Research on Collaboration in Security Intelligence Work in the Big Data Environment: A Case Study of Counter-terrorism Intelligence Work (Postprint)

Authors: An Lu, Zhou Yiwen

Date: 2023-04-01T00:00:00+00:00

Abstract

[Purpose/Significance] The big data environment imposes heightened demands on collaborative security intelligence operations. Investigating the challenges and solutions within such collaboration facilitates coordinated efforts among relevant security intelligence agencies and enhances operational efficacy. [Method/Process] This study explores potential challenges in collaborative security intelligence operations within big data environments, using counter-terrorism intelligence as a case study. By integrating the intelligence workflow, it analyzes the operational entities and collaborative requirements of security intelligence work, subsequently proposing a collaborative framework for counter-terrorism intelligence operations. [Results/Conclusion] The proposed collaborative framework for counter-terrorism intelligence operations entails: under the guidance of intelligence requirements issued by the Counter-Terrorism Leadership Group, specialized agencies such as the Ministry of Public Security collaborate with general business departments—including the People' s Bank of China, Ministry of Transport, Ministry of Industry and Information Technology, and General Administration of Customs—as well as social forces from the financial, transportation, telecommunications, healthcare, non-profit sectors, and the general public, to execute the collection, processing, analysis, application, and feedback of domain-specific counter-terrorism intelligence.

Full Text

Preamble

Volume 64, Issue 19, October 2020

Research on the Collaboration of Security Intelligence Work in the Big Data Environment—Taking Counter-Terrorism Intelligence Work as an Example

An Lu[1],[2], Zhou Yiwen[2]

[1]Center for Studies of Information Resources, Wuhan University, Wuhan 430072
[2]School of Information Management, Wuhan University, Wuhan 430072

Abstract: [Purpose/Significance] The big data environment imposes higher requirements for collaboration in security intelligence work. Research on the problems and solutions in security intelligence work collaboration can help relevant departments work together to improve the effectiveness of security intelligence operations. [Method/Process] This paper discusses the potential problems in security intelligence work collaboration under the big data environment, takes counter-terrorism intelligence as an example, analyzes the main actors and collaboration needs in security intelligence work in conjunction with the intelligence workflow, and proposes a collaboration scheme for counter-terrorism intelligence work. [Result/Conclusion] The proposed collaboration scheme for counter-terrorism intelligence work is as follows: Under the guidance of counter-terrorism intelligence requirements issued by the Counter-Terrorism Leading Group, specialized departments such as the Ministry of Public Security collaborate with general business departments including the People' s Bank of China, Ministry of Transportation, Ministry of Industry and Information Technology, and General Administration of Customs, as well as social forces from the financial, transportation, telecommunications, medical, and non-profit sectors and the general public, to carry out the collection, processing, analysis, application, and feedback of counter-terrorism intelligence in specific fields.

Keywords: security intelligence; counter-terrorism intelligence; collaboration; intelligence process; big data

Classification Number: G203
DOI: 10.13266/j.issn.0252-3116.2020.19.006

Security intelligence refers to security information that influences security management [1]. Security intelligence work helps maintain national security and social stability. On October 18, 2017, during the 19th National Congress of the Communist Party of China, General Secretary Xi Jinping stated that "adhering to the overall national security concept, coordinating development and security, enhancing awareness of potential dangers, and being prepared for danger in times of safety constitute a major principle of our Party in governing the country." He emphasized that "we must uphold national interests as paramount, take people' s security as our purpose, political security as our foundation, coordinate external and internal security, territorial and national security, traditional and non-traditional security, and individual and collective security, improve our national security system, strengthen national security capabilities, and resolutely

safeguard national sovereignty, security, and development interests." According to the connotation of the overall national security concept, the national security intelligence system should be a collaborative organic unity [2]. Under this concept, leveraging scale advantages through intelligence sharing and collaboration is an implicit requirement [3].

Traditional intelligence work methods are not fully applicable to security intelligence work in the big data environment. Such work relies not only on professional intelligence personnel to provide security intelligence but also on extracting security intelligence from massive data across various industries. The diversification of intelligence sources makes the security intelligence process more complex. Without effective collaboration, this not only leads to duplicated efforts but may also result in insufficient professional knowledge and skills within individual business or intelligence departments, affecting the effectiveness of intelligence work. A collaborative security intelligence process can improve efficiency, enable knowledge and skill exchange and sharing, and save time and material costs. The root cause of most collaboration problems lies in the fact that traditional security, self-security, and common security are not adequately addressed. Therefore, it is necessary to conduct research on security intelligence work collaboration from the perspective of the intelligence process to address the questions of "how to collaborate" [4].

The concept of "security intelligence" encompasses national security, public safety, and production safety [5]. Intelligence required by organizations related to counter-terrorism tasks is called counter-terrorism intelligence [6]. Counter-terrorism is one of the responsibilities of the U.S. Department of Homeland Security [7], and China has also incorporated counter-terrorism into its national security strategy [8]. Counter-terrorism intelligence differs from security intelligence in that it involves a narrower scope—security intelligence covers broader domains, while counter-terrorism intelligence focuses solely on counter-terrorism work.

Big data is characterized by large volume, diverse types, high velocity, and low value density. It presents both challenges and opportunities for security intelligence. On one hand, big data can provide rich intelligence; on the other hand, traditional intelligence work methods are not entirely suitable. This study takes counter-terrorism intelligence work as an example to examine security intelligence work collaboration from the perspective of the intelligence process. It analyzes specific collaboration problems in each stage of the counter-terrorism intelligence process and constructs a collaboration scheme for counter-terrorism intelligence processes.

