Bulletin of Chinese Academy of Sciences

Volume 35 | Issue 7 Article 13

July 2020

Develop Visualization Technology of Cyberspace to Support Construction of Comprehensive Prevention and Control System of Cyber Security

GUO Qiquan

Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences, Beijing 100101, China; Cyber Security Department, The Ministry of Public Security of the People's Republic of China, Beijing 100741, China

See next page for additional authors

Develop Visualization Technology of Cyberspace to Support Construction of Comprehensive Prevention and Control System of Cyber Security

Abstract

Cyber security is the basis of national security in the information age, and the visualization of cyberspace is of vital importance for comprehensive prevention and control of cyber security. Based on the theory of "man-land-network" nexus, this study proposed the connotation and technical path of cyberspace visualization and described the visualization of the cyberspace elements, cyberspace relations, and cyberspace security events. Based on the cyberspace geography, the exploration and application of cyberspace visualization technology is an important content of constructing the mapping relations between cyberspace and real world as well as drawing a cyberspace map, which will provide a significant support for the realization of the cyberspace map in the comprehensive prevention and control of cyber security.

Keywords

man-land-network relationship; cyberspace map; cyberspace; geographical space; visualization

Authors

GUO Qiquan, GAO Chundong, HAO Mengmeng, and JIANG Dong

Corresponding Author(s)

HAO Mengmeng [1*]

1 Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences, Beijing 100101, China

HAO Mengmeng Assistant Researcher of Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences.Her research focuses on cyberspace geography, geographic information system, etc.E-mail:haomm@igsnrr.ac.cn

Citation: GUO Qiquan, GAO Chundong, HAO Mengmeng, JIANG Dong. Develop Visualization Technology of Cyberspace to Support Construction of Comprehensive Cyber Security System [J]. Bulletin of Chinese Academy of Sciences, 2020 (7): 917–924.

Develop Visualization Technology of Cyberspace to Support Construction of Comprehensive Cyber Security System

GUO Qiquan[1,2], GAO Chundong[1], HAO Mengmeng[1], JIANG Dong[1]

1. Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences, Beijing 100101, China;
2. Cyber Security Department, The Ministry of Public Security of the People's Republic of China, Beijing 100741, China

Abstract: Cyber security is the basis of national security in the information age, and the visualization of cyberspace is of vital importance for cyber security. Based on the theory of human–land–network nexus, this study proposed the connotation and technical path of cyberspace visualization and described the visualization of cyberspace elements, relationship in cyberspace, and cyber security events. Based on the cyberspace geography, the exploration and application of cyberspace visualization technology is an important content of constructing the mapping relationship between cyberspace and real world as well as drawing a cyberspace map, which will provide significant support for cyberspace mapping in the ensurement of cyber security. **DOI:** 10.16418/j.issn.1000-3045. 20200302004-en

Keywords: man–land–network relationship; cyberspace map; cyberspace; geographic space; visualization

With the rapid development of global informatization, humankind has been increasingly dependent on cyberspace, a new field that countries from all over the world compete for. Therefore, cyber security has become a basis of national security [1,2]. General Secretary Xi Jinping has pointed out that there is no national security without cyber security. For the traditional geographic space, map, as an important carrier depicting geographical phenomena, has been taken as an indispensable tool to command a battle since ancient times. It is in urgent need to construct a cyberspace map that can display cyberspace information in an all-round way [3,4], and further establish the connection between cyberspace and geographic space. Cyberspace maps can be combined with the intelligent brain of the network security situation awareness platform to realize operation with cyberspace map.

Cyberspace map not only aids the cyber security functional departments, industrial management departments, network operators, and Internet-based enterprises, but also bolsters the international politics and laws as well as the domestic economy, politics, culture, and rule of law involving cyberspace. Drawing a cyberspace map is to realize the visualization of cyberspace, which is a foundation for understanding cyberspace. The proposal of cyberspace geography provides theoretical support for the mapping of cyberspace [1,2]. Based on the theory of human–land–network nexus, the exploration and application of cyberspace visualization technology is an important content of drawing real-time, reliable, and effective cyberspace maps. This is conducive to the revealing of cyberspace and the construction of cyber security system.

