# The Inter-network Politics of Cyber Security and Middle Power Diplomacy: A Korean Perspective

Sangbae Kim
Seoul National University

October 2014

EAI MPDI 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.

EAI takes no institutional position on policy issues and has no affiliation with the Korean government. All statements of fact and expressions of opinion contained in its publications are the sole responsibility of the author or authors.

 is a registered trademark.



ISBN 978-89-92395-92-2 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

# The Inter-network Politics of Cyber Security and Middle Power Diplomacy: A Korean Perspective

Sangbae Kim
Seoul National University

October 2014

## I. Introduction

In recent years, South Korea has come to be regarded as an emerging middle power in world politics, and growing are concerns that South Korea should play diplomatic roles corresponding to its increased material capabilities. South Korea has recently strived to figure out a new vision of middle power diplomacy: what kinds of roles are expected of it, and in which issue areas it plays those roles in effective ways. The exemplary fields, about which South Korea's roles of middle power are discussed, include non-traditional security issues such as atomic energy, global warming, and cyber security, and other economic issues such as official developmental aid (ODA), global trade and finance. Of them, cyber security issues are considered as one of the newly rising agendas that South Korea is likely to play a meaningful role as a middle power.

Cyber security 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 then it grew, and everything changed. Although cyberspace offered the arena for business and social activities, it also became an environment for crime, hackings and terrors. Governments, private companies and non-state actors are making efforts to develop indispensable 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 turning into 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, are recently conflicting with each other over hackings and espionage. The issue of cyber security is becoming ever larger 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 (Lieberthal and Singer, 2012: pp.1-2).

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 North Korea's offences. It is worried 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 offences through cyberspace. However, securing cyberspace is not solely based on fostering material capabilities, but also figuring out diplomatic solutions among committed actors. In this context, this paper analyses the opportunities or difficulties that South Korea's middle power diplomacy is facing in the cyber security sector.

This paper maintains that existing studies of middle power are inadequate for providing a guideline for South Korea, particularly in the realm of cyber security. They mostly look to individual countries' attributes or capabilities to explain the generalized roles of middle power in world politics (Gordon, 1966; McLin, 1967; Holbraad, 1971; Pratt ed., 1990; Cooper, Higgot and Nossal, 1993; Cooper ed., 1997; Otte, 2000). Thus, they fail to explain the proper roles of middle power under a certain structural condition that might be a more essential determinant for middle powers' action than for world powers'. In contrast, network theorists in International Relations adopt an anti-attribute imperative that rejects all attempts to explain actors' actions solely in terms of actors' attributes. They maintain that it is an actor's "position," not its attributes, that creates opportunities for a country, and that how actors are connected to others influences its diplomatic discretion. In this context, this paper adopts this notion of "positional approach," which has an origin from network theories, to understand middle power diplomacy (Hafner-Burton and Montgomery, 2006; Goddard, 2009; Nexon and Wright, 2007; Nexon, 2009; S. Kim, 2014a; 2014b).

Relying on the positional approach, this paper primarily identifies complex structures of the cyber security sector. Indeed, this approach provides a framework to understand the distinct modalities and dynamics of cyber security issues, which this paper calls the "asymmetric inter-network politics." It looks at the triple structures: i) techno-social structure of cyberspace, ii) issue-specific political structure in global cyber security governance, and iii) geopolitical structure generated by the U.S.-China competition. Identifying the structural conditions in the domain, this paper explores the possibilities or the dilemma of South Korea's middle power diplomacy in the cyber security sector. In particular, this paper uses network theories to deduce a series of conditions under which South Korea's middle power diplomacy is more or less likely.

This paper is composed of five sections. In the first section, it outlines the notions of structural positioning and positional power as theoretical frameworks. In the second section, it explores the technological structure and social dynamics of cyberspace, in which various actors are interacting. In the third section, it examines the inter-network politics of global cyber security governance, and investigates competing ideas and interests behind it. In the fourth section, it looks at the U.S-China conflicts over cyber hackings, regulatory policies, and security discourses. In the fifth section, applying the positional approach to middle power diplomacy, it suggests that South Korea should manage three strategies of brokerage, collection, and complement in coping with the inter-network politics of cyber security. This paper concludes with a brief summary of this paper, and presents further research concerns.

## II. Positional Approach to Middle Power Diplomacy

Network theories provide IR theorists with an alternative account of middle power diplomacy; they hold that a particular type of network creates favorable conditions for participating actors and how actors are positioned in the network facilitates their ability to compete or cooperate with others (Goddard, 2009: p.253). In this view, middle power's actions are dependent upon the structural condition of the network in which a country ties to others. In other words, depending on how the structure is shaping, middle powers are likely to enjoy a certain degree of roles. Then, comparing to other theoretical approaches, how does the network perspective define the structural condition—i.e., "structure" in general?

