

Theoretical basis and technical methods of cyberspace geography

GAO Chundong¹, GUO Qiquan², *JIANG Dong¹, WANG Zhenbo¹,
FANG Chuanglin¹, HAO Mengmeng¹

1. Institute of Geographic Sciences and Natural Resources Research, CAS, Beijing 100101, China;
2. 11th Bureau of the Ministry of Public Security, Beijing 100741, China

Abstract: Cyberspace is a new spatial realm of activities involving both humans and data, and it has become a cornerstone of the national security of every country. A scientific understanding of cyberspace is essential for analyzing cyberspace incidents, governing cyberspace and ensuring cybersecurity. Accordingly, cyberspace has become a new field of geographic research in the Information Age. Against the backdrop of fierce international competition over cyberspace, there has been an urgent need to strengthen research between the fields of geography and cybersecurity, leading to theoretical and methodological innovations that have created the sub-discipline of cyberspace geography. Cyberspace geography (CG) extends geographical research from real spaces to virtual spaces, and its theoretical basis is the evolution of the traditional geographic human-land relationship theory into a human-land-network relationship theory. CG research includes constructing mapping relationships between cyberspace and real space, redefining the traditional geographic concepts of distance and regions for cyberspace, creating a language, models and methodologies for visually representing cyberspace, drawing maps of cyberspace, and researching the principles governing the evolution of cyberspace structures and behaviors. The technical methods of CG include collecting and integrating data on elements of cyberspace, visually representing cyberspace and conducting cyberspace situational and behavioral intelligence awareness. Intelligence awareness covers cyberspace situational status assessments, network hotspot event dissemination and traceability analysis, and network event situational simulations and risk predictions. CG offers new perspectives on the scientific understanding of cyberspace, the development of disciplines such as geography and cybersecurity, and the creation of national cybersecurity prevention and control mechanisms as well as a community of common future in cyberspace.

Keywords: human-land-network relationship; cyberspace map; cyberspace; geographical space; visual representation

1 Introduction

With the development of technologies such as the Internet, the Internet of Things and mobile

Received: 2019-09-10 **Accepted:** 2019-10-12

Author: Gao Chundong (1976–), specialized in the management of science, technology and education.
E-mail: gaoecd@igsnr.ac.cn

***Corresponding author:** Jiang Dong (1972–), Professor, specialized in resource & environment information system.
E-mail: jiangd@igsnr.ac.cn

www.geogsci.com www.springerlink.com/content/1009-637x

communications, cyberspace has become a second space for human production and life. It stands in juxtaposition to the real spaces of land, sea, air and outer space as the fifth largest strategic space (Guo, 2016). As profound advancements have occurred in global information technology (IT), improving cybersecurity prevention and control capabilities has become a basic requirement for ensuring national security. Countries around the world are strengthening their cybersecurity, making it a part of their national security strategies and issuing relevant guidance documents. In 2018, the United States issued its *Department of Defense Cyber Strategy* and *National Cyber Strategy*, with the aim of achieving hegemony over cyberspace (Lange, 2018). China, Russia and European countries reacted proactively. The geographical structure of the world's cyberspace is centered around the US, China, Russia and Europe (Huang, 2019). The importance of cyberspace links in international geographical relations is constantly increasing, and differences and conflicts over cyberspace have become a new form of geopolitical conflict. The IMF's Fintech Policy Paper, *Fintech: The Experience So Far*, released on June 27, 2019 shows that cybersecurity has become a primary concern of most countries around the world (IMF and WB, 2019). Since the 18th National Congress of the Communist Party of China in 2012, the Party Central Committee has attached great importance to cybersecurity work and proposed a national cyber development strategy. China's President Xi Jinping has emphasized that, "There can be no national security without cybersecurity," and that, "Cyberspace is a common space for human activities, and countries should jointly build a cyberspace community of common destiny" (Lin and Liu, 2017). In May 2016, in order to accelerate training of high-level cybersecurity personnel, the Academic Degrees Committee of the State Council made cybersecurity a first-level discipline within the field of engineering.

Cyberspace has become a new field of geospatial and geographical expansion in the Information Age. Geographical space contains the physical resources and roles of cyberspace, and cyberspace provides a new domain for geospatial behavior. Cyberspace includes both physical elements, such as network infrastructure and hardware devices, as well as virtual elements, such as software systems and information flows (Boos, 2017). Both its physical and virtual parts cannot exist separately from geographical space (Batty, 1997). Geographical space is a foundation of the existence and development of human society. Geographers are constantly attempting to further their understanding of living space.

In 1987, Qian Xuesen proposed the field of geographical science, which he positioned as a scientific system between the natural sciences and social sciences and listed among the 11 major scientific systems, including the natural sciences, social sciences, mathematical sciences and systems sciences (Qian, 1994). As science and technology and economic and social development have progressed, geography has continuously absorbed and integrated the essence of more and more disciplines, and expanded into other fields. Following on from mechanization and electrification, the widespread application of IT has brought human society into a new era of informationization. Enormous information resources have created the conditions for theoretical development and knowledge innovation in geography, and the integration of modern IT and geography have led to the emergence of new subdisciplines, such as geographic information science, geographic information systems and remote sensing.

In the current cyber information age, air-ground and human-computer integration of cyberspace have developed (Zhang and Qin, 2010). An in-depth and scientific understanding

of cyberspace is an important cornerstone of cyber resource management as well as for ensuring and making decisions on cybersecurity. Under the two major driving forces of state requirements and discipline integration, research on measuring, understanding and representing cyberspace has emerged, leading to new concepts such as communication geography (Falkheimer and Jansson, 2006) and geography of information and communication (Martin, 2001; Adams, 2009). In order to accurately describe theoretical connotations, resource elements, map creation and the mapping relationship between cyberspace and real space, it has been necessary to make theoretical and methodological innovations on the basis of traditional geography and to strengthen the interplay between geography and cybersecurity, which has created the sub-discipline of cyberspace geography (CG). CG is a branch of geography that expands the content of geographical research from real space to virtual space. It focuses on the mapping relationship between cyber space and geographical space and reveals the operating mechanisms and guaranteed pathways of cybersecurity. As an important direction and academic frontier of geographical research, the creation of CG is not only a strategic requirement to bolster national cybersecurity, but also a requirement of the time to accelerate the development of the discipline of geography. Based on a comprehensive analysis of research results on domestic and international cyberspace, this paper discusses the geographical attributes of cyberspace and seeks to expound the implications and extrapolations of CG, analyze its multidisciplinary characteristics and theoretical basis, propose technical methods, and analyze and forecast the development prospects of CG.