1 Development status of cyberspace visualization

Surveying and mapping of cyberspace resources, which can detect, integrate, and draw a variety of resources and their attributes in cyberspace, are now relatively mature for cyberspace visualization [5,6]. Representative works include the Plan X [7] of the Defense Advanced Research Projects Agency, the SHINE Program [8] of the United States Department of Homeland Security, and the TreasureMap program ① of the National Security Agency. In addition, agencies such as Norse ② of the United States and Kaspersky ③ of Russia drew real-time maps of cyber threats by collecting the data of network attacks. The Network Asset Surveying and Analysis System—Network Exploration D01 developed by a research institution has preliminarily realized the surveying and mapping of assets in cyberspace. A security enterprise drew a cyberspace map of the world's 4.2 billion IP addresses based on the network infrastructure detected by Zoomeye④. Although surveying and mapping of cyberspace explores and displays the main elements of cyberspace, it

Received: 2020-7-2

① Grant T. On the military geography of cyberspace. Proceedings, 9th International Conference on Cyber Warfare & Security (ICCWS2014). 2014: 66–76.
② http://norsenet.com.
③ https://cybermap.kaspersky.com.
④ https://www.zoomeye.org.

only visualizes partial information of cyberspace rather than fully displays it.

Martin and Rob [9,10] deeply studied the visualization of cyberspace and wrote two representative works: *The Atlas of Cyberspace* and *Mapping Cyberspace*. In the first book, they selected four different objects, i.e., network basic settings and traffic, World Wide Web, online session and community, as well as art, literature, and film in cyberspace, each of which was endowed with a cyberspace map. In the second book, they proposed a cognitive way to understand the appearance of cyberspace based previous studies, drawing parts of the cyberspace map in terms of spatiality, spatial form, and spatio-temporal relationship, while analyzing the association and interaction between cyberspace and geographic space. Although these efforts are beneficial for presenting cyberspace, they fail to depict the whole picture of cyberspace and realize cyberspace visualization in a real sense. Moreover, due to the insufficiency of presenting the structured organization and aggregation regarding cyber security information, the available results cannot support decision making and further responses. Thus, the application requirements for ensuring cyber security cannot be fully met.

2 Driving force and support for cyberspace visualization

At present, the research on cyberspace visualization is still in its infancy. The development of cyberspace visualization should be oriented to the application requirements of operation departments and supported by mature theoretical systems and technical bases.

2.1 Application requirements of operation departments drive the development of cyberspace visualization

The traditional operation work of cyber security mainly involves the query and display in the form of texts and charts. Due to the massive information, various types, and complicated representation forms of cyberspace, the traditional working pattern that ignores the mapping relationship between cyberspace and geographic space is unable to directly display the multidimensional characteristics of cyberspace information. It thus takes difficulties in providing clear and definite information support from multiple aspects. Only by integration of big data of geography, assets, events, and information with visualization technology, can cyber security become more intelligent, automatic, and visualized.

Cyberspace visualization is the foundation of cyber-related international political and legal issues such as international relations, international law, and community law, in addition to cyber security. It guarantees the cyber-related domestic economy, politics, culture, and rule of law involving resources, property rights, supervision, and administration of justice. Besides, cyberspace visualization is the basic element and guarantee for the modernization of national governance system and governance performance. The urgent demands of various businesses not only drive the development of cyberspace visualization but also provide information support and direction guidance for it. To expand the application field of cyberspace visualization will be one of the key explorations.