While the neo-realists notion of structure understands structure as an entity that is derived from the categorical attributes of actors (Waltz, 1979), network theories look at the relational context of actors' interaction. Structure is emerging from "continuing series of transactions to which participants attach shared understandings, memories, forecasts, rights, and obligation" (Tilly, 1998: p.456; Goddard, 2009: p.254). Here, structure is understood as the relational configuration among actors or the patterns of transaction themselves. Relatively durable, but fundamentally dynamic interactions constitute the structural conditions in which actors operate (Nexon, 2009: p.25). In short, structure is not a kind of fixed entity reducing to actors' internal properties or attributes, but a social relationship among or across actors (Nexon and Wright, 2007).

This view is useful to identify the role of middle power occupying a specific position in the network. It is not an actor's attributes or interests but its positions that enable middle power's agency. The positional perspective in social network theory holds "that how actors are positioned in a network facilitates their ability to act as entrepreneurs. Because social and cultural ties provide power, information, and ideas, an actor's ability to introduce new norms, manipulate symbols, and radically influence political outcomes, all depends on network position" (Goddard, 2009: p.257). Middle powers' strategies are more likely to succeed if they accommodate the requirements of the structural conditions in the network. If the concept of middle power is defined in terms of structural position in a network, what specific roles would a middle power play under a certain network structure?

Among various roles of middle power, this paper pays special attention to the advantages of brokerage empowered by positioning within a strategically important spot in a particular network structure. According to Ronald Burt, people who hold brokerage positions enjoy a competitive advantage over others who are less well placed. When they capture strategic places that connect otherwise disconnected groups, those people can exercise a special kind of power. In particular, he gives us some analytic insight; the unique forms of cleavages, which usually are conceptualized as "structural holes," found in a network which provide structural opportunities for some actors—known as brokers. By bridging the structural holes, brokers occupy central positions in a network structure, acting as nodes through which multiple transactions coalesce (Burt, 1992).

It is this structural position, not an actor's attribute that enables middle powers to exercise a certain kind of power. The structural conditions of a network—e.g., number of nodes, pattern of links, and architecture of the whole network—enable or disables middle powers to play particular roles and thus to have more possibilities to exercise powers. In this sense, the power of broker—i.e., brokerage power—could be called "positional power" (Gould and Fernandez, 1989; Chang, 2009). Positional power is contrasted to the existing notion of "re-

source power," which refers to the power based on resources held by actors. In this respect, positional power is one aspect of recent theoretical attempts concerning "network power" that derives from one's relationships with others (i.e., networks) rather than its attributes (Grewal, 2008; Castells, 2009; Hafner-Burton, Kahler and Montgomery, 2009; Ha and Kim ed., 2010; S. Kim, 2014b).

In wielding the positional power, the pre-stage of the game is to identify the nature of network committed, and to contextualize middle power's position within the network structure of the whole system. In other words, a major task here is to comprehend the overall configuration of the network, and define the coordinating or conflicting interests of the actors who are engaging the network game. For a middle power, a central task at this stage is to read the context of which world powers set the scheme. Only after reading the context, a middle power can assign itself roles within the network. Those roles of middle power could be articulated by understanding three aspects of network strategies: brokerage, collection, and complement.

First, situated at the interstices of networks, a middle power is likely to play the role of brokerage. Brokerage may alter network structures, leaving actors with a fundamentally different set of network ties, and changing the agenda in a network. This occurs because the brokerage process is usually accompanied by the process of "asymmetric coordination of relationships." This is to make certain ties stronger and to sever others. Simply, a process of network diplomacy is to break existing ties on the one hand, and to build new relationships on the other hand. It is this process of integrating and destroying ties that lies at the heart of brokerage. Indeed, this process of connecting and disconnecting ties belongs to the realm of strategic choices at the risk of opportunities costs.

Second, the enriched pool of supporters in the network enables middle powers to play active brokerage roles. In fact, a large portion of middle power's brokerage roles comes from its ability to bring more actors than others do. Being aware of the limitations of their brokerage roles, middle powers have to rely on collecting and attracting as many like-minded countries as possible. This carries with it the basic ideas of network power—i.e., "social power" (Hafner-Burton, Kahler and Montgomery, 2009; Kahler ed., 2009) or "collective power" (S. Kim, 2014a). The patterns of power remind us of online collaboration, conceptualized as "collective intelligence" (Levy, 1999). In particular, middle powers seek to exercise the collective power through coalitions or alliances.