2 Related Research

2.1 Security Intelligence

Security intelligence is an interdisciplinary field combining intelligence studies and security science [9]. Existing research primarily focuses on security intelligence law systems, methods, and institutional frameworks. For instance, Wang Bing et al. explored the concept and evolution of security intelligence from a safety science perspective [5] and proposed conceptual and implementation models for intelligence-led security management [10]. Gao Jinhu [11] emphasized the need to create an integrated national security intelligence work mechanism and proposed reform paths for the national security intelligence system. Zhang Yalei et al. [12] discussed the essential competencies required of security personnel under the overall national security concept, namely security intelligence literacy, which refers to the ability to acquire, analyze, and utilize security intelligence [13]. Qin Dianqi et al. [14] noted that in the big data environment, the intelligence literacy of security intelligence personnel is crucial for information security, requiring openness, development, and interactivity. Li Hui et al. [15] pointed out that in national security intelligence work, intelligence perception and analysis must consider massive information and complex environments, posing significant challenges to intelligence personnel' s analytical capabilities and workload.

Although scholars have explored security intelligence from various perspectives, few have studied security intelligence work collaboration in conjunction with big data characteristics, and research on specific collaboration mechanisms from the intelligence process perspective remains insufficient.

2.2 Intelligence Process

The intelligence process is the fundamental procedure for conducting intelligence work, and its importance is self-evident. It refers to a series of steps or stages in intelligence work [16] and can also be described as several stages centered on specific phases [17]. A clear intelligence process helps clarify personnel composition and work objectives at different stages, thereby enhancing an organization' s information collection capabilities, decision-making capacity, and competitiveness [18].

Currently, there is no unified understanding of the intelligence process. Academia has proposed various models, including linear progression models, intelligence cycle models, multiple iteration models, network interaction models, and target-centric models [19]. R. Chakraborty et al. [20] interviewed Indian police and highlighted the positive role of intelligence processes in crisis management during terrorist attacks. A. Williot et al. [21] similarly noted that process strategies can significantly affect police crisis detection capabilities. Li Jianhui et al. [22] studied public security intelligence processes, dividing them into four stages: data mining, data management, analysis and prediction, and intelligence product distribution and feedback. F. Bartes summarized previous

research and proposed a counter-competitive intelligence cycle divided into five stages: planning and direction, data collection, analysis, action, and evaluation [23].

Most existing research examines intelligence processes from the perspective of intelligence activity stages, using highly generalized models. While such studies have universal applicability, they lack specificity when applied to particular domains. Currently, few studies focus on counter-terrorism intelligence processes. Some researchers have examined public security intelligence processes, which are similar but have unique characteristics. Counter-terrorism intelligence activities require nationwide participation, making their actor composition more complex than public security intelligence and involving multiple departments. Counter-terrorism intelligence user needs are also more diverse. Existing research has not considered counter-terrorism intelligence work collaboration from the intelligence process perspective. However, collaborative processes can improve efficiency and maximize benefits through functional complementarity, cooperation, and resource sharing.

2.3 Collaboration Theory

To better accomplish security intelligence work, we need to establish a sensitive, multi-threat-responsive intelligence organization network with good collaborative effects. T. W. Malone et al. defined collaboration as harmonious cooperation and noted that reasonable information sharing is one of the most important issues in achieving overall objectives [24]. In organizations, collaboration is a key factor in enhancing competitiveness [25]. For organizations, collaboration refers to inter-departmental cooperation that creates total value greater than the sum of individual parts [26]. Synergetics suggests that without good collaboration, organizations fall into disorder and chaos [27]. Whole-of-government theory is an important framework for government department collaboration, emphasizing integration and coordination to establish cross-organizational cooperation and optimize government functions. It stresses not only cooperation based on shared goals but also mutual reinforcement through collaboration [28].

Security intelligence involves multiple domains. For emergency intelligence, Yang Qiaoyun [29] proposed using holistic governance to promote government emergency intelligence collaboration. For strategic intelligence, Wang Xin suggested a differentiated collaborative strategic intelligence research model [30]. For think tank intelligence, Zhang Haitao et al. [31] studied service innovation mechanisms from a collaboration theory perspective.

Although some existing research on security intelligence collaboration touches upon intelligence processes, these studies do not deeply analyze specific collaborative work in each intelligence process stage. Moreover, research on counter-terrorism intelligence process collaboration is scarce. Analyzing security intelligence process collaboration from the intelligence process perspective can intuitively demonstrate specific collaboration models. Therefore, this study exam-

ines security intelligence work collaboration in the big data environment from the intelligence process perspective, using counter-terrorism intelligence work as an example.

