Policy Recommendation for South Korea's Middle Power Diplomacy: Cyber Security

Sangbae Kim
Seoul National University

March 2015

EAI MPDI Policy Recommendation Working Paper

Knowledge-Net for a Better World

East Asia Institute(EAI) is a nonprofit and independent
research organization in Korea, founded in May 2002.
EAI strives to transform East Asia into a society of nations based on
liberal democracy, market economy, open society, and peace.

ISBN 979-11-86226-18-6 95340

East Asia Institute
#909 Sampoong B/D, Eulji-ro 158
Jung-gu, Seoul 100-786
Republic of Korea
Tel 82 2 2277 1683
Fax 82 2 2277 1684

Policy Recommendation for South Korea's Middle Power Diplomacy: Cyber Security

Sangbae Kim
Seoul National University

March 2015

Cyber security issues have recently become considered as some of the most pertinent emerging agenda items that South Korea is likely to play a meaningful role as a middle power. These issues have largely been the domain of computer experts and specialists since the Internet began as a small community where an authentication layer of code was unnecessary and the development of norms was simple. But as it grew, everything changed and although cyberspace offered an arena for business and social activities, it also became an environment for crime, hacking, and terror. Governments, private companies and non-state actors are making efforts to develop stronger capabilities for securing their resources and activities in cyberspace. Foreign policy makers and International Relations scholars are struggling to understand cyberspace's basic structures and dynamics, which are different from traditional security sectors. It is obvious that cyber security issues are becoming a major concern of International Relations in various senses.

Amid the fast spread of hacking technologies, many countries and international organizations focus more on crafting security measures and enhancing multilateral cooperation to fend off cyber threats, which could be as devastating as physical military strikes. For example, they are making efforts to build a global framework for Internet governance, of which cyber security is one of the contentious sub-fields; but their consensus has not been framed yet. In particular, the United States and China, two world powers in the 21st century, have recently been in conflict with each other over hackings and espionage. The issue of cyber security is becoming an ever larger presence in U.S.-China relations and is seriously affecting threat perceptions on both sides. Indeed, despite it being such a new issue, the cyber realm is proving to be as challenging as the more traditional concerns that have long dominated the U.S.-China agenda.

South Korea, which has a high reputation as an "Internet Strong Nation," is expected to play a contributive role in the cyber security sector. South Korea boasts cutting-edge digital technology, efficient computer networks and the world's top high-speed Internet penetration rate. But behind these feats is an unpleasant truth: its vulnerability to cyber threats, suspected as the work of North Korea. There is a concern that the on-line attacks are likely to be coupled with off-line nuclear attacks. It is urgent and crucial for South Korea to build capabilities enough to fend off any attacks through cyberspace. However, securing cyberspace is not solely based on fostering material capabilities, but also figuring out diplomatic solutions among committed actors.

In recent years, South Korea as an Internet power is likely to play diplomatic roles in easing cyber conflict between world powers, and to building a new global mechanism for cyber security governance. To achieve these tasks of middle power diplomacy in the sector, it is essential that South Korea properly identify the structural conditions in which it currently operates, and determine adoptable options for the future to aid in its success. In other words, a major task here is to comprehend the overall configuration of the technological and political structures, and define the coordinating or conflicting interests of the actors who are engaging the game. In this context, it is essential for South Korea to identify the structural condition that could be epitomized at three levels.

- First of all, cyber security issues have a number of particular technological and structural characteristics, which are different from traditional security issues. Among them, the key to understanding the potential magnitude of cyber threats is the complex character of the Internet as a network of networks. Cyber threats are continuously evolving, as well as increasingly blurring distinctions between civil and military domains, non-state and state actors, and even human and non-human actors.

- Second, two groups of countries are competing for global cyber security governance. The existing model of cyber security, in a broader sense global internet governance, has been driven by Western countries that believe the Internet should be more open and free. In recent years, however, the challenges, driven by a coalition of states—including Russia, China and other developing countries, are organized and have a clear, more state-controlled vision for the Internet.

- Finally, the United States and China—two world powers in the 21st century—are competing over cyber security. For the last few years, the issue of cyber security (or IT and the Internet in general) as a leading sector has been elevated to a top

priority within the overall U.S.-China relationship. Different approaches to cyber security in technical standards, regulatory policies, and security discourses are contrasting between the two world powers and such differences are likely to spill over into a broader tension between them.

