Research on the Governance of Cyber Terrorism under the Construction of National Trust

Xiangtao Ma*

Postgraduate College, People's Public Security University of China, BeiJing, China

*Corresponding author, e-mail: 3288552152@qq.com

DOI: 10.37420/j.mlr.2020.010

***Abstract**: The international governance of cyber terrorism is a process of mutual interest game and trust interaction between countries. Enhancing national trust provides strategic goals and security guarantees for the governance of cyber terrorism. Trust theory provides a new research paradigm for the governance of cyber terrorism. At present, the governance of international cyber terrorism mainly has differences in national interests, strategic suspicion between subjects, imbalances in power control, differences in governance concepts, and lack of trust among countries such as poor intelligence resource sharing. The dilemma caused. To eliminate these governance dilemmas, it is necessary for the actors of various countries to explore the construction of trust relations between countries in terms of rationality, emotion, culture, system, and process, in order to promote the development and improvement of cyber terrorism governance.*

***Key words**: Cyber terrorism; Governance; Trust*

Introduction

In the context of globalization and informatization, a new type of cyber terrorism, which is different from traditional terrorism, is rapidly emerging and spreading in global regional networks. Cyberterrorism is initiated by non-state organizations or individuals to attack or threaten computer systems, programs, software, and data, thereby creating social panic, endangering public safety, and infringing on personal property, in order to affect government decisions and achieve political goals (Zhao & Chen, 2020). Because cyber terrorism is more harmful and involves scope The characteristics of wider light and greater concealment have a huge impact on network information security, and severely endanger national political, economic, cultural, ideological security and people's property security. In addition, network information systems are open, cross-regional and cross-border, and network activities are concealed, decentralized, and technical, making cyber terrorism an international non-traditional security governance problem.

As far as the international community's response to cyber terrorism is concerned, governance strategies are generally adopted from the levels of strategy, law, technology, action, and cooperation. However, the global governance of cyber terrorism also has real dilemmas caused by differences in national interests, strategic suspicion of governance subjects, differences in value concepts, imbalances in power control, and poor sharing of intelligence resources. Therefore, this article attempts to build a trust governance mechanism between state actors and relevant governments, build trust from the rational, emotional, cultural, institutional, and process levels, and use the trust mechanism between state actors and governments to make the fight against cyber terrorism cooperation trend To develop in a deeper, broader, and longer-term direction, so as to solve the problems of the international community in the governance of cyber terrorism, such as the strategic suspicion of governance entities, the imbalance of technological power control, and the poor sharing of intelligence resources.

Trust Construction in the Governance of Cyber Terrorism

Trust is an integrated mechanism that generates and maintains unity in social relations and social systems. It can anticipate people's behavior, create a sense of community, and simplify cooperative relations, thereby playing an important role in maintaining social order and stabilizing social relations. Similarly, trust between countries will increase trust and dispel doubts, reduce misjudgments, and reduce transaction costs, thus becoming a necessary condition for cooperation between countries.

Connotation of National Trust

In recent years, the issue of trust between countries has received more and more attention from the governments of various countries, and the academic community has also expanded trust from the traditional sociological field to related research on international issues. German sociologist Schimmel believes that general trust is inseparable in the process of interpersonal communication, otherwise the society itself will become a mess and social relations will be difficult to maintain, and trust is one of the most important comprehensive forces in society (Zimmel, 2009). Princeton University professor Andrew Kidd used game theory to analyze the relationship between trust and cooperation between countries and pointed out National mutual trust means that a country believes that another country is trustworthy, and is therefore willing to strengthen mutually beneficial cooperation (Andrew, 2005). It can be seen the importance of establishing trust relationships in the process of international exchanges to the governance of cyber terrorism. Inter-country trust means that a country has made a positive assessment of the intentions and actions of another country or an international organization, and has adopted an attitude of ignoring the uncertainties and risks that may exist objectively. An international organization produces subjective judgments of psychological identity and belonging.

