press, Washington DC, 2011. https://doi.org/10.17226/13260.
26. 13637 - Deputy National Intelligence Officer, Science and Technology, Joint Duty Number:ODNI-18-0406U. https://www.dni.gov/icjointduty/vacancies/odni-18-0406u.htm.
27. "Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community (unclassified version)," 2013. Our emphasis.
28. Hannas, Mulvenon, Puglisi, *Chinese Industrial Espionage* (*CIE*), Routledge (New York and London), 2013; Hannas and Chang, "China's Access to Foreign AI Technology—an Assessment," Georgetown University, Center for Security and Emerging Technology, September 2019; Hannas and Tatlow, eds., *China's Quest for Foreign Technology: Beyond Espionage,* Routledge, 2020.
29. "Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community (unclassified version)," 2013. Our emphasis.
30. "Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community (unclassified version)," 2013. Our emphasis.
31. Huo, Zhongwen (霍忠文) and Wang Zongxiao (王宗孝), 国防科技情报源及获取技术 (*Sources and Methods of Obtaining National Defense Science and Technology Intelligence*), Beijing, Kexue Jishu Wenxuan Publishing Company, 1991.
32. "Report of the National Commission for the Review of the Research and Development Programs of the United States Intelligence Community (unclassified version)," 2013.
33. Hannas et al, *CIE*, chapter 2 "China's Use of Open Sources."
34. "1956-1967年科学技术发展远景规划纲要 (Outline of the Long-term Plan for the Development of Science and Technology from 1956 to 1967), State Council," August 1956. Ratified in December 1956.
35. For example: "甲子辉煌—中国科学技术信息研究所成立60周年纪念 (*60 Years of Glory—The 60th Anniversary of the Founding of the Institute of Science and Technical Information of China*) ," 中国科学技术信息研究所 (ISTIC), Beijing, 2016, p. 3. (Hereafter *60 Years of Glory*); Wu Heng (武衡), "周恩来对我国科学技术事业的关怀和指导 (Zhou Enlai's Care and Guidance to China's Science and Technology Enterprise)," *People's Daily Online*, January 4, 2006. http://cpc.people.com.cn/GB/69112/75843/75872/5165752.html; and Liu Zhaodong (刘昭东) "回顾、感言与期盼 (Looking back, impressions and expectations)," *China S&T Daily* (科技日报), October 15, 2016. http://digitalpaper.stdaily.com/http_www.kjrb.com/kjrb/html/2016-10/15/content_351389.htm?div=-1.
36. There are two (similar) versions of Zhou's directive circulating: "你们工作这么几年，连个情报机构都没有建立，你们的仗是怎么打的?" cited by Liu Zhaodong (刘昭东) "回顾、感言与期盼 (Looking back, impressions and expectations)," *China S&T Daily* (科技日报), October 15, 2016, and "搞科研像打仗，你们搞了这么多年科研，连个情报机构都没有建立，你们的仗是怎么打的?" cited in *60 Years of Glory*, p. 3.
37. "1956-1967年科学技术发展远景规划纲要" (Outline of the Long-term Plan for the Development of Science and Technology from 1956 to 1967), State Council, August 1956. https://zh.wikisource.org/wiki/1956-1967年科学技术发展远景规划纲要.

38. Cited in Lai Maosheng (赖茂生), "新环境、新范式、新方法、新能力—新时代情报学发展的思考 (New Environment, New Paradigm, New Means, and New Capabilities: Reflections on the Development of Information Science in the New Era)," 情报理论与实践 (*Information Studies: Theory & Application*), 2017:40 (12), pp. 1-5.
39. Wu was CAS vice secretary from 1954 to 1957. https://baike.baidu.com/item/武衡. Wu also presided over the first National STI Work Conference in 1958 as Deputy Secretary-General of the State Council Science Planning Committee (第一次全国科技情报工作会议由国务院科学规划委员会副秘书长武衡主持), as cited in *60 Years of Glory*, p. 9.