2 Domestic and international cyberspace research

2.1 Literature analysis

Searches for the keywords “cyberspace” and “cybersecurity” on the Web of Science Core Collection database and China National Knowledge Infrastructure (CNKI) database for the period from the 1970s to August 2019 returned 2290 cyberspace-related items by overseas authors and 1613 items by Chinese authors. Analysis of these items showed that overseas cyberspace research began in 1977, 21 years before China (1998), and relevant literature increased rapidly overseas beginning in 1994, 15 years before China (2009).

Looking at distribution by country, the country network map has 39 nodes and 43 connections. The United States has the most (839), followed by China (176), the United Kingdom (166), Canada (79), Australia (72), South Korea (62) and Germany (41). However, Australia has the highest centrality, indicating that Australia’s cyberspace research has the greatest international influence (Figure 1a). Looking at issuing organizations, there are 137 nodes and 54 connections across the world, with network density of 0.0058, indicating that there is a loose relationship between research institutions, there is little cooperation in research and academic exchanges could be strengthened. Looking at numbers of documents issued by organizations, the Massachusetts Institute of Technology, University of Toronto, Chinese Academy of Sciences, University of Wisconsin, Deakin University and Tsinghua University all have high volumes of publications, but there is no authoritative research institution with absolute advantage. In terms of research content, a keyword map of international research has 238 nodes and 447 connections, with a network density of 0.0158 and a strong correlation between keywords. “Internet,” “cyberspace,” and “cybersecurity” are the most fre-

quently cited keywords (Figure 1b).

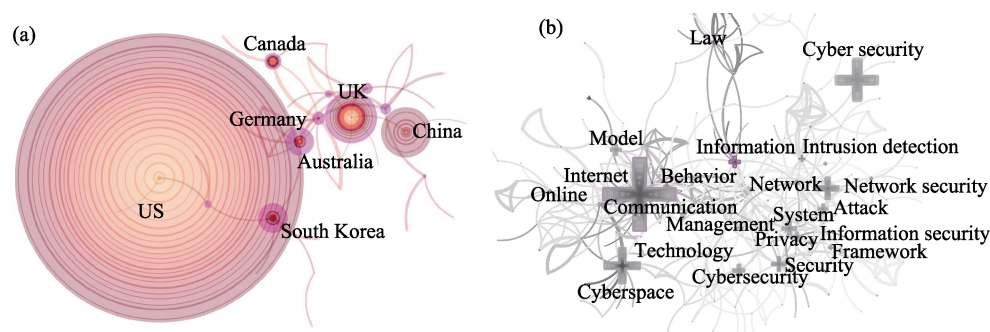


Figure 1 Country network map (a) and keyword map (b) of international cyberspace (1977 to August 2019)

Cyberspace research in China is still in its infancy. At present, its network map has a total of 131 nodes and 36 connections, with network density of 0.0042, indicating that cooperation between institutions is still limited. Looking at its keyword map, there are 289 nodes and 358 connections, with a network density of 0.0086, indicating a lower correlation than at the international level. “Cybersecurity,” “cyberspace,” “wireless sensor network,” “data security,” “*sai-bo* [Chinese transliteration of ‘cyber’] security,” “cybersecurity,” cyberspace governance” and “national security” are the most commonly cited keywords. “Data security” and “national security” have the highest centrality (Figure 2).

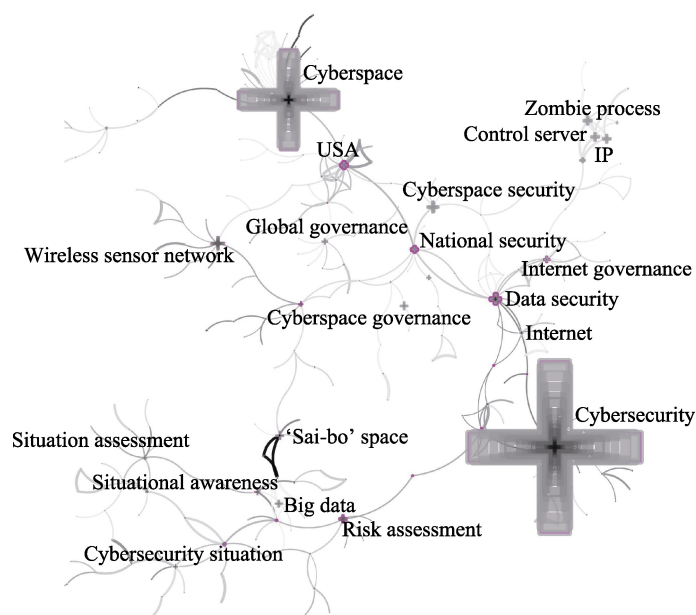


Figure 2 Keyword map of cyberspace and cybersecurity research in China (1998 to August 2019)

2.2 Thematic analysis of cyberspace research

2.2.1 Meaning and characteristics of cyberspace

Cyberspace refers to a network that connects various IT infrastructure, such as the Internet,

telecommunications networks, sensor networks, internal industrial and military networks, industrial systems with embedded controls, the Internet of Things made up of processing devices, various computers systems, and interactions between virtual space and people constructed by information and data (Zhang, 2018). Cyberspace can be divided into five levels: the geographical layer (including basic geospatial support elements), the physical network layer (including IT equipment and infrastructure), the logical network layer (including data, applications and network processes), the cyber-persona layer (made up of network or IT user accounts) and the persona layer (real space entities) (Boos, 2017). Cyberspace is a real digital space, a new public social realm and a virtual space completely different from traditional geographical space (Qi, 2004; Sun *et al.*, 2007). The United States, Italy, Russia and China all define cyberspace differently (WH, 2008; PCM, 2013; Fang *et al.*, 2016; RFC, 2016). In general, however, cyberspace is agreed to consist of the following: a spatial domain in which humans use computer technology to complete activities, an enormous database with strategic importance and IT infrastructure providing important support (Huang, 2003; Fang *et al.*, 2016).