Cyber security issues do not belong to the realm of "international politics" between nation-states competing over traditional security issues; but do belong in the realm of asymmetric "inter-network politics" between complex actors. Moving beyond the traditional framework of inter-governmental organization, various state and non-state actors are recently participating to the new global frameworks for cyber security; at some point in the future, it may be possible to reinforce these global frameworks with certain fundamental norms, but the world is at an early stage in such a process. The next decade is going to be filled with various clashes as those complex actors in world politics are competing for their own political needs and desires.

Under these circumstances, it is critical for South Korea as a middle power to understand the structure and dynamics of the cyber security sector, and to figure out what kinds of specific roles are expected of its middle power diplomacy. Here, it is most important for South Korea to have the ability of contextual and positional intelligence, which reads constantly evolving contexts and identifies its moving positions in cyber security. The discussion about structure and position offers the directions of diplomatic strategies that a middle power has to pursue. Based on these notions, this paper suggests three strategic pillars of middle power diplomacy—brokerage diplomacy, collective diplomacy, and complementary diplomacy.

Policy Recommendations

1. Brokerage Diplomacy in Cyber Security: South Korea should learn how to coordinate the asymmetric relationship in the inter-network politics of cyber security, but must not forget to pursue compatibilities between world powers.

Identifying overall structural conditions of the cyber security sector, South Korea has to contextualize its position within the structure of cyber security politics. In other words, required for South Korea would be the strategies of adjusting itself to the structural conditions of the sector. With regard to the adjustment strategies, this paper pays special atten-

tion to the middle power's strategic roles of "brokerage," which means the role of a broker and more than a mere connector, providing a mode of transition, switching, transforming and translation between different actors in the system. The unique forms of cleavages found in the sector are likely to provide middle powers with structural opportunities of brokerage. But, the structural conditions are also likely to create a situation threatening South Korea's attempts for brokerage on the following three aspects.

a. **Pursuing Compatibilities between Different Standards:** Brokerage issues in the cyber security sector would be concerned with choosing a technical standard between the United States and China. In the case that China takes a technological offensive with its cyber security standards, what would be the decision for South Korea, which has heavily relied on U.S. technical standards, such as Microsoft's Windows operating systems and Internet Explorer, and Cisco's network equipment? This sort of choice must be very tough because it is not only related to technologies, but also involved in diplomatic issues: will South Korea stick to the U.S.-Korea alliance or will it broaden the existing Sino-Korea cooperation? Indeed, the choice means a process of "asymmetric coordination of relationships" that might build new relationships on the one hand, and break existing ties on the other hand. This process of integrating or destroying ties lies at the heart of brokerage. Recognizing the roles of brokerage diplomacy, South Korea has to be familiar with managing the asymmetric coordination game among network partners, but must not forget to pursue compatibilities between two networks.

b. **Developing a "Meta-model" of Policies and Institutions:** In building the Internet policy and governance models, South Korea's choice is placed between the private-sector-driven model of *multistakeholderism,* pursued by the United States and the state-interventionist model of Internet control supported by China. Is South Korea likely to play a brokerage role between these two seemingly incompatible models of Internet policies and institutions? Here, we note that a middle power's role as a broker has an affinity with the strategies of combining or mixing existing models and developing the so-called "meta-model," rather than creating entirely new models. South Korea's experiences in politico-economic development provide good examples for the meta-model, in the sense that the South Korean model of political economy, which is called the "Seoul Consensus," is likely to combine the concerns of developing countries as well as those of advanced countries. It is a plausible scenario to develop a model of a "Seoul Consensus for cyber security" in the sense

that South Korea has achieved prosperity in the Internet economy, initiated by the private sector, although it is still regarded as a country that has state initiatives against social activities in cyberspace.

c. **Implementing Complex Strategies of Global Governance:** South Korea has difficulties in positioning itself between two different visions for global Internet governance. One vision has been driven by Western countries that believe the Internet should be more open and free; the other driven by developing countries' support for the inter-governmental approach and state sovereignty over cyberspace. South Korea's official position is now known to support the open and flexible approach to global Internet governance initiated by various international entities such as United Nations (UN), International Telecommunication Union (ITU), Organization for Economic Cooperation and Development (OECD), and Internet Corporation for Assigned Names and Numbers (ICANN). The approach could be called the complex strategy of Internet governance, combining the two competing visions. However, it is expected that South Korea would have difficulties in structural positioning in the sector. For example, South Korea was crammed between advanced countries and developing countries in the vote for updating the International Telecommunication Regulations (ITRs) at World Conference on International Telecommunications (WCIT) in 2012. Right after South Korea's vote, a South Korean newspaper denounced that the South Korean government when it revealed its intention to control the Internet.