40. Wu Heng (武衡), "周恩来对我国科学技术事业的关怀和指导 (Zhou Enlai's Care and Guidance to China's Science and Technology Enterprise)," *People's Daily Online*, January 4, 2006.
41. Guan Jialin (关家麟) and Zhang Chao (张超), "我国科技信息事业发展的回顾与展望 (Review and Outlook for Scientific and Technological Information Undertaking of China)," 情报科学(*Information Science*), 2007:25 (1), pp.1-7.
42. *60 Years of Glory*, pp. 9-10.
43. Chen Chao (陈超), "科技情报近六十年政策层面的发展回顾 (Looking back at the development of STI policy for the past 60 years)," January 21, 2019. From Chen's address to the Shanghai Library Association in 2018. https://www.sohu.com/a/290461007_693747.
44. Xiao Yong (肖勇), "中国科技情报 (科技信息) 事业与中国情报学的学科定位所在(I)--中国科技情报 (科技信息) 事业 (S&T Intelligence (S&T Information) in China and Its Position within Chinese Intelligence (Information) Science)," 图书情报工作 (*Library and Information Service*), 2009: 53 (18), pp. 52-55.
45. Zeng Jianxun (曾建勋), "基于国家科技管理平台的科技情报事业发展思考 (Reflections on the Development of the STI Industry Based on the National Science and Technology Management Platform)," 情报学报 (*Journal of the China Society for Scientific and Technical Information*), March 2019: 38 (3), pp. 227-238.
46. Zeng Jianxun, Reflections on the Development of the STI Industry Based on the National Science and Technology Management Platform.
47. We discuss the choice between "intelligence" and "information" as translations for the Chinese 情报 (*qingbao*) later in Section G.
48. 科技情报工作 (*S&T Intelligence Work*) and later 中国信息导报 (*China Information Review*).
49. Wu Heng (武衡), "周恩来对我国科学技术事业的关怀和指导 (Zhou Enlai's Care and Guidance to China's Science and Technology Enterprise)," *People's Daily Online*, January 4, 2006.
50. Chen Zeqian (陈则谦) and Bai Xianyang (白献阳), "我国科技信息事业发展的轨迹 (The Locus of Development for China's S&T Information Enterprise)," 现代情报 (*Journal of Modern Information*), December 2007: 12. pp. 11-15.
51. Hannas, William, James Mulvenon and Anna Puglisi, *Chinese Industrial Espionage*, Routledge, 2013.
52. Guan and Zhang , "Review and Outlook for Scientific and Technological Information Undertaking of China" and Chen and Bai, "The Locus of Development for China's S&T Information Enterprise."
53. Zhou Xiaoying (周晓英), et al., "中国科技情报事业发展历程与发展规律研究 (Research on the Development Process and Law of Scientific and Technical Information Career in China," 科技情报研究 (*Scientific Information Research*), 2019: 1(10), pp. 13-28.
54. *60 Years of Glory*, p. 55, and Guan and Zhang, "Review and Outlook for Scientific and Technological Information Undertaking of China," 2007:25 (1), pp.1-7.
55. Chen and Bai, "The Locus of Development for China's S&T Information Enterprise."
56. Chen Jiugeng (陈久庚), "我国科技信息服务系统的实力 (Actual Strength of S&T Information Service System in China)," 中国信息导报 (*China Information Review*), 2006: 10, pp. 17-22.
57. Miao Qihao, "Technological and Industrial Intelligence in China: Development, Transition and Perspectives." In Prescott and Gibbons, eds., *Global Perspectives on Competitive Intelligence*, Alexandria, VA: Society of Competitive Intelligence Professionals, 1993.p. 49-53.
58. Op. cit.
59. Hannas, William, James Mulvenon and Anna Puglisi, *Chinese Industrial Espionage*, Routledge, 2013.
60. *60 Years of Glory*, p. 57, and Guan and Zhang, "Review and Outlook for Scientific and Technological Information Undertaking of China," 2007:25 (1), pp.1-7.

61. "1978-1985年全国科学技术发展规划 (Regulations on National S&T Development 1978-1985)." State Science and Technology Commission, 1977.