2.2.2 Global governance of cyberspace

The global nature of cyberspace has made it a new arena of interactivity between countries, which has inevitably shifted the focus toward its governance (Shen, 2014). This focus has been divided between cyberspace governance for data security and governance of public affairs. As cyberspace develops, its global governance is changing from a self-governance model to “cyber-balkanization” (Cai, 2013; Hou and Wang, 2017) with the formation of different interest groups (Hou and Wang, 2017). The formulation and improvement of international laws on cyberspace and decisions on cyberspace sovereignty have contributed to the creation of a system of international co-governance (Fang *et al.*, 2016). For a long time, China has actively participated in the global governance of cyberspace. In 2015, President Xi Jinping proposed at the Second World Internet Conference that, “Nations should jointly build a cyberspace community of common destiny” (Lin and Liu, 2017). At the end of 2016, the Cyberspace Administration of China released the *National Cybersecurity Strategy*, marking the elevation of cyberspace governance to the level of a national strategy.

2.2.3 Cybersecurity and protection

Cybersecurity refers to methods and actions for managing security risks that are adopted by countries and agencies to protect confidentiality, integrity and the availability of data and assets in cyberspace (Schatz *et al.*, 2017). It touches upon political, social, economic and cultural security elements (Song, 2016). Network vulnerabilities and attacks are the main focus of cybersecurity prevention and control measures (Abomhara and Køien, 2015). Assessing and measuring the security of cyberspace is a prerequisite for ensuring online security (Zhang and Zhao, 2018), and situational awareness, indicator systems and evaluation models are the main focuses of research on assessing cybersecurity (Huang and Wang, 2004; Wang *et al.*, 2006; Zhang and Tang, 2014). The basic processes of cybersecurity defense include conducting situational analysis, establishing security objectives, selecting security policies, developing security plans, conducting timely risk assessments and implementing real-time monitoring (Zhao, 2015; Wang, 2019). Cybersecurity defense needs to be forward-looking, immediately aware of risks and vulnerabilities, able to affect repairs and able

to ensure the data security of computer users (Yang, 2019).

2.3 Issues and trends in cyberspace research

Surveying Chinese and international research on cyberspace reveals that there is still no consensus in terms of its conceptual connotations and theoretical basis. Moreover, although cyberspace is the data environment of human lives in the Information Age, current literature shows that core elements, such as software systems and information flows, lack unified standards and basic theories, and the mapping relationship between cyberspace and traditional geographical space remains undefined (Boos, 2017). Indeed, the mapping relationship between space, time, scale and dimensions is unclear, and the theory, models, methods and tools for revealing the mapping relationship are imperfect. As such, it is necessary to construct different spatial mapping relationships and models to measure precisely the movement of data in cyberspace and its life cycle.

3 Theoretical basis of cyberspace geography

3.1 Basic content of cyberspace geography

Space is a form of material existence. It is a manifestation of the extensiveness and extensibility of material existence (Chen, 2009). The process of human development is one in which human beings continue to deepen their understanding of themselves and their living space, and geographical space is the foundation for the existence and development of human society. Geography is a discipline that studies the spatial distribution, temporal evolution and regional characteristics of humans (human activities) and the Earth (natural environment), exploring the structures, evolutionary processes and regional differences in physical geography and human uses of and adaptations to the geographical environment. The essence of geographical methodology is understanding regional differences and interval dependence (Lu, 2011). Traditional geography's methods of understanding the geographical environment include descriptions of geographic attributes and spatial distribution as well as feature analysis and mechanism induction.

In the 1980s, the integration of geography and IT produced the sub-discipline of geo-information science, which looks at physical phenomena on Earth and uses IT to acquire, analyze, manage and visualize geospatial data. Spatial differentiation (patterns) and time series differentiation (evolutions) of the human-land relationship are its core content (Ma *et al.*, 2002). "Digital Earth" is an effective geospatial visualization tool for displaying and understanding geo-information science. It is guided by system theory and integrates observation technology, geospatial IT and computer network communication technology to simulate changes in Earth's development and predict scenarios under different models to support government decision-making (Zhou and Lu, 1998; Gao, 2017). Following developments in big data and Digital Earth, the new generation of Digital Earth uses enormous volumes of multi-resolution, multi-temporal, multi-type and multi-source Earth observation data and socioeconomic data as well as analysis algorithms and models to construct a virtual Earth. Through the efficient organization and unified management and expression of enormous volumes of spatial data and socioeconomic data on the digital earth platform, scientific data

extraction and analysis can be carried out in a refined data space (Michael *et al.*, 2012). The emergence of cyberspace and its related concepts is the result of a combination of the rapid development of the Internet and IT around the world and the continuous innovation of traditional geography in the Information Age. It involves geography, IT, big data, AI and many other subject areas. Corresponding to geographical space, cyberspace is a new spatial domain constructed from computer networks and based on geographical space.

Areas of research in CG include constructing the mapping relationship between cyberspace and real space, redefining the basic concepts of distance and regions in traditional geography, constructing language, models and methods to visually represent cyberspace, drawing cyberspace maps, and exploring the principles governing the evolution of cyberspace structures and behaviors. Cyberspace is not a Euclidean space. There is no metric meaning of distance and orientation as in traditional geographical space (Sun and Wang, 2013). As a result, existing cyberspace visualization mainly uses topological structure to express information content, focusing on online/offline accessibility and other topological information, simplifying the distance between node connections and the orientational relationship of node switching (Ai, 2008). There is also still no unified theoretical framework, complete technical system or typical examples of cyberspace-geographical space associations, cyberspace feature analysis and behavioral cognition (Table 1). To this end, there is an urgent need to promote research in CG by deeply integrating geography and cybersecurity.

