A Three-Perspective Theory of Cyber Sovereignty

By Hao Yeli

The cybercrime and cyber terrorism raging today are the most visible symptoms of a more pervasive problem concerning cyber security. How to establish a fair and just governance regime in cyberspace and establish international rules spark a storm of controversy. The controversy reflects the competing interests and demands of three distinct cyberspace actors: the state, the citizen, and the international community. By focusing only on one's own interests, each actor ignores the interests of the other two, resulting in the current situation in which each sticks to its own argument and refuses to reconcile. The establishment of a new order in cyberspace requires a comprehensive review from the perspective of all three major actors. This article proposes a "three-perspectives" theory based on the three actors. It divides cyberspace into three levels; the base level, the application level, and the core level. Treating each level differently, it seeks to identify the largest common ground, and transcends the single perspective vulnerability of interpreting everything in terms of binary opposition. Three-perspective thinking makes it possible to deal with the binary opposition of exclusivity and transferability with respect to state sovereignty.

Three Disputes Over Cyber Sovereignty

Cybersecurity has emerged as a global challenge and is becoming a tier one security threat for sovereign states. Heated debate rages in international forums concerning the rules of cyberspace, and the systemic and revolutionary challenges to global governance in cyberspace. Cyber sovereignty has inevitably become the focus of great controversy. Although a certain degree of consensus was originally achieved by the Information Security Group of Governmental Experts (GGE) of the United Nations, deep differences and doubts continue to divide the international community, particularly with respect to three issues.

First, the contradiction between cyber sovereignty and the spirit of the internet; the exclusivity of classical state sovereignty runs contrary to the spirit of the internet, which rests on the concept of unrestricted interconnectivity. If the emphasis is placed on cyber sovereignty, this may cause each country to set up a separate cyberspace of its own, thus resulting in the fragmentation of the internet.

Major General Hao Yeli, Chinese People's Liberation Army (ret.), is a senior advisor at the China International Institute for Strategic Society and a senior advisor at the China Institute for Innovation and Development Strategy.

Second, the contradiction between cyber sovereignty and human rights. This reflects the tension between the internet principle of freedom of speech, and state intervention in the name of cyber sovereignty, which restricts the free flow of information. Such criticism mostly targets the establishment of internet firewalls in China.

The third is the contradiction between cyber sovereignty and involvement of multiple stakeholders in governance. It is argued that cyber sovereignty will provoke controversy on the pattern of internet governance; that is, sovereign government-led governance will challenge the existing pattern of multi-party governance.

The concept of cyber sovereignty plays an important role in establishing the international rules of cyberspace. This is the root of the problem tree and the source of other problems. To clarify and resolve the differences, and to achieve international consensus and cooperation on these issues, are the challenges for the international community in the cyber domain.

The key is to adapt the traditional sovereignty concept to the globalized world in the cyberspace era with a more scientific approach and understanding of the controversies, in order to achieve the greatest common denominator and greatest acceptance by the international community. I am indebted to my Chinese and foreign friends and colleagues who participated in various international dual track dialogues—e.g. Sino–United States, Sino–Russia, and Sino–Europe—who gave me inspiration and insights into diverse perspectives. Even the most complicated problems can be solved with the correct approach. That encouraged me to build an objective theoretical framework and dialectical approach to clarifying and resolving contradictions.

Three Perspective Theory

In-depth analysis of these three major contradictions reveals the interests and demands of three main cyberspace actors: the nation-state, the citizen, and the international community. Focusing only on its own interests, each actor routinely ignores those of the other two, which has led us to the current situation, a situation in which compromise and reconciliation are difficult to achieve.

The actors behind the contradiction of cyber sovereignty and the spirit of the internet are the state and the international community. Behind the contradiction of cyber sovereignty and human rights are the state and the citizen. The contradiction of cyber sovereignty and multi-stakeholder governance involves the state, the citizen, and the international community.

