Cyber Counter-terrorism Research in China: Status, Issues, and Future Prospects (Postprint)

Authors: Huang Wei, afterglow, Yuefeng Li

Date: 2017-11-08T00:00:00+00:00

Abstract

【Objective】 To summarize the current state of domestic cyber counter-terrorism research, identify deficiencies, and propose future response directions.

【Literature Scope】 A total of 60 journal articles and books published since 2002 were selected from CNKI, Wanfang Data, Web of Science, ScienceDirect, and Engineering Village databases using "cyber counter-terrorism" as the theme.

【Method】Through bibliometric analysis methods, cyber counter-terrorism issues were analyzed from three perspectives: counter-terrorism data analysis, public opinion dissemination, and early warning and response.

【Results】 The current state of domestic cyber counter-terrorism research is based on the collection and analysis of terrorism data, achieving cyber counter-terrorism through analysis of terrorism-related speech and public opinion. Existing problems include insufficient capability in big data analysis for counter-terrorism, immature non-text data matching technologies, and the need for further improvement in cyber counter-terrorism related laws and education.

【Limitations】 The literature sources primarily consist of academic journals and books, with insufficient collection of materials from actual counter-terrorism practice.

【Conclusion】 Research on cyber counter-terrorism remains in a developmental stage and requires coordinated efforts across multiple dimensions including technology, management, and regulations. Both publicity and enforcement efforts should be strengthened, with particular emphasis on accelerating integration with big data technologies.

Full Text

Current Status, Problems, and Future Prospects of Online Anti-terrorism Research in China

Huang Wei[1],[2], **Yu Hui**[1], **Li Yuefeng**[1]
[1]School of Economy and Management, Hubei University of Technology, Wuhan 430064, China
[2]School of Management, Wuhan University of Technology, Wuhan 430072, China

Abstract

[**Objective**] This paper reviews the current state of online anti-terrorism research in China, identifies existing deficiencies, and proposes future directions for addressing these challenges.

[**Coverage**] We selected 60 journal articles and books published since 2002 from CNKI, Wanfang Data, Web of Science, ScienceDirect, and Engineering Village databases, using "online anti-terrorism" as the primary search theme.

[**Methods**] Through bibliometric analysis, we examined online anti-terrorism issues from three perspectives: counter-terrorism data analysis, public opinion dissemination, and early warning and crisis response mechanisms.

[**Results**] Current research in China emphasizes collecting and analyzing terrorism-related data to combat online terrorism through discourse analysis and public sentiment monitoring. However, significant problems remain, including insufficient capabilities in big data analytics for counter-terrorism, immature non-textual data matching technologies, and the need for further improvement in online anti-terrorism legislation and education.

[**Limitations**] The literature sources were primarily academic journals and books, with inadequate collection of materials from actual counter-terrorism operations.

[**Conclusions**] Research on online anti-terrorism is still in its developmental stage and requires coordinated efforts across technology, management, and regulatory dimensions. Both publicity and enforcement efforts should be strengthened, particularly through accelerated integration with big data technologies.

Keywords: Online anti-terrorism; Internet public opinion; Anti-terrorism warning; Network structure

---

1. Introduction

Since the 2001 "9/11" attacks in the United States, followed by the East Turkestan incidents and the rise of ISIS, terrorist events have continued

unabated. The domestic counter-terrorism situation in China remains grave, as terrorist organizations supported by anti-China and hostile forces disrupt domestic religious practices, create ethnic and political tensions, and threaten national integrity [1]. With the development of Internet and mobile network technologies, cyberspace has become another battlefield for terrorist organizations. Since 2013, large quantities of violent terrorist audio and video materials have been disseminated domestically by organizations such as the "East Turkestan Islamic Movement." In 2014, numerous terrorists were found participating in illegal religious activities and viewing violent terrorist videos, indicating that terrorist ideology is spreading rapidly and the scale of cyber terrorism is accelerating. Relevant state and government departments must accelerate policy guidance for online counter-terrorism, seizing the high ground both technologically and strategically to effectively respond to various terrorist activities in cyberspace.

Current challenges urgently demand in-depth research. These include untimely and inaccurate collection of online terrorist information, incomplete research on dissemination models and theories of terrorism-related information, unsystematic online and offline emergency response methods for terrorist incidents, and imperfect legal frameworks for online counter-terrorism.