Finally, middle powers may exercise a "programming power" as new architects of the network program. However, middle power's programming power is concerned with the ability to complement and possibly further renovate the whole system, designed by world powers. Indeed, its unique position in the existing system requires middle powers to play a comple-

mentary role to the existing world order, not to play an exploitive role through challenging world powers' initiatives. In this sense, they do not necessarily have to be a whole system designer; for middle powers, sufficient is to be a complementary programmer, who can provide system adjustments and adaptations that increase interoperability and compatibility, and further reinforce normative values and legitimation.

Theoretical notions, introduced in this section, are useful to understand the structural conditions of the cyber security sector, and South Korea's middle power strategies under the unique structural conditions. 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. Now let us turn to the discussion about the cyber security sector, characterized by triple structures as described below.

## III. Complex Networks in Cyber Security

Cyberspace is now an unavoidable reality that covers the earth with complex networks. Networked computers that make up cyberspace are global in its design and development, and have dissolved the traditional boundaries of the territorial nation state. Cyberspace has evolved so quickly that individuals and organizations have to adopt proper measures for security. The challenge is that cyber security issues have unique technological characteristics, which are different from traditional security issues. In particular, the complex character of network systems is the key to understanding the potential magnitude of cyber threats; it is indispensable to understand the unique conditions of structures, dynamics, and actors in cyberspace. This section points out the six features of cyber security issues.

First, cyber terrors and attacks are taking places in the network environment, characterized as a complex system. Cyberspace is a mixture of physical infrastructure and virtual properties. The Internet involves multiple hardware, software and contents. And actors are diverse—sometimes virtual and anonymous. The complexity of cyberspace makes it hard to discern the major culprit of cyber-attacks. Even if the culprit could be identified, it would be very problematic and even futile to single out a culprit due to the complexity of engaged actors, and even the network itself is a culprit. Moreover, in the case of system

failure or issue, it is difficult to determine whether that is the result of intentional attacks or a mere incident of system malfunction. In the case of the Stuxnet virus taking effect on the Natanz nuclear centrifuges in Iran, the virus was not discovered until June 2010, not by the Iranians, but by a Belarusian cybersecurity firm. These features are all originated from the intrinsically non-leaner causal mechanism of cyberspace as a complex system.

Second, the complexity of cyberspace makes it plausible to adopt the theory of "securitization," presented by the Copenhagen School of security studies in International Relations (Buzan et al, 1998; Wæver et al., 1993; Wæver, 1995; Hansen and Nissenbaum, 2009). According to Barry Buzan, the securitization of particular issues is constituted by "the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects" (Buzan et al. 1998: p.25). Cyber security issues are typical examples of securitization in the sense that threats to security in cyberspace, at least so far, tend to be a matter of constituting discourses, rather than that of hunting down real threats. Because cyber-attackers may operate at a distance obfuscating their identities, locations, and paths of entry, the culprits are presumed rather than proven to be guilty. In fact, cyber security has long been highly politicized and securitized by dozens of government agencies and traditional corporations.

Third, cyber attackers are exploiting structural elements in network systems. No matter how sophisticated a computer or information system design is, each have bugs and holes, a by-product of high levels of technological complexity, which make them as vulnerable to penetration and change. These holes could be targets for hackers in attacking the network and are called "exploits" (Galloway and Thacker, 2007). Computer viruses and malicious codes exploit the holes, which might be a critical point for interoperability or compatibility between various programs in the entire network. Thus, the one seeking to penetrate a computer network, at least so far, is at a great advantage relative to the defender. Moreover, due to the network character of complex systems, cyber incursions by adversaries could paralyze the whole social system, which could seriously impact people's lives. Those exploits are likely to work as "structural black holes" that make the whole system collapse (S. Kim, 2014a).

Fourth, computer viruses, malicious codes, and the network itself are playing active roles as "non-human actors" in cyber-attacks. Various kinds of computer viruses and malicious codes exploit vulnerable points of the system and degrade the functioning of the system; examples known so far include Stuxnet, Flame, and Shamoon. It is noteworthy that those computer viruses are not mere instruments of human actors, but sometimes an active actor that has abilities affecting the system. The case of DDoS (Distributed Denial of Service) attacks provides a typical example of non-human actor's agency. In DDoS attacks, a

large number of compromised hosts are used to flood a target system with network requests; the "zombie computers" are used as part of a botnet with various non-human actors. Since the early 2010s, a more sophisticated approach has increased rapidly and effectively; a particularly worrisome change has been the rise of "advanced persistent threats (APTs)."