2.2 Mature theoretical systems and technical methods are the foundations of cyberspace visualization

The development of emerging disciplines calls for mature theoretical systems and technical methods. In the beginning, cyberspace was taken as a virtual reality world with the location attribute and coordinate expression corresponding to its geographic space [11]. As the characteristics of cyberspace virtualization became increasingly prominent, dynamic network topological diagram was viewed as a way reflecting the information relationship in cyberspace①. Driven by the rapid development of science and technology, the theories of community, map, and mapping in cyberspace were put forward on the theoretical basis of geography, graphics, computer communication, and information visualization. Basic approaches of cyberspace visualization were then established through the intersection of disciplines and technologies ②. Since 2010, Chinese scientists have introduced the idea of map and made great efforts to explore the way to represent cyberspace. Referring to the representation of maps, they proposed that a standardized cyberspace symbol system could be formulated to represent various elements and information changes in cyberspace [12,13]. On the basis of the form of raster data in a map, cyberspace can be divided into physical grid, logical grid, and social domain grid according to different properties. The connotation and representation concerning each grid form can then be explored [14]. Inspired by the map model, Chinese scientists put forward the construction system of cyberspace map model which involves the cyberspace element symbol system, multi-scale representation ways, and application analyses [15,16]. On the whole, the above-mentioned theories are relatively fragmented, mostly conceptions without mature theoretical systems and technical methods.

Considering the relevant studies, Gao et al. [1,2] introduced the idea of geography into cyberspace and proposed the concept of cyberspace geography for the first time. They systematically elucidated the theoretical bases, research contents, and technical paths of cyberspace geography, and

① http://pdfs.semanticscholar.org/1bd3/0afd5b67239588fd363a4fc01ef4d9e5a097.pdf.

② Smith M A, Drucker S M, Kraut R E, et al. Counting on community in cyberspace. Conference: CHI'99 extended abstracts, 1999.

put forward that cyberspace visualization was one of the main contents in cyberspace geography. The construction of cyberspace geography ameliorated the weak theoretical bases and technical methods for cyberspace visualization to some extent.

3 Main contents and technical paths of cyberspace visualization

The complete system theories and mature cartographical thoughts in geography provide a good criterion for drawing cyberspace maps. The theory of human–land–network nexus is the core of geographical research. With the rapid development of information technology, the limitation of geographic space among people has been broken and the human–land–network nexus has been gradually established [3,4]. With the interaction and integration of human–land–network, the introduction of the theoretical approaches of geography into cyberspace provides a new idea for realizing cyberspace visualization. Cyberspace visualization mainly involves the visualization of cyberspace elements, relationship in cyberspace, and cyber security events (Figure 1).

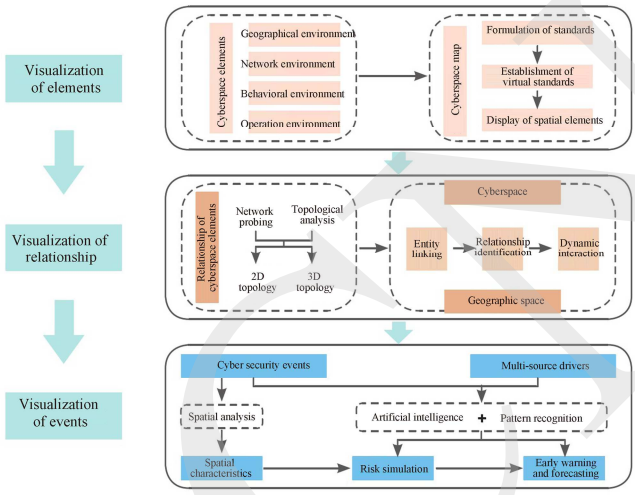

Figure 1 Connotations and technical paths of cyberspace visualization

Cyberspace is extremely complicated and has close association with geographic space. They two constitute the real space of human activities. The combination of multiple techniques is required for drawing a set of cyberspace maps that can reflect the real-time, dynamic, and true cyberspace and integrate geographic space. (1) The visualized geographic space can be integrated with the data of cyber security events and cyberspace assets to enrich visualization from the dimensions of geography, assets, and events. In this way, the distribution and attributes of cyberspace resources can be comprehensively displayed to realize the visualization of cyberspace elements. (2) On the basis of the visualization of cyberspace elements, the association and mutual effect of digital information data with human, network, and geographic space can be discussed, and then the mapping of network topology into geographic space can realize the visualization of relationship in cyberspace. (3) With events as a triggering condition, events, assets, and geographical elements can be rapidly strung together via graph. Interactions between all elements can be clarified for the formation of a set of dynamic, real-time, and reliable maps for commanding cyberspace operation. This ensures clearer asset bases, more accurate discovery of events, and more precise positioning, more intelligent analysis, and more automatic tracing of threats. The capacity and efficiency of operation departments in event discovery, evidence taking, and tracing are thus improved, and their work becomes more intelligent, automatic, and visualized.