62. The Publication Board (PB) of the Department of Commerce, the Armed Services Technical Information Agency (AD) ASTIA Documents, NASA, and Department of Energy (DOE) reports. China's exploitation of the AD reports is discussed in *CIE* pp. 27-32.
63. *60 Years of Glory*, p. 93-94.
64. 科技情报工作的科学技术. July 2, 1983.
65. 国防科技情报工作条例. July 30, 1984.
66. Adapted from *CIE*, chapter 2, with updates.
67. 关于调整和加强全国科技情报系统文献工作的意见, State Science and Technology Commission (国家科委), January 1989. Also, "国家科委关于调整和加强全国科技情报系统文献工作的意见," 图书情报工作 (*Library and Information Service*), 1989: 33(3), pp. 42-44. Chinese terms are provided as per the original.
68. COSTIND expands to "Commission on Science and Technology Industry for National Defense." COSTIND became the State Administration for Science and Technology Industry for National Defense (SASTIND, 国家国防科技工业局) in 2008.
69. China Defense Science and Technology Information Center (CDSTIC, 中国国防科技信息中心) until 2017.
70. "Opinions on Restructuring and Strengthening National S&T Information System Document Work." A more recent taxonomy adds a fourth tier made up of some 3,600 "enterprise units" (企事业单位) at local levels (http://www.baiven.com/baike/224/283180.html).
71. www.nstl.gov.cn.
72. Liansheng Meng and Yan Quan Liu, "The Present and Future of China's National Science and Technology Library: A New Paradigm of Sci-tech Information Resource Sharing," *New Library World*, 2005: 106 (7/8), pp. 343-351.
73. Zhang Xuefu (张学福), "An Introduction of National Science and Technology Library of China (NSTL), June 2, 2017. Zhang is a NSTL board member. The schematic agrees with our independent reconstruction of the network in 2013 (*CIE*, p. 34).
74. He Defang (贺德方), "我国科技情报行业发展方向的探讨 (Discussion on the Development Direction of STI Industry in China)," 情报学报 (*Journal of the China Society for Scientific and Technical Information*), 2008: 27 (4), pp. 483-489.
75. *CIE*, pp. 41-42.
76. He Defang, "Discussion of the Development of STI Industry in China," pages 483-489. See also and Zheng Yanning (郑彦宁) and Song Zhenfeng (宋振峰), "我国科技情报行业现状与发展对策分析 (Present Condition of China's S&T Information Field and Analysis of Development Countermeasures)," 情报学报 (*Journal of the China Society for Scientific and Technical Information*), 2008: 26 (5), pp. 790-795. Zheng and Song acknowledge what most analysts of the Chinese system take for granted, namely, that information sources are purchased once (if at all) and shared universally: "These member units follow the principle of 'unified procurement, standardized processing, joint internet access, and resource sharing." (这些成员单位按照 "统一采购、规范加工、联合上网、 资源共享" 的原则).
77. Hannas, *CIE*, pp. 35-36 and Chen, "Actual Strength of S&T Information Service System in China," *China Information Review*, October 2006.
78. Chen, "Actual Strength of S&T Information Service System in China," *China Information Review*, 2006: 10, pp. 17-22.
79. www.las.ac.cn.
80. The two organizations—NETL and ISTIC—typically are referenced together, or are treated as one and the same. See *60 Years of Glory* , pp. 273, 359.
81. Peng Yiqi, "隆重纪念国家科技图书文献中心成立二十周年 (Grand Commemoration of the 20th Anniversary of NSTL's Establishment)," 数字图书馆论坛 (*Digital Library Forum*), 2020: 7, pp. 1-2.
82. Zeng Jianxun (曾建勋), "基于国家科技管理平台的科技情报事业发展思考 (Reflection on the Development of the Scientific and Technical Information Industry Based on the National Science and Technology Management Platform)," 情报学报 (*Journal of the China Society for Scientific and Technical Information*), 2019: 38 (3), pp. 227-238.