Fifth, cyber terrors and attacks are basically launched by non-state actors such as hackers and crackers, which are not systematically organized, and thus are operating as transnational network actors. The low price of entry, anonymity and asymmetries in vulnerability means that smaller non-state actors exercise a certain amount of power. Cyber terrors and attacks are understood as a type of "asymmetric war" in terms of actors, means, and goals. While state actors have greater resources, they also have greater vulnerabilities. World powers have greater capacity than other state and non-state actors, but it makes little sense to speak of dominance in cyberspace. If anything, dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by non-state actors. Well-known non-state actors include such hacker groups as Anonymous and Cutting Sword of Justice.

Sixth, cyber security is not so much a concern of non-state actors as for state actors. Amid rising concerns over the potential impact of cyber-attacks on national security, many countries have begun expanding the role of their militaries to cover the cyber domain, defining cyberspace as the "fifth battlefield" after land, sea, air and space. In 2007, Russian non-state groups launched massive DDoS attacks on Estonia. Attacks by Russian groups also struck Georgia in 2008 and Kyrgyzstan in 2009 (Evron, 2008; T.L. Thomas, 2009; Hansen and Nissenbaum, 2009). In June 2010, the United States was thought to have developed the Stuxnet in cooperation with Israel to attack Iran's computer systems. North Korea has also been capitalizing on cyber warriors to attack South Korea's network systems. Indeed, safeguarding and securing cyberspace are rapidly becoming a matter of international conflicts and one of the major concerns for national security.

To summarize, cyber security issues are featured by the dynamics, structures, and actors in complex networks, which distinguish them from traditional security issues. Cyber threats are continuously evolving, and increasingly blurring distinctions between territorial boundaries. The lines between state and non-state actions in cyberspace are also shifting and blurred. In this sense, the politics of cyber security is characterized by the notion of asymmetric "inter-network politics" between complex actors, rather than by the traditional notion of "inter-national politics" between nation-states (S. Kim, 2014b).

## IV. Global Governance in Cyber Security

Over the last decade, the world has been exploring a new order for cyber security, which will be established in due consideration of the complexity of the domain. Recalling the history since the late-1990s, cyber security issues have been handled as one of the sub-fields in Internet governance rather than a *sui generis* issue area (Mueller, 2010; DeNardis, 2013). There has not been substantial progress, with the world failing to reach consensus over various issues including how to establish norms, laws and rules of engagement for cyber warfare and to what extent regulations should be imposed on cyber activities. Currently, there is a confrontation between two camps at multiple levels, in which we identify the *de jure* structural conditions of the domain.

### 1. Multistakeholderism vs. Inter-governmentalism

In its early days, Internet governance was conducted by a decentralized multistakeholder network of interconnected autonomous groups drawing from civil society, the private sector, governments, academic and research communities, and national and international organizations. This multistakeholder governance model, sometimes known as a multistakeholder initiative (MSI) or multistakeholderism, is a governance structure that seeks to bring stakeholders together to participate in the dialogue, decision making, and implementation of solutions to common problems and/or goals. The global framework of Internet governance has also been constituted by the initiative of those multistakeholders whose activities are mainly based on the United States; not by the consensus of government representatives in the diplomatic arena of international organizations.

A remarkable example of the multistakeholder model is found in the Internet Corporation for Assigned Names and Numbers (ICANN), which is a non-state organization headquartered in California, USA. Since the early years of the Internet, ICANN has overseen the assignment of globally unique identifiers on the Internet. ICANN must be a global governance model of private-public partnership since it has been governed by an international board of directors drawn from across the Internet's technical, business, academic, and other non-commercial communities. However, in the sense that the U.S. Department of Commerce continues to have final approval over changes to core issues, the ICANN model has been suspected as a tool of U.S. de facto hegemony (Mueller, 2002; 2010).

Against the ICANN model Russia, China and other developing countries have raised objection; they continue to advocate for the use of a traditional international organization—e.g., the United Nations' voting procedures—instead of the ICANN model, for making global deci-

sions, and defend their right to control domestic cyber activities. They maintain that, even if the U.S. leadership as a first mover has been tolerated in the embryonic stage of Internet development, the world now has to establish a new inter-governmental consensus on global Internet governance. It is because the Internet has evolved so quickly that nations find their interests conflicting. The state's intervention to cyberspace seems to be legitimized as a part of territorial sovereignty. In particular, the rising significance of cyber security issues as a matter of national security provides state actors with imperatives to intervene and regulate cyberspace.