3.1 Visualization of cyberspace elements

3.1.1 Cyberspace element system

Visualization of cyberspace elements lays a foundation for cyberspace visualization. However, the systematic classification system of cyberspace elements has not been formed yet. Traditional cyberspace elements are only classified according to their physical and social attributes, with the geographical attributes being ignored. Under the theoretical frame of man–land–network, the classification of cyberspace elements should be extended from cyberspace to cyber-geographic space. According to the structures and characteristics of cyberspace elements, as well as the requirements of cyber security, we classified cyberspace elements into four layers: geographical environment, network environment, behavioral agent, and business environment (Figure 2).

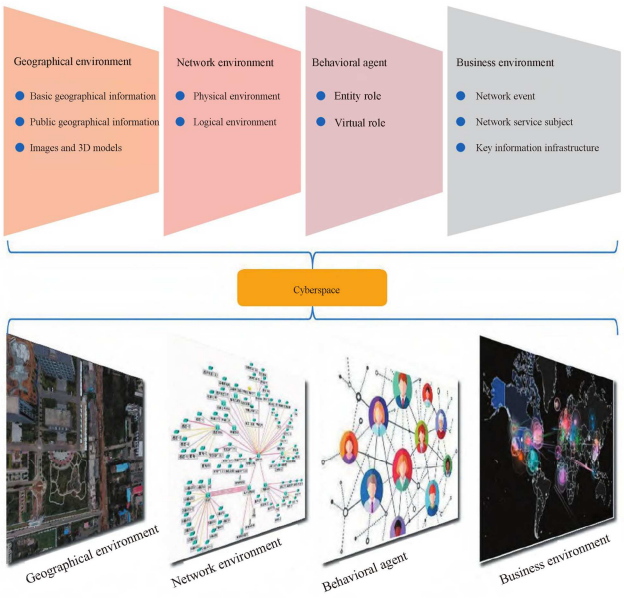

Figure 2 Cyberspace elements

(1) Geographical environment is the carrier of various cyberspace elements, the geographical attributes of which are the focus. The geographical location, spatial distribution, and regional characteristics regarding network infrastructure and network behavioral agent involve the concepts of distance, scale, region, boundary, and spatial mapping. (2) Network environment mainly refers to the nodes and links of various cyberspace elements, i.e., the logical topological relationship. It can be further divided into physical environment and logical environment, including network equipment, network applications, software, data, IP, and protocols. (3) Behavioral agent refers to entity and virtual roles, with the emphasis on interactive behaviors and social relationships of network behavioral agents. It mainly involves information flow, virtual community, and public activity space. (4) Business environment mainly includes various cyber security events (legal cases), cyber security service subjects, and cyber security protection objects that operation departments pay special attention to. Elements of the geographical environment, network environment, behavioral agent and business environment are interrelated and interact with each other, constituting a system.

3.1.2 Visualization methods

The visualization of cyberspace involves the type, layer, spatio-temporal reference, representation standard, and scale of cyberspace elements. These elements are displayed in the form of cyberspace geographical maps. In the visualization of cyberspace elements, multi-scale spatial objects are abstracted from the network geographical entities in geographic space based on the geographical mapping and map building in cyberspace. The results of network detection and the data of network topology, in combination with spatial connection and entity mapping, are used to construct the cyberspace map. (1) The data standard and cartographic specification for geographical maps in cyberspace can be formulated on the basis of the index system of key cyberspace elements. (2) Through geocoding, entity mapping, and building information modeling (BIM), the geographical environments and network entities can be spatialized to realize the 3D modeling of virtual geographical environment. (3) Network resources and corresponding security events can be comprehensively obtained by detection of network assets. After mapping of cyberspace elements into geographic space, a cyberspace infrastructure and network asset map can be drawn in the forms of geographical information map, logic diagram, and topological graph. (4) The layered display can comprehensively and intuitively depict the spatio-temporal distribution, attribute states as well as changes of cyberspace elements, which generates a set of dynamic, real-time, and reliable cyberspace element maps.