The earliest definition of cyber terrorism was proposed by FBI expert Pollitt in 1997, who described it as politically motivated, premeditated violence against civilians, carried out by state actors or clandestine individuals targeting information, computer systems, computer programs, and data [2]. Cyber terrorist activities can be summarized into two implementation methods, as shown in Table 1 . Li Benxian et al. argue that repelling terrorism from the Internet perspective represents an important direction for online counter-terrorism [3]. Fan Yanfang contends that we must not only combat the terrorist activities of online terrorist organizations but also establish counter-terrorism intelligence systems as quickly as possible [4]. Robert Pape, from a strategic and tactical balance perspective, suggests that while preventive measures against terrorist incidents should be implemented, proactive strikes against terrorism are equally necessary [5]. Li Ou proposes that ensuring network security is essential for effectively preventing and combating terrorism [6]. In the "post-Bin Laden" era, terrorist organizations have become more structured, networked, simultaneously tight-knit and loosely organized, and more internationalized [7].

2. Literature Scope and Methods

The number of Chinese-language publications on online counter-terrorism is limited. A search for articles with "online anti-terrorism" in the title yields only 78 documents in CNKI, while searches in Web of Science, ScienceDirect, and Engineering Village for literature since 2002 using "Network Anti-terrorism" as the subject term return 29, 11, and 42 documents respectively. This paper uses literature on online anti-terrorism and mass incidents as important reference materials, focusing on selecting 60 recent documents related to counter-terrorism

achievements and research directions.

We conducted a comprehensive review of scholars' research from the perspective of online counter-terrorism, analyzing the current status, existing problems, and potential solutions across three dimensions: counter-terrorism data collection and analysis, terrorist public opinion dissemination, and online anti-terrorism early warning, emergency response, and prevention.

3. Counter-terrorism Data Collection and Analysis

The foundation of online counter-terrorism lies in the collection of terrorism-related online information. Only through in-depth analysis of terrorist organization information can effective strikes be implemented.

3.1 Counter-terrorism Intelligence Collection As early as 1997, Chaudhuri et al. pointed out that information extraction tasks are crucial because they facilitate the creation of multidimensional online analytical processing (OLAP) [8]. A continuously updated terrorism semantic dictionary is fundamental for locating relevant information and key to applying counter-terrorism information systems in actual operations. Appelt believes that knowledge engineering performs well in information extraction, with syntax and semantics also being helpful for such tasks [9]. These linguistic resources refer to semantic dictionaries. Conlon et al., in their online information extraction semi-automatic system, indicated that a manual vocabulary semantic list must be established before information extraction [10], demonstrating the importance of counter-terrorism semantic dictionaries.

In big data environments, further research is needed on search technologies, intelligent information processing technologies, and massive data storage technologies involved in counter-terrorism data collection. Compared with general search engines, vertical search technology is a customized, directed, and optimizable deep collection technology focused on specific domains, as shown in Table 2 . Xu Fajian et al. argue that vertical search engines are critical for such counter-terrorism information systems. They analyzed the information processing procedures of vertical search technology and proposed paying more attention to technical details, customizing and optimizing semantic structures, and correlation analysis and ranking processing techniques [11]. Precise collection of online counter-terrorism information should make greater use of vertical search engine technology.

Many countries have established their own counter-terrorism foundational databases according to their national characteristics [12-13]. However, big data processing technologies remain immature in addressing dynamic terrorist activities. Technologies such as real-time perception based on dynamic networks and terrorist organization modeling require further development. How to balance combating terrorism with protecting citizens' privacy and freedom is also a critical consideration.

3.2 Network Structure Obtaining information about network structures is an important source for research departments, with interpersonal networks being typical intelligence collection networks [14]. Strong ties are used to establish weak ties, expanding interpersonal networks outward to continuously broaden intelligence sources, as shown in Figure 1 [Figure 1: see original paper] [15]. This tree-like structure, when improved, approaches a mesh structure, facilitating the development of more weak ties into strong ties, as shown in Figure 2 [Figure 2: see original paper] [16].

Exploring terrorist network structures is typically understood as network analysis in the narrow sense, which can be categorized into three types: hierarchical structure, uniform distribution structure, and complex mesh structure. Different scholars use different names for these classifications, but they can generally be divided into these three categories, with simplified structural diagrams shown in Figure 3 [Figure 3: see original paper] [17].

The hierarchical structure is the earliest form of terrorist organization, characterized by strong command capabilities that make it relatively easy to identify central figures. The uniform distribution structure features relatively hidden personnel relationships that make counter-terrorism intelligence analysis difficult, though organizing terrorist activities is also more challenging for such structures. In complex mesh structures, nodes are dispersed but closely connected, making them difficult to combat. We summarize the characteristics of these three network structures in Table 3 .

Real-world terrorist organizational networks are not single types but rather fusions of these structures. Experts utilize social network analysis to develop countermeasures, with the most mainstream approach being the analysis of network central nodes to identify key figures in terrorist organizations for in-depth analysis. The BBC emphasizes centrality research to determine who is more important to the network, such as studying betweenness centrality. Both betweenness centrality and degree centrality are standard metrics proposed in social network analysis [18]. In fact, terrorist organizations also use social networks to disseminate terrorist information. Roberts et al. as early as 2009 pointed out the significance of high betweenness centrality (BC), though they did not consider factors such as gender at that time [19]. Everton et al. believe that betweenness centrality and degree centrality are important measures for extreme network communication [20]. This method is relatively cost-effective; however, even if terrorist organizations can be successfully combated using this approach currently, their branch organizations can still carry out certain terrorist activities.

