I am honored to introduce a very unique addition to the Security Roundtable website. The following paper was written by my former counterpart from China when I was working at the Pentagon as the Acting Deputy Assistant Secretary of Defense for Cyber Policy and the Senior Military Cyber Advisor, from 2012-2015.

Major General Hao Ye Li served in the Peoples’ Liberation Army when I served on active duty in the U.S. Army. She has since retired from active duty and serves as the Vice Chairman of the China Institute for Innovation and Development Studies. She also serves as an advisor to the China Institute for Strategic Studies, and in this capacity she wrote this paper providing her views about cyber sovereignty.

General Hao’s paper reflects an evolution in China’s thinking about the topic of sovereignty as it applies to cyberspace. She describes a modern view of cyberspace from three perspectives: the nation, the citizens, and the international community. She argues that each of these perspectives is critical to avoiding a “single point myth or binary opposition.” In other words, she argues for a more inclusive view of the multiple parties and stakeholders involved in the cyberspace environment.

She also describes the layers of cyberspace using a triangle that connects the perspectives of nations, citizens, and the international community. The base layer of the triangle is the infrastructure that comprises cyberspace. On top of that rides the application layer which is used by each of the three perspectives. Finally, the smallest, top layer of the triangle is the core interests, which applies to the nation perspective.

This is a view which indicates something I found fascinating and important about the evolving view of sovereignty from General Hao’s perspective ... that a nation’s core interests and control over the cyber environment has significant limits and must be balanced with the interests of the international community and individual citizens. Hao’s thought leadership in this regard is contributing to a much more inclusive, balanced and stable description of cyber sovereignty and I believe this is a much more realistic direction in thought than I had ever experienced in all of my previous interactions with China while serving in the military and government.

Critically, I do think there is something that should be added to General Hao’s description and triangle diagram. In my view, the “glue” that connects each of the three perspectives and each layer (although possibly less so the core interests layer) is represented by the global private sector. I would respectfully submit for consideration the addition of this aspect to General Hao’s model, and I encourage a continuing evolution toward a more inclusive, flexible and participatory view of sovereignty as it applies to cyberspace.

This introduction represents my personal views about General Hao’s paper, and is not a reflection of any endorsements from Palo Alto Networks.

John A. Davis
Major General, U.S. Army (Retired)
Vice President, Chief Security Officer (Federal)
Palo Alto Networks
Unity of Opposites in Cyber Sovereignty as per Three-Perspective Theory
Unity of Opposites in Cyber Sovereignty as per Three-Perspective Theory

Hao Yeli

[Abstract] Currently, cybercrime and cyber terrorism are raging, with numerous problems concerning cyber security. How to conduct global cyberspace governance and establish a fair and just international rule sparks off a storm of controversy. Essentially, it reflects the interest demands of three international cyberspace actors: nation, citizen and international community. Focusing only on one's own, each actor always ignores the interests of the other two, thus results in current situation in which each one sticks to its own argument and refuses to reconcile. The establishment of new order in cyberspace requires comprehensive review from the perspective of all three major actors. “Three-Perspective” theory bases itself on “three points”: nation, international community and citizen, which in turn gives birth to three boundary conditions. In a stable triangle area of common view, it divides the cyberspace into “three levels”: the base level, the application level and the core level. Treat each level differently, it tries to seek for the largest common ground, and thus jumps out of single point myth or binary opposition. Viewing from the dimension of cyberspace community of common destiny, “Three-Perspective” thinking makes it possible to deal with the binary opposition of exclusivity and transferability scientifically from a looking-down perspective.

I. Three major focuses of the international community on the disputed cyber sovereignty

Cyberspace security has become a global challenge and is on the rise to become the top security threat for the sovereign states. Countries conduct heated debate on the international rules and the system revolution of global governance in cyberspace, while cyber sovereignty undoubtedly becomes the focus of controversy. Although it has received certain degree of approval from “Information Security Group of Governmental Experts of the United Nations”, the international community still has deep differences and doubts on this issue, which mainly focus on the following three aspects:

First, the contradiction between cyber sovereignty and the spirit of the Internet. The idea is that the exclusivity of sovereignty runs contrary to the spirit of the Internet, i.e. interconnection. If the emphasis is placed on cyber sovereignty, each country may try to set up the cyberspace of its own, thus result in the fragmentation of the Internet.

Second, the contradiction between cyber sovereignty and human rights. The thought suggests that the Internet should support freedom of speech, but the intervention in name of cyber sovereignty prevents the free flow of information. Such criticism mostly targets the establishment of Internet firewall in China.