---

3 Demand Analysis and Existing Problems in Security Intelligence Work Collaboration

3.1 Collaboration Demand Analysis in Security Intelligence Work Under Big Data Environment

In the big data era, security intelligence work faces challenges including large data volumes, diverse data structures, multiple data sources, and low data value density. These issues permeate the entire security intelligence workflow and require joint efforts from all participating organizations. Collaboration is an effective means to improve security intelligence work efficiency in the big data environment. Big data collection, storage, processing, and utilization impose high requirements on hardware and software capabilities. Collaboration helps better leverage big data information resources. For instance, using big data resources requires high-performance computer equipment, increasing costs. Intelligence personnel can access large amounts of data, but verifying authenticity and tracing sources is difficult. Moreover, different intelligence workers may draw different conclusions from the same data. Addressing these issues requires collaborative sharing of experience, capabilities, and wisdom. Additionally, big data does not represent all data, and different training and test set selections affect final results. Through collaboration, security intelligence workers can more efficiently utilize big data resources, obtain more accurate analysis results, and improve intelligence work efficiency through information and capability sharing.

3.2 Shortage of Professionals

Most cross-organizational collaboration designs depend on the experience and capabilities of specific personnel [32]. However, relying on experienced individuals makes flexible and effective inter-organizational collaboration difficult. Big data imposes higher requirements on security intelligence work collaboration. Collaboration can only be achieved when personnel can effectively utilize external information [33]. Intelligence personnel competencies are closely related to data collection and analysis methods [34]. The large volume and structural diversity of big data increase the difficulty for organizational members to utilize external information, demanding higher competencies from intelligence personnel.

Counter-terrorism intelligence work also faces professional shortages [35]. The 2015 Counter-Terrorism Law of the People' s Republic of China mandates establishing a national counter-terrorism intelligence center to coordinate China' s counter-terrorism intelligence work and strengthen inter-departmental coop-

eration. Subsequently, provinces and cities established counter-terrorism intelligence centers, such as Lanzhou' s transformation of its counter-terrorism intelligence comprehensive analysis center in 2017 [36] and Anhui' s launch of a provincial counter-terrorism intelligence center system construction project in 2018 [37]. Additionally, the Ministry of State Security, Armed Police, and People' s Liberation Army are involved in counter-terrorism operations, with databases containing counter-terrorism intelligence. Different databases have inconsistent storage structures, increasing the cost of intelligence sharing and making intelligence interpretation dependent on professionals. Therefore, professional shortages reduce counter-terrorism intelligence work efficiency, making it difficult to timely address challenges and meet demands. Professional training is a long-term endeavor requiring substantial time investment, so counter-terrorism intelligence work schemes need to reduce dependence on internal professionals.

3.3 Insufficient Horizontal Interaction Between Organizations

In the big data era, the nature, time, space, content, and form of security intelligence elements are being reconstructed [38]. To improve efficiency, research on security intelligence work collaboration from the intelligence process perspective is necessary. The intelligence process is crucial for collaboration and should match intelligence requirements. Security intelligence work is not a single-objective task, and rigid processes hinder collaboration [39-40]. Defining intelligence requirements is the first step in intelligence work [41]. Horizontal interaction between intelligence departments better meets intelligence needs [42]. For example, U.S. intelligence agencies fully mobilize national resources to ensure horizontal and vertical information transfer between intelligence service agencies and intelligence requirement entities [43]. Only with sufficient horizontal interaction between departments can valuable security intelligence be provided [44]. Currently, China' s security intelligence workflow suffers from insufficient horizontal interaction [45].

In counter-terrorism intelligence work, although the core purpose is counter-terrorism, requirements vary across contexts. For instance, pre-event counter-terrorism intelligence needs focus on prevention, while during-event needs focus on response. The former represents unclear requirements, while the latter represents clear requirements. Thus, counter-terrorism intelligence work is not a single-objective task. The counter-terrorism intelligence process should accommodate both early warning needs and task-specific requirements. Therefore, to achieve collaboration, the counter-terrorism intelligence process must be more flexible to promote horizontal interaction between departments. Only through sufficient horizontal interaction can efficiency in obtaining effective intelligence from big data resources be improved.

4 Construction of a Counter-Terrorism Intelligence Collaboration Scheme

4.1 Counter-Terrorism Intelligence Actors

To address the collaboration problems in counter-terrorism intelligence work under the big data environment identified in Section 3, this study constructs a counter-terrorism intelligence collaboration scheme based on whole-of-government theory [28] and incorporates social forces by drawing on the U.S. intelligence outsourcing model. The scheme elaborates on counter-terrorism intelligence actors and their specific collaboration methods.

Under China' s nationwide counter-terrorism context, counter-terrorism intelligence actors should include the Counter-Terrorism Leading Group, specialized departments, general business departments, and social forces. According to the Counter-Terrorism Law, the Counter-Terrorism Leading Group provides unified leadership and command, coordinating counter-terrorism work across departments. Specialized departments include the Ministry of Public Security, Ministry of State Security, People' s Armed Police, and People' s Liberation Army—organizations with professional counter-terrorism intelligence collection and analysis personnel that have counter-terrorism as their primary mission. General business departments include the People' s Bank of China, Ministry of Transportation, Ministry of Industry and Information Technology, and General Administration of Customs—government agencies that do not primarily focus on counter-terrorism but provide auxiliary services.

Social forces are important sources of counter-terrorism intelligence, including enterprises, non-profit organizations, and the public. Enterprises span finance, transportation, telecommunications, services, manufacturing, and other industries. Financial institutions (banks, securities firms, mobile payment providers) can provide information on abnormal financial flows. Transportation (rail, air, road) can provide data on personnel movement and dangerous goods transport. Telecommunications (operators, social media platforms, e-commerce) can provide information on individuals disseminating terrorist content online. Services (hotels, hostels) can provide suspicious personnel whereabouts. Manufacturing enterprises using or producing dangerous goods can provide lists of individuals purchasing such items. Non-profit organizations include public welfare groups, rights protection associations, religious groups, and cultural-educational organizations, which can provide domain-specific information such as dangerous infectious sources or abnormal business activities.