Table 1 Comparative analysis of attributes of geography and cyberspace geography

Subject		Geographical space & geography	Cyberspace & cyberspace geography
Spatial representation		Real space	Virtual space
Research target		Human-land relationship	Human-land-network relationship
Scale expression		Multiple spatial scales	Any spatial scale
Attribute	Infrastructure	Airports, ports, bridges	Routers, servers
	Resource	Physical resources Limited resources	Physical and virtual resources Unlimited resources
	Behavior	Physical: material flows, energy flows	Virtual: data flows, network flows
	Relationship	Adjacent, intersecting, inclusive spatial relationships	Network topology
	Natural	Affected by natural conditions	Unrestrained by natural conditions
	Social	Physical society	Network society
	Economic	Real economy industry	Internet industry
	Urban	Visible cities	Invisible cities, shared cities

3.2 Theoretical basis: From the human-land relationship to the human-land-network relationship

3.2.1 Human-land relationship theory

The human-land system is made up of the natural, economic and social subsystems. It is an enormous complex and open system of intertwined and interacting humans and their activities as well as geographical environments (Wu, 1998). Managing the contradictions between humans and land in this system is an enduring theme of geographical research (Mao, 1995). Traditional human-land relationship theory focuses on the interactions between, and coordinated development of, populations, resources, environments, societies, economies and other

factors, with the emphasis on harmonious coexistence between humans and land (Lu, 2011). As early as 1979, academician Wu Chuanjun proposed in a report titled *Dilixue de zuotian, jintian he mingtian* (*Geography's Yesterday, Today and Tomorrow*) that the human-land relationship sits at the core of geographical research, and coordinating the relationship is its central goal (Lu and Guo, 1998). The essence of the theory on the harmonious symbiosis of humans and land is that a relationship between humans and land has existed objectively since the origin of humankind and that it is symbiotic and reciprocal, and when humans develop and utilize natural resources and the environment, they must remain in harmony with the natural environment and maintain balance in three symbiotic relationships: land-land, human-land and human-human relationships (Fang, 2004).

3.2.2 Research on the human-land-network relationship

The rapid development of informatization has accelerated flows of various factors of production on a global scale. The role of geographical space in human constraints is diminishing, while the status and role of cyberspace is increasingly prominent. Interactivity between, and the integration of, cyberspace and geographical space has had a systematic impact on the human-land relationship and gradually formed a new “human-land-network” relationship. There are clear distinctions and inextricable links between cyberspace and geographical space. Geographical space is the basic space that humans rely on for their survival, as well as the basic space for geographical research. It is the form of existence of geospatial physical elements, spatial information, material energy and behavioral expressions in the objective world. Physicality, distance and boundaries are the main attributes that reflect the finiteness of geographical space (Batty, 1997; Li *et al.*, 2016). Cyberspace, on the other hand, is a virtual space built by networks, computer systems and data that connect various IT infrastructure. The National Natural Science Foundation of China invested in mapping ideas from cyberspace to real-space between 2010 and 2014, with the focus on simulating communication between cyberspace and real-space (Tsou, 2012). Cyberspace is not a simple abstract virtual space, but involves a large number of human activities and interrelationships in geographical space (Wang and Zheng, 2016). For example, cyberspace plays a role in determining and reconstructing the layout of urban functions, including decentralized development that promotes urban function structures, with fragmentation and agglomeration as the main spatial dynamic forms (Malecki, 2002). Therefore, both virtual space and real space belong to the broad category of “space” and are inseparable, but over-emphasis of one side can easily lead to cognitive bias, affecting the grasp of the overall characteristics and laws of the two types of space (Figure 3).

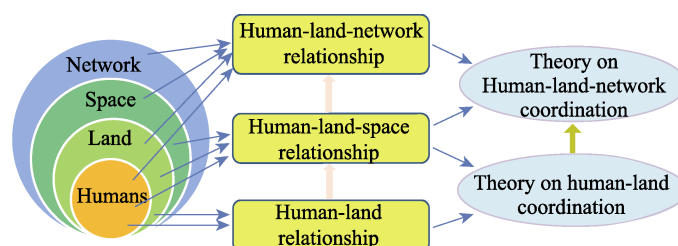


Figure 3 Evolutionary framework from the human-land relationship to the human-land-network relationship

The core proposition of CG is to study the human-land-network relationship. This is a new development on the human-land relationship in traditional geography for the Information Age. There are three main relationships in CG. The first is the human-land-network interaction mechanism. Of these elements, “human” refers to human activities, such as production and socioeconomic development, in geographical space as well as human activities in cyberspace. The second is the mapping relationship between cyberspace and real space. Cyberspace and real space are intertwined and closely related, and they have spatial differentiation characteristics. There are spatial differences in network infrastructure, differences in regional characteristics of behavioral agents and differences in regional characteristics of network data. Therefore, using location information as the link, introducing geography theories, methods and cognitive means is an effective way to connect two spaces and cognitive network worlds. The third main relationship is the logical structure and system of elements of cyberspace. For example, the elements, types, levels, spatio-temporal benchmarks, standards of expression and scale issues of cyberspace should be measurable and calculable to support data mining and spatio-temporal analysis. With the development of satellite Internet and possibly the development of interplanetary Internet, the scope of CG research may also expand into the field of aerospace.

4 Technical methods of cyberspace geography

The technical methods of CG are a set of research methodologies (Figure 4) that include the collection and integration of data on cyberspace, visual representations of cyberspace and cyberspace situational and behavioral intelligence awareness.

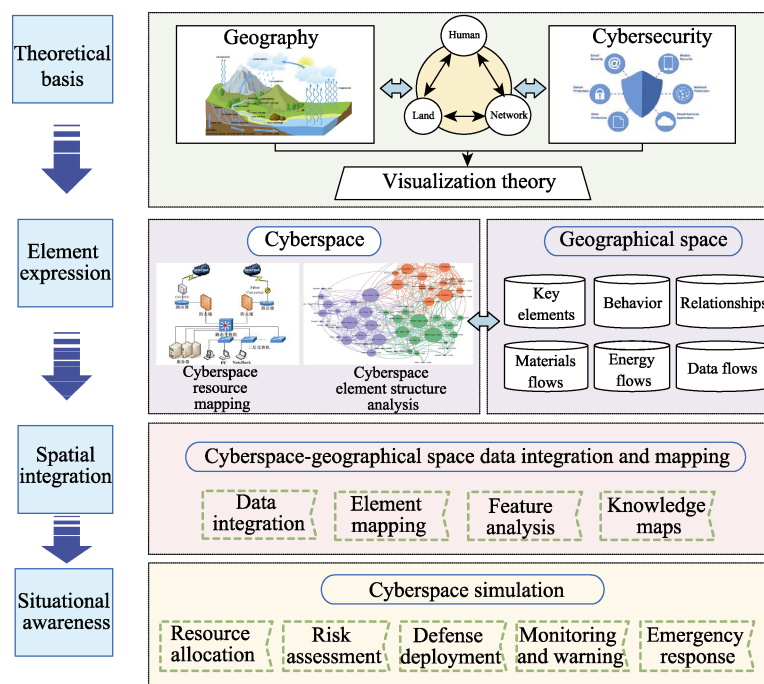


Figure 4 Technical methods of cyberspace geography

4.1 Collection and integration of data on elements of cyberspace

Collecting data on cyberspace elements is the basis for correctly understanding cyberspace so as to effectively control and manage it. With continuous improvements and increasing accuracy of network positioning methods, the mapping of cyberspace resources has become the main method of collecting data on cyberspace elements. It brings together network resource detection, network topology analysis, entity positioning and other means, to detect and analyze cyberspace elements from multiple dimensions in real time, so as to obtain the attributes of virtual resources and physical resources in cyberspace and geographical space. These include entities in the physical domain, communication and network protocols in the logical domain, and information and behavior in the social domain (Wang *et al.*, 2019). The spatial scale includes four levels: IP, router, POP and AS. Data includes time-space distribution changes such as resource types, states, attributes and changes in relationships between elements.