Zero-sum games based on binary opposition usually lead to deadlock or the less than satisfactory outcome where "one succeeds, while all others sacrifice." Today's doubts and questions in the international community are the result of unilateral logic, one-way thinking, and viewing problems from a single perspective. When seeing things from one point of view, while ignoring the other two, one may tend to draw intractable conclusions that are either absolute or radical. We must transcend the single point myth and binary opposition, recognize a higher, holographic dimension, and adopt three-perspective thinking. To better understand the concept of the three actors and three perspectives in cyberspace envision a dark space with three lamps: lighting a single lamp enables us to see a point; two lamps reveal a flat, two dimensional surface; whereas, three lamps enable us to see the three dimensional whole. With three-perspective thinking, we can envision a more realistic cyberspace, where the roles and demands of each actor, as well as their internal relations and mutual impacts, converge to form a unity of diverse and contradictory opposites.

Theoretical Framework of the Three-Perspective Construct

In mathematics we always set boundary conditions in order to solve a multiple-equation problems ($n>x>0$). The variable is neither infinite nor

infinitesimal when solving the equation in a range. The significance of the three-perspective construct is that we can set three boundary conditions from the perspective of three actors, which is more inclusive. It forms a stable triangle and co-viewing area to make effective dialogue to seek common ground, thus making the problem convergent, and focused to avoid one dimensional thinking that may easily lead to a "fire and forget" attitude.

Traditional and substantial national sovereignty implies natural exclusivity. It emphasizes the supreme authority internally, and stresses the inviolable independence externally, of the sovereign state. Because of the openness and global nature of cyberspace, however, the voices of the other two actors must be heard. When speaking of national sovereignty in this context, it is necessary to expand the perspectives of the international community and the citizen.

The citizen (or netizen in this case) pursues personal freedom. Today, the total number of netizens has reached 3.2 billion globally; in China alone the figure reaches 710 million. While also citizens of states and of the international community, it is in the nature of netizenship to pursue individual net freedom. In this disorderly environment, however, the fact is that individual self-governance based on self-discipline will not work, and freedom sought will have no guarantor. To ensure the freedom of every netizen, it is necessary to impose order so that cyberspace is bound and governed by the law. The establishment and formation of order requires external forces, as well as the establishment of rules at national or governmental levels to administer cyberspace and protect the legitimate rights and interests of netizens. Technology itself does not provide order nor security, so it needs sovereignty to provide appropriate legal protection.

The state pursues national security and development. A state has to ensure its safety while seeking development, and likewise must manage cyberspace while making use of it. At this point, the relationship between state and citizen is actually not antagonistic, but interdependent. In his speech on April 19th, 2017, Peoples Republic of China President Xi Jinping put it well when he said, "Cyberspace is people-centered. We should make the internet better benefit the people. The people on the internet equal public opinions on the internet. Our leading cadres go where the masses are; they must learn to follow the mass line through cyberspace and respond positively to the concerns and doubts of netizens." In China, we used to say that the party branch is organized on a company basis, but now, the regime must be built on the internet. We must listen to the voice of the people online, understand public opinion, pool their wisdom, and guide democracy; all of these reflect the intentions of the ruling Party. In the same way, the freedom and vigor of the internet will bring prosperity and national development.

The international community seeks openness and inclusiveness in cyberspace. The internet represents the mainstream of technological development, and a profound development of civilization. The international community must seek openness and inclusiveness, because there exist in the world not only competitions between the major powers, but also a collision of Eastern and Western cultures. Moreover, due consideration must be given to balancing the benefits of globalization and the digital revolution between the developed and developing countries.

The exclusiveness of national sovereignty and the openness of the international community while seemingly in conflict, can be reconciled and balanced in reality. On the one hand, the state must assume responsibility for emancipating minds, changing ideas, and promoting an objective and balanced understanding of the relationship between security and development. Only in this way can the internet work for us, helping us to maximize benefits while avoiding harm. A state integrates into the international system by transferring some portion of its national sovereignty, while international

connectivity and interoperability will deliver greater developmental opportunities, promote cultural exchanges, economic cooperation, and collaborative security efforts. The relationship between the state and the international community is one of interdependence, inclusive and transferable, which contributes to the unity of opposites.