3.3 Terrorism-related Data Analysis Terrorist network analysis focuses more on the dynamic evolution of networks, primarily applying theories such as social network theory, interpersonal network analysis, point-to-point networks, and complex network theory. Experts have provided definitions for network centralization. Based on existing centralization indicators, the definition of

centralization degree CA in a network W with n nodes is shown in Formula 1 [21].

These classic social network analysis methods were applied in the analysis of the U.S. "9/11" event, where core members could be identified through scores of degree, average distance, and betweenness [22]. However, actual terrorist organizations and behaviors are dynamically changing, and information collection is susceptible to various noises that can produce meaningless interference information. Traditional static analysis methods are unsuitable for such analysis. Consequently, researchers have devoted themselves to dynamic network analysis technologies. McCulloh et al. proposed dynamic metadata analysis methods and developed dynamic network analysis tools capable of simultaneously processing information on tens of millions of people, contributing to in-depth network research [23].

In 2001, Arquilla et al. [24] proposed Social Network Analysis (SNA), a data mining technique that simulates terrorist organization network structures based on relational data, analyzes the characteristics and internal information transmission methods of terrorist organizations, identifies weak points in the network, and locates key figures in terrorist organizations [25]. The model combining data mining and analysis technologies with publicly available data and information collected by counter-terrorism departments has become a research hotspot for various countries [26]. The process of mining terrorist information is shown in Figure 4 [Figure 4: see original paper] [27].

Although online counter-terrorism research has yielded some results, many challenges remain. Beyond structural network research, many other properties of centrality need to be studied. For instance, men are generally considered representative of terrorist organizations [28]. However, the latest longitudinal data in Manrique et al.' s research shows that although men are more numerous in ISIS, women hold positions with higher network connectivity, which contributes to the robustness and survivability of the potential system [29]. Observations indicate that new female-centric approaches can influence such networks and raise questions about how individual contributions should be evaluated in high-pressure systems. Science magazine published Bohannon' s latest experimental results in June 2016: women' s betweenness centrality is on average twice that of men [30]. This suggests that controlling the ideas of central female figures could serve as an effective counter-terrorism measure, allowing counter-terrorism organizations to leverage gender differences in their operations. In another experiment, he found that monitoring a small terrorist organization might help discover larger ones. Cohen in 2013 discussed how women have participated in some African conflicts just like men, and in certain situations such as bloodlust and violence, even more so [31]. These studies may not appear closely related to network structure but represent important future research directions for counter-terrorism networks.

Such hidden and counterintuitive information is difficult to discover, and open-source data quality is low, making processing difficult and information value den-

sity low. Terrorist organizations use various covert forms to organize activities. Currently, online counter-terrorism data analysis lacks corresponding dynamic analysis tools technologically and cannot effectively address the dynamic trends of terrorist organizations. Moreover, social ethics impose certain limitations because innocent civilians' rights and interests may be involved [32]. Therefore, to improve online counter-terrorism data analysis, it is necessary to handle the relationship between counter-terrorism and daily life properly, encouraging citizens to participate in online counter-terrorism by providing valuable information without affecting their normal lives or compromising their safety and privacy. Additionally, integration with big data mining technologies must be strengthened. Online counter-terrorism data analysis is part of big data analysis, possessing the 4V characteristics of big data (Volume, Variety, Velocity, Value), though counter-terrorism data is more covert and directly related to citizen safety, while big data is currently mainly applied in business. Breaking down barriers between big data mining and online counter-terrorism data mining and leveraging various advanced technologies from big data platforms will undoubtedly greatly enhance the processing capabilities of online counter-terrorism information analysis.

4. Terrorist Public Opinion Dissemination

Controlling online public opinion is another crucial aspect of online counter-terrorism. Research shows that ISIS is the organization with the strongest ability to gain online support and disseminates terrorist public opinion globally [33]. The spread of terrorist ideology online may cause broader and more lasting harm than actual terrorist acts.

4.1 Characteristics of Terrorist Public Opinion Zou Dongsheng et al. believe that online terrorism has four characteristics in public opinion: use of labeling language to intentionally provoke internal strife or hatred; proliferation of rumors that increase control difficulty; support for actual terrorist actions; and extensive influence of public opinion [34]. Some scholars directly analyze the characteristics of terrorist organizations, such as Ding Hongjun et al., who identified four features when interpreting ISIS' s online terrorism: clear propaganda objectives; diversified communication methods; professionally organized and highly provocative propaganda; and strong interactivity [35].

