

Discussions on the Eliminating and Controlling of the Public Risks in Cyberspace

QUE Tianshu

East China University of Political Science and Law, Shanghai, China

Dual public risks existing in the interconversion between the virtual space and the real space create a new perspective to understand the orders in cyberspace. As an important means to predict and avoid public risks, orders in cyberspace have three uncertainties: lack of information, information surplus, and information distortion, which may lead to the failure of the prediction. Orders in present-day cyberspace, such as technology controlling, legal controlling, and made orders further increase the public risks. Against such backdrop, according to the logic of the mutual conversion between real and virtual society, the reconstruction of the orders in cyberspace should be conducted through three paths: from virtual to real space, from real to virtual space, and from virtual to virtual space, so the public risks could be reduced and avoided to the maximum extent.

Keywords: public risk, cyberspace order, virtual space, reality

Introduction

The rapid expansion of the cyberspace carries out the out of touch between supply and demand of the orders of the cyberspace, which makes it possible for the risks of the ordered activity in cyberspace. Especially given the circumstance that China is currently in transformation period in which the institutional construction and systematic cyberspace are still imperfect and lacking of orders, chaos in cyberspace becomes even worse. Hence, provided the backdrops of the rapid developing cyberspace on the one hand and the imperfect cyber orders on the other hand, reconstructing the orders in cyberspace and achieving the coordination in cyberspace have been important tasks ahead of Chinese government.

Dual Public Risks in Interconversion of the Virtual Space and the Real Space

Cyberspace, as a public field developing based on Internet technology, has an important direct or indirect influence on the survival and development of human beings. The conversion between virtual and real space brings people positive impacts as well as huge risks.

Risks in Virtual Power's Conversion to Reality

The essence of the risks does not exist when it takes place, but it may take place (Adam, Beck, & Loon, 2005). Likewise, the risks in cyberspace do not exist in its generating, but it may bring out real problems when conversing from virtual space to real space. Since the year 1994, when the Internet fully spread in China, forces

Que Tianshu, Ph.D. in Politics, professor, Political Science Institute, East China University of Political Science and Law, Shanghai, China.

Correspondence concerning this article should be addressed to QUE Tianshu, Political Science Institute, East China University of Political Science and Law, No. 555, Long Yuan road, Songjiang District, Shanghai, China.

in cyberspace have been promoted and expanded. From the microscopic perspective, the risks in conversion from virtual space to real space can mainly be found in following aspects:

(1) Fraud through Internet. Activities in cyberspace reflect social reality. Hence, individual behaviors in cyberspace may threat the real space. Fraud through Internet is an activity in cyberspace as well as an action based social reality. Such behaviors may bring out negative influence to social orders, which should be restricted by the rule of law.

(2) Trust issues. Trust is not limited by time and space, so it could converse between virtual and real space. For this reason, freedom of speech in virtual space may lead to the lack of trust, which may even influence the real space.

(3) Information hurt. Information hurt includes hurt by subjective information and hurt by objective information. Both the subjective information and objective information hurt can converse the virtual forces to real crisis.

(4) Negative cyber culture. Long-term activities in cyberspace can shape cyber culture. Positive cyber culture can play a role in avoiding social risks while negative cyber culture may intensify the public risks.

Risks in Real Activities' Conversion to Cyber Public Opinion

Samuel Huntington holds that modernity will bring stability, and modernity will bring instability (Huntington, 1988). However, in developing countries, risks come from the uncertainties in both modernization and modernity (Zhang, 2012). As an emerging technology, network is produced by human beings for the pursuit of modernity. The development of the cyberspace is the precondition for cyber modernization. Therefore, development of network technology and the emerging of cyberspace are the important activities as well as the important process in promoting modernization. Accompanied with the modernization, these real activities' conversing to cyber virtual space may have huge risks:

(1) Contradiction conversion. Problems and disputes in reality can be conversed to problems and disputes in cyberspace through the spreading of the information on network. Small disputes can be conversed to big disputes; big disputes can be conversed to small disputes; no disputes can be conversed to disputes; existing disputes can be conversed to no disputes. The results of these conversions can be influenced by many factors, which make it uncontrollable.

(2) Multiple personality. Personalities in cyberspace and reality may show different characteristics. Some personalities, which cannot fully express themselves in reality, can present fully in cyberspace. If such expression develops toward an unhealthy way, split personality may occur.

(3) Defect avoidance. There's no perfect man in reality, while it is just the opposite in cyberspace. In reality, some individuals pursue perfection, trying to avoid their defects in reality. For this reason, these people become enthusiasm in role-playing online. Such conversion from reality to cyberspace brings public risks.

(4) Information leakage. Personal information in real lives may be exposed to the public through spreading in cyberspace. Information may be made with various purposes, to make individuals face risks.