Actors are divided into leadership and execution layers [46], as shown in Table 1 .

4.2 Counter-Terrorism Intelligence Work Collaboration Scheme

In counter-terrorism intelligence work, "collaboration" means achieving complementary advantages and mutual benefit among actors. Based on the actors

described in Section 4.1, this section explores the collaboration scheme between them.

Following the literature [16], the collaboration scheme is constructed according to intelligence planning, collection, processing, analysis, application, and feedback. As shown in Figure 1 [Figure 1: see original paper], based on network interaction models [47] and target-centric models [48], the core of the intelligence process should be clear intelligence requirements or objectives, making "clarifying requirements" the starting point. Following multiple iteration models [16] and network interaction models, intelligence process stages are not fixed but flexible. When applied to specific counter-terrorism intelligence tasks, this manifests as collaboration among different actors at different stages, as detailed in Figure 1.

Numbers represent horizontal interactions: 1—task assignment; 2—submission of processed intelligence; 3—expert secondment; 4—external expert hiring; 5—reporting to specialized departments. To address professional shortages, this scheme incorporates general business departments and social forces as counter-terrorism intelligence actors, assigning them partial intelligence collection, processing, and analysis tasks. Cross-organizational expert secondment also reduces dependence on internal professionals. For example, when government departments need financial data analysis, they can collaborate with financial experts from the People' s Bank of China or academia rather than hiring dedicated financial analysts.

To address insufficient horizontal interaction, the Counter-Terrorism Leading Group coordinates departmental work while enabling horizontal information transfer between actors. When no specific counter-terrorism intelligence task exists, actors conduct counter-terrorism intelligence work for early warning purposes. In this context, social forces, general business departments, and specialized departments must interact horizontally during intelligence collection and processing, transferring counter-terrorism intelligence. Specialized departments must interact horizontally with general business departments and social forces during intelligence analysis to second experts. When specific tasks arise, actors conduct counter-terrorism intelligence work under the Leading Group' s leadership. Due to their special nature, specialized departments can conduct task-oriented intelligence work based on specific assignments.

4.2.1 Collaboration in the Intelligence Planning Stage Intelligence planning involves planning the entire intelligence workflow based on requirements, defining organizational responsibilities and objectives [49]. In the big data environment, departments face diverse and massive data types. Clear counter-terrorism intelligence planning helps departments clarify responsibilities and conduct work effectively. For example, the U.S. Director of National Intelligence can coordinate national intelligence agencies and clarify their counter-terrorism intelligence tasks [50].

In Figure 1, after clarifying requirements, the Counter-Terrorism Leading Group formulates macro-level intelligence plans, issuing counter-terrorism intelligence tasks through notices, policies, and systems. Specialized and general business departments develop specific intelligence plans based on macro plans and actual conditions, also issuing tasks through notices and policies. For instance, if the Leading Group issues a task for online counter-terrorism intelligence collection, the Ministry of Industry and Information Technology would adjust its cyber intelligence plan accordingly, such as collecting accounts posting abnormal information on social media. Social forces (enterprises and non-profits) with complex structures must also consider internal division of labor, generating internal collection schemes based on tasks from the Leading Group and supervisory departments. This planning approach clarifies responsibilities, ensures operability, and improves collaboration efficiency.

4.2.2 Collaboration in the Intelligence Collection Stage Intelligence collection involves obtaining information according to intelligence plans. The big data context requires multiple information sources, including both non-public (government confidential information, undisclosed business information, professional intelligence collection) and public sources (online information, voluntarily disclosed organizational information).

Counter-terrorism intelligence collection should not be the sole responsibility of security departments; it requires multi-departmental cooperation. Specialized departments can collect from both public and non-public sources, while general business departments and social forces play crucial roles in open-source collection. Terrorist activities often require weapons like explosives and firearms obtained through purchase or theft. Collecting information on dangerous goods purchases and transport helps identify terrorists early [51]. Incorporating general business departments and social forces provides relevant intelligence. For example, the Ministry of Industry and Information Technology can aggregate dangerous goods purchase information from telecommunications providers, while the Ministry of Transportation can aggregate passenger and freight lists to identify abnormal personnel movement and weapons transport.

In the collection stage, social forces collect and store industry information in business databases for subsequent processing in real time. Financial institutions collect fund flow information; transportation collects passenger and freight data; telecommunications collect communication and dangerous goods purchase information; non-profit hospitals collect infectious source information. General business departments collect domain-specific information in real time for their business databases: the People' s Bank of China collects financial information; the Ministry of Transportation aggregates transportation data; the Ministry of Industry and Information Technology collects telecommunications and dangerous biochemical raw material purchase information; the General Administration of Customs collects inspection, quarantine, and entry-exit information. Specialized departments collect multiple information sources in real time for their

counter-terrorism databases, conduct task-oriented professional human intelligence collection, and gather cyber counter-terrorism intelligence in real time. They also aggregate information from general business departments and social forces in real time. Real-time collection improves efficiency, enabled by big data and internet technologies.

Since organizations' daily operations already involve industry data collection, having them collect domain data ensures professionalism, reduces duplication, and leverages organizational strengths.