Terrorist organizations exploit these characteristics to elevate conflicting topics to the ethnic level, creating greater chaos and using public opinion to intensify netizens' emotions and create terror effects. This simultaneously makes terrorist organizations more radicalized. Public opinion thus transitions from latent opinion to manifest opinion in communication studies, triggering behavioral public opinion and causing real-world terrorist incidents.

4.2 Impact of Terrorist Public Opinion Dissemination Currently, terrorist ideology is spreading rapidly through network technology, impacting the

dissemination of correct values. Yang Yong et al., focusing on the counter-terrorism situation in special regions such as Xinjiang, proposed five impacts [36]: network dissemination is transnational, and such dissemination in intermediate regions affects national security; changes in the international pattern may transform terrorist public opinion into a factor affecting domestic political security; terrorist ideology further impoverishes the economy of these regions; it affects social stability; and it impacts the growth of youth [36], attracting potential individuals to join terrorist organizations. Large amounts of terrorism-related audio and video materials are likely to attract some lawbreakers or impressionable young people. Conway et al., in their study of ISIS members, found that current data tends to show female members 'attracting' while males are 'recruited' [37]. Recruitment is also a goal of terrorist organizations in disseminating public opinion. Scholars have found that recruiters affect not only sensitive regions but also potential terrorism-related organizations. Ding Hongjun et al., focusing on ISIS' s online terrorism, proposed impacts of terrorist ideology dissemination on domestic counter-terrorism: causing the spread of some extreme ideas domestically; enabling extremists to form terrorist groups; increasing the horror level of terrorist acts; and making terrorist organizations more unscrupulous [35]. Overall, the spread of terrorist ideology expands terrorist situations and the scale of terrorist organizations, posing greater threats to the nation and its people.

4.3 Control of Terrorist Public Opinion Dissemination Although terrorism-related online public opinion differs in severity from other types of mass online public opinion, it has similar origins and problems. Ye Zhanbei, combining other online public opinion issues, summarized deficiencies in three aspects: response methods, governance systems, and the use of computer and network means, as shown in Table 4 [38].

Zou Dongsheng et al. believe that in the mobile Internet era, efforts should focus on four aspects: clarifying political positions and strengthening public opinion guidance; enhancing public awareness of counter-terrorism to prevent exploitation by terrorist organizations; seizing the initiative to dominate public opinion; and combating terrorism according to law by governing public opinion through legislation [34]. Yang Yong et al. primarily propose legal and regulatory strategies, such as network real-name systems, establishing dissemination regulations, strengthening moral control, and improving technical network control capabilities [36].

In addition to mechanism issues in guiding public opinion, the main challenge in controlling terrorist public opinion dissemination is identifying terrorism-related information. Non-standard text, diverse languages, multiple communication channels, and non-textual information such as images and video files increase the difficulty of identification and processing. For fast-paced modern life, video and animation dissemination can convey large amounts of information in short periods and is relatively easy to consume, making it a very important infor-

mation transmission channel. However, automated supervision of multimedia data dissemination pathways is challenging. Available non-technical resources should be utilized, such as strengthening and improving citizen reporting mechanisms, given that terrorist organizations represent a tiny proportion of the total population, thereby leveraging the human resource advantage to guide citizens in properly handling illegal information. Mass media should serve as a powerful counter-terrorism force, supplementing technical deficiencies through its constructive, structural, and leadership capacities [39].

Terrorist incidents create panic before they occur, and terrifying memories and images after the event cause sustained psychological pressure and harm. Developing effective countermeasures against terrorist public opinion can not only inhibit the spread of terrorist ideology but also reduce the harm caused by terrorist acts and even help lock down data sources to identify terrorists.

5. Online Anti-terrorism Warning, Emergency Response, and Prevention

Since the U.S. "9/11" attacks, countries worldwide have focused on counter-terrorism. However, terrorist attacks continue to occur. Research on pre-incident warning mechanisms, faster and better emergency response implementation post-incident, and effective prevention can significantly reduce the harm caused by terrorist events.

5.1 Online Anti-terrorism Warning An international trend has emerged shifting the focus of counter-terrorism work from emergency response to early warning [40]. In terms of research approaches, warnings are primarily achieved through predicting or identifying terrorist intelligence, such as identifying the locations of unexpected events [41]. The United States has systems like the "Integrated Crisis System"[42] and the "Computer-Assisted Passenger Prescreening System" [43]. China has also developed the "Skynet Project," which monitors open-source intelligence through network public opinion to achieve early warning [44]. Du Yilin et al., from a smart city perspective, proposed an early warning mechanism combining intelligence, warning, and contingency plans to enable timely warning issuance and corresponding strategic responses [45].

