Application of Big Data in Counter-Terrorism Intelligence Analysis and Early Warning

Heng-Liang Yang(✉)

College of Information Engineering, Engineering University of PAP, Xi'an, China
516861336@qq.com

Abstract. Counter-terrorism intelligence plays a critical role in counter-terrorism operations. This paper analyzes the inherent requirements of counter-terrorism intelligence work in the information age and proposes the application of Big Data in counter-terrorism intelligence from four aspects: the rapid collection of intelligence, storage and processing of intelligence, analysis and extraction of intelligence, and assistance in counter-terrorism combat decision-making. The application of Big Data technology to counter-terrorism intelligence analysis can solve the problem of complicated sources of counter-terrorism intelligence information and the ineffectiveness of traditional collection and analysis methods, thereby improving the level of counter-terrorism early warning capabilities.

Keywords: big data · Counter-terrorism intelligence · application

1 Introduction

Terrorism is becoming more frequent, more extensive and more serious. Only by mastering intelligence and information in counter-terrorism combats can we firmly grasp the initiative in the fight against terrorism. The focus of counter-terrorism work has gradually shifted to "counter-terrorism early warning" to reduce the harm caused by terrorist activities across the world [1]. Under the context of the information network era, intelligence information from a variety of sources, numerous irrelevant interference information, so it is difficult to analyze and analyze, and traditional intelligence information collection and analysis methods are difficult to be effective.

In this situation, should take advantage of the information dominance, attach great importance to the role of anti-terrorist intelligence early warning, using big data technology, counter-terrorism intelligence collection, analysis, mining, and timely warning information, auxiliary anti-terrorism combat decision-making, implementation of anti-terrorist intelligence digital, intelligent, initial bud will stop in various terrorist activities, to ensure social stability and national security.

N. Radojević et al. (Eds.): ICAID 2022, AHIS 7, pp. 1193–1200, 2023.
https://doi.org/10.2991/978-94-6463-010-7_123

2 Analysis on the Characteristics of Anti-terrorism Intelligence in the Era of Big Data

2.1 Strong Concealment of Terrorist Activities and High Difficulty in Intelligence Collection

In the information age, terrorist organizations focus on the participation of people who are proficient in advanced technology and have a relatively high level of knowledge and ability, and their abilities to use the Internet and other high-tech capabilities are increasing. Compared with the past, modern terrorism is more rigorously organized, terrorist activities are becoming more diverse, and the mode of action is more concealed. At the same time, Terrorist activities often take place suddenly, with terrorists in the dark and our anti-terrorism forces and people in the open. Terrorist organizations and terrorists have been hiding in legal social organizations and individuals for a long time, so it is difficult to collect their information and data. This dictates that counter-terrorism intelligence services must employ advanced technology to uncover hidden information that is not easily detectable and to unearth hidden intelligence data.

2.2 Intelligence Information from a Variety of Sources and Numerous Irrelevant and Interference Information

In the traditional media era, there are fewer social networking software and less data generation. In the era of Big Data, information networks generate massive quantitative data in real-time. Taking the Spring Festival Transport in 2019 as an example, the national railways transported more than 11 million passengers per day for 13 days, and the railway public security authorities seized 77,000 counterfeit tickets. The ticketing data information includes name, ID number, places of departure and arrival, ticket payment information, etc. There are many types of data and a huge amount of information. For such a situation where the source of information is huge and varied and too much irrelevant interference information exists, traditional intelligence information collection and analysis methods are difficult to achieve.

2.3 Strong Comprehensiveness of Counter-Terrorism Intelligence and High Difficulty in Intelligence Analysis

Counter-terrorism intelligence involves many aspects such as politics, economy, communications, finance, and transportation, serving as a kind of comprehensive intelligence. How to analyze and correlate seemingly isolated intelligence data sources to form a complete and accurate judgment is crucial to counter-terrorism intelligence work. This kind of analysis and judgment cannot be effectively solved by relying solely on manpower. With the application of advanced technology, the professionalism and counter-surveillance of terrorists are gradually increasing, which requires counter-terrorism intelligence departments to improve the application of emerging technologies in intelligence collection and analysis, especially the ability to collect, monitor, analyze, and extract intelligence in real-time via using Big Data technology.