4.2.3 Collaboration in the Intelligence Processing Stage Intelligence processing involves processing collected data, including verifying authenticity, assessing value, and integrating and organizing data [16]. In the big data context, massive data contains much false information that must be filtered out. For example, the internet contains vast amounts of "junk information"—contradictory or irrelevant content that must be cleaned to retain valid information and unify storage formats for subsequent analysis.

In counter-terrorism intelligence processing, processors are not unique but distributed across multiple departments and regions. Specialized departments bear primary responsibility, but general business departments and social forces also conduct simple processing tasks, including preliminary value assessment and classification. For example, to predict suspect movement trajectories, the transportation industry must preliminarily process passenger and freight information by removing duplicates, structuring data, and integrating information. The Ministry of Transportation further processes this data by assessing value, removing duplicates, and integrating submissions from different regions and enterprises. For effective collaboration, actors should use consistent data storage structures.

In the processing stage, social forces process collected intelligence in real time and submit processed data to general business and specialized departments. General business departments further process submissions from across their domains and forward processed data to specialized departments in real time. Specialized departments process multi-source counter-terrorism intelligence in real time or in a task-oriented manner, using information technology for automated processing and storing results in relevant databases. After processing, general business and specialized departments proceed to intelligence analysis, while social forces proceed to intelligence feedback. If specialized departments require external experts, social forces can select domain experts for recommendation during the analysis stage.

4.2.4 Collaboration in the Intelligence Analysis Stage Intelligence analysis involves using analytical tools to analyze data and produce intelligence products based on requirements [52]. Analysis should yield intelligence distinct from raw data [53]. Before the big data era, open-source information was difficult to apply to statistical analysis due to volume. Technological advances now enable precise analysis of terrorist activities using open-source information and

government business data. Different data require different analytical methods: traditional statistical analysis for small data; clustering and classification for big data to predict terrorist trajectories or identify weapons flows; deep learning methods like Convolutional Neural Networks (CNN) or Recurrent Neural Networks (RNN) for analyzing audio, video, and text data to identify terrorists by comparing photos and surveillance footage with existing databases. In practice, the U.S. has developed passenger screening systems using big data to provide suspicious passenger lists for aviation security [54].

Intelligence product quality depends on analysts'capabilities and is influenced by their thinking patterns and professional backgrounds—a skilled financial analyst may not be competent in military intelligence analysis. Expert secondment improves analytical quality. For example, the U.S. hires experts from academia and industry for short-term counter-terrorism intelligence analysis [55].

Specialized departments first determine whether to second experts. If not, they directly produce intelligence products. If needed, they collaborate with general business departments for cross-departmental secondment or hire external experts from social forces. For example, when analyzing financial counter-terrorism intelligence, specialized departments can collaborate with financial experts from the People' s Bank of China or academia rather than hiring dedicated financial analysts. General business departments analyze only domain-specific intelligence: the People' s Bank of China produces abnormal financial activity lists; the Ministry of Transportation produces passenger and freight trajectory information; the Ministry of Industry and Information Technology produces abnormal communication, online shopping, social media account, and dangerous biochemical raw material purchase lists; the General Administration of Customs produces inspection, quarantine, and abnormal entry-exit lists.

Specialized departments produce intelligence products at task-oriented, real-time, and daily frequencies. General business departments produce products at real-time and daily frequencies. Specialized departments conduct task-oriented work, enabling real-time analysis through artificial intelligence algorithms and daily manual analysis by experts. After analysis, both general business and specialized departments proceed to intelligence application.

In the analysis stage, collaboration between specialized departments and general business departments/social forces through expert secondment reduces dependence on internal experts.

4.2.5 Collaboration in the Intelligence Application Stage Intelligence application involves using intelligence products to support decision-making. Counter-terrorism intelligence application supports decisions including counter-terrorism operation deployment and work planning. Specialized departments use intelligence products in two ways [56]: (1) using products from demand-oriented intelligence activities, such as the U.S. pre-deploying personnel to Afghanistan for intelligence work to combat terrorist organizations [57];

(2) selecting from existing intelligence products. In the big data context, specialized departments can query various business databases for intelligence products, which may be from previous demand-oriented activities or produced by intelligence producers based on their domains (e.g., abnormal financial activity lists from the People' s Bank of China).

In the application stage, general business departments first determine whether they can handle incidents. If beyond their scope, they should actively cooperate with specialized departments by submitting relevant counter-terrorism intelligence. For example, when the Ministry of Industry and Information Technology identifies suspects through dangerous biochemical raw material purchase and abnormal communication lists, it should proactively communicate with specialized departments and submit suspect lists.

The Counter-Terrorism Leading Group applies various departmental work reports. Specialized departments first assess whether existing intelligence products meet requirements. If yes, they apply them directly; if not, they provide feedback to generate or adjust intelligence plans. General business departments determine whether tasks can be completed internally; if not, they report to specialized departments. If they can handle tasks, they proceed independently. For example, the People' s Bank of China can recommend freezing suspect funds; the Ministry of Transportation can add suspects to passenger and freight blacklists; the Ministry of Industry and Information Technology can legally conduct IP tracking; the General Administration of Customs can add infectious sources to inspection lists or include suspects in abnormal entry-exit lists. Social forces apply various policies and regulations to adjust intelligence collection and processing. After application, general business and specialized departments proceed to intelligence feedback.