Online counter-terrorism warning work primarily involves warning analysis of terrorist intelligence. In terms of terrorist intelligence work, China does not have a dedicated counter-terrorism intelligence early warning system, with intelligence collection typically assigned to public security departments. However, public security intelligence and counter-terrorism intelligence are different in nature, as shown in Figure 5 [Figure 5: see original paper].

Many countries have independent counter-terrorism intelligence agencies, such as Russia' s Intelligence Analysis Bureau, which is one of the four major institutions of the National Anti-Terrorism Committee [46]. The United States has also integrated its intelligence agencies multiple times to highlight the importance

of counter-terrorism intelligence [47]. Addressing China' s current situation, Li Benxian et al. proposed a framework process for domestic counter-terrorism intelligence early warning, as shown in Figure 6 [Figure 6: see original paper] [48]. This framework requires the involvement of counter-terrorism intelligence professionals and has limitations in both the quantity and quality of intelligence collection, suggesting that future research should strengthen counter-terrorism intelligence processing capabilities.

Liu Huijuan compared domestic and international civil aviation counter-terrorism early warning and proposed insights for improving domestic counter-terrorism early warning systems, as shown in Figure 7 [Figure 7: see original paper] [49]. The warning system can be divided into three modules: in the intelligence system, China should broaden intelligence collection channels and connect intelligence systems across different departments; in the decision-making system, the state should ensure the authority of warning decisions and processes; and in warning response, warnings should be classified and graded to respond to terrorist events with maximum efficiency.

5.2 Online Anti-terrorism Emergency Response In actual counter-terrorism operations, rescue and evacuation are the primary objectives of emergency response. Jia Zhicheng believes that remote monitoring plays an important role in counter-terrorism and rescue, constructing a remote monitoring system based on Ad Hoc networks to provide conditions for video applications in special environments [50]. Guo proposed a life signal identification method based on neural networks, using ultra-wideband life detectors to penetrate walls and ruins to detect signs of life. Simulation results show that using BP neural network systems can greatly improve the accuracy of life signal identification, enabling more targeted counter-terrorism rescue operations [51].

In intelligence research, Yang Lingzhi et al., in their study of urban emergency incidents, proposed that emergency management should be combined with information management, using information to support emergency management [52]. Lin Xi et al. summarized the current status of domestic emergency intelligence systems and identified problems in emergency management, including unclear legal guarantees for intelligence work, incomplete intelligence personnel training, and network connectivity issues [53].

To improve emergency response, scholars' proposed problems must be addressed, including perfecting legal guarantee systems for emergency intelligence work and emphasizing the cultivation of emergency management talents. Additionally, multi-agency joint responses to emergencies should be implemented. In the Guangzhou Railway Station terrorist violent attack, Guangzhou General Hospital of Guangzhou Military Region arranged emergency rescue operations, achieving seamless connection between pre-hospital and in-hospital care [54], improving the efficiency of treating the wounded, and proposing the establishment of a volunteer emergency medical training system to improve hospital rescue systems [55]. When emergencies or terrorist incidents occur, a single depart-

ment can hardly handle emergency affairs within a short time. Various relevant agencies should establish their own internal emergency systems and coordinate to handle emergencies to reduce harm.

5.3 Online Anti-terrorism Prevention In the face of direct network attacks by terrorist organizations, Jones proposed ten countermeasures: firewalls, the principle of minimalism, using the latest software, eliminating "spam" vulnerabilities, suppressing backdoor access, double-checking security, managed network server risks, ensuring network application security, dial-up services, and ensuring adequate virus checking [56]. Direct network attacks generally do not cause harm like traditional terrorist attacks, but using direct attacks to create chaos and thereby create opportunities for traditional terrorist incidents must be taken seriously. Therefore, prevention and response measures in this area should also be strengthened, such as enhancing education and establishing network real-name systems.

In counter-terrorism education, on the one hand, young people should be instilled with proper values to prevent participation in terrorist activities; on the other hand, citizens should be guided on how to cooperate with the government in prevention before terrorist incidents occur and how to save themselves during such incidents. At the legal level, as early as 2002, foreign countries began legislating counter-terrorism data and researching counter-terrorism legislation. Pounder analyzed the various impacts of legislation on counter-terrorism data acquisition and processing [57]. Zhu Wen believes that internationally interoperable laws are needed to unify definitions of terrorist crimes, establish international cooperation in online counter-terrorism, coordinate criminal jurisdiction among countries, and strengthen international judicial collaboration [58]. Pi Yong, in evaluating domestic counter-terrorism legislation drafts, indicated that China should establish specific crimes for combating online terrorism information dissemination and inciting terrorism-related actions as soon as possible, and that counter-terrorism legislation should be consistent with international counter-terrorism legislation, providing specific recommendations from comprehensive legislation and criminal law perspectives [59].