3.2 Visualization of relationship in cyberspace

Visualization of relationship in cyberspace involves both the relationships between cyberspace elements and between cyberspace and geographic space. It mainly studies the structural characteristics of cyberspace as well as the multi-scale topological relationships between cyberspace and geographic space on the basis of the interactive mapping between cyberspace elements and geospatial elements. This will realize the structural mapping of network entities in cyberspace and geographic space.

In terms of the relationship among cyberspace elements, network detection and topology analysis methods can be used to analyze the attributes of network resources and form the topology of rich network entity connections. Visualization of network topologies with different levels and granularities can display the topological relationships of various scopes including 3D geographical topology and 2D logical topology in the world, between countries, within a country, between autonomous systems (ASs) ①, and within ASs. Geographic space and cyberspace take a complex coupling relationship. The key to its visualization is to realize the dynamic interaction between these two spaces. With the visualization of cyberspace elements, the detection of network assets, the spatialization of network topology, the association of integrated 2D and 3D network geographical data, the entity connection and relationship identification of multi-scale geographic space and cyberspace can be studied. These studies will reveal the associations among space, information, and human behavior to achieve the multi-scale, multi-dimensional, and dynamic visualization of geographic space and cyberspace.

Figure 3 illustrates the relationships among urban network nodes and between cyberspace and geographic space. The relationship among urban network elements is often displayed in the form of 2D logical topology, with a low level of visualization. According to the relationships of nodes in the core layer, convergence layer, and access layer and the layered display regarding the locations of urban geographical elements in 2D and 3D topologies, each node is linked to a geographical entity on the map. Layered display of network topology not only clearly visualizes the relationship in cyberspace but also establishes an adequate connection with geographic space.

3.3 Visualization of cyber security events

Visualization of cyber security events (including legal cases) is to analyze the driving factors and internal mechanisms for these complex and dynamic events on the basis of their behavioral agent, object, and impact. Visualization of cyber security events helps realize the situation awareness as well as the early warning by drawing images and showing event processes in cyberspace maps.

① AS (autonomous system). The global Internet is divided into 65 536 ASs.

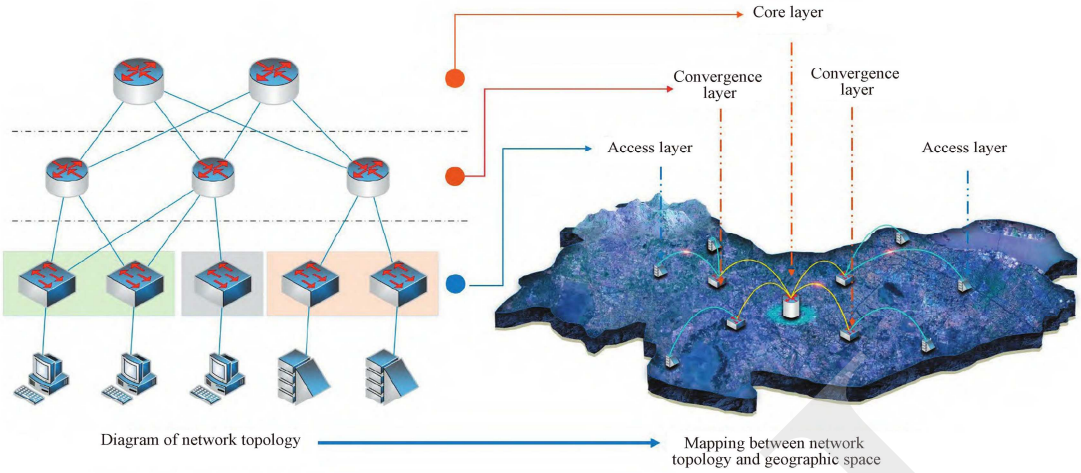

Figure 3 Schematic diagram of cyberspace network

According to the hierarchical model, network is usually divided into core layer, convergence layer, and access layer. The relationships among layers are shown in the form of topology (left in Figure 3). The geographical locations of key nodes in each layer are identified for the mapping between network topology and geographic space (right in Figure 3), which can improve the visualization.