3 Analysis of the Characteristics and Requirements of Counter-Terrorism Intelligence Information

3.1 The Rapidity Requirements of Intelligence Information

Terrorist activities often occur suddenly and violently, so the acquisition of counter-terrorism intelligence must be timely, accurate, and reliable. In actual work, it is necessary to accelerate the collection, processing, and analysis of information related to terrorists and terrorist activities [2]. The faster the intelligence information is obtained, the shorter the time for analysis and research is, and the more effective it will be. If terrorist activities have already occurred or are about to occur when counter-terrorism intelligence analysis is extracted, then the usefulness of such intelligence will be greatly degraded.

3.2 The Scientific Requirements of Intelligence Information

In the early warning process of counter-terrorism, timely processing of collected intelligence information sources, as well as the analysis and extraction of intelligence information play a very important role. Especially when terrorist activities occur, the closer to the time of the incident is, the higher the utilization rate of intelligence data will be [3]. On account of this, the intelligence and information analysis department must study carefully in normal times, and gradually explore a set of scientific judgment standards and judgment procedures for various terrorist activities, so that the rules can be used to judge and analyze possible tendencies.

3.3 Timely Warning Requirements of Intelligence Information

The ultimate goal of counter-terrorism intelligence work is to accurately grasp the movements of terrorists and efficiently perform early warning and response work. Once the intelligence information of terrorist activities is analyzed and confirmed, relevant departments must promptly and accurately issue all information related to terrorist activities [4]. Through the analysis of intelligence and scientific assessment, timely issuance of early warning terrorist information, and multi-level analysis of the development of terrorist events, effective response measures are proposed in a timely manner.

4 The Main Application of Big Data in Counter-Terrorism Intelligence Work

The harmful effects of terrorism become increasingly severe. Under this situation, we should give full play to the information-leading advantages and use Big Data technology to collect, analyze, and mine counter-terrorism intelligence, thereby boosting the efficiency of counter-terrorism intelligence work.

Table 1. The Way Intelligence Information Access

Intelligence type	Intelligence sources	Access
More table copy[a]		
Open-source intelligence	Internet data	Web crawler and text feature extraction
Video intelligence	Various monitoring facilities	Image monitoring and biological detection
Secret intelligence	Mobile monitoring, hidden recording, and spectrum detection	Electronic surveillance and satellite monitoring

4.1 Quick and Comprehensive Collection of Intelligence Information Sources

1) *Collecting the Internet intelligence information*

Information sources are the foundation of counter-terrorism intelligence. In today's era of Big Data, terrorist organizations are highly concealed and have various communication methods. The following methods should be focused on extensively collecting intelligence information sources, as shown in Table 1.

In the information network age, people's work and life are closely related to the Internet, and the network is active in daily activities. Terrorists' communication, planning, organization, and implementation of violent terrorist activities are inseparable from the network, all of which can be traced on the network. Big Data technology is to use web crawler technology, direct collection method, and indirect collection method to collect open-source intelligence information sources in the Internet environment and excavate useful intelligence information deeply.

2) *Collecting all kinds of monitoring information*

In modern society, surveillance cameras exist in various places. It is recommended to make full use of urban traffic and the monitoring equipment installed by the public sector, enterprises, and individuals in the society to video and take photographs, thus collecting the activities of rioters and all kinds of suspicious people at major traffic arteries, airports, terminals, stations, shopping malls, banks, and hotels, etc. In this way, it can quickly track the traces of people involved in terrorism and collect available intelligence information.

3) *Collecting all kinds of electronic monitoring information*

Through cell phone surveillance, hidden recording, spectrum detection, and other electronic surveillance, real-time monitoring of terrorists can be carried out; at the same time, satellite monitoring can also be used for 24-h monitoring and photography of various targets, accurate tracking of cell phone signals, and timely detection of rioters' traces. This way of electronic surveillance is concealed, and it is difficult to be easily detected by the intercepted object, which can obtain intelligence information with high accuracy and high-value level. At the same time, satellite monitoring can also be used to monitor all kinds of targets 24 h a day, take photos, accurately track phone signals, and timely find traces of violent terrorists, providing favorable guarantees for our anti-terrorism operations.