With state actors moving to tighten control over cyberspace, some argue that too much government involvement would undermine freedom, creativity and openness. Here, we find a confrontation between two ideas on how to govern the Internet in general, and the cyber security domain in more detail. And this ideational confrontation has been reflected to various challenges to institutionalize global Internet governance. The inter-governmental approach to the Internet and cyber security issues has been pursued by international entities, such as the United Nations' International Telecommunication Union (ITU) and the Organization for European Economy Cooperation (OECD), and by regional bodies, such as the North Atlantic Treaty Organization (NATO).

First, the United Nations' organizations are expanding their jurisdiction to the realm of Internet governance. For example, ITU, an international organization that traditionally has an authority over telecommunications, began to deal with the Internet. In 2003 in Geneva and in 2005 in Tunis, ITU held the World Summit on the Information Society (WSIS), U.N.-sponsored conferences about information, communication and, in broad terms, the information society. WSIS' chief issues included such international issues as bridging global digital divide, cultural diversities, and securing cyberspace. WSIS established the Internet Governance Forum (IGF) to open an ongoing, non-binding conversation among multiple stakeholders about the future of Internet governance.

Second, OECD, an inter-governmental framework of advanced countries, has also participated in global Internet governance, especially securing the Internet environment for electronic commerce and the Internet economy. OECD has developed key indicators to provide a knowledge-base for digital governance policies. In a similar vein, advanced countries have held the Conference on Cyberspace since 2011 in London; and subsequently in Budapest in 2012, and Seoul in 2013. The Conferences on Cyberspace particularly aim to develop a better collective understanding of how to protect and preserve the tremendous opportunities that the development of cyberspace offers. The issue of cyber security has quickly been making its way up the agenda in the Conferences.

Third, the regional frameworks of alliance are also mobilized to cope with cyber threats from non-state actors and to prepare cyber warfare with other state actors. Among those re-

gional efforts, the Tallinn Manual is noteworthy (Schimit, 2012). As for the rules of engagement in cyber warfare, the Tallinn Manual has laid the foundation for international discussions. Written in 2013 by a group of independent experts at the request of the NATO Cooperative Cyber Defense Center of Excellence (CDCOE), the non-binding manual carries academic opinions about the application of international law to cyber conflicts and cyber warfare. However, because the manual was mainly prepared by Western countries, excluding Russia and China, it was blamed to represent the interests of the United States and European countries after the 2007 cyber-attacks against Estonia.

In short, a variety of state and non-state entities provide some form of Internet governance, but no one organization is central to Internet governance on the global level. With the absence of an established order in global Internet governance and the cyber security realm, two different ideas concerning the issues are competing to initiate the institutionalizing process: one could be conceptualized as multistakeholderism; the other might be called intergovernmentalism. This confrontation raised concerns about a challenge to the existing global Internet order managed by the United States; the concerns were fully emerged to the surface at the NETmundial recently hosted by Brazil in 2014.

## 2. The U.S. and Europe vs. Russia and China

Behind the ideational confrontation for global Internet governance, there are conflicts of interests among countries. Led by the United States, Western countries have argued that freedom, openness and trust should be the basic principles in cyberspace. It also believes that various actors including individual citizens, civil society, businesses and governments should participate in the creation of international norms and rules. On the contrary, non-Western countries including Russia and China have maintained that information control should be possible in cyberspace for the purpose of national security, and that they cannot accept regulations that seem to unfairly benefit Western countries. This tension between the two camps shows up by the efforts of Russia, China, and other developing countries to create inter-governmental frameworks as follows.

First, on September 22, 2011, a "Draft Convention on International Information Security" was released at an international meeting of high-ranking officials responsible for security matters in Yekaterinburg, Russia. Key provisions of the draft Convention may be at odds with the Western consensus on basic concepts of Internet security. The sixth article of the draft Convention obliges "not to use information and communication technologies for the interference into other state's internal affairs", and "to abstain from slanderous statements, abusive or hostile propaganda for the implementation of intervention or interference into

internal affairs of other states." The document contains a very important stipulation: the governments may make limitations "for the protection of national and public security" (Cankaoxiaoxi, November, 11, 2011).