Trust Construction in the Governance of Cyber Terrorism

Mutual trust is an indispensable element in international exchanges. Especially in today's rapid development of science and technology, the Internet spreads all over the world, and national sovereignty extends from the real world to cyberspace, cyberspace has become the main battlefield and important carrier for the game of sovereign states. At the same time, both developed countries and developing countries with relatively backward network technology are facing difficulties brought about by cyberspace governance. In addition, cyber terrorism, cyber virus attacks, and other terrorist criminals who use the Internet to commit crimes often occur, and the governance of cyber terrorism is inseparable from the mutual trust between countries. Therefore, countries need to build trust relationships to provide effective paths for cyberspace governance.

According to different influencing factors, the trust relationship between countries can be divided into rational trust, institutional trust, emotional trust, cultural trust and process trust. By further analyzing the influencing factors of these types of trust, the trust relationship between countries can be effectively established, which can effectively solve the network terrorism governance problems faced by countries.

Commentary on the Current Situation and Predicaments of the International Community’s Governance of Cyber Terrorism

Current Status of Cyber Terrorism Governance in Various Countries

Under the military attack of the international community,the disintegrated "Islamic State" terrorist organization began to rapidly spread to Southeast Asia, Africa, Europe and other regions, and joined the "Cyber Caliphate" and other cyber terrorist organizations to march and transfer positions on the Internet, and successively established networks The action team planned and implemented a number of vicious cyber incidents, created a terrorist atmosphere on the Internet, recruited and mobilized online, and raised funds for activities to further expand its influence. Some major countries in the Americas, Europe, and Asia have adopted a series of effective measures in accordance with their respective national conditions and needs, so that the international community has achieved certain results in the governance of cyber terrorism. At present, the international community’s efforts to combat cyber terrorism mainly focus on the following aspects:

First, at the strategic level. As one of the most informatized and networked countries in the world, the United States promulgated legal documents such as the Patriot Act in 2001 to improve cybersecurity to the level of national security strategy, especially the 2017 National Security Strategy Report The content of network security has been mentioned many times, focusing on information and network security, and considering information and network security in the first place from the perspective of national security strategy. Russia is one of the most hacked countries in the world. In order to monitor, combat, eliminate and prevent hidden network security risks, Putin signed a presidential decree in January 2013, requiring the Federal Security Agency to establish a national network information security mechanism, putting network security at the top of the national security strategy. The European Union has long been aware of cyber security regulations. Promoting the integration and integration of counter-terrorism intelligence based on legal foundations, judicial procedures, advanced technology and other measures, and carrying out the governance of cyber terrorism within the EU system provides an overall strategic view and a basis for counter-terrorism awareness.

Second, at the legal level. The United States has successively promulgated a series of various laws, regulations and normative documents to combat hacking, cyber terrorism, and protection of cyber security, such as the "Computer Security Act", "Cyber Security Act" and "Cyberspace Security State". Strategy" and other policy documents. After frequent cyber attacks, Russia has strengthened its legislation on cyber security, and has successively promulgated laws and programs such as "Russian Cyber Legislation Concept", "National Information Security Doctrine", "Russian Federation Computer Software and Database Legal Protection Law" Sexual documents to lay the legal foundation. The first "Network and Information System

Security Directive" of the EU legislature was officially released in July 2016. The Directive is a regional document to strengthen basic services, network and information system security, and cooperation between member states.

Third, at the technical level. As a country with the most developed Internet technology, the United States not only specifically promulgated the "Network Information Security Enhancement Act" to improve domestic information security technology standards. With the strong support of the government, and led by mainstream online social media such as Google and Twitter, various targeted measures have been taken in an attempt to fundamentally block the path of cyber terrorist actions. The EU requires member states to establish emergency response teams, establish prevention, detection, handling and corresponding coordination mechanisms, and improve information sharing mechanisms to improve network resilience and anti-terrorism capabilities. While Australia, Japan, South Korea and other countries attach importance to personnel training in the process of cyber terrorism governance, they also pay special attention to the improvement of ordinary citizens' anti-terrorism quality, and conduct regular publicity and anti-terrorism knowledge training to the public to raise citizens' awareness of anti-terrorism online.

Fourth, at the operational level. After the "9.11" terrorist incident, the United States successively established a homeland security office, an anti-terrorism office, and a cyber security office. An "anti-terrorist cyber force" with high IQ and high network technology has also been established to combat cyber terrorism. EU member states use the European Counter-Terrorism Center and Europol to hold cyber-counter-terrorism exercises to realize intelligence sharing, cyber information identification, and cyber-counter-terrorism capability training. Japan organizes cyber security experts and people from all walks of life to hold cyber attack and defense exercises every year, and optimizes the anti-terrorism system through the establishment of cyber counter-terrorism forces, forming a situation of cyber security and cooperation between the military, police, government, enterprises, and civilians.