On the other hand, from the perspective of the international community, internet technology offers the promise of global interconnectivity. But as long as states exist, it is impossible to ignore national boundaries and national sovereignty. We ought therefore to avoid the excessive pursuit of unregulated openness, in order not to cross a tipping point beyond which global cultural diversity is subordinated to a single dominant culture. Those states with great cyberspace capacity should take the initiative to bridge the digital gap and actively transfer and share cyberspace resources and management experience, restraining their impulse to use asymmetric means in pursuit of narrower and short-term, national interests.

We would all benefit from more conjunction points of interest based on one global network to help all the countries of the world achieve economic growth, cultural prosperity, and security, all consistent with the spiritual essence of the internet: "interconnection and shared governance." Recently in China, certain prescribed terms of the new national antiterrorism law that aroused intense international concern, such as local data storage and interface providing, were deleted from the original draft. This shows that China is seeking to find the correct balance between openness and security.

States need to open up to the international community as they seek national security and development; citizens are in need of procedural safeguards from states in their pursuit of freedom; and the international community must tolerate cultural and national diversity in its pursuit of openness in cyberspace. These multilateral relations, though seemingly opposite and conflicting, are interdependent in reality. Actors cannot always blindly pursue absolute maximization of their own individual interests; they must demonstrate a certain degree of mutual consideration. Only thus will they reach an optimal balance in the triangular co-viewing area described above, existing peacefully in the global village of cyberspace.

In conclusion, the relationship between national development and national security is both a dynamic equilibrium as well as what we in China refer to as a yin and yang duality. Freedom and order, openness and inclusiveness are in fact both static and dynamic balances. The competing demands of these three actors are not in absolute conflict, nor are they absolutely contradictory, though in different contexts they will show a certain degree of antagonism. In the end, what we must all seek is an overall balance within the broadest context, built upon inevitable concessions, a desire for harmony, and acceptance of the principle of the possible unity of opposites. Through the exchange of ideas and the evolution of perspectives, we can resolve contradictions in many cases.

Cyber Sovereignty in the Three-Perspective Model

Although traditional sovereignty is naturally exclusive, cyber sovereignty must accept or at least consider a reasonable transfer of control in the era of globalization. Each state should carefully determine and decide what elements of sovereignty it must retain and what can be transferred, and to what extent. Let us further examine and analyze the concept of transferring partial sovereignty on the basis of the three-perspective model.

It is an uncontroversial fact that the debate on cyber sovereignty has been over whether or not sovereignty in cyberspace should be an extension of traditional sovereignty. Cyberspace has already become the fifth domain of conflict after land, sea, air, and space. The United States and NATO have

both defined cyberspace as a battle domain and have created cyber combat troops. Although there are different formulations of cyber sovereignty, countries still regulate their own cyberspace to protect against external interference and damage without exception at a practical level. This reflects the recognition of practical cyber sovereignty requirements. Differences are not over whether or not we practice cyber sovereignty, but over which sectors cyber sovereignty will cover; in colloquial terms, will sovereignty cover the area "above or below the neck?" States have different "pain spots" concerning cyber sovereignty, and the international community must respect and understand the different concerns of states.