2. Collective Diplomacy in Cyber Security: To fulfill the brokerage roles, South Korea has to learn how to bring together like-minded countries in the cyber security sector, and to attract supportive forces in world politics.

To attain the goals of middle power diplomacy in cyber security, South Korea has to rely on the strategies of collecting and attracting as many like-minded countries as it can. In fact, a large portion of a middle power's brokerage role comes from its ability to bring more actors than others do. In particular, middle powers seek to exercise collective power through coalitions or alliances. With regard to collecting like-minded countries in the cyber security sector, a study conducted by the Centre for International Governance Innovation (CIGI) identified some interesting patterns among certain groups of states voting at WCIT 2012 (Maurer and Morgus, 2014). A core group of potential swing states—a total of 30 countries—is identified based on their voting behavior. The research "essentially marries the

voting record on the ITRs with a series of other indicators to identify patterns and the group of countries likely to act as swing states in the global Internet governance debate in the future due to path dependence, logic of appropriate behavior and state interests." These 30 swing states are sorted into the four groups of countries as follows.

- **Group I** includes 13 swing states voting against the ITRs: Albania, Armenia, Belarus, Colombia, Costa Rica, Georgia, India, Kenya, Moldova, Mongolia, Peru, Philippines and Serbia. These 13 swing states are noteworthy because they are not part of any group of states, but their positions at the WCIT set a precedent for similar behavior in the future. These states also have the resources to persuade other countries to change their behavior and to significantly influence the outcome of Internet governance discussions.

- **Group II** includes 3 OECD countries, Mexico, Turkey and South Korea; and **Group III** includes Ghana and Tunisia—2 members of the Freedom Online Coalition (FOC).[1] All these 5 states supported previous commitments by both the OECD and FOC, and thus their membership and commitments are at odds with their ITRs voting record. Moreover, they are likely to experience significant pressure from their peers in the future to change their behavior to be appropriate with their membership and commitments.

- **Group IV** includes 12 countries voting for the ITRs: Argentina, Botswana, Brazil, Dominica, Indonesia, Jamaica, Malaysia, Namibia, Panama, Singapore, South Africa and Uruguay. They are potential swing states because several indicators, adopted by the research, show the importance of the Internet for those countries and various characteristics of these states suggest that there are opportunities to engage with them to potentially change their behavior in the future.

This grouping of the 30 swing states provides South Korea's middle power diplomacy with some implications for collecting and attracting like-minded countries and formulating coalitions in the cyber security sector.

a. First, it is conceivable that South Korea pursues coalition with countries voting for the ITRs, which belong to Group II. Interestingly, three countries in Group II—Mexico, Turkey, and South Korea—are participants of MIKTA (a coalition of Mexico, Indonesia, Korea, Turkey, and Australia), which has gained increasing attention

in recent years. It is also probable that South Korea extends the MIKTA coalition to FOC countries, Ghana and Tunisia, which belong to Group III.

b. Second, it would be more interesting for South Korea to associate with the positional swing states in Group IV. Among them, Indonesia is the first candidate since it is a member of MIKTA. Also, two IBSA (India, Brazil and South Africa) countries, Brazil and South Africa, are possible partners that keep pace with South Korea in the fields of global Internet governance. Impressively, these countries, especially Brazil, have played a leading role in renovating the ICANN system.

c. Finally, it is imaginable that South Korea may form solidarity with another IBSA country, India for example, which belongs to Group I as it is voting against the ITRs. And, Australia, which is not included as a part of the 30 states, is likely to have a similar mind view with South Korea since it is a member of MIKTA.

In implementing collective diplomacy, South Korea should be flexible in choosing partners and in coalescing issues. For example, South Korea has to figure out which agenda is appropriate for the selected coalition partners. Various issues on global Internet governance in general could be linked to the specific issues of cyber security. Beyond the boundaries of Internet governance, other security and economic issues could be linked to cyber security issues in order to increase the effectiveness of collective diplomacy. For example, official development aid (ODA) must be a good item of issue linkage politics for South Korea's middle power diplomacy in cyber security. Also, South Korea could grasp opportunities through combining non-traditional security issues together, such as cyber security, atomic energy, and ecological security, as world powers are still competing for the priority of, and even the goal of, governance mechanisms.

3. Complementary Diplomacy in Cyber Security: South Korea as a middle power could be an architect, not a whole system designer but a complementary programmer, who can provide useful patch programs for the whole system operated by world powers.