No one is born a terrorist. Understanding the causes facilitates the development of better education methods and countermeasures. First, major terrorist events are often related to regional politics and Western value influences. Second is the non-correlated economic factor: although no specific quantitative relationship can be identified, scholars still believe there is some relationship between counter-terrorism and the economy. Third is the religious issue: religion has considerable influence on terrorism, but it does not cause terrorism—rather, it is exploited by terrorism. Fourth, terrorism has existed for a long time, making it necessary to understand its historical origins [60]. Research on strategies to deradicalize terrorists and separate them from terrorist organizations is currently scarce and shows no short-term results, but it has far-reaching significance for counter-terrorism research. Overall, online counter-terrorism legislation and ed-

ucation are crucial. Laws can have immediate effects, warning some terrorist organizations to restrain themselves and strengthening the role of education. Combining these approaches with the domestic counter-terrorism situation can continuously improve and perfect counter-terrorism education and legislation to more effectively prevent terrorist activities.

6. Conclusion and Future Directions

This paper analyzed the current state of online counter-terrorism research from hot topics including information collection, network analysis, dissemination control, early warning, and prevention, primarily from analytical prediction and dissemination perspectives. In the data collection and analysis stage, current research lacks tools and technologies for analyzing dynamic networks and has insufficient big data analytical capabilities. In controlling terrorist public opinion dissemination, more advanced identification and matching technologies are needed, particularly for processing non-textual information, and ethical considerations must balance citizens' online freedom with control over terrorist event dissemination. Post-incident handling and prevention should receive greater research attention, as current studies rarely provide in-depth analysis from these angles. Overall, most existing research approaches the issue from sociology and communication studies or provides only brief overviews of counter-terrorism measures, lacking specific, feasible technical and management implementation plans.

Future online counter-terrorism work in China should, in addition to technological, legal, and moral constraints, emphasize the development of "soft" counter-terrorism efforts to purify the online environment. Future research can be developed in three directions:

(1) **Counter-terrorism data collection**: Develop advanced technologies and equipment for broader searches to provide more factual intelligence information; establish comprehensive counter-terrorism dictionaries and knowledge bases to enhance network information collection and processing capabilities; and on this basis, establish a counter-terrorism foundational database with Chinese characteristics to further improve the counter-terrorism intelligence system.

(2) **Terrorist public opinion dissemination**: First, improve citizens' counter-terrorism awareness through legislation and education, enabling the public to become rational guardians of the network and encouraging opinion leaders to guide online public opinion through network channels. Second, strengthen the ability to identify terrorism-related information, particularly regarding non-textual information processing, and supplement and improve online counter-terrorism reporting mechanisms. Finally, in public opinion control and guidance, preset executable response plans for each stage and degree of terrorism-related public opinion to respond calmly when incidents erupt and to some extent reassure the

public.

(3) **Counter-terrorism intelligence, response, and decision-making**: Conduct extensive research on these three aspects to comprehensively improve the practical effectiveness of early warning systems. With the aid of social network ubiquitous computing and big data mining as means, once terrorist events can be correctly predicted, corresponding emergency measures should be immediately activated to strike terrorist organizations and conduct evacuation and rescue operations for the public.

References

[1] Zhang Ting, Wang Shacheng. Study on the Intelligence Network Model of Public Security's Border Counterterrorism Based on Social Network [J]. Journal of Intelligence, 2014, 33(6): 17-21.

[2] Pollit M. Cyber Terrorism [C]. In: Proceedings of the 20th National Infomation Systems Security Conference. 1997.

[3] Li Benxian, Jiang Chengjun, Fang Jinqing. Network Science' s Challenges and Opportunities in Counter-Terrorism Research [J]. Complex Systems and Complexity Science, 2014, 11(1): 60-66.

[4] Fan Yanfang. The Use of Terror Crime Network the Focus of the Current Anti-Terrorism Network [N]. Social Sciences in China, 2012-09-03(A08).

[5] Ye Huijue. Terrorism Experts Robert Peiper: The Fight Against Terrorism Requires Tactical and Strategic Balance [N]. 21st Century Business Herald, 2014-07-03(002).

[6] Li Ou. Comment on Counter Cyber-terrorism and Its Control Method [J]. Journal of Jiangxi Police Institute, 2006(3): 92-95.

[7] Sageman M. Understanding Terror Networks [M]. University of Pennsylvania Press, 2004: 132-137.

[8] Chaudhuri S, Dayal U. An Overview of Data Warehousing and OLAP Technology [J]. ACM SIGMOD Record, 1997, 26(1): 65-74.

[9] Appelt D E. Introduction to Information Extraction [J]. AI Communications, 1999, 12(3): 161-172.

[10] Conlon S J, Abrahams A S, Simmons L L. Terrorism Information Extraction from Online Reports [J]. Journal of Computer Information Systems, 2015, 55(3): 20-28.