4.2 Using Big Data to Process and Store Intelligence

Counter-terrorism intelligence comes from a wide range of sources and has a huge amount of data. The adoption of Big Data technology, together with the corresponding management and operation mechanism, can facilitate the processing and storage of a large amount of mobile counter-terrorism intelligence information data.

1) *Using Big Data to process intelligence information sources*
   The data sources of counter-terrorism intelligence information include not only general types of structured data, but also a large amount of unstructured data such as real-time video, audio, and smart device perception data [5]. Using Big Data technology, the intelligence information sources are firstly classified into text and multimedia data, and the intelligence information is pre-processed regularly by using standard, standardized, and unified "exchange model"; secondly, through the operations of "extraction, transposition, and loading", the information is imported into Automap and ORA software for data aggregation, analysis, and processing and indexing data resources according to metadata standards. This process will remove a large amount of invalid information, improve the "accessibility" of data resources, and achieve data alignment. In this way, data alignment can be realized from "distributed" to "centralized", from "multi-source" to "single-source", from "heterogeneous" to "isomorphic", thus improving the efficiency of anti-terrorism intelligence processing.
2) *Using Big Data to store intelligence information*
   Big Data technology adopts distributed database technology and distributed file system, which can easily scale up the server and build a distributed information cloud storage service. At the same time, Big Data technology is used to adopt Hadoop distributed file storage system to establish a counter-terrorism intelligence big data storage platform, which can effectively store and manage intelligence data and avoid the time-consuming, labor-intensive, and inefficient shortcomings of manual management of intelligence data, thus providing a large-capacity, highly fault-tolerant storage for counter-terrorism intelligence. Users can quickly access the data management center through parallel applications to realize distributed data processing. At the same time using big data technology using the Hadoop distributed file storage system, establish a counter-terrorism intelligence big data storage platform, effective data storage management intelligence, to avoid time-consuming, consumption of artificial intelligence data management, the shortcomings of low efficiency, data storage management related information in time to facilitate frontline commander clearly grasp the dynamic information, updated in real time intelligence data, To facilitate efficient and flexible disposal by anti-terrorism teams.

4.3 Data Mining to Extract Intelligence for Timely Warning

In the wake of pre-processing various intelligence information sources, Big Data mining technology is used to analyze and process various data information sources, extract counter-terrorism intelligence via data mining, and issue early warning information according to the risk level determination.

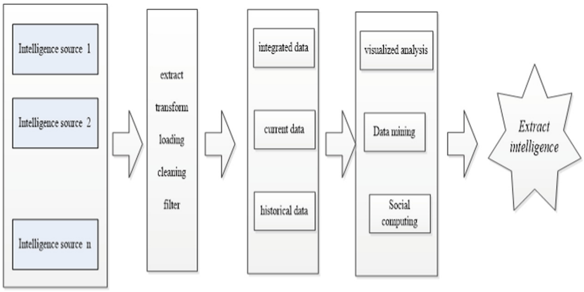

Fig. 1. The steps of Intelligence analysis extraction.

1) *Data Mining to Extract Intelligence*
Intelligence analysis and extraction is an important step of counter-terrorism for early warning. Intelligence departments based on big data mining technology, utilized semantic analysis, feature analysis, graphical correlation analysis, web network analysis, and other data mining analysis methods; a variety of "suspicious" trace information that was left in the riot activities or mass events can be collected for correlation analysis, from which the intelligence information related to the time and space of the terrorists and their activities can be found. the steps of intelligence analysis and mining are generally shown in Fig. 1. In the actual data mining analysis, the "one point rolling expansion" method is usually used. starting from the screen name, cell phone number, IP address and other clues, a multi-point search and in-depth mining methods are adopted to analyze their family information, personnel location, communication records, chat information, and other related intelligence information data, At the same time using big data technology using the hadoop distributed file storage system, establish a counter-terrorism intelligence big data storage platform, effective data storage management intelligence, to avoid time-consuming, consumption of artificial intelligence data management, the shortcomings of low efficiency, data storage management related information in time to facilitate frontline commander clearly grasp the dynamic information, updated in real time intelligence data, To facilitate efficient and flexible disposal by anti-terrorism teams.
2) *Data forecast for dynamic early warning*
The important application of counter-terrorism intelligence is to predict violent terrorist activities. Riot activities are generally difficult to be predicted. From a large number of terrorist preparation activities, Big Data analysis technology is utilized to analyze and find their related common characteristics, and position them into "riot risk" data points [6], and give a comprehensive determination for existing intelligence information through calm analysis, judgments one by one, and setting zero into a whole. Data mining methods such as socially aware computation are commonly used to predict the dynamic trends of individuals and groups and compare them with historical "riot risk" data points to predict future development trends and realize riot risk monitoring. At the same time, in accordance with the requirements of focusing on ourselves, vertical comparison and horizontal comparison, relying on the information system established by the military and local authorities, the information obtained was repeatedly verified with multiple information units, and verified in