Second, in 2012, a similar divergence was starkly apparent at the World Conference on International Telecommunication (WCIT), a conference convened in Dubai by ITU. Though the meeting was ostensibly about updating telephony regulations—the International Telecommunications Regulations (ITRs), the underlying issue was the ITU's role in Internet governance. Authoritarian regimes and many developing countries believe that their approach to sovereignty, security and development would benefit from the multilateral processes that the ITU employs. But democratic governments fear that these processes are too cumbersome, and would undercut the flexibility of the multistakeholder approach, which stresses the involvement of the private and non-profit sectors, as well as governments. The conference ended with the notable result; 89 states signing the new ITRs and 55 publicly opposing them. The result of the vote reinforces the image of confrontation in which there are two competing visions for the future of the Internet.

Third, the most notable development concerning cyber security came in 2013 at the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Since 2004, the UN GGE has examined the existing and potential threats from cyberspace and possible cooperative measures to address them, including the original 1998 Russian proposal. In June 2013, the UN GGE made a series of recommendations on voluntary measures to build trust, transparency and confidence, as well as international cooperation to build capacity for cyber security. These have been seen as milestones in the efforts to bring about global cyber security cooperation. However, it is noteworthy that the UN GGE report includes the significant affirmation that international law, and in particular the UN Charter, is applicable to the security issues in cyberspace.

To summarize, two groups of countries are competing in the global governance of cyber security. With the United States and Europe working as a team and Russia and China as another, the group of advanced countries and the group of former socialist, authoritarian states have sought to maximize their own national interests in the process of shaping a new order in cyberspace. Whether or not the latter group's challenges attain the goal, these two visions of the Internet are unlikely to go away any time soon. The next decade is going to be filled with similar clashes. In this context, it is required for a middle power to see the cleavage that reflects structural conditions of the cyber security sector or Internet governance in general.

## V. U.S.-China Competition in Cyber Security

Cyber security issues have recently become a major source of both tension and potential cooperation for the U.S.-China relationship (Shen, 2010; Manson, 2011; Cai, 2012; Liberthal and Singer, 2012; S. Kim, 2012). The two countries' competition for world hegemony in the 21st century lies behind the competition in the cyber security domain. In fact, according to IR theories, the competition in leading sectors mirrors the overall hegemonic competition in world politics. For the last years, the issues of cyber security (or IT and the Internet in general) as a leading sector have been elevated to a top priority within the overall U.S.-China relationship. This current form of world power rivalry underlines the increasing strategic importance of cyberspace.

### 1. U.S.-China Cyber Conflict

In June 2013, U.S. President Barack Obama and Chinese President Xi Jinping reached a consensus that cyber security is one of the major issues between the two powers, along with the denuclearization of North Korea. This consensus on cyber security has elevated the issue of cyber security to a top priority within the overall bilateral relationship. In spite of the developments, U.S.-China conflict over hackings and espionage are emerging. U.S.-China cyber conflict seemed to reach its peak when the U.S. Attorney General Eric Holder indicted five Chinese military officers in May 2014. He announced that the Chinese officers have engaged in the hacking of prominent U.S. companies' computers to steal commercial secrets, presumably for the benefit of Chinese companies. Beijing's response to the indictments was unusually strong; Beijing maintained that the United States caused serious damage to mutual trust between the sides. Beijing also accused the United States of hypocrisy, recalling Edward Snowden's revelations in June 2012 that the U.S. National Security Agency (NSA) had overseen the hacking of Chinese companies (Guardian, May 20, 2014).

China's fear about the U.S. technological hegemony underlies the cyber conflict described above. China has concerns that the United States allegedly uses its technological advantages to wield its hegemony, depriving China of sharing information on the Internet and creating backdoors in its software to facilitate hacking (Swaine, 2013: pp.5-6). It is especially worried that heavy dependence on U.S. cyber security technologies would result in political disadvantages and military threats to China's security (Lu, 2013). In fact, U.S. technological companies have monopolized major technologies for cyber security in the Chinese market. The awareness that these companies are subject to U.S. law, including the U.S. Patriot Act, undoubtedly triggered a reaction in China as policymakers and ordinary

users realize the huge disadvantage of their dependence on U.S.-controlled networks (Deibert, 2013).

The indictment of Chinese military officers in 2014 ignited the Chinese fear about the U.S. technological dominance. China seemed to adopt a strategy of economic retribution, striking at U.S. technological companies operating within China—Microsoft, IBM, and Cisco—over security concerns (MK Business News, May 23, 2014). The first target was Microsoft, as China announced that government offices were forbidden from running the company's Windows 8 operating system (Asia Economy. July 29, 2014). In a similar vein, the Chinese government pushed domestic banks to remove high-end servers made by IBM and replace them with a local brand (Huamqiu, May 29, 2014). Cisco, which was suspected as an accomplice in NSA spying operations, has also come under fire; it was accused of creating "backdoors" in its routers to aid in U.S. government espionage—a similar accusation to those made against Huawei when it was seeking to break into the U.S. market (Economy Insight, January 1, 2014).