[11] Xu Fajian, Wang Hongwei, Yang Jie. Application Research on Vertical Search Technique Used in the Information Analytic System of Anti-terrorism in Internet [J]. Journal of Fujian Police College, 2010(2): 11-15.

[12] Dugan L F L. Introducing the Global Terrorism Database [J]. Terrorism & Political Violence, 2007, 19(2): 181-204.

[13] Lafree G. The Global Terrorism Database: Accomplishments and Challenges [J]. Perspectives on Terrorism, 2010, 4(1). http://www.terrorismanalysts.com/pt/index.php/pot/article/

[14] Qin Dianqi. On Human Intelligence Network in Ubiquitous Information Society [J]. Journal of Intelligence, 2013, 32(7): 24-27.

[15] Lin Juren. Social Network Analysis: Theory, Methods and Applications [M]. Beijing: Beijing Normal University Publishing House, 2009.

[16] Luo Jiade. Social Network Analysis Notes [M]. Beijing: Social Sciences Academic Press, 2010.

[17] Penzar D, Srblinovic A. About Modeling of Complex Networks with Appiication to Terrorist Group Modeling [J]. Inter-Disciplinary Description of Complex Systems, 2005, 3(1): 35-43.

[18] Estrada E. The Structure of Complex Networks [M]. Oxford University Press, 2012.

[19] Roberts N, Everton S F. Strategies for Combating Dark Networks [J]. Journal of Social Structure, 2009, 12(2): 1-32.

[20] Everton S F, Cunningham D. Terrorist Network Adaptation to a Changing Environment [A].// Crime and Networks [M]. Routledge, 2013.

[21] Krebs V. Mapping Networks of Terrorist Cells [J]. Connections, 2001, 24(3): 43-52.

[22] Freeman L C. Centrality in Social Networks: I. Conceptual Clarification [J]. Social Networks, 1979, 1(3): 215-239.

[23] McCulloh I, Carley K M. Longitudinal Dynamic Network Analysis: Using the Over Time Viewer Feature in ORA[R]. Social Science Electronic Publishing, 2009.

[24] Arquilla J, Ronfeldt D F. Networks and Netwars: The Future of Terror, Crime, and Militancy [M]. Santa Monica, California: RAND Corporation, 2001.

[25] Zhang Hai, Sun Duoyong. Stuty on the Terrorist Covert Networks from the Perpective of Social Network Analysis [J]. Journal of Safety and Environment, 2011, 11(3): 259-264.

[26] Martino F, Spoto A. Social Network Analysis: A Brief Theoretical Review and Further Perspectives in the Study of Information Technology [J]. Psychology Journal, 2006(1): 53-86.

[27] Li Benxian, Li Mengjun, Sun Duoyong, et al. A Brief Review of Applications of Social Networks Analysis Against Terrorism [J]. Complex Systems and Complexity Science, 2012, 9(2): 84-93.

[28] Silke A. Holy Warriors: Exploring the Psychological Processes of Jihadi Radicalization [J]. European Journal of Criminology, 2008, 5(1): 99-123.

[29] Manrique P, Cao Z, Gabriel A, et al. Women' s Connectivity in Extreme Networks [J]. Science Advances, 2016, 2(6): e1501742.

[30] Bohannon J. How to Attack the Islamic State Online [J]. Science, 2016, 352(6292): 1380.

[31] Cohen D K. Female Combatants and the Perpetration of Violence: Wartime Rape in the Sierra Leone Civil War [J]. World Politics, 2013, 65(3): 383-415.

[32] Bohannon J. News Investigating Networks: The Dark Side [J]. Science, 2009, 325(5939): 4l0-411.

[33] Weiss M, H. asan H. ISIS: Inside the Army of Terror [M]. Regan Arts, 2015.

[34] Zou Dongsheng, Ding Keyin. Involvement of Mobile Internet Era May Network Public Opinion and Counter-Terrorism Strategy [J]. Gansu Social Sciences, 2015(2): 195-198.

[35] Ding Hongjun, Chen Dejun. ISIS' s Cyber Terrorism Acticity Impacts on China' s Counter-terrorism and the Countermeasures [J]. China Public Security: Academy Edition, 2015(2): 95-97.

[36] Yang Yong, Yang Xiaoping. Research on the Challenges and Countermeasures of the Network Communication in Xinjiang Under the Anti-Terrorism Situation [J]. Journal of Karamay, 2014, 4(6): 26-31.

[37] Conway M, Mcinerney L. What' s Love Got to Do with It? Framing 'JihadJane' in the US Press [J]. Media War & Conflict, 2012, 5(5): 6-21.

[38] Ye Zhanbei. Jiangsu Network Group Events of Public Opinion Counseling [J]. Reality Only, 2016(4): 66-67.

[39] Jin Miao. International Anti-terrorism and Mass Media from the Perspective of Power Field [J]. Journal of PLA Nanjing Institute of Politics, 2012, 28(6): 94-98.