The third is the contradiction between cyber sovereignty and involvement of multi-stakeholders. It is said that the cyber sovereignty will provoke the controversy on the pattern of Internet governance, i.e. government-led multilateral governance pattern will challenge the existing pattern of multi-party governance.

It can be seen that cyber sovereignty plays an important role in establishing the international rules of cyberspace, which is the root of the problem tree and the source of other problems. To clarify the difference and to achieve the consensus are the basis for international cooperation on this issue.

For the concept of traditional sovereignty, the problem is how to obtain the greatest common divisor and acceptance in the era of globalization of cyberspace with a more scientific connotation
We should create more conjunction points of interest on the basis of the global cyberspace to help the countries all of the world achieve economic boom, cultural prosperity and security, which is in agreement with the spiritual essence of the Internet: "interconnection and shared governance." Recently, Chinese antiterrorism law deleted some prescribed terms in the original draft that aroused intense international concern, such as local data storage and interface providing. This shows that China is making necessary transfer between openness and security.

Nations need to open to the international community when they seek national security and development; citizens are in need of procedural safeguards from the nations in the time of freedom pursuit; the international community needs culture diversity to tolerate different nations when it seeks openness. These multilateral relations are uniform and interdependent in reality although seemingly opposite and contradictory. Actors can not always blindly pursue the maximization and absolutization of their own interests; they need certain degree of mutual "transfer". They will reach optimal balance in the triangle area of common view, that is, they will seek mutual help on the boat of the global village of cyberspace.

In conclusion, the relationship between development and security is a static and dynamic equilibrium as well as yin and yang equilibrium. Freedom and order, openness and inclusiveness are both static and dynamic balances. In fact, the demands of these three actors are not absolutely conflicting and contradictory, only in different categories will they show certain degree of antagonism. But in the end what we seek is an overall balance under a large pattern with concession and harmony as well as unity of opposites. Along with the change of ideas and the transformation of perspectives, we can resolve contradictions in many cases.

IV. Characteristics of cyber sovereignty as per “Three-Perspective” theory

Although traditional sovereignty is exclusive, cyber sovereignty needs to consider reasonable transfer in the era of globalization. We should measure in mind, and decide when to exclude and when to transfer, and to what extent. I will further analyze and measure the extent on the basis of “Three-Perspective” model.

It is simply a fact without controversy that we used to put the focus of the debate of cyber sovereignty on whether or not cyberspace should obtain sovereignty, that is, the focus is the “evolution” or the “extension” of sovereignty. Cyberspace has already become the fifth territory after the land, ocean, air and sky. President Obama has already defined it as a battle field in his speech and has set up 133 cyber combat troops. Although there are different formulations about cyber sovereignty, countries still regulate their own cyberspaces to protect against external interference and damages without exception at a practical level. These are the practical recognition of cyber sovereignty. Differences rest not in whether or not we will approve cyber sovereignty, but in what field the cyber sovereignty may cover —— or in informal terms, it covers the area above or below the "neck", which reflects that different countries have different pain spot concerning the cyber sovereignty. The international community should respect and understand the different concerns of nations.

Therefore, we believe that the key of the study is to analyze concrete divisibility of cyber sovereignty by means of layered approach, and then find the applicable domain of sovereignty “exclusivity” and “transferability".
Bottom level: The physical level includes cyberspace infrastructure. The key of this level is the pursuit of standardization, global cyberspace and interconnection. Countries should make collective transfer at this level, strong sides must take the initiative to transfer to the vulnerable sides; developed countries must export their achievements to developing countries to bridge the digital divide.

Middle level: The application level includes wide application of Internet platform in the real world, the carriers of Internet have integrated into different human activities, such as technology, culture, economy, trade and other aspects of daily life. At this level, the effect 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.

Top level: The core level comprises regime, law, political security and ideology, which is unchallengeable and involves the ruling foundation, embodies the core interests of the country. Due to the different national condition, religious and cultural background, differences do exist. Cultural diversity is the norm of human existence which can not be formatted by any single culture. We should respect differences and tolerate diversity. You may not agree to a country’s social system and ideology, but you should respect its existence, tolerate its difference and understand its national condition.

It is clear that at the middle and bottom levels of the triangle, the cyber sovereignty can be transferred to a certain degree, which allows more stakeholders to participate in the governance and results in the multi-stakeholder governance model. At the top level the emphasis mainly lays on the leading role of the government —— “the right to make public policy on Internet is part of a country’s sovereign, and each country naturally has judicial power over the information conveyed by domestic information infrastructure”, which is the consensus that affirmed by the Experts Group of United Nations. To respect countries’ free choices of cyberspace developmental paths and cyberspace management models is the basic premise for the governments to assume national responsibility and carry out international cooperation.