Answering the question about the Internet security review by the Chinese government, Chinese Foreign Ministry spokesman Qin Gang said "whether discussing foreign companies or joint ventures, an important prerequisite is to respect China's laws and regulations, in line with China's national interests, and in line with China's national security" (Xinhua, May 28, 2014). The statement by spokesman Qin reveals the perception of the Chinese government, which U.S.-China conflict over computer and cyber security technologies is not a mere technological issue; rather it is also involved with the competition over Internet policies and regulatory institutions.

## 2. Internet Policies and Regulatory Institutions

The similar competition in cyber security technologies is also found in the conflict between U.S. technological companies and the Chinese government over the policies and institutions for Internet censorship. While the Internet was originally designed to be free of censorship in the United States, the Internet came with the state's Internet censorship system in China. The Chinese government argues that it is a legal privilege of a sovereign state to impose the Internet censorship system on foreign technologies and companies in order to filter harmful and insecure information for national security. In this context, U.S. companies such as Microsoft, Cisco, Yahoo, and Google had to admit regulatory standards of self-censorship if they want to enter into and stay in the Chinese domestic market (Hughes, 2010).

However, tensions exploded in January 2010 when Google announced that it was withdrawing from business in China. The case involved three issues: alleged efforts by the Chi-

nese government to steal Google's intellectual property; intrusion into the G-mail accounts of Chinese activists; and in response, Google's decision to stop complying with censorship of searches by Google China, although Google had been complying for four years. Google's decision inflicted a noticeable cost upon Chinese soft power (Nye, 2011: pp.13-14). Thus, the Chinese government responded quickly to this series of events. It officially argued that it was not involved in the intrusion into Google, and that it does not make sense for the government to mobilize hackers to launch cyber-attacks on a private company. It maintained that any business activities of IT companies in China must follow the laws of China.

On January 15, 2010, the U.S. government became involved, and supported Google's position on the conflict. In particular, Secretary of State Hillary Clinton mentioned Google's example at a speech on Internet freedom on January 21 (Clinton, 2010). The Obama administration announced the plan of arms sales to Taiwan, and a plan of Obama's meeting with the Dalai Lama. The problems with exchange rates of Chinese Yuan and trade barriers, such as anti-dumping duties, were raised. The Google case seemed to be expanding across the U.S.-China relationship. In a broader sense, the 2010 Google dispute revealed the differences in the models of political economy. If Google's decision came from the private-public relationship, which was rooted in the Silicon Valley, the attitude of the Chinese government is based on China's state-driven model. In this sense, the Google case reflected the competition between two institutional models of political economy: the Washington Consensus vs. the Beijing Consensus (S. Kim, 2012).

The attitude of the Chinese government expressed in the Google case in 2010 has been reinforced with the 2013 Snowden case and the 2014 indictment case of Chinese Army officers. For example, in the Brazilian Congress speech on July 16, 2014, Xi Jinping, referring to "shoes theory," maintained that "Only people who wear shoes know whether or not they fit … there is no universal model of development and we should continue to firmly support each other's path of development suited to their own national conditions" (Aju Business Daily, July 17, 2014). His address was interpreted as China giving warning to Western countries due to their intervention in China's human rights problems and territorial conflicts with other East Asian countries. Perceptual and institutional differences between the two countries were reflected on the development of international norms of the global governance mechanism, as discussed in the previous section.

## 3. Competing Securitization of Cyber Security

At the most abstract level, U.S-China competition over cyber security issues enhances the competition for securitizing the domain. In fact, the cyber security domain, in which

threats are still imagined virtual, and thus are not yet regarded as real, is a terrain on which multiple discourses compete (Rid, 2013). Thus, the securitization of cyber security is important: to define what cyber security is, what challenge it presents, who poses threats, where the threats are originated, and how it mitigates the cyber security threats (Deibert, 2002; Hansen and Nissenbaum, 2009). In this view, U.S.-China cyber conflict and Internet policy frictions are all predicated upon the competition for preoccupying security discourses in cyberspace. It is because the competition is not related only to ideational difference, but also deeply involved with interest conflict that affects the future of the reality. This paper addresses U.S.-China differences of security discourses for three aspects.