Visualization of massive cyber security events with geographical information transforms the cyber big data into the information resources via resource integration. The spatio-temporal distribution characteristics and agglomeration effect of cyber security events can be analyzed and displayed referring to the spatial analysis methods in geography. As for a certain kind of cyber security events, their material, social, and geographical attributes should be comprehensively considered. Then, the cyberspace element set related to such events is obtained. Machine learning algorithm can be adopted to simulate their risks and then forecast the risk distribution. In this process, such events are taken as the agents on a spatial scale and the related cyberspace element set as the eigenvector. Therefore, operation departments can adopt deep learning and pattern recognition to conduct early warning and forecast on the development trends of such events, improve their detecting and handling ability, and finally achieve the early detection of, early warning of, and early response to cyber security events.

In the case of a cyber attack, the sentinel probe, threat intelligence, and relevant data are first matched with historical data for the analysis of the characteristics and source of the attack (Figure 4). Entity positioning technology is then used to determine the location and springboard of the attack. The method, type, and direction of the current attack are indicated by color, width, and direction, respectively, on the map. This helps to quickly understand and timely deal with the attack. In addition, the attack should be timely included in the database

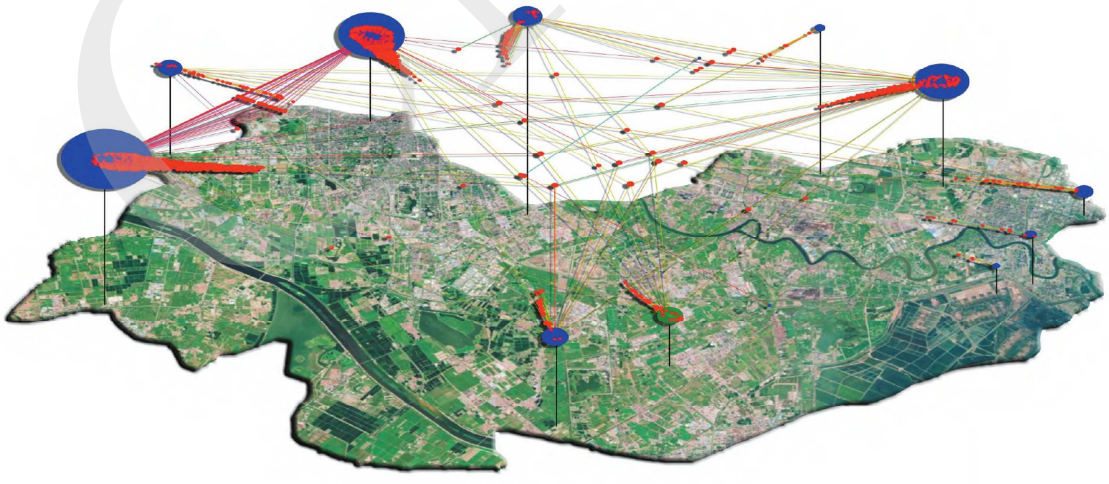

Figure 4 Visualization of a cyber attack

Attacks can be displayed in the geographic space. The entity positioning technology can be used to determine the attacker and the geographical location of the node being attacked. The attacked node is located on the 2D and 3D maps with the node color, node size, connecting line, line color, and line width representing its type, importance, attack path, attack type, and attack frequency, respectively.

of cyber security events and taken as the background data for subsequent attack events. With respect to the vulnerability discovery in cyber security events, 3D modeling of key protection units can be utilized to quickly locate the spatial position where the vulnerability occurs. The information of vulnerability and its physical spatial location can be quickly and accurately reported to the contact person of the involved unit. Thus, the rapid treatment of vulnerability can be achieved and the working requirements of operation departments can be met at different scales of the map.

To sum up, the visualization of cyber security events intensively represents the entire analysis process in the form of spatial graph and network graph. It depicts the attack, attacker and attack means based on artificial intelligence and big data technology, and displays a full life-cycle scenario including the cyberspace elements, model operation, and emergency response. When being applied to the typical business scenarios such as the real-time monitoring of cyber attacks, source tracking of cyber security events, awareness of cyber security situation, notification and early warning, emergency response, detection and fight, command and dispatch, visualization of cyber security events can make the work of operation departments more intelligent, automatic, and visualized.