Horizontal interaction between general business and specialized departments during application enables rational task allocation, improving overall efficiency.

4.2.6 Collaboration in the Intelligence Feedback Stage Intelligence feedback refers to information generated after intelligence work execution that further adjusts all process stages. In the big data context, databases can record specific implementation plans and feedback for each counter-terrorism intelligence operation. Successful operations provide feasible models for similar future tasks, while feedback information offers references.

In Figure 1, the Counter-Terrorism Leading Group generates or adjusts intelligence plans in a task-oriented manner. Specialized departments generate or adjust plans when existing products meet or fail to meet requirements, summarizing application situations to adjust future planning. When existing products meet needs, they produce monthly and annual work reports. General business departments report to specialized departments if they cannot handle incidents; if they can, they produce monthly and annual reports. Social forces produce monthly and annual work reports—monthly reports summarize short-term appli-

cation situations to adjust medium- and short-term plans, while annual reports summarize yearly situations to adjust long-term macro plans. Social forces also adjust collection schemes based on policies and regulations. After feedback, actors re-enter the intelligence planning stage.

The feedback stage includes both task-oriented and regular feedback, enabling timely identification of planning deficiencies and adjustment of organizational tasks to achieve complementary advantages and mutual benefits.

---

5 Prospects for Security Intelligence Work Collaboration in the Big Data Environment

Big data is characterized by large volume and diverse types. Constructing a counter-terrorism intelligence work scheme for the big data environment enables prospects for security intelligence work. To build a collaborative security intelligence work scheme, future efforts should focus on three aspects:

5.1 Strengthen Information Resource Sharing and Exchange

Because big data involves massive volumes, intelligence work becomes more burdensome. Strengthening information resource sharing and exchange in security intelligence work can reduce duplication, improve overall efficiency, and save costs. The proposed counter-terrorism intelligence collaboration scheme enhances exchange among the Counter-Terrorism Leading Group, specialized departments, general business departments, and social forces, integrating security intelligence information to avoid "information silos" and saving time on collection, processing, and analysis.

5.2 Strengthen Intelligence Service Outsourcing

Big data has large volume but low value density, making some collection and processing tasks low-value. Strengthening intelligence service outsourcing can avoid internal duplication and reduce low-value work. The proposed scheme assigns partial collection and processing tasks to general business departments and social forces, reducing pressure on specialized departments and enabling them to allocate more resources to higher-value, more professional tasks, thereby improving overall resource utilization efficiency.

5.3 Standardize Intelligence Work Models

Individual organizations have limited data processing capacity. In the big data environment, more organizations may participate in security intelligence work through cooperation or outsourcing. Standardizing intelligence work models clarifies participant responsibilities and facilitates error correction and self-improvement. The proposed counter-terrorism intelligence scheme clarifies responsibilities through the Counter-Terrorism Leading Group and enables error

correction through feedback, allowing timely problem identification and resolution. Standardizing models in security intelligence work clarifies responsibilities, prevents buck-passing, and helps identify and adjust workflow vulnerabilities.

References

[1] Wang Bing, Wu Chao. Analysis of the Mechanism and Value of Security Intelligence in Security Management [J]. Information Studies: Theory & Application, 2019, 42(2): 38-43.

[2] Zhang Jianian. Integration of Security Intelligence and Strategic Resilience from the Perspective of National Security: Countermeasures [J]. Journal of Intelligence, 2017, 36(1): 1-8, 22.

[3] Wang Ying, Wang Tao. The Intelligence Concept in China' s Network and Information Security Policies and Laws [J]. Data and Information Management, 2019, 40(1): 15-22.

[4] WANG Y, LIU Y, CANEL C. Process coordination, project attributes and project performance in offshore-outsourced service projects [J]. International journal of project management, 2018, 36(7): 980-991.

[5] Wang Bing, Wu Chao. The Origin, Evolution and Meaning of the Security Intelligence Concept: Reflections from a Safety Science Perspective [J]. Library and Information Service, 2019, 63(3): 45-52.

[6] Du Yilin, Wu Xiao. Research on Improving Counter-Terrorism Early Warning Mechanisms from a Smart City Perspective [J]. Journal of Intelligence, 2015, 34(7): 13-17, 33.

[7] Cai Shilin. Intelligence Fusion in U.S. Homeland Security Affairs [J]. Journal of Intelligence, 2019, 38(1): 8-12, 18.

[8] Li Heng, Deng Fengbin. The Application Value and Legal Practice of Counter-Terrorism Intelligence Information from a National Security Perspective [J]. Journal of China Criminal Police University, 2019(1): 28-35.

[9] Xiao Lianjie, Meng Tao, Wang Wei, et al. Research on Intelligence Analysis Method Recognition Based on Deep Learning: Taking the Security Intelligence Field as an Example [J]. Data Analysis and Knowledge Discovery, 2019, 3(10): 20-28.

[10] Wang Bing, Wu Chao. Intelligence-Led Security Management (ILSM): Basis, Meaning and Model [J]. Information Studies: Theory & Application, 2019, 42(6): 56-61.

[11] Gao Jinhu. On the Reform Path of the National Security Intelligence System [J]. Journal of People' s Public Security University of China (Social Sciences Edition), 2019, 2(2): 1-26, 123.

[12] Zhang Yalei, Wu Chao, Wang Bing. Security Intelligence Literacy: Essential Competencies for Security Personnel Under the Overall National Security Concept [J]. Journal of Intelligence, 2019, 38(3): 33-38, 113.