Fifth, at the level of cooperation. In order to jointly combat and control cyber terrorism crimes, the international community has carried out extensive cooperation. The 26 member states of the European Union and government officials from 30 countries including the United States, Japan, Canada, and South Africa signed the Cybercrime Convention on November 23, 2001 to promote judicial cooperation in combating and preventing cyber terrorism by the international community . In 2018, the NATO Cyber Defense Center of Excellence held the "2018 Looked Shields" international combat cyber defense exercise in Tallinn, Estonia. In addition, the United Nations has adopted multiple agreements on the governance of cyber terrorism, aiming to strengthen cooperation in combating and managing cyber terrorism at the level of member states, regional organizations, and international organizations.

The Dilemma of International Cyber Terrorism Governance

In the era of global informationization, cyber terrorism has become a public hazard affecting the survival and development of mankind. Due to the openness and borderlessness of the Internet, coupled with the hidden nature of cyber terrorist activities, terrorists have anti-detection capabilities, making the scope and consequences of terrorist activities more serious. In the practice of governance, countries and governments have different sovereign jurisdictions. There are problems such as divergence of interests, strategic mutual doubts, conflicts of values, imbalances in power control, and poor intelligence sharing, which make cyberterrorism prevention, discovery, investigation, and evidence collection. , Investigation and punishment, crackdown, and governance work have become more difficult.

(1) The Lack of Rational Trust Leads to Differences in National Interests

Pursuing and safeguarding national interests is the starting point and foothold of state actors and governments in their foreign actions (Su & Guo, 2020). In the international cooperation of governance of cyber terrorism, the state and government that the rational choice of "interest considerations" affects the achievement of cooperation, leading to governance dilemmas. Based on "interest considerations", countries define "cyber terrorism" with political goals and "double standards." For example, under the banner of "freedom" and "democracy", the United States insists on granting individuals complete network use rights and the right to free flow of data, and opposes the establishment of network barriers in data circulation by countries. And often under the banners of "human rights" and "freedom of speech," discredit other countries' actions and measures on terrorism-related issues in the field of international public opinion, create discourse space for terrorist forces, and use their cyber hegemony to lead the identification standards. Interference with the international community’s joint efforts to combat cyber terrorist activities (Yang, 2016).

(2) The Lack of Emotional Trust Causes Strategic Suspicion among Governance Subjects

Strategic decision-making between countries cannot be separated from the long-term accumulated emotional basis. Emotion is the lubricant that maintains the long-term strategic partnership between countries. Ideological differences are the fundamental reason that affects emotional stability. In the interaction between countries, due to large ideological differences and other reasons, it is often difficult for countries to accurately analyze, judge, and determine the strategic intentions of other countries. The lack of emotional foundation will lead to strategic mutual doubts between the partners. Strategic mutual doubts between countries and governments restrict the breadth and depth of cooperation in the governance of cyber terrorism, and are an important source of the difficulty in achieving effective results in international governance of cyber terrorism. For example, the United States and its allies have maintained long-term strategic interactions based on the same or similar values or ideologies, adopting strategic mutual trust with allied countries, and constantly improving the cooperation mechanism with traditional allied countries; while for non-allied countries due to lack of emotional foundation Holds an attitude of strategic mutual suspicion, and does not attach importance to institutional cooperation with AU countries on the governance of cyber terrorism. Therefore, the serious lack of strategic mutual trust between state actors is one of the important causes of the strategic dilemma in the international governance of cyber terrorism.