4 Discussion

The ultimate goal of cyberspace visualization is to fully display cyberspace information in the form of cyberspace maps and realize the visualization and digitization of cyberspace so as to provide intuitive and valuable information for decision-makers and reduce the uncertainties of decision-making. The cyberspace should be visualized on the basis of the visualization of geographic space and include cyberspace elements and cyber security events. Visualization content can be enriched from the dimensions of elements, relations, and events. Cyberspace maps should be drawn with a set of images showing the entire processes of various events. This is to achieve operation with cyberspace map for the public security agencies, thereby improving the monitoring and early warning of cyberspace.

There are several problems including weak theoretical basis and immature technology at the early stage of cyberspace visualization development. The proposal of theoretical systems and technical methods concerning cyberspace geography opens a new angle for the cyberspace visualization studies. Many disciplines such as geography, information technology, big data, and artificial intelligence are involved in cyberspace visualization. Therefore, multi-collaboration and interdisciplinary integration help meet the application requirements of cyberspace visualization so as to jointly promote the construction of the comprehensive cyber security system.

References

1 Gao C D, Guo Q Q, Jiang D, et al. The theoretical basis and technical path of cyberspace geography. Acta Geographica Sinica, 2019, 74 (9): 1710–1722.
2 Gao C, Guo Q, Jiang D, et al. Theoretical basis and technical methods of cyberspace geography. Journal of Geographical Sciences, 2019, 29 (12): 1949–1964.
3 Meng W. 网络安全:国家战略与国际治理. Contemporary World, 2014, (2): 46–49 (in Chinese).
4 Zhao F, Luo X Y, Liu F L. Research on cyberspace surveying and mapping technology. Chinese Journal of Network and Information Security, 2016, 2 (9): 1–11 (in Chinese).
5 Jin W X. 网络空间面临的战争威胁和应对策略. China Information Security, 2015 (11): 113–115 (in Chinese).
6 Guo L, Cao Y N, Su M J, et al. Cyberspace resources surveying and mapping: The concepts and technologies. Journal of Cyber Security, 2018, 3 (4): 1–14 (in Chinese).
7 Nakashima E. With Plan X, Pentagon seeks to spread US military might to cyberspace. The Washington Post, 2020-05-31.
8 Müller-Maguhn A, Poitras L, Rosenbach M, et al. Treasure map: The NSA breach of telekom and other German firms. Spiegel Online, 2012-04-16.
9 Dodge M, Kitchin R. The Atlas of Cyberspace. Massachusetts: Addison-Wesley Reading, 2001.
10 Dodge M, Kitchin R. Mapping Cyberspace. London: Routledge, 2003.
11 Benedikt M. Cyberspace: First Steps. Massachusetts: MIT Press, 1991
12 Zhang Z. The Research on Theory of Cybermap. Zhengzhou: PLA Information Engineering University, 2012 (in Chinese).
13 Ai T H, Zhou M J, Chen Y J. The LOD representation and treemap visualization of attribute information in thematic mapping. Acta Geodaetica et Cartographica Sinica, 2013, 42 (3): 453–460 (in Chinese).
14 Jiang B C, Wan G, Xu R. Research on cyberspace division and visualization method. Journal of System Simulation, 2017, 29 (S1): 1–8 (in Chinese).
15 Zhang L, Zhou Y, Shi Q S, et al. Cyberspace map tightly coupled with geographical space. Journal of Cyber Security, 2018, 3 (4): 63–72 (in Chinese).
16 Zhang L, Zhou Y, Tian J P, et al. Design method of semantic-driven cyberspace resource symbol. Computer Science, 2019, 46 (4): 83–88 (in Chinese).

(Translated by TIAN Y)

GUO Qiquan, Inspector, Deputy Director and Chief Engineer of the Cyber Security Department, the Ministry of Public Security of PRC. The distinguished professor of Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences. His research focuses on national cyber security. E-mail: xxaqgc@163.com

HAO Mengmeng, corresponding author, Assistant Professor of Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences. Her research focuses on cyberspace geography, geographic information system, etc. E-mail: haomm@igsnrr.ac.cn