[13] Wu Chao, Wu Lin. Discussion on Security Management Models from a Security Intelligence Perspective [J]. Journal of Guangzhou University (Social Science Edition), 2020, 19(2): 25-32.

[14] Qin Dianqi, Zhang Yuwei. Intelligence Literacy: A Core Element of Information Security Theory [J]. Information Studies: Theory & Application, 2015, 38(4): 30-33.

[15] Li Hui, Chen Xuefei, Liu Ru, et al. Research on Intelligence Supply-Side Reform from the Perspective of National Security and Development: Based on a Supply-Side Pentagon Model [J]. Information Studies: Theory & Application, 2019, 42(10): 9-14.

[16] Lowenthal M M. Intelligence: From Secrets to Policy [M]. Translated by Du Xiaokun. Beijing: Jin Cheng Publishing House, 2015.

[17] Zhang Jianian, Zhuo Xiangzhi. Research on the Organizational Structure and Operational Mechanism of Chinese Think Tanks from the Perspective of Integrated Intelligence Processes [J]. Journal of Intelligence, 2016, 35(3): 42-48.

[18] CAO G, DUAN Y, CADEN T. The link between information processing capability and competitive advantage mediated through decision-making effectiveness [J]. International journal of information management, 2019, 44: 121-131.

[19] Peng Zhihui. Intelligence Process Research: Review and Reflection [J]. Journal of the China Society for Scientific and Technical Information, 2016, 35(2): 177-188.

[20] CHAKRABORTY R, AGRAWAL M, RAO H R. Information processing under stress: a study of Mumbai police first responders [J]. Acta psychologica, 2018, 187: 9-18.

[21] WILLIOT A, BLANCHETTE I. Can threat detection be enhanced using processing strategies by police trainees and officers? [J]. International journal of disaster risk reduction, 2018, 28: 214-224.

[22] Li Jianhui, Chen Junxu, Shan Yiwei. Research on the Impact of Big Data on Public Security Intelligence Processes [J]. Journal of Hubei University of Police, 2015(3): 20-23.

[23] BARTES F. Counter-competitive intelligence cycle [C]//KOURIEK A. Proceedings of the 11TH international conference on knowledge management and knowledge technologies. Liberac: Technical University Liberac, 2013: 18-26.

[24] MALONE T W, CROWSTON K G. What is coordination theory and how can it help design cooperative systems [C]//HALASZ F. Proceedings of the 1990 ACM conference on computer-supported cooperative work. New York: ACM, 1990: 357-370.

[25] MU W, BÉNABEN F, PINGAUD H. Collaborative process cartography deduction based on collaborative ontology and model transformation [J]. Information sciences, 2016, 334: 83-102.

[26] Yi Yaqun, Liu Yi, Li Yuan. Analysis of Organizational Resource Synergy Mechanisms and Their Effects [J]. Economic Management, 2003(16): 12-16.

[27] Xu Xueguo. Research on Organizational Collaborative Learning Mechanisms and Empirical Studies [J]. Journal of Systems & Management, 2010, 19(3): 284-297, 322.

[28] PERRI 6. Joined-up government in the western world in comparative perspective: a preliminary literature review and exploration [J]. Journal of public administration research and theory, 2004, 14(1): 103-138.

[29] Yang Qiaoyun. Research on Emergency Intelligence System Coordination from a Holistic Governance Perspective [J/OL]. Information Studies: Theory & Application. [2020-04-20]. http://kns.cnki.net/kcms/detail/11.1762.G3.20190821.1113.002.html.

[30] Wang Xin. Reflection and Exploration on Strategic Intelligence Research Models: Planning, Dynamic or Collaborative [J]. Information Studies: Theory & Application, 2013, 36(8): 1-5.

[31] Zhang Haitao, Zhang Nianxiang, Wang Dan, et al. Think Tank Intelligence Service Innovation Under Big Data Background: From a Collaboration Theory Perspective [J]. Journal of Modern Information, 2018, 38(9): 57-63.

[32] MONTARNAL A, MU W, BÉNABEN F, et al. Automated deduction of cross-organizational collaborative business processes [J]. Information sciences, 2018, 453: 30-49.

[33] Sun Kai, Liu Renhuai. Analysis of Cross-Organizational Information Sharing Strategies Based on Information Processing Theory [J]. Chinese Journal of Management, 2013, 10(2): 293-298.

[34] Li Pin, Yang Jianlin. Research on the Development Path of Intelligence Discipline Based on Big Data Thinking [J]. Journal of the China Society for Scientific and Technical Information, 2019, 38(3): 239-248.

[35] Zhai Jiasheng. Analysis of Counter-Terrorism Talent Training in Police Academies: Taking the Criminal Investigation Police University of China as an Example [J]. Journal of Yunnan Police Officer Academy, 2017(5): 46-50.

[36] China Government Procurement Network. Announcement of Winning Bid for Lanzhou Public Security Bureau' s Counter-Terrorism Intelligence Comprehensive Analysis Center Renovation and Equipment Purchase Project [EB/OL]. [2020-04-20]. http://www.ccgp.gov.cn/cggg/dfgg/zbgg/201710/t20171017_{8996726}.htm.