Cyberspace resource mapping technology is already relatively mature. In 2016, China's Ministry of Science and Technology announced its national key research and development plan project titled "Cyberspace Resource Mapping Technology," and the First Research Institute of the Ministry of Public Security designed and developed the "Network Asset Mapping Analysis System—Web Exploration D01" project, which are powerful efforts aimed at discovering network assets, quickly responding to sudden security incidents, mastering the security situation of unknown hidden assets and establishing a comprehensive and efficient network asset security inspection system.

Integration of cyberspace data is based on data collection results. It combs, combines and stores multi-elemental and multi-source heterogeneous data on cyberspace and geographical space. The key techniques involved are, first, the network data and geographical location high-precision automatic matching technique. Large volumes of multi-source heterogeneous data on network resources, network events and geographical space are integrated to achieve high-precision automatic matching of network data and location based on reference landmarks, time delay measurements and topological analysis results (Jiang, 2012). The second key technique is spatio-temporal feature analysis and knowledge map construction of network data. Based on cyberspace, geographical space and social human spatiotemporal big data, the mining and analysis (classification, clustering, correlation, time series analysis, etc.) of spatiotemporal features is carried out, and cyberspace knowledge maps are constructed to comprehensively analyze and express cyberspace forms, patterns and evolutions (Figure 5).

4.2 Cyberspace visualization

Recent Chinese and overseas research on cyberspace visualization has focused on the physical network layer and the logical network layer, with the emphasis on the description and positioning of network devices as well as statistical analysis of network operation data. Nevertheless, there is still a big gap between visualization results and application requirements. In fact, cyberspace visualization should span the entire five layers of cyberspace, covering all network elements (Figure 6).

Geovisualization research has been developing for a long time. It primarily entails creating systems of symbols for geographic information, cartographic synthesis, layer

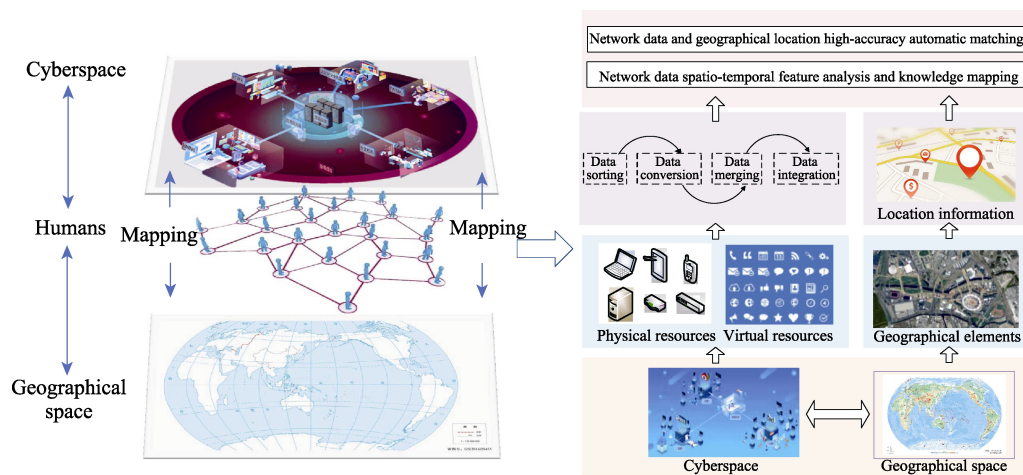


Figure 5 Collection, mapping and fusion of data on cyberspace elements

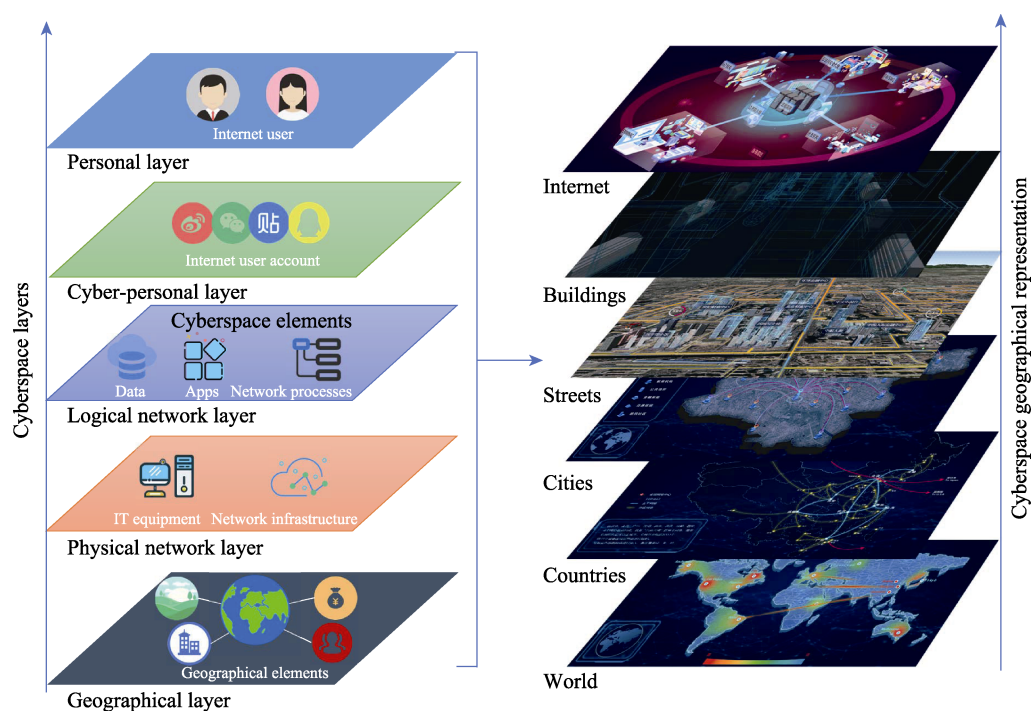


Figure 6 Multi-layer visual representation of cyberspace

rendering and human-computer interactions. It includes two- and three-dimensional visualization as well as virtual geographic environments to represent dimension and scope. Cyberspace visualization first requires the construction of a mature system of technology based on the technology used in geovisualization. The following key breakthroughs are as: The first is visualization of network elements. Cyberspace needs a “network map” that can fully describe and display the attributes and information of cyberspace, supported by IP address-based network entity geolocation technology, so as to display the number and spatial distribution of various cyberspace elements (Li, 2012). Second is a visual representation of