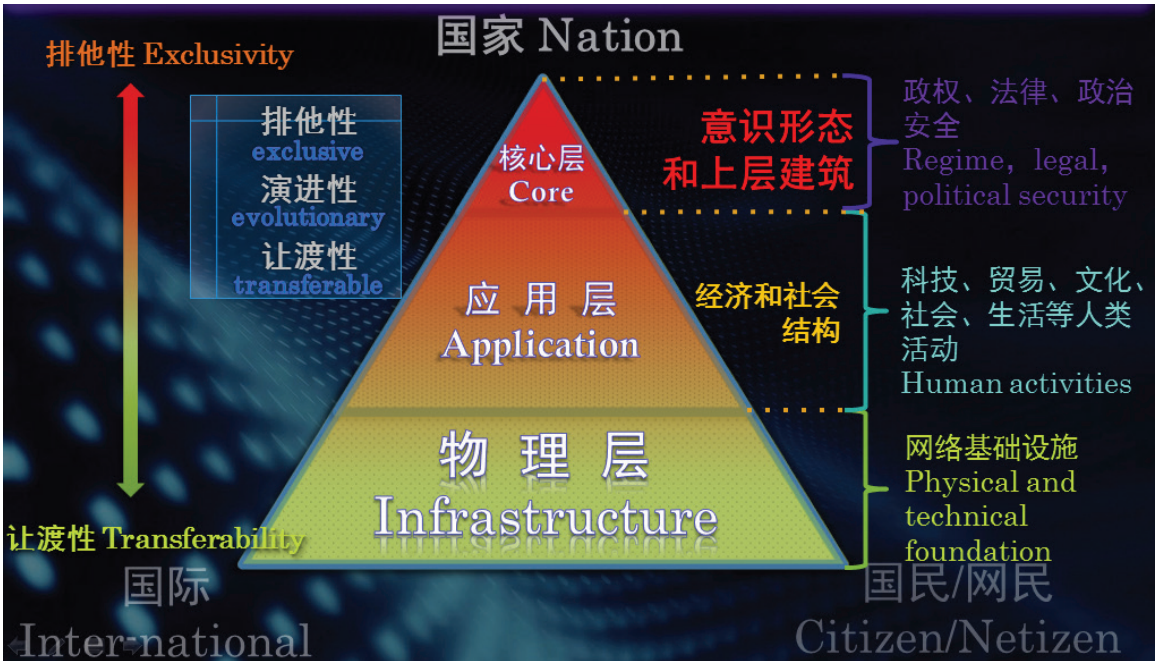
The key is to examine the divisibility of cyber sovereignty using a layered approach, and identify which elements of sovereignty must remain exclusive, and which are transferable.

In Figure 1 the lowest level, or the physical level, represents cyberspace infrastructure. The key at this level is the pursuit of standardization in global cyberspace and interconnectivity. At this level states should be willing to collectively transfer authority in the interest of standardization and interconnectivity. States with well-developed cyber capacity must take the initiative to extend standardization and connectivity to the less capable states; developed countries must export their achievements to developing countries to bridge the digital divide.

The middle level in the figure above represents the application level, and includes the many internet platforms and internet carriers in the real world that have integrated such different sectors as technology, culture, economy, trade, and other aspects of daily life. At this level, the degree of cyber sovereignty should be adapted to local conditions, with the aim to achieve dynamic equilibrium, multilateral, and multi-party joint administration, as well as balance between freedom and order.

The top or core level comprises regime, law, political security, and ideology, which is unchallengeable and includes the governing foundations and embodies the core interests of the country. Due to unique national

FIGURE 1: A Layered Approach to Cyber Sovereignty.



conditions, religious, and cultural backgrounds, legitimate differences do exist between states. Diversity is the norm of human existence which cannot be formatted according to any single culture. Differences and diversity should be tolerated. You may not agree with a country's social system and ideology, but you should understand its national conditions, respect its existence, and tolerate its differences.

It is clear that at the middle and bottom levels of the triangle, cyber sovereignty can be transferred to a certain degree, allowing a greater number of stakeholders to participate in governance, leading to a multi-stakeholder governance model. At the top level the emphasis remains on the leading role of the government. According to the consensus affirmed by the GGE "the right to make public policy on internet is part of a country's sovereign role, and each country naturally has judicial power over the information conveyed by the domestic information infrastructure." To respect countries' free choice of cyberspace developmental paths and cyberspace management models is a basic premise for both governmental responsibility and international cooperation.

A comprehensive understanding of these three levels further clarifies the differences between multilateral (meaning driven by state sovereignty) and multi-party governance modes. In fact, the two modes do not conflict; they have different applicability in different areas and levels of cyberspace. With respect to ideology, policy, law, institutional and governmental security issues, national governments will certainly give full play to their leading roles, and fully embrace the advantages of multilateral governance, while accepting multi-party governance at other levels.

Resolving the Contradictions

Earlier we noted the apparent contradiction between cyber sovereignty and the unrestricted spirit of the internet. There is no doubt that we live in "one world, one cyberspace." But exerting limited cyber sovereignty is consistent with the spirit of the internet; indeed cyber sovereignty is the necessary tool to help states participate equally in the global governance of the internet, contributing not only to interconnectivity, but also to shared responsibility.