83. Chen Jiugeng, "Actual Strength of S&T Information Service System in China," *China Information Review*, 2006: 10, pp. 17-22.
84. Xia Chengyu (夏承禹), "科技情报部门领导在新形势下的新角色 (A New Role for Leaders of S&T Information Departments under the New Circumstances)," 科技进步与对策 (*Science & Technology Progress and Policy*), 2001: 1, pp. 104-105.
85. Wu Yishan (武夷山), "关于我国科技情报工作的几点思考 (Some Thoughts of China's STI Work)," 中国科技资源导刊 (*China Science & Technology Resources Review*), 2009: 41 (6), pp. 73-76.
86. Chen Jiugeng (陈久庚), "关于情报和信息 (On Intelligence and Information)," 情报杂志 (*Journal of Intelligence*), 2000: 19 (1). The concern was with overseas Chinese perceptions of ISTIC's mission.
87. https://www.istic.ac.cn/isticcms/html/1/151/155/index.html. The NETL, a virtual organization, functions *through* ISTIC's Information Resource Center . ISTIC affirms the IRC "is responsible for the construction and operation of the National Engineering and Technology Library." https://www.istic.ac.cn/isticcms/html/1/151/155/347.html.
88. The arrangement is not as far-fetched as it seems. Until 2005, the director of the U.S. Central Intelligence Agency was dual-hatted as the "Director of Central Intelligence" (DCI), that is, the manager both of CIA and the intelligence community (IC) of which CIA is a part. Similarly, ISTIC's director is dual-hatted as the director of NETL (国家工程技术图书馆设馆长一名，由中国科学技术信息研究所所长担任). *60 Years of Glory*, p. 270.
89. https://www.istic.ac.cn/isticcms/html/1/151/152/409.html.
90. www.istic.ac.cn.
91. *CIE*, p. 37.
92. http://digitalpaper.stdaily.com/http_www.kjrb.com/kjrb/html/2016-10/15/content_351387.htm?div=0, https://www.istic.ac.cn/isticcms/html/1/151/155/347.html, accessed September 2020.
93. *CIE*, p. 37.
94. *CIE*, p.37.
95. http://www.most.gov.cn/zzjg/zzjgzs/zzjgsyzxs/.
96. http://www.itxww.com/html/english/istic_e2.htm. Accessed July 2020. Also *60 Years of Glory* , pp. 326, 418.
97. *CIE*, p. 38.
98. https://www.istic.ac.cn/isticcms/html/1/185/364/index.html.
99. https://www.istic.ac.cn/isticcms/html/1/357/359/index.html.
100. https://www.istic.ac.cn/isticcms/html/1/151/155/345.html.
101. https://www.istic.ac.cn/isticcms/html/1/151/155/346.html.
102. *60 Years of Glory*, pp. 322, 373.
103. https://www.istic.ac.cn/isticcms/html/1/151/155/345.html.
104. https://www.istic.ac.cn/isticcms/html/1/151/155/353.html.
105. https://www.istic.ac.cn/isticcms/html/1/151/154/index.html.
106. http://www.safea.gov.cn/kjbgz/201610/t20161024_128321.htm.
107. Speech by Chen Chao (陈超), director of the Shanghai Institute of STI's (上海科学技术情报研究所) affiliated library, at the Shanghai Library Association 2018 annual meeting (https://www.sohu.com/a/290461007_693747).
108. Chen Dazhi (陈达植), "我国国防科技情报工作的回顾与展望 (Retrospect and Prospect of China's National Defense S&T Intelligence Work)," in 中国信息导报 (*China Information Review*), November 1996, pp. 8-9.
109. http://mil.news.sina.com.cn/2004-03-18/1130188143.html.
110. 国防科学技术情报工作条例 (*Regulations on National Defense Science and Technology Information Work*), PRC State Council, July 1984, Article 5.
111. 国防科学技术情报工作条例 (*Regulations on National Defense Science and Technology Information Work*), PRC State Council, July 1984, Article 9.
112. 国防科学技术情报工作条例 (*Regulations on National Defense Science and Technology Information Work*), PRC State Council, July 1984, Article 8.