network relationships. This includes both the relationships between network elements and the relationships between virtual space and geographical space. The third key breakthrough area is visual analysis of network events. Virtual and dynamic network events should be successively presented and undergo multi-elemental analysis on a cyberspace map according to the acting entity, object and influence (Zhang, 2013).

4.3 Cyberspace situational and behavioral intelligence awareness

Cyberspace situational and behavioral intelligence awareness mainly includes assessments of cyberspace situations, dissemination and traceability analysis of network hotspot events and situational simulation and risk prediction of network events.

4.3.1 Cyberspace situation assessment

Assessment of cyberspace situations generally takes place within the context of a large-scale network environment. For certain kinds of cyberspace events, event data is deeply mined and analyzed, allowing an overall assessment of the status of cyberspace. Cyberspace situation assessments are the basis of cyberspace intelligence awareness, and they are a prerequisite for managers to have a macroscopic understanding of, and make decisions concerning, cyberspace. Currently, cybersecurity situation assessment methods are mainly based on mathematical models, knowledge inference and pattern recognition. These methods have relatively mature applications, but their visual representations are poor, as they are unable to reflect directly the agglomeration and regional differentiation of cyberspace situations. The status of an object in cyberspace and the spatial analysis of a phenomenon in geography are highly similar. Taking crimes in cyberspace as an example, the occurrence of such events has significant regional differences. In cyberspace, some attributes of cybercrimes are highly correlated; in geographical space, one sees spatial agglomeration and dispersion of a phenomenon. As a result, cyberspace situation assessments can be carried out using ideas from geospatial analysis. For example, kernel density analysis is a hotspot analysis method commonly used in geography. It can vividly and visually represent the distribution of hotspots of a certain geographical phenomenon, and it can also show the hotspot distribution of cyberspace events based on certain attributes. The difference is that in cyberspace, hotspot analysis explores hotspot distribution in terms of “network distance.”

4.3.2 Dissemination and traceability analysis of network hotspot events

The dissemination and traceability of network hotspot events is an important area of research in cybersecurity. The core scientific issues include dissemination models and predictions, dissemination traceability, dissemination structural analysis and key node identification, and dissemination visualization. At present, Chinese and overseas researchers mainly use time series analysis, dynamic models and stochastic processes for event modeling; stochastic graph models, network stability theory and complex network theory to analyze event dissemination structures and key nodes; and time-series and GIS-based methods to display visualizations of dissemination processes of hotspot events. Overseas companies such as Twitter and Facebook combine event geographic information with event location information to carry out visualization analysis of large-scale natural disasters and political events. Domestically, Weibo, Baidu and others provide visual analysis components and technologies based on GIS and time series.

With the development of communication technologies such as 5G, social media is developing rapidly. On large-scale networks, genuine hotspot events are being disseminated quickly, their dissemination modes are complex, tracing and positioning key nodes are difficult and multiple networks have overlapping development. It is, therefore, necessary to focus on and research the semi-supervised classification of hotspot event dissemination modes, in order to classify different events; to research personalized modeling and early predictions of hotspot events based on graph deep learning, in order to achieve early detection and discovery of hotspot events; to research the dissemination structure of hotspot events and measure critical transmission paths and nodes, in order to intervene in and control events; and to research the modeling of cross-network hotspot events based on coupled social network analysis, so as to conduct multi-social network hotspot event analysis.

4.3.3 Situational simulation and risk prediction of network events

Situational simulations and risk predictions of network events surmise and estimate future development trends of network situations by analyzing and evaluating the current network status and historical information. This is an effective means of providing cybersecurity early warnings and forecasts and achieving active defense capabilities. Due to the complexity of the network environment and the uncertainty of network attacks, traditional research methods have struggled to meet application requirements for situational simulations of network events. The successful application of AI technology in interdisciplinary fields will receive increasing attention in situational simulations of network events.

Machine learning algorithms and AI techniques have been successfully applied in all aspects of geographical research, including remote sensing image processing, geological hazard forecasting, environmental epidemiology and land use change. Due to the complexity of both cyberspace and geographical space, network events and geographic events are the result of interactions between multiple elements in different spaces. Moreover, simulating geographic and network events can be understood in terms of the hierarchical process “data-information-knowledge-wisdom.” It is, therefore, feasible to apply research ideas from machine learning algorithms and AI techniques in geography to situational simulations and risk predictions of network events. In cyberspace, network events are driven by real-world elements and affected by various cyberspace elements. First, multi-source data fusion technology can be used to integrate the driving elements in different dimensions into a unified space-time reference. Then, machine learning methods, including genetic algorithms and neural networks, can be used to adjust self-learning abilities and construct situation prediction models, so as to simulate network behavior and provide early warnings of network risks (Figure 7).

5 Conclusion and prospects

The virtual nature, diversity of agents and openness of cyberspace have brought new challenges to traditional human methods of understanding. Cyberspace geography is a new discipline that has arisen from the integration of geography and cybersecurity. Cyberspace visualization and cognitive technology, which are based on cyberspace geography, combine the concepts of geographic units, distance, topological relationships and cyberspace from traditional geography with the unique concepts of nodes, links, data flows and cyberspace

patterns from cyberspace, to create powerful tools for understanding and mastering cyberspace.