We also noted the tension between cyber sovereignty and cyberspace freedom. As for setting up internet firewalls, China is forced to do so. Faced with the deteriorating security situation in cyberspace and the severe challenges posed by so-called color revolutions to developing countries that lack strong cyber capability, no country can remain indifferent to the real threats originating in cyberspace. We would not expect any country facing the everyday threat of terrorist attacks to dissolve its armed forces. Likewise, we oppose any cyberspace power taking advantage of its national capability to traverse the firewalls put in place by other countries. As the cyberspace security situation improves, and with the deepening of mutual trust, maturity of democracy, and the development of technology, China will continue to improve its accuracy in blocking harmful information and scale down the firewall. As we can see, the top level covers the smallest area, and excessive expansion of or preoccupation with the top level is not conducive to achieving consensus on cyber sovereignty among parties, which remains our ultimate objective.

With respect to the tension between multilateral and multi-party governance in cyberspace, advocating cyber sovereignty does not imply rejection of the multi-party or multi-stakeholder governance model. Governments are also among the multiple stakeholders; they should play appropriate roles in multi-party governance, but also respect and encourage other entities to participate in governance, including enterprises, communities, experts, and think tanks, taking advantage of their professional and technical contributions. Collectively we should prevent any stakeholder from excluding the participation of governments, or denying governments' appropriate

role in key issues. At the core and application levels, the leading role of state governments must be ensured. When dealing with ideological, political, legal, institutional, and security issues the state role must be respected. For instance, the United States and Europe published the EU–United States Privacy Shield Agreement this year to eventually replace the abolished Safe Harbor Agreement, due to the Snowden leaks. The new agreement reflects in essence the implication of cyber sovereignty; meanwhile, it is the actual law practice in maintaining cyber sovereignty under the guidance of the government, which deserves our research and study. It is indisputable that government is the decisive pan-balance star in both international and domestic events. The government must act fast before it is too late. It is unavoidable that the government must assume responsibility and decide when to let go or to control.

The above analysis can be summarized as follows: in the cyberspace era, with the pervasive emergence of globalization, cyber sovereignty is divisible. The core level is inviolably exclusive, while the physical and the application levels are characterized by open and shared transferability. While challenging the core interests of sovereign states by abusing internet connectivity should be prohibited, shaking the foundation of the internet by imposing traditional sovereign exclusivity should also be prohibited. The proportion of sovereign transferability to exclusivity is flexible and ever changing, up to whether or not cyber sovereignty will be respected in the international rules.

Conclusion

Based on the principles of modern international jurisprudence, cyber sovereignty should reflect national rights and responsibilities. No state or government that is responsible and conscientious will ignore the development and security of this new domain. Nor should it reject or obstruct any other countries' reasonable demands concerning sovereignty and global co-governance. Respect for cyber sovereignty is a prerequisite for international cooperation in this domain, and the basis for the construction of a beneficial cyberspace order.

Against the background of globalization and the internet era, the emerging cyber sovereignty concept calls for breaking through the limitations of physical space and avoiding misunderstandings based on perceptions of binary opposition. Reinforcing a cyberspace community with a common destiny, it reconciles the tension between exclusivity and transferability, leading to a comprehensive perspective. China insists on its cyber sovereignty, meanwhile, it transfers segments of its cyber sovereignty reasonably. China rightly attaches importance to its national security, meanwhile, it promotes international cooperation and open development.

China has never been opposed to multi-party governance when appropriate, but rejects the denial of government's proper role and responsibilities with respect to major issues. The multilateral and multi-party models are complementary rather than exclusive. Governments and multi-stakeholders can play different leading roles at the different levels of cyberspace.

In the internet era, the law of the jungle should give way to solidarity and shared responsibilities. Restricted connections should give way to openness and sharing. Intolerance should be replaced by understanding. And unilateral values should yield to respect for differences while recognizing the importance of diversity. PRISM

Photos

Page 108: Wikimedia/O01326. Licensed under Creative Commons Attribution-Share Alike 4.0 International <https://creativecommons.org/licenses/by-sa/4.0/>. Photo unaltered.