113. Huo and Wang, *Sources and Methods of Obtaining National Defense Science and Technology Intelligence*, 1991.

114. "钱学森国防科技情报信息系统建设研讨会举行 (Seminar Held on Qian Xuesen Construction of a National Defense STI Information System)," http://finance.china.com.cn/roll/20111215/426559.shtml, December 15, 2011.
115. http://www.gov.cn/gzdt/2007-05/29/content_629609.htm.
116. *CIE*, p. 40.
117. *CIE*, pp. 40-41.
118. 中 国人民解放军装备科技信息工作条例 http://www.gov.cn/jrzg/2005-08/08/content_21283.htm.
119. "揭秘高科技成果背后的 '创新智囊' : 中国国防科技信息中心 (Demystifying the 'Innovation Brain Trust' behind High-tech Achievements: CDSTIC)," http://www.81.cn/jwgz/2016-03/23/content_6972538.htm.
120. http://www.yanzhaowang.com.cn/zhaosheng/gfkjxx/20651.html.
121. http://bj.offcn.com/html/2020/02/221551.html.
122. http://bj.offcn.com/html/2020/02/221551.html.
123. "Tracking" (跟踪) has been a major goal of China's STI enterprise since its inception in 1956 on both the civilian and military sides. See Zeng Jianxun (曾建勋), "基于国家科技管理平台的科技情报事业发展思考 (Reflection on the Development of the Scientific and Technical Information Industry Based on the National Science and Technology Management Platform)," 情报学报 (*Journal of the China Society for Scientific and Technical Information*), 2019: 38 (3), pp. 227-238.
124. Huo and Wang, *Sources and Methods*, 1991, chapter 1. References are to the English translation, done some years ago by the present authors, whose online version lacks pagination. (https://fas.org/irp/world/china/docs/sources.html).
125. Li Gang (李剛), "从情报研究到智库研究 (From Intelligence Research to Think Tank Research)," 图书馆论坛 (*Library Tribune*), 2017: 37 (9), pp. 50-54.
126. Qian Xuesen (钱学森), "科技情报工作的科学技术 (The Science and Technology of STI Work)," 国防科技情报工作 (*National Defense S&T Intelligence Work*), July 1983, pp. 3-12.
127. Liu Zhihui (刘植惠), "情报学基础理论讲座第七讲钱学森同志关于情报学的新见解 (Lecture on Basic Theory of Information Science, Lecture 7: Comrade Qian Xuesen's New Views on Information Science)," 情报理论与实践 (*Information Studies: Theory & Application*), 1988: (4), pp. 42-44.
128. Chen Jiugeng (陈久庚), "关于情报和信息 (On Intelligence and Information)," 情报杂志 (*Journal of Intelligence*) January 2000, pp. 4-6 and *60 Years of Glory* , p. 110.
129. Huo and Wang, *Sources and Methods*, 1991, chapter 1.
130. Claude Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, 1948.
131. Huo and Wang, *Sources and Methods*, 1991, chapter 1.
132. Huo and Wang, *Sources and Methods*, 1991, chapter 1.
133. Huo and Wang, *Sources and Methods*, 1991, chapter 3.
134. Huo and Wang, *Sources and Methods*, 1991, chapter 4.
135. Huo and Wang, *Sources and Methods*, 1991, chapter 1.
136. https://fas.org/irp/world/china/docs/sources_chap1.html.
137. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/index.html.
138. "2019军队文职人员招聘军事科学院军事科学信息研究中心职位表" posted to China's Military-Civilian Personnel Recruitment Network (军队文职人员招聘网), http://jzg.huatu.com/jdwz/zwk/bj/bm25.html.
139. 2020中国人民解放军军事科学院军事科学信息研究中心招聘. http://bj.offcn.com/html/2020/02/221551.html.
140. https://baike.baidu.com/item/情报学报.
141. https://baike.baidu.com/item/中国科技资源导刊.
142. http://tie.istic.ac.cn/qbgc/ch/first_menu.aspx?parent_id=20150323095003001.