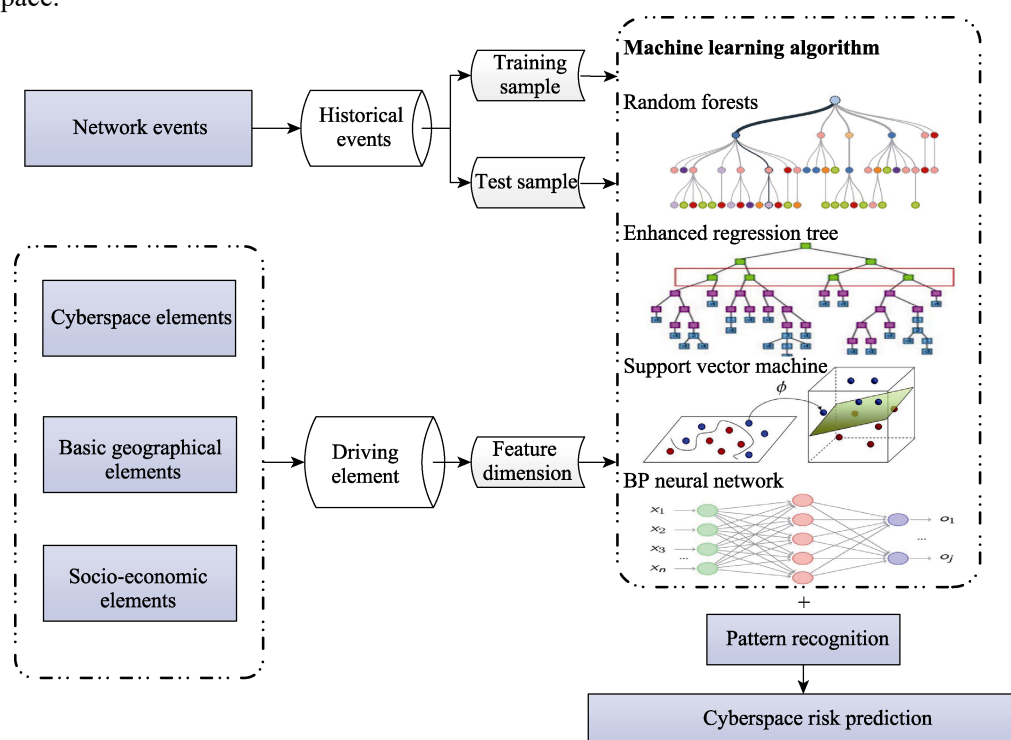


Figure 7 Cybersecurity event simulation and prediction

The results of Chinese and overseas research in recent years show that the integration of geography and cybersecurity has provided a new perspective on cyberspace research. In addition, the emergence and development of the unique spatial form that is cyberspace has had a strong impact on basic concepts in traditional geography, presenting both a challenge and an opportunity for the discipline. Since its birth, geography has remained open, compatible and comprehensive. It has always been self-critical and self-adjusting, and it has always been full of vitality. Cyberspace geography enriches geography, expands the bounds of geographical research and extends the vision of geographers from real space to virtual space. The deepening exploration and application of theoretical methods of cyberspace geography will undoubtedly promote the development of the discipline of geography.

The applications of cyberspace geography are broad and include efficient management and rational allocation of cyberspace assets, cyberspace situational awareness, critical infrastructure protection, network event analysis and early warning based on cybercrime maps and geographic portraits, and construction of comprehensive cybersecurity protection systems. Cybersecurity incidents are complex social events driven by various social subsystems. Because cybersecurity threats come from geographical, human and social environments and the Internet itself, cybersecurity situational analysis should first screen factors affecting cybersecurity to fully understand geographic, human, social and network environment elements, establish a cybersecurity indicator system, and then use network big data mining technology and deep learning technology to evaluate and predict cybersecurity situations

and simulate and forewarn of cybersecurity events.

In the course of developing cyberspace geography, we must fully integrate new technologies and concepts, such as satellite Internet, 5G, IPV6, blockchain, Internet of Things, Internet of Vehicles and smart homes, as well as the latest concepts and results from geography, cybersecurity and other disciplines, and focus on future applications and requirements, so as to provide scientific support to cyberspace knowledge and cybersecurity prevention and control measures.

Acknowledgements

During the writing process, we held four cyberspace geography seminars, and we would like to thank Wang Yingei, Xu Yunfeng, Zhu Guobang, Fan Chunling, Lu Lei, Hu Guangjun, Sun Degang, Wu Yu, Xu Fanjiang, Wang Zhiwei, Jing Tao, Cheng Jian, He Shujin, Li Jiaxin and Gao Qing for their comments and suggestions.

References

- Abomhara M, Køien G M, 2015. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security*, 4(1): 65–88.
- Adams P, 2009. Geographies of Media and Communication. Oxford: Wiley-Blackwell.
- Ai T H, 2008. Maps adaptable to represent spatial cognition. *Journal of Remote Sensing*, 12(2): 347–354. (in Chinese)
- Batty M, 1997. Virtual geography. *Futures*, 29(4/5): 337–352.
- Boos T, 2017. Geographies of cyberspace: Internet, community, space, and place//Inhabiting Cyberspace and Emerging Cyberplaces. The Case of Siena, Italy. USA: Palgrave Macmillan, 13–38.
- Cai C H, 2013. The cyberspace governance amid the interaction of states, markets and society. *World Economics and Politics*, (9): 90–112, 158–159. (in Chinese)
- Chen Z L, Ci H, 2009. Shanghai: Shanghai Lexicographical Publishing House, (in Chinese)
- Falkheimer J, Jansson A, 2006. Geographies of Communication: The Spatial Turn in Media Studies. Goteborg, Sweden: Nordicom.
- Fang B X, Zou P, Zhu S B, 2016. Research on cyberspace sovereignty. *Strategic Study of CAE*, 18(6): 1–7. (in Chinese)
- Fang C L, 2004. Recent progress of studies on man-land relationship and its prospects in China. *Acta Geographica Sinica*, 59(Suppl.1): 21–31. (in Chinese)
- Gao J, 2017. The 60th anniversary and prospect of *Acta Geodaetica et Cartographica Sinica*. *Acta Geodaetica et Cartographica Sinica*, 46(10): 1219–1225. (in Chinese)
- Guo H S, 2016. Cyberspace Security Strategy. Beijing: Aviation Industry Press. (in Chinese)
- Hou Y H, Wang F X, 2017. Global governance of cyberspace and its “China Program”. *News and Writing*, (1): 5–9. (in Chinese)
- Huang A W, 2019. Overview of the dynamic development of global cyberspace security in 2018. *Civil-Military Integration on Cyberspace*, 20(1): 72–76. (in Chinese)
- Huang L M, Wang H, 2004. Multilevel fuzzy comprehensive evaluation method of network security. *Journal of Liaoning Technical University*, 23(4): 510–513. (in Chinese)
- Huang S H, 2003. On the social characters of the internet space. *Journal of Lanzhou University*, 31(3): 62–69. (in Chinese)
- International Monetary Fund (IMF), World Bank (WB), 2019. Fintech: The experience so far. IMF Policy Papers. <http://www.imf.org/external/pp/ppindex.aspx>.
- Jiang Y L, 2012. Research on rules and methods of information mapping of entity’s physical space and cyberspace [D]. Dalian: Dalian Polytechnic University. (in Chinese)
- Lange K, 2018. DOD’s cyber strategy. <https://www.defense.gov/explore/story/Article/1648425/>.
- Li F H, Wang Y C, Yin L H *et al.*, 2016. Novel cyberspace-oriented access control model. *Journal on Communications*, 37(5): 9–20. (in Chinese)
- Li W, 2012. Research and implementation of the IP geolocation technology [D]. Beijing: Beijing Jiaotong University. (in Chinese)
- Lin B H, Liu B, 2017. Xi Jinping’s Thought of “Destiny Community of Cyberspace” and its contemporary value.