[40] Wu Zhaomei, Liu Chong. Thoughts on the Improvement of the Anti-Terrorism Early Warning System in China [J]. Journal of Wuhan Public Security Cadre' s College, 2011, 25(3): 24-26.

[41] Cai Huali, Liu Lu, Li Hong. Rule Reasoning-based Occurring Place Recognition for Unexpected Event [J]. Journal of the China Society for Scientific and Technical Information, 2011, 30(2): 219-224.

[42] O' Brien S P. Crisis Early Warning and Decision Support: Contemporary Approaches and Thoughts on Future Research [J]. International Studies Review, 2010, 12(1): 87-104.

[43] Berrick C A. Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges [R]. United States General Accounting Office, 2004.

[44] Wang Feiyue, Qiu Xiaogang, Zeng Dajun, et al. A Computational Experimental Platform for Emergency Response Based on Parallel Systems [J]. Complex Systems and Complexity Science, 2010, 7(4): 1-10.

[45] Du Yilin, Wu Xiao. Terrorist Warning Mechanism Under Perfect Wisdom Urban Perspective [J]. Journal of Intelligence, 2015, 34(7): 13-17.

[46] Fan Mingming, Xiao Huan, Tao Xiangjun. A Comparative Analysis on the U. S. and Russia' s Terrorism Early Warning System [J]. Journal of Intelligence, 2014, 33(12): 6-9.

[47] Whittaker A G, Smith F C, Mckune A E. The National Security Policy Process: The National Security Council and Interagency System [R]. National Security Council, 2008.

[48] Li Benxian, Mei Jianming, Li mengjun. China' s Counter-Terrorism Intelligence and Early Warning System Framework Design [J]. Journal of Chinese People' s Public Security University, 2012, 28(4): 117-125.

[49] Liu Huijuan. Comparative Analysis of Anti-terrorism Alert Systems for Civil Aviation in Western Countries[J]. China Civil Aviation, 2013(6): 61-62.

[50] Jia Zhicheng. Research and Implementation of Ad Hoc Network Based on the Remote Monitoring and Control System of Counter Terrorism [J]. Automation & Instrumentation, 2014(3): 108-112.

[51] Guo H. A Method of Life Signal Identification Based on BP Neural Network [C]. In: Proceedings of the 4th International Congress on Image and Signal Processing. 2011.

[52] Yang Lingzhi, Ding Jingda. On Emergency Information Management of City Thunderbolt [J]. Information Science, 2009, 27(3): 351-355.

[53] Lin Xi, Yao Leye. Analysis on Current Situation and Issues of China' s Intelligence Work in Emergency Management [J]. Library and Information Service, 2014, 58(23): 12-18.

[54] Qin Weiyi, Tang Shaohui, Li Shuangming, et al. Emergency Response Analysis of Guangzhou "5 • 6" Railway Station Terrorist Violent Attack [J]. Chinese Journal of Injury Repair and Wound Healing: Electronic Edition, 2015, 10(3): 37-40.

[55] Fuse A, Yokota H. Lessons Learned from the Japan Earthquake and Tsunami, 2011 [J]. Journal of Nippon Medical School, 2012, 79(4): 312-315.

[56] Jones D. Semantic Attacks —A New Wave of Cyber Terrorism [M]. NTA Monitor, 2002.

[57] Pounder C. Anti-terrorism Legislation: The Impact on The Processing of Data [J]. Computers & Security, 2002, 21(3): 213-223.

[58] Zhu Wen. Network Terrorism: International Law "Weaving Nets Above and Snares Below" [J]. China Information Security, 2014(10): 86-89.

[59] Pi Yong. Research on Cyber-Terrorism in China and the Related Criminal Law—Comment on the Provisions in the Draft of 9th Amendment of Penal Code and the Draft of Anti-terrorism Law [J]. Journal of Political Science and Law, 2015(1): 68-79.

[60] Li Benxian, Mei Jianming. The Hot Issues and Future Direction of China' s Anti-terrorism Research [J]. Journal of People' s Public Security University of China: Social Sciences Edition, 2015, 31(3): 1-9.

Author Contributions

Huang Wei: Conceived the research idea, designed the research framework, and revised the final manuscript.
Yu Hui and Li Yuefeng: Collected, processed, and analyzed data, and drafted the manuscript.

Conflict of Interest Statement

All authors declare no conflict of interest.

Supporting Data

Supporting data can be found in the online version of the journal at http://www.infotech.ac.cn.
[1] Huang Wei, Yu Hui, Li Yuefeng. Search Results.xlsx. Search Results.
[2] Huang Wei, Yu Hui, Li Yuefeng. Relevant Literature in Search Results.xlsx. Relevant Literature.

Received: 2016-06-21
Revised: 2016-09-09

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