Multiplied Uncertainties: Three Possibilities of Failure in Orders in Cyberspace

China is in the critical period of social transformation. Social problems' conversion between real and virtual space has dual risks. Hence, establishing effective orders of cyberspace and avoiding the public risks are the top priority of current leadership. However, due to the uncertainties in cyberspace, current orders are not

fully effective.

Public Risks Brought by Insufficient Information

Insufficient information refers to the lack of information. Insufficient information's influence on orders in cyberspace is mainly reflected in following aspects:

First, insufficient information may lead to collective unconscious behaviors. In cyberspace which is lack of information, people may simply follow the mainstream instead of thinking themselves. In such a case, they may do some unconscious behaviors and even cause the public risks.

Second, insufficient information may lead to possible loophole in cyber regulatory. Effective regulation in cyberspace depends on plenty of reliable and true information. Insufficient information will easily bring out loophole such as drug sales through Internet. Sellers communicate with each other and advertise through Internet which is secret and uneasy to be exposed. Because of the insufficient information of the policy, some trade, which cannot be accomplished in reality, can be finished in virtual space.

Third, insufficient information will make the decisions rely on ex-post facto result. Against the backdrop of insufficient information, policy makers have two choices in most of the times—make immediately decisions and shoulder the risks, or delay times and make decisions later relying on ex-post facto result. Because of the exaggerating role of the Internet (Zhang, 2011), many governments are likely to choose the latter, so as to reduce the risks in online public opinion.

Public Risks Brought by Information Surplus

Currently, the world is in an era of information explosion. The failure of many decisions does not root from lack of information but the information surplus. According to Wu (2009), "Uncertainties have direct connection with social orders. The more uncertainties exist, the worse of the social orders" (p. 92). Information surplus is among the contributions to the uncertainties, which may affect the orders in cyberspace in three aspects:

First, information surplus makes the cyberspace more "virtual". In fact, most of the times, only a few descriptions on a fact are true and critical while there are too many descriptions online, the role of most of which is just repeating and stressing.

Second, information surplus leads to false information in cyberspace. The risks in information surplus do not exist in the information itself, but some false information may integrate into huge amount of information. In some occasions, such false information meets the needs of people with contradictions, which make these false information mainstreams and spread online. Public risks in society will be increased then.

Third, information surplus leads to chaos online. Effective regulation should be based on some frameworks. However, according to He (2012), "the development of the Internet breaks the technological and institutional limitations in public fields" (p. 99). Especially with the increasing of the information brought by the Internet, old management model has been broken. Against this backdrop, until the successful establishment of new regulations on current cyberspace, information will be quite chaotic in cyberspace which has not enough institutional restrictions now.

Public Risks Brought by Information Distortion

Unlike traditional paper or media, Internet allows the spreading of both true and false information with no controlling on the quality of the information; therefore, true information could be out of control (Katz, 1998). At this time, true information will be distorted. There are two reasons contributed to this: the first reason is that

subjectively, some people make use of the cyberspace to spread false information with ulterior motives. The second reason is that objectively, information lacks fidelity in its spreading process. No matter for subjective or objective reason, the distortion of the information will increase public risks.

Information distortion may undermine the orders in cyberspace. Firstly, information distortion may lead to social unrest. Because of the unknown truth, some people may be inducted and have negative sentiments, which may cause unrests. Secondly, because there are huge amount of groups of people on Internet, real events may be made use of and distorted by some ill-wishers. Under such circumstance, information distortion will lead to the intensification of the contradictions. Thirdly, information distortion may lead to the lack of honesty in society. As long as there is too much false information online, mutual trust in the society will be affected. Also, some information has been distorted to misunderstand the governmental behaviors, uncertainties will be multiplied and the image of the government will be undermined then (Diao, 2001).

Strengthening and Controlling the Risks in Disordered Cyberspace

Lack of information, information surplus, and information distortion have increased uncertainties in cyberspace, which also brings risks in orders in cyberspace. Current cyberspace has already been in a disordered condition. Factors, including technological controlling, legal controlling, made orders, and multiple equilibriums, further intensify the public risks.

Limitations of Technological and Legal Controlling

Regulations and controlling on cyberspace are quite different from them in reality. However, most of the times, governments tend to view them as the same. There are two defects in such action: firstly, the network technology is a double-edged sword. To some extent it can play a role as orders to avoid risks while sometimes it may also bring convenience to the disorder in cyberspace. It is without doubt that many problems in cyberspace are caused by the development of network technology itself (Kochanowicz, 2005). Secondly, the update circle of the network technology is decreasing and the environment of the cyberspace becomes increasingly complex. Current regulatory technology cannot keep step with the demands of the development of the cyberspace. Therefore, it is difficult to regulate and control the cyberspace through aged technological framework.