(3) The Lack of Cultural Trust Makes the Anti-Terrorism Concept Different

Culture is the spiritual bond of a country, region and nation. The difference in cultural concepts is one of the important factors that cause differences in the governance concepts of different countries for the same problem. Taking China and the United States as examples, China has mostly implemented a centralized governance model under the influence of a centralized culture, while the United States has generally implemented a decentralized governance model under the influence of federal culture. Therefore, influenced by Eastern and Western cultures, there are two governance models for international cyberspace security governance. The first is the "multi-party model" proposed by developed countries on the Internet. The second is the "multilateral model" proposed by network developing countries (Bao, 2020). The two models are different from each other on the surface. The cognition difference between the "global commons" and the "sovereign realm" of the two types of cyberspace attributes is actually the difference between the primary concerns of cyberspace developed countries and cyberdeveloping countries. In the process of governance of cyber terrorism, diversified governance bodies inevitably include diversified cultural concepts. The conflict and collision of cultural concepts between Eastern and Western countries has led to the fragmentation of the value of the international community in the process of governance of terrorism, and the governance bodies hold different views. The concept of anti-terrorism leads to the "conflict" between the anti-terrorism mechanism and anti-terrorism path advocated by it, which hinders the governance efficiency of cyber terrorism under the framework of this governance model.

(4) The Lack of Institutional Trust Causes an Imbalance of Data and Technical Power

Good order requires a good system as a guarantee. The development of data and network technology has promoted the coupling between virtual space and the real world, and has an expanding effect on the projection of the real society, thus deepening the destruction of cyber terrorism to the world security order. On the one hand, the rapid development of network technology will increase the technical difficulty of managing cyber terrorism. On the other hand, it will increase the network security management workload. In the specific governance practice, the governance of cyber terrorism mainly relies on the Internet and information and communication technology. Due to the uneven development of networks and information technology among countries, the "data and technical power" of the governance body is unbalanced. Western countries, headed by the United States, have a large number of network core technologies and data management powers, and are the main makers and greatest beneficiaries of the existing cyberspace system. They also have the leading power and the right to speak in the governance of cyber terrorism. The United Nations and developing countries have long been in a disadvantaged position in terms of cyber data sovereignty, and have no right to speak on key cyber issues, so they are in a passive state of governance in cyber anti-terrorism. Therefore, only by changing the existing cyberspace system in which developed countries have the dominance and the right to speak, can we change the passive situation of countries with no right to speak in the development of the Internet, accelerate the progress of cyber terrorism governance, and jointly maintain the world security order.

(5) Lack of Process Trust Causes Poor Intelligence Resource Sharing

The governance process of cyber terrorism is essentially a process in which state actors exchange and interact in counter-terrorism intelligence information. It is difficult for countries in the international community to share counter-terrorism intelligence information resources based on factors such as "interest considerations," and "strategic mutual suspicion." First of all, in a big data environment, network information has the characteristics of complexity and redundancy. It is difficult to determine the true origin and actions of terrorist attacks, and it is even more difficult to effectively monitor information on terrorist activities. Secondly, different countries have different levels of technological means, making it difficult to obtain counter-terrorism intelligence resources. In addition to mastering high technology, developed countries also have specialized intelligence analysis talents. The acquisition of intelligence resources and the analysis and research of information data are highly efficient. However, in the process of governance, Internet developed countries disdain to communicate and communicate with Internet developing countries on counter-terrorism intelligence, resulting in poor international intelligence sharing, and it is more difficult to obtain international cyber counter-terrorism information. Finally, due to the different environments in which countries live and the degree of cyber-terrorism infringements, there are subjective differences in the understanding of cyber-terrorism intelligence, which hinders the sharing of counter-terrorism intelligence resources.

The Governance Path of Cyber Terrorism under Trust Construction

Trust is a process of continuous construction rather than a result. It requires the country to continuously cultivate and maintain it in the process of continuous interaction. The governance application of national trust in cyber terrorist activities is an interactive process. The governance of cyber terrorism is a natural extension of the transition of national sovereignty from the real world to the virtual world for governance. Based on different factors such as interest game, value concept, and other factors, there are differences in the governance of cyber terrorism. Establish a relationship of mutual trust between them, and use emotional foundation, institutional norms, communication and interaction to maintain a trust relationship in the process of interaction, so as to avoid differences, reach an agreement in the process of cyber terrorism governance, and jointly combat the cancer of cyber terrorism.