143. https://baike.baidu.com/item/情报理论与实践.
144. https://baike.baidu.com/item/情报杂志.
145. https://baike.baidu.com/item/现代情报.
146. https://baike.baidu.com/item/情报资料工作.
147. http://www.yuez.net/qikan/xinxikeji/9516.html.
148. http://www.las.cas.cn/xscbw/tsqbgz/.

149. 科技管理研究 (*Science and Technology Management Research*) and 科技进步与对策 (*Science and Technology Progress and Policy*) both out of Guangdong.
150. 省级科技情报机构是我国科技情报行业的中坚力量和支撑力量. Liu Mingzhu (刘明珠), "基于期刊论文的我国省级科技情报机构科研现状分析 (Analysis on Research Status of Provincial S&T Intelligence Agencies in China Based on Journal Articles)," Nanjing University M.A. thesis, 2019.
151. Liu Mingzhu, Analysis on Research Status of Provincial S&T Intelligence Agencies in China Based on Journal Articles, 2019.
152. Peng Yiqi (彭以祺), "传承发展续写辉煌——隆重纪念国家科技图书文献中心成立二十周年 (Inheritance and Development Continue to Write Brilliant--Grand Commemoration of the 20th Anniversary of the Establishment of the National Science and Technology Library)," 数字图书馆论坛 (*Digital Library Forum*), 2020: 7, pp. 1-2.
153. Xiaomu Xu and Ling Leng, "Narrowing the Gap of the Digital Divide: How NSTL Contributes," 16th IFLA ILDS Conference 2019: Beyond the Paywall, Praha (CZ), October 9, 2019. Xu and Leng are both at CAS National Science Library in Beijing. (https://repozitar.techlib.cz/record/1378/files/idr-1378_1_paper.pdf).
154. https://baike.baidu.com/item/中国科学技术情报学会.
155. Yuan Youxiong (袁有雄) and Zhang Xiaoqi (张晓祺), "中国国防科学技术信息学会第五次会员代表大会召开 (Fifth Member Representative Conference of the China National Defense Science and Technology Information Society Held)," February 26, 2014 (http://www.mod.gov.cn/academy/2014-02/26/content_4492855.htm).
156. "Strategic and Competitive Intelligence Professionals", formerly the "Society of Competitive Intelligence Professionals" (https://www.scip.org/).
157. Authors' personal recollection.
158. https://intelligence.house.gov/uploadedfiles/hpsci_china_deep_dive_redacted_summary_9.29.20.pdf.
159. The IP Commission Report, *The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*, February 2019. Wm. C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage* (London and New York: Routledge, 2013). Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy" (Washington, DC: Defense Innovation Unit Experimental, February 2017). Office of the United States Trade Representative, "Section 301 Report into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation," March 27, 2018. U.S.-China Economic and Security Review Commission, "2019 Annual Report to Congress," November 2019. Anastasya Lloyd-Damnjanovic and Alexander Bowe, "Overseas Chinese Students and Scholars in China's Drive for Innovation," U.S.-China Economic and Security Review Commission, October 7, 2020.
160. Congressional Research Service, "The Global Research and Development Landscape and Implications for the Department of Defense," updated November 8, 2018 (https://fas.org/sgp/crs/natsec/R45403.pdf).
161. Wm. C. Hannas and Huey-Meei Chang, "China AI-Brain Research," Georgetown University, Center for Security and Emerging Technology, September 2020.
162. Gryphon Scientific, "China's Biotechnology Development: The Role of U.S. and Other Foreign Engagement," A report prepared for the U.S.-China Economic and Security Review Commission, February 14, 2019 (https://www.uscc.gov/sites/default/files/Research/US-China%20Biotech%20Report.pdf) and Editorial Staff, "The Next Biotech Superpower," *Nature Biotechnology* 37, 1243 (2019) (https://www.nature.com/articles/s41587-019-0316-7#citeas).

CSET.GEORGETOWN.EDU | CSET@GEORGETOWN.EDU