multiple ways to avoid one-sidedness and ensure timely and accurate information. Through scientific research and judgment, risk assessment, prediction of event location, occurrence time or development trend, accurate early warning can be achieved to prevent terrorist activities in advance and give early warning.

4.4 Providing Intelligence Support for Counter-Terrorism Combat Decision-Making

Command decisions must be based on effective intelligence information [7]. In the process of preventing terrorist activities, Big Data technology is used to closely track and pay attention to suspected personnel, financial flows of key areas, transaction information and other data changes; the part of the key personnel and activities can be incorporated into the monitoring scope in advance. At the same time, the social network analysis technology can be utilized to analyze the law of terrorist organizations' activities, simulate the evolution of terrorist organizations, and find out their weak points, so as to take action in advance to interfere with and disrupt the activities of terrorist organizations. In the practice of counter-terrorism, data mining analysis methods such as emotion-oriented analysis, semantic analysis, and graphical correlation analysis are used to locate the activity time and scope of action of terrorist organizations; through a large number of data regularity analyses, a map of terrorists and their organizational relationships is drawn, a dynamic network of spatio-temporal evolution is constructed, and the relevant characteristics of violent terrorist activities and the next development trend are analyzed, so that the plan can be modified and improved in a timely manner and disposal actions can be taken in a targeted manner. In counter-terrorism practice, emergency response commanders rely on counter-terrorism databases to quickly find terrorist organizations or terrorist-related characteristics data, so as to quickly determine the identity of possible terrorists and related relatives information and obtain historical information such as the background and tactics of terrorist organizations, with an effort to make the right judgment and confirm the appropriate operational decisions with the help of Big Data technology.

5 Conclusion

In order to effectively combat terrorism, the focus of global counter-terrorism has gradually shifted from "emergency response" to "counter-terrorism early warning". In the face of the increasingly severe anti-terrorism situation, we must improve the efficiency of anti-terrorism intelligence work. In order to effectively prevent and combat terrorism, it is necessary to improve the effectiveness of counter-terrorism intelligence work. The next step is to further study the early-warning evaluation model of anti-terrorism intelligence analysis and mining based on big data, optimize the method of data mining, and improve the effectiveness and scientificity of data information acquisition. Finally, the anti-terrorism intelligence analysis and early warning system and its operating mechanism based on big data are constructed. The application of this system will enhance counter-terrorism intelligence analysis which will reduce the harm caused by terrorist activities, maintain social stability, and safeguard national security.

References

1. Zhaomei W, Chong L (2011) Thoughts on improving China's counter-terrorism early warning mechanism. J Wuhan Public Secur Cadre Coll (3):24–26
2. Tian L (2016) Research on Improving China's Counter-terrorism Early Warning Mechanism. Yanshan University, Qinhuangdao
3. Yaru S (2015) The problems and adjustments of china's counter-terrorism model under the new normal of terrorism. J Beijing Police Coll (6):36–40
4. Tongguang S (2018) Research on Xinjiang Counter-terrorism and Stability Maintenance Management. Chang'an University, Xi'an
5. Jiguang G, Sheng H (2017) Research on military intelligence analysis and service system architecture based on big data. J China Acad Electron (4):389–393
6. Yuling H (2015) The application of big data in the construction of the integrated mechanism of counter-terrorism intelligence and guidance. J Jiangxi Police Coll (6):42–46
7. Yueying S (2018) Research on the counter-terrorism intelligence early warning mechanism of the beijing winter olympics. J Beijing Police Coll ((5)33–37):57–64. https://doi.org/10.1109/SCIS.2007.357670