Realize Rational Trust—the Rational Choice of Governance Entities Provides Conditions for Cyber Terrorist Governance

The construction of trust between countries is influenced by acceptability factors. The country, as a foreign policy decision maker, judges whether a country is trustworthy based on calculable factors such as the strength of both parties, geographical distance, and common interests. National decision makers analyze the behavior of the other party , Make the best choice for your country (Chen & Cai, 2016). In response to cyber terrorism, the governance of developed and developing countries The attitude is quite different. Western countries, led by the United States, often adopt double standards. Out of considerations of interest, they choose governance standards that are beneficial to their country to respond to cyber terrorist crimes; developing countries represented by China are based on fair, reasonable, and win-win governance. The idea faces the same problem. Therefore, facing the same network governance problem, the rational choice made by the network governance entities upholding the mutual benefit and win-win concept of both parties can provide a realistic basis for the realization of the trust relationship between the two parties, which is conducive to jointly coping with the governance problems of cyber terrorism.

Stabilizing Emotional Trust—the Emotional Presentation of Governance Concepts Provides the Basis for Cyber Terrorist Governance

Trust itself is a behavior that contains emotional factors, which can be divided into two parts: the personal psychology of the decision-maker and the national emotion (Chen, 2017). The personality traits of the leader of one party are trustworthy or the leaders of both parties If people have emotional links, it is easier to establish a trust relationship between the two countries. In the face of non-traditional security threats such as terrorist activities in cyberspace, when state leaders have the same or similar governance concepts, countries can establish trust relationships based on the emotional state of decision makers, which is conducive to addressing cyber terrorism from an emotional dimension Ideological governance issues. The cultivation and maintenance of emotional trust is not only affected by the emotional and psychological factors of decision-makers, but also the national sentiment between the two countries is also one of the important influencing factors. The good relationship established between the two peoples can surpass the calculation of the interests of the two countries. Even when the government relationship is faced with the challenge of conflicts caused by the governance of cyberspace, it can become a breakthrough point for the improvement of the relationship, which is conducive to the resolution of the two countries. Contradictions and conflicts caused by terrorism crime management such as cyber terrorist attacks and computer-based cyber viruses.

Develop Cultural Trust—the Cultural Homogeneity of the Governance Context Provides the Cornerstone for Cyberterrorism Governance

As a large social system, countries are affected by subjective factors such as cultural concepts. Countries with similar cultural homogeneity will have less mutual uncertainty and the possibility of mutual understanding and consensus. The greater the sex (Yin, 2011), so as to enhance the relationship between the two countries Transparency and trust in communication make it easier to form partnerships. Governments of all countries must work together to promote mutually beneficial cooperation in the humanities fields such as education and culture in order to form governance consensus on the basis of cultural identity. The first is to give full play to the soft and unique charm of "cultural diplomacy" and strengthen the sense of cultural identity and historical responsibility among nations and ethnic groups. The second is to actively promote cooperation in the field of education, and try to avoid international terrorist organizations from taking advantage of it (Zhang, 2020). In addition, national leaders are often a symbol of a country's status and represent a country When the government interacts with the decision makers of the other party, it is often that each individual carries its own culture, and each has inconsistent knowledge and understanding of itself and the culture of other countries, which may lead to deviations in behavior expectations. Therefore, in the international community's governance of cyber terrorism, relying solely on international governance rules can only treat the symptoms and not the root cause. It also requires countries to reduce cognitive biases based on cultural identity, thereby helping to fundamentally solve governance problems.

Shaping Institutional Trust—the Institutional Constraints of Governance Norms Provide Guarantee for the Governance of Cyber Terrorism

The system, as a norm to restrict the interaction process between actors, once formed, will provide external institutional guarantees for the interaction and cooperation of actors. The establishment, maintenance and development of institutional trust between countries cannot be separated from the international environment. Once international rules are established, they will have their own vitality, which is conducive to coordinating the governance of cyber terrorism caused by information asymmetry among countries. In order to ensure the smooth progress of information transmission and interest exchanges between countries in the real world and virtual space, international institutions are needed to act as the main body and trust platform of institutional trust between countries. The 68th United Nations General Assembly reviewed and revised and passed the "United Nations Global Counter-Terrorism Strategy" resolution for the fourth time. According to China’s proposal, for the first time clearly the content of combating and managing cyber terrorism was included in the global counter-terrorism strategy framework. The United Nations counter-terrorism agency, in conjunction with various countries and relevant international organizations, strengthens the governance and crackdown on terrorist acts committed by terrorist organizations and terrorists using the Internet (Ming & Shi, 2020). This resolution provides institutional guarantees for the international community to combat and manage cyber terrorism. The international system not only restricts the behavior of countries, but also helps to alleviate anarchy. Therefore, governance entities between countries need to jointly abide by international systems and norms and establish institutional trust in order to make the international system in the process of governance of cyber terrorism Play real effectiveness.