While South Korea needs to engage in building world order in the cyber security sector, its diplomatic strategies, if any, should be complementary to the existing system. South Korea's complementary diplomacy in the sector has to begin with a more thorough understanding of the structural conditions of the cyber security sector. Indeed, the world power's' simplistic approach, based on the traditional conception of "power politics", does not fit into the nature of cyberspace, which is strongly predicated upon complexity. In this context, the

possibilities of middle powers' complementary roles would be emerging. In particular, middle powers are likely to privilege for problematizing normative aspects that the existing world order may lack. For middle powers that have less military capabilities and economic resources, norm- or value-oriented diplomacy are crucial and effective means to attain the goals. Indeed, diplomatic strategies which are inclusive and close to international norms are more likely to be attractive to other countries. In this context, this paper presents three ideas on the normative approaches, which South Korea needs to develop.

a. **Normative Diplomacy for Demilitarized Peace Discourse:** South Korea as a middle power could criticize and complement the security discourse of world powers, based on the Cold War metaphor and the analogy of the arms race. Recently, concerns have grown to view the cyber threat from the perspective of militarization in cyberspace. Cyber-conflict is after all the newest mode of warfare and cyber-weapons have been described as weapons of mass disruption. In reality, the United States and China are strengthening their capacity to engage in both defensive and offensive cyber actions against each other, presenting the prospect of a cyber-arms race while potentially intensifying the already high level of distrust between the two countries. Attentions on the military dimensions of cyberspace are justifiable. However, there will be no solution for a security dilemma as long as the world powers keep relying on the analogy of an arms race as the zero-sum game. In this context, it is meaningful for South Korea to stress the other aspect of cyber-conflict, by developing the demilitarized peace discourse in cyberspace.

b. **Normative Diplomacy for Post-international Discourses:** South Korea has to complement the current security discourses of international laws—a national or international approach to cyber security with legal minds. Recently, scholars point out the lack of an international legal framework that defines the use of force in cyberspace; they examine the legal dilemmas regarding the use of force in cyberspace and question how the Law of War can be applied to cyber-threats. The Tallinn Manual is a noteworthy example that applies international norms to transnational threats in cyberspace. However, considering operational difficulties in deterring and identifying cyber-attacks and the asymmetric dimension of cyber-conflicts, inadequate are international laws and norms, predicated upon the dichotomy of actors—i.e., offense and defense—in the modern international politics. What we need is more complex discourses and norms that are able to handle the post-international or inter-network dynamics of cyber security issues. In this context,

South Korea as a middle power could contribute by developing a new network discourse complementing the existing international discourses.

c. **Normative Diplomacy for Cyber Ethics:** South Korea could complement the world powers' security discourse with cyber ethics. Cyber ethics encompasses Internet user's behavior and what computers are programmed to do, and how this affects individuals and society. Previous examples of cyber ethics include various issues concerning personal information or privacy: Who owns digital data? What should users be allowed to do with it? And, how much access should there be to obscene contents online? Now those ethical questions should be extended to international or transnational issues of cyber security. As an ever increasing amount of people connect to the Internet, there is a susceptibility to identity theft, cybercrimes and computer hacking. Historically, security has long been a topic of ethical debate. Likewise, it is expected for such ethical debates to arise in the cyber security sector. In this context, South Korea as a middle power is likely to develop new discourses in cyber ethics as an underdeveloped field, which complement the realist or the liberal discourses of the world powers. ■

Endnotes

[1] The membership of the Freedom Online Coalition (FOC) currently includes 22 countries. This coalition defines itself as "an inter-governmental coalition committed to advancing Internet freedom—free expression, association, assembly, and privacy online—worldwide" (Maurer and Morgus, 2014: pp.7-8).

References

Maurer, Tim and Robert Morgus. 2014. "Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate." CIGI Internet Governance Papers No.7 Series: Internet Governance. https://www.cigionline.org/sites/default/files/no7_2.pdf

Author's Biography

Sangbae Kim
Seoul National University

Sangbae Kim is a professor of international relations at the Department of Political Science and International Relations, Seoul National University. His major research concerns are with information, communication, and networks in international relations. His selected works include *Standards Competition in the Information Age: Wintelism and the Japanese Computer Industry* (in Korean), (Paju: Hanul Academy, 2007); *Information Revolution and Power Transformation: A Perspective of Network Politics* (in Korean), (Paju: Hanul Academy, 2010); *International Relations of Arachne: Challenge of the Network Theory of World Politics* (in Korean), (Paju: Hanul Academy, 2014).

Knowledge-Net for a Better World

- East Asia Institute acknowledges the MacArthur Foundation for its support to the Middle Power Diplomacy Initiative.