Besides technological controlling, governments also have legal controlling through the rule of law. To some extent, legal controlling can play a role in avoiding and preventing the problems in cyberspace from happening. However, because the cyberspace is a virtual space without center, boundary, or time limitation, it will be quite difficult for traditional legal controlling to cover every aspect in cyberspace. Many problems caused by the interconversion between virtual and real space cannot be resolved by traditional legal controlling. In this regard, legal controlling has some defects: firstly, the cost of the legal controlling will increase dramatically with the increasing of the complexity in cyberspace. To deal with various kinds of activities in cyberspace, legal controlling should try to cover most of the aspects, which will make it bloated. Secondly, many social activities are just on the boundary between legal and illegal definition. Thirdly, concealment in cyberspace provided convenience to illegal activities. Fourthly, in some occasions, members of a group have some tendency at first, and then after discussion, the whole group moves toward an extreme direction. Such phenomena cannot be simply resolved by legal controlling.

Confusion in Spontaneous Orders and Made Orders

Spontaneous orders in cyberspace refer to operation orders which can maintain the self-regulation, interrelated communication, and interdependence of cyberspace. Made orders in cyberspace are the sum of people's purposeful activities with the goals of maintaining harmonious and ordered cyberspace. However, the orders in cyberspace are attacked by people all the time (Wei, 2000). Hence, spontaneous orders in cyberspace always become out of control and the made orders are also easy to be out of function.

For the first reason, the target of the cyberspace is not very clear, which leads to too many made orders. Cyberspace is a rather more multicenter space than a no-center one in regard of orders, which makes the made orders relatively orderless.

For the second reason, the orders in cyberspace are in alienation with the changes in time and space. Free orders do not necessarily lead to free homeland; it may be alienated to freedoms' shackles (Bai, 2009). The purpose of the orders in cyberspace is clearing the environment of the cyberspace. But in reality, things do not turn out the way people expect.

For the third reason, the static structure of the orders in cyberspace makes it lack of flexibility. As long as an order in cyberspace has been established, it would become regular and static. However, such static structure cannot fit the flexible cyberspace.

Multiple Equilibrium and Liquidity of the Orders in Cyberspace

Envisioning that some peasants have their lands near a lake, like Figure 1, because of lack of arable land, peasants want to cut down trees in other lands. Soil erosion will take place only when trees in two neighboring lands are cut together. So there are three equilibriums here, each of equilibriums can be achieved when only one of the two neighboring lands is cut. Similarly, equilibriums in orders of the cyberspace are also necessary.



Figure 1. Multiple equilibriumin cyberspace.

In the meantime, the vulnerability in the equilibriums can also be reflected in Figure 1. As long as a part of the whole violates the rules, the unhealthy results will take place. Hence the equilibriums in orders of the cyberspace are very hard to be achieved; they can only be maintained by mobility in orders of the cyberspace. Firstly, cyberspace reflects the real space and hotspots in cyberspace are always hotspots in real life. Hotspots are likely to hide public risks. Hence, the mobility will be useful in regulating the public opinion in cyberspace.

Secondly, mobility can be helpful in knowing the values of the online activities. The degree of activities of the online forums and websites can reposition the values. Thirdly, mobility can be helpful in perceiving the moving direction of the interests, so as to regulate the public risks in cyberspace. Fourthly, mobility can be useful in testing governmental influence in different fields. However, after all, relying on mobility of the orders in cyberspace can just provide a temporary solution. The key to the problems is the integration of the multiple equilibriums.

Avoiding the Risks: Reconstruct the Orders in Cyberspace

Interconversion between cyber and real space brings out many risks. To reduce and avoid these risks, governments should respect the spontaneous orders and reestablish the made orders. According to the logic of the interconversion between the two spaces, the reconstruction of the orders in cyberspace should be carried out through three paths: from virtual to real space, from real to virtual space, and from virtual to virtual space.

Orders Reconstruction From Virtual Space to Real Space: Cyber Accountability Mechanism

Risks are the crisis in incubation period. To prevent contradictions from becoming crisis, a proper contradiction dredging mechanism should be established. The cyber accountability mechanism should play a dredging role in cyberspace. Contradictions' conversion from virtual space to real space originated from the lack of effective channel to deal with existing contradictions. Avoiding the public risks in cyberspace should have the thoughts of risks controlling, or the orders in cyberspace will be easily alienated. Orders in cyberspace should service the public interests. The cyber accountability mechanism could maintain public interests; it could also be helpful in promoting the demands of expression of contradictions and interests and avoiding the public risks. Therefore, only under this precondition, the orders in cyberspace can be reconstructed.

Such accountability mechanisms should be responsible to the governments, beyond the accountability of governments and including online political affairs. Also, accountability mechanisms should be diversified, so as to ease the contradictions in various fields.