- Leading Journal of Ideological & Theoretical Education*, (8): 37–41. (in Chinese)
- Lu D D, 2011. Development of geographical sciences and research on global change in China. *Acta Geographica Sinica*, 66(2): 147–156. (in Chinese)
- Lu D D, Guo L X, 1998. Man-earth areal system: The core of geographical study – On the geographical thoughts and academic contributions of Academician Wu Chuanjun. *Acta Geographica Sinica*, 53(2): 97–105. (in Chinese)
- Ma A N, Wu L, Chen X W *et al.*, 2002. Development on geographical information science. *Geography and Territorial Research*, 18(1): 1–5. (in Chinese)
- Malecki E J, 2002. The economic geography of the internet's infrastructure. *Economic Geography*, 78(4): 399–424.
- Mao H Y, 1995. Study on Human-earth System and Regional Sustainable Development. Beijing: China Science and Technology Press, 48–60. (in Chinese)
- Martin D, 2001. Atlas of Cyberspace. Essex: Pearson Education Ltd.
- Michael F, Goodchild M F, Guo Huadong *et al.*, 2012. Next-generation digital earth. *PNAS*, 109(28): 11088–11094.
- Presidency of the Council of Ministers (PCM), 2013. National strategic framework for cyberspace security [EB/OL]. (2013-12-01) https://www.enisa.europa.eu/topics/national-cybersecurity-strategies/ncssmap/IT_NCSS.pdf.
- Qi A M, 2004. The attribute of cyberspace as well as its influence on the laws related. *Journal of Guizhou University (Social Sciences)*, 22(2): 16–22. (in Chinese)
- Qian X S, 1994. On Geography Science. Hangzhou: Zhejiang Education Publishing House. (in Chinese)
- Russian Federation Council (RFC), 2014. Концепция стратегии кибербезопасности российской федерации [EB/OL]. (2014-01-10). <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf>.
- Schatz D, Bashroush R, Wall J, 2017. Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, 12(2): 53–74.
- Shen Y, 2014. Global cyberspace governance and BRICS cooperation. *International Review*, (4): 145–157. (in Chinese)
- Song W L, 2016. Multilayer governance model of EU cyberspace and its enlightenment. *Study Monthly*, (16): 17–19. (in Chinese)
- Sun Z W, Lu Z, Wang Y, 2007. The geography of cyberspace: Review and prospect. *Advances in Earth Science*, 22(10): 1005–1011. (in Chinese)
- Sun Z W, Wang Y, 2013. Information and communication geography: Discipline nature, development process, and research topics. *Progress in Geography*, 32(8): 1266–1275. (in Chinese)
- The White House (WH), 2008. National security presidential directive/NSPD54/homeland security presidential directive/HSPD-23 [EB/OL]. (2008-01-08). <http://fas.org/irp/offdocs/nspd/nspd54.pdf>.
- Tsou M H, 2012. Mapping ideas from cyberspace to real space. <http://mappingideas.sdsu.edu/>, 2012-11-4
- Wang H Q, Lai J B, Zhu L *et al.*, 2006. Survey of network situation awareness system. *Computer Science*, (10): 5–10. (in Chinese)
- Wang J W, Zheng H Y, 2016. Study on the countermeasures of urban planning based on the concept, attribute and function of cyberspace: With a review of related research abroad. *Urban Development Studies*, 23(9): 40–45. (in Chinese)
- Wang Y, Li X, Ren G M *et al.*, 2019. Review on the current research of global cyberspace maps. *Information Technology and Network Security*, 38(5): 1–6.
- Wang Z L, 2019. Application analysis of intrusion detection technology in network security. *Digital Technology & Application*, 37(1): 209–210. (in Chinese)
- Wu C J, 1998. Man-Earth Relationship and Economic Allocation. Beijing: Academy Press, 28–33. (in Chinese)
- Yang K, 2019. Towards automatic fingerprinting of IoT devices in the cyberspace. *Computer Networks*, 148: 318–327.
- Zhang G, 2013. Studies on cyberspace [D]. Wuhan: Huazhong University of Science and Technology. (in Chinese)
- Zhang H G, Qin Z P, 2010. Introduction to Evolution Cryptology. Wuhan: Wuhan University Press. (in Chinese)
- Zhang L, 2018. Cyberspace map tightly coupled with geographical space. *Journal of Cyber Security*, 3(4): 63–72. (in Chinese)
- Zhang Y M, Zhao X L, 2018. Analysis and research of network security measurement and evaluation. *On-line Excellent Papers of Chinese Scientific and Technological Papers*, 11(4): 328–338. (in Chinese)
- Zhang Y J, Tang J, 2014. Analysis and assessment of network security situation based on cloud model. *Computer Engineering & Science*, 36(1): 63–67. (in Chinese)
- Zhao Z W, 2015. Overview of security defense of the wide area network. *Science Mosaic*, (3): 117–120. (in Chinese)
- Zhou C H, Lu X, 1998. Preliminary discussion on geo-information science. *Acta Geographica Sinica*, 53(4): 372–380. (in Chinese)