[37] Anhui Government Procurement Network. Anhui Provincial Public Security Department Provincial Counter-Terrorism Intelligence Center System Construction [EB/OL]. [2020-04-20]. http://www.ccgp-anhui.gov.cn/cmsNewsController/cmsNewsDetail.do?newsI
e886-41be-8c6f-067f3f35a2fc.

[38] Wang Shiwei. On the New Characteristics and Requirements of Information Security in the Big Data Era [J]. Library and Information Service, 2016, 60(6): 5-14.

[39] BARTHÉ-DELANOY A, MONTARNAL A, TRUPTIL S, et al. Towards the agility of collaborative workflows through an event driven approach-application to crisis management [J]. International journal of disaster risk reduction, 2018, 28: 214-224.

[40] Hua Bolin, Li Guangjian. Construction of an Intelligence Method System Oriented to the Intelligence Process [J]. Journal of the China Society for Scientific and Technical Information, 2016, 35(2): 177-188.

[41] NAJAFI-TAVANI S, NAJAFI-TAVANI Z, NAUDÉ P, et al. How collaborative innovation networks affect new product performance: product innovation capability, process innovation capability, and absorptive capacity [J]. Industrial marketing management, 2018, 73: 193-205.

[42] Li Xiaodong. Preliminary Study on the Impact of Intelligence Systems on Joint Operations Intelligence Requirements [J]. Journal of Intelligence, 2010, 29(S2): 111-113, 110.

[43] Zhang Zhihua, Zhang Lingke. Research on National Competitive Intelligence Strategy Based on Network Information Security: The U.S. Example [J]. Library Theory and Practice, 2016(8): 36-41, 76.

[44] Tang Shiguo. The Integration Trend of Contemporary Science and the Formation of Intelligence Science [J]. Information Science, 1982(2): 8-12.

[45] Xu Xianghua, Liu Zhixin. Review and Legislative Improvement of Shanghai' s Environmental Risk Emergency Management System [J]. Law Science Magazine, 2011, 32(S1): 169-174.

[46] An Lu, Zhou Yiwen, Yang Yuxi. Research on the Collaborative Organizational Structure of Counter-Terrorism Intelligence Work [J]. Information Studies: Theory & Application, 2019, 42(8): 17-24.

[47] U.S. Joint Chiefs of Staff. Joint publication 2-01, joint and national intelligence support to military operations [R]. Washington D.C.: GPO, 2004: III-2.

[48] CLARK M R. Intelligence analysis-a target-centric approach [M]. Washington D.C.: CQ Press, 2006: 10-15.

[49] Li Jianchao, Si Youhe, Zhai Weixi, et al. Correlation Analysis Between Enterprise Competitive Intelligence Process and Enterprise Performance [J]. Modern Information, 2011, 31(5): 123-126.

[50] Yuan Li, Yao Leye. Exploration of "Data-Resource-Application"Intelligence Fusion Model in Emergency Management [J]. Library and Information Service, 2014, 58(23): 26-32.

[51] Jia Yu, Li Heng. Research on Intelligence Information Collection of Terrorist Organizations and Personnel [J]. Journal of Intelligence, 2017, 36(2): 32-39.

[52] Duan Chenjie. Difficulties and Countermeasures in Public Security Intelligence Analysis [J]. Information Research, 2018(12): 87-91.

[53] LANGEFORS B. Infological models and information user views [J]. Information systems, 1980, 5(1): 17-32.

[54] Jin Bo, Yang Tao, Wu Songyang, et al. Overview of Digital Forensics and Identification Development [J]. Chinese Journal of Forensic Sciences, 2016(1): 62-74.

[55] Sun Zongyi, Zhao Jinping. Research on the Intelligence Contracting Mechanism of Private Companies in the U.S. Intelligence Community [J]. Journal of Intelligence, 2016, 35(3): 49-53.

[56] Liu Ru, Li Menghui, Zhang Huina, et al. Deep Mining and Exploration of User Intelligence Needs in the Willingness Economy Environment [J]. Library and Information Service, 2017, 61(1): 14-24.

[57] Peng Yaping. Reflections on the Role of U.S. Intelligence Work in Counter-Terrorism War [J]. National Security Communications, 2002(4): 30-31.

Author Contributions:
An Lu: Research design, paper revision;
Zhou Yiwen: Paper writing and revision.

Abstract (English):
[Purpose/Significance] Big data puts forward higher requirements for the collaboration of security intelligence work. Studying the problems and solutions in the collaboration of security intelligence work is helpful for relevant departments to work together to improve the effectiveness of security intelligence work. [Method/Process] This paper discusses the possible problems in the collaboration of security intelligence work under the big data environment, takes counter-terrorism intelligence as an example, analyzes the main body and collaboration needs of security intelligence work in combination with the process of intelligence work, and proposes a collaboration scheme for counter-terrorism intelligence work. [Result/Conclusion] The proposed collaboration scheme for counter-terrorism intelligence work is: Under the guidance of counter-terrorism intelligence needs issued by the counter-terrorism leading group, professional departments such as the Ministry of Public Security cooperate with general business departments such as the People' s Bank of China, the Ministry of Transportation, the Ministry of Industry and Information Technology, and the General Administration of Customs, as well as social forces such as the financial, transportation, telecommunications, medical and non-profit sectors and the masses, to collect, process, analyze, apply and feedback counter-terrorism intelligence in specific fields.

Keywords: security intelligence; counter-terrorism intelligence; collaboration; intelligence processes; big data

Note: Figure translations are in progress. See original paper for figures.