Orders Reconstruction From Real Space to Virtual Space: Effective Response Mechanism

Voices in virtual space should be responded by the reality. Effective response is in essence a kind of soft controlling; it can play a role in maintaining orders in cyberspace and reducing the public risks. In its spreading process, information may be distorted, expanded, narrowed, and alienated. Without effective dredging in information's conversion from real space to virtual space, accumulated contradictions may break out when it reaches to a certain extent, and then public crisis will take place. Therefore, effective response mechanism is an important part in orders of cyberspace.

Effective response mechanism should have several meanings: Firstly, it should include the governmental response mechanism. Governments' role in orders of cyberspace is quite special. Their response to cyberspace reflects governments' social functions as well as their social responsibility for the society. Secondly, main bodies of the effective response mechanism should be diversified. With the change of the cyber environment, the connotation of the response mechanism should also expand. Thirdly, the key factors of the effective response to the voices in cyberspace, can the public risks be avoided.

Orders Reconstruction From Virtual Space to Virtual Space: Space Governance Mechanism

CONTROLLING OF THE PUBLIC RISKS IN CYBERSPACE

The basic ideas of governance are principles of participation, publicity, transparency, response, equality, responsibility, and legality (Sun, 2004). Governance in cyberspace should also follow similar principles. During the governance in cyberspace, main bodies in cyberspace orders should actively participate in and respond to the governance, the information of governance should be disclosed, the result of the governance should be equal, and main bodies should take the initiative to shoulder the responsibilities. Virtual space is the reflection of real space. Coordination and cooperation in virtual space can avoid contradictions and reduce public risks in cyberspace.

Just the same as in response mechanism, main bodies in space governance mechanism should also be diversified. Although the contradictions in cyberspace originated from real space, they are much more complex than them in real space. Hence, governance in cyberspace should make bodies in various fields joint together to achieve diverse collaborative governance.

Public risks in cyberspace are derived by the conversions not only from the real to virtual space, but also from the virtual to real space. The uncertainties caused by these conversions doom that the governance in cyberspace calls for long-term efforts. Cultural construction can be an important guarantee to the cyberspace governance. In such a case, we should guide the development of the culture in cyberspace toward a positive and healthy direction, so as to maintain the sustainable and coordinated development of the cyberspace governance and reduce the public risks in it.

Conclusion

Based on the analysis above, orders in cyberspace are important means of avoiding the dual risks in public risks. However, there are two important aspects that undermine the effectiveness of cyber orders: (1) Three uncertainties—lack of information, information surplus, and information distortion, are superimposed in orders. (2) Problems in current cyberspace, such as technology controlling, legal controlling, and made orders, restrict the further improvement of the orders. In such a case, orders in cyberspace should be reconstructed by establishing cyber accountability mechanism, effective response mechanism, and space governance mechanism. Then the risks existing in the interconversion between the virtual space and the real space can be reduced to a large extent.

References

- Adam, B., Beck, U., & Loon, J. V. (Eds). (2005). *The risk society and beyond: Critical issues for social theory*. (Y. D. Zhao & Y. Ma, Trans.). Beijing: Beijing Publishing House.
- Bai, S. Y. (2009). Studies on virtual orders (in Chinese). Study & Exploration, (4).
- Diao, S. F. (2001). Between reality and illusion: Moral controlling on social problems in cyberspace (in Chinese). *Journal of Dialectics of Nature*, (6).
- Huntington, S. P. (1988). Political order in changing societies. (S. P. Li, Trans.). Beijing: Huaxia Publishing House.
- He, X. M. (2012). Functions and prospects: Development of public fields in China's cyberspace (in Chinese). *The Journal of Jiangsu Administration Institute*, (1).

Katz, J. E. (1998). Struggle in cyberspace: Fact and friction on the World Wide Web. *American Academy of Political and Social Science*, (560), 194-199.

Kochanowicz, J. (2005). Trust, confidence, and social capital in Poland: A historical perspective. In B. Rothestein (Ed.), *Social traps and the problem of trust* (pp. 63-83). Cambridge, UK: Cambridge University Press.

Sun, B. Y. (2004). Porary local governance: Challenges to the 21st century (in Chinese). Beijing: China Renmin University Press.

Zhang, H. B. (2012). Governance on public risks: Theoretical model and practical path (in Chinese). Beijing: Social Sciences

CONTROLLING OF THE PUBLIC RISKS IN CYBERSPACE

Academic Press.

Zhang, Y. L. (2011). Current situation of online public opinion and guidance of governments (in Chinese). *People Forum*, (9). Wu, Q. C. (2009). Discussion on public risks brought by "Uncertainties" (in Chinese). *Journal of Zhengzhou University*, (4). Wei, G. F. (2000). Studies on orders in cyberspace (in Chinese). *Journal of Henan University (Social Science)*, (6).