Establish Process Trust—Communication and Interaction in The Governance Process Provide Impetus for Cyber Terrorism Governance

As a specific agency that represents a country’s internal and external powers, the government’s institutionalized exchanges and interactions between governments are the continuous driving force for trust between countries. Countries exchange intelligence and information through intergovernmental communication and interaction (Liu & Yang, 2016). This can reduce friction and misjudgment due to disagreements, help countries build trust relationships through government interaction, and to a certain extent eliminate mutual doubts caused by lack of communication. Actively promoting the interaction of existing governance mechanisms and building an interactive mechanism system is an effective way to promote governance entities to build mutual trust in the exchange process. For example, countries have established a discussion mechanism on the international governance of cyber terrorism under the global Internet conference mechanism, which can promote dialogue and exchanges between different governance entities during the interaction process, and reduce mutual strategic suspicion by establishing process trust. Cyber terrorism governance issues such as cyber warfare, cyber crime, and cyber infringement affect the cyber security of various countries to varying degrees. In the face of these governance problems, in addition to regulating and sanctioning through international systems and laws, it is necessary to communicate through various governments. Only by interacting with each other, under the premise of ensuring that the root interests of all countries are not violated, actively establishing and maintaining a relationship of trust, strengthening cooperation and information exchange with each other, and enhancing information transparency, can we fundamentally solve the problem of cyber terrorism governance.

Summary

As a product of the information age, cyber terrorism not only seriously endangers the actual security of all countries, but also poses a serious threat to the security of cyberspace. It is difficult to effectively combat and manage cyber terrorism by relying solely on the strength of a certain country or a certain region. However, in the face of this malignant governance problem, the international community has many governance dilemmas such as differences of interest. The root cause of the dilemma lies in the lack of trust in rationality, system, and culture among countries. To resolve the real dilemma of the international governance of cyber terrorism, it is necessary for countries to establish a trust relationship in rational, emotional, cultural, institutional, and process aspects, which will help to fundamentally solve the governance problems of various countries in response to this problem.

References

Zhao, X., & Chen, Z. R. (2020). The characteristics, development trends and countermeasures of cyber terrorism. *Journal of Jiangsu Police Officer Academy*, (4),59.

Zimmel. (2009). *Philosophy of Currency*. Guizhou: Guizhou People's Publishing House.

Andrew, H. K. (2005). *Trust and Mistrust in International Relations*. Princeton University Press.

Su, H. H., & Guo, R. (2020). Institutional Dilemma and Optimal Paths of International Governance of Cyber Terrorism. *Intelligence Magazine*, (2), 23-24.

Yang, M. X. (2016). On the prevention and control of cyber terrorist activities in the context of global governance. *Journal of Beijing University of Posts and Telecommunications (Social Science Edition)*, (5), 36-42.

Bao, Z. H. (2020). The dilemma and path of the construction of cyberspace synergy governance model. *Journal of Henan University of Science and Technology*, (5), 18-19.

Chen, L. Y., & Cai, J. H. (2016). Theoretical exploration of the formation and maintenance of mutual trust between countries. *Nanjing Social Sciences*, (4), 73-74.

Chen, L. Y. (2017). Emotional trust: a deep form in the relationship of mutual trust between countries. *Academia Bimestrie*, (6), 50-51.

Yin, J. W. (2011). Culture and International Trust—A Comparative Analysis Based on the Formation of East Asian Trust. *Diplomatic Review*, (4), 24-25.

Zhang, H. T. (2020). Research on the self-consistent logic and construction mechanism of cultural anti-terrorism. *Theory Monthly*, (7), 27-28.

Ming, L. Q., & Shi, Y. C. (2020). The Dilemma and Path of Cyber Terrorism Crime Governance. *Journal of Jiangsu Police Officer Academy*, (1), 32-33.

Liu, C. M., & Yang, H. (2016). The construction of trust in East Asian countries from the perspective of social networks: theoretical framework and implementation path. *National Watch*, (6), 4-5.