Comprehensive understanding of these three levels further clarifies the differences between multilateral and multi-party modes. In fact, the two modes are not conflicting, in stead, they have different applicability in different areas and levels of cyberspace. When it involves ideology, policy, law, institutional and governmental security issues, national governments will certainly
give full play to their leading roles, and fully embody the advantages of multilateral governance.

Based on this theory, we can answer three questions about cyber sovereignty raised earlier.

The first is the question about the contradiction of cyber sovereignty and the spirit of the Internet. Persisting in cyber sovereignty is consistent with the spirit of the Internet. There is no doubt about “One World, One Cyberspace”. The acknowledgement of the “cyber sovereignty” is the foundation to help the countries participate equally in the global governance of the Internet, which contributes to not only interconnection, but also shared governance.

The second is about the differences of cyber sovereignty and cyberspace freedom. As for setting up internet firewall, China is forced to do so. Faced with the deteriorating security situation in cyberspace and the severe challenges of “color revolution”, developing countries without strong cyber confrontation capability can not remain indifferent to the safety of regime. Just like the countries facing everyday threat of terrorist attacks, it is impossible for them to put down anti-terrorism alert and dissolve armed forces. Therefore, we oppose cyberspace powers taking advantage of their national power to traverse other countries’ firewalls. But with the improvement of security situation, deepening of mutual trust, maturity of democracy and the development of technology, we will continue to improve the 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 the top level is not conducive to achieving consensus on cyber sovereignty among parties, which is what we have been constantly researching and improving.

The last is about the doubts on multilateral and multi-party opposition. The advocating of cyber sovereignty aims not to replace the multi-stakeholder governance model. Governments are also among the multiple stakeholders, so they should not only play roles in the multi-party governance, but also respect and encourage enterprises, communities, experts and think tanks to maximize their professional and technical advantages and participate in governance. Whereas, we should prevent it from happening that other stakeholders may exclude the participation of governments and deny their leading role in key issues. At the core level and application level, the leading role of the national government must be ensured, and the advantages of multilateral governance must be fully revealed when dealing with ideological, political, legal, institutional and security issues. For instance, the U.S. and Europe published “EU-U.S. Privacy Shield Agreement” this year to replace eventually the abolished “Safe Harbor Agreement” due to Snowden leaks. The new agreement reflects in essence the implication of cyber sovereignty; meanwhile, it is the actual law practice in maintaining the 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 the international and domestic events. The government must act fast before it’s too late. It is unavoidable for the government to assume the responsibility and decide when to let go or to control.

According to above analysis, the unity of opposites in cyber sovereignty as per the “Three-Perspective” theory can be summarized as follows: In the era of cyberspace with in-depth development of globalization, cyber sovereignty is divisible. Firstly, the core level is inviolably exclusive. Secondly, the physical level and the application level are characterized by open and shared transferability. On the one hand, it should be prohibited to challenge the core interests of sovereignty by abusing Internet connectivity; on the other hand, it should also be prohibited to
Unity of Opposites in Cyber Sovereignty as per Three-Perspective Theory

shake the foundation of the World Wide Web by abusing traditional sovereign exclusivity. The proportion of transferability and exclusivity is flexible and ever changing, up to whether or not cyber sovereignty will be respected in the international rules.

V. Conclusion

To begin with, taking root in modern jurisprudence, cyber sovereignty is a comprehensive reflection of national rights and responsibilities. No nation or government that is responsible and conscientious will ignore the development and security of the new space, nor will reject and obstruct other countries’ reasonable demands concerning sovereignty and global co-governance. To respect “cyber sovereignty” is a prerequisite for international cooperation and the basis for the construction of good order.

Next, under the background of globalization and the Internet era, the new “cyber sovereignty view” calls for breaking through the limitations of physical space and avoiding the misunderstanding of binary opposition. Standing on the dimension of cyberspace community of common destiny, it masters scientifically the unity of opposites of exclusivity and transferability in a comprehensive perspective. China insists on cyber sovereignty, meanwhile, it transfers cyber sovereignty reasonably. China attaches importance to national security, meanwhile, it promotes international cooperation and open development.

Thirdly, China has never opposed to multi-governance, but we must avoid the exclusion of government’s role and responsibilities in major issues. Multilateral pattern and multi-party pattern are complementary rather than exclusive. Governments and multi-stakeholders can play different leading roles at the different levels of cyberspace.

Finally, in the Internet era, the law of the jungle should transfer to solidarity and shared hardships. Inhibition of movements should give way to openness and sharing. Intolerance should be replaced by symbiotic relationship. Focused value should make concession to the respect of differences and the inclusiveness of diversity.