First, while the United States points to "cyber security" against their computer and network system by attacks to crash, slow or paralyze vital infrastructure, and by the theft of proprietary commercial data or information, China securitizes trans-border information flows and diffusion of resistant political discourses as threats to its regime, and asserts "information security" including a kind of overt censorship. Formulating the discourses of "Chinese hackers' threats," the United States asserts that a growing number of destructive cyber-attacks on commercial enterprises and government institutions originate from China (Dahong, 2005; US-China Economic and Security Review Commission, 2009; Barboza, 2010; Hvistendahl, 2010; Clark, 2011). In 2013, for example, the California-based U.S. cyber security firm Mandiant linked "a number of attacks to a military-affiliated group based in Shanghai" (Guardian, May 20, 2014). In comparison, China has been more concerned about the political aspects of security in cyberspace. According to Wangxiu Jun, deputy director of the State Council Informatization Office, China is "concerned about network security, including ideological security, data security, technical security, application security, and capital security … Overall, political security is fundamental" (Takong, May 18, 2014).

Second, while the United States highlights cyber security at the individual level such as protection of privacy, human rights, and freedom of expression, China has been more concerned about Internet freedom at the national level through means to secure domestic political stability such as censorship and regulations, restricting the freedom of press. U.S. cyber security discourses emphasize securing individual rights in cyberspace as an open space, and are cautious of possible threats to these values. Hillary Clinton's address on January 21, 2010, around the time when Google decided to retreat from the Chinese market, shows well the value of Internet freedom that the United States appreciates (Clinton, 2010). In comparison, China legitimizes Internet censorship and policy autonomy for elevating national freedom rather than individual freedom, and maintains that freedom of the Internet is subject to the laws and morality of a nation. The Chinese government's position to-

ward the 2010 Google case, and its policies to implement Internet security reviews over the foreign IT companies could be legitimized in terms of national rights and freedom to protect security in the Internet (Wang and Xu, 2011: p.107).

Third, while the United States security discourses have been based on the neo-liberal visions on the free flows of information in cyberspace, the Chinese discourses are composed of anti-hegemonic and nationalist visions of state sovereignty in that the globalized Internet poses a major threat to the sovereign authority of nation-states. Since the early age of the Internet, the United States has assumed cyberspace to be a global space, in which information flows transnationally, and has presented an Internet discourse that urges to remove any obstacles that impede the establishment of a liberal order in cyberspace. The discourse is consistent with the U.S. position appearing in the process of building international norms as discussed above. In comparison, China advocates the need for a government to identify the boundaries of cyber territory and protect it against cyber threats (Swaine, 2013: p.3). For example, President Xi Jinping called for respect of all countries' cyberspace sovereignty on July 16, 2014, telling the Brazilian congress that "although the Internet is highly globalized, the sovereignty of the information of all countries should be respected" (Aju Business Daily, July 17, 2014).

To summarize, two world powers are competing over cyber security at multiple levels. In the sense that these two powers are leading the aforementioned two groups or networks of countries that have different orientations to Internet governance, their competition could be called a form of "inter-network politics," which this paper presents to conceptualize the politics of cyber security. Certainly, whether the United States and China have a basically cooperative or antagonistic relationship over the coming several decades, this will be a significant structural condition for South Korea that pursues middle power diplomacy in the domain.

## VI. Middle Power Diplomacy in Cyber Security?

Now let us turn to middle power diplomacy in the cyber security sector, of which structural conditions are conceptualized as "asymmetrical inter-network politics." Then, what diplomatic roles would South Korea play under the structural conditions? Before going for middle power diplomacy, it would be wise for South Korea to build "cyber capabilities" to fend off cyber terror and threats. Could South Korea be referred to a "Cyber Security

Strong Nation" corresponding to its reputation of an "Internet Strong Nation"? In the wake of a series of North Korean cyber-attacks, South Korea has sought to strengthen those capabilities by developing firewalls, cyber specialists, cyber warfare command, educational organizations and legal frameworks to push for cyber protection. Putting off the discussion about South Korea's cyber capabilities, however, this paper examines for South Korea's middle power diplomacy in the sector, adopting three conceptual pillars of middle power diplomacy—brokerage, collection, complement—presented in the second section.

## 1. Brokerage Diplomacy in Cyber Security?

Identifying overall structural conditions of the sector, South Korea has to contextualize its position within the network 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 attention to the middle power's strategic roles of "brokerage." 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.

First of all, it is probable that South Korea has opportunities and difficulties between two different technical standards. In fact, brokerage issues in the cyber security sector would be concerned with choosing a technical standard between the United States and China. Does South Korea keep compatibility with dominant standards of the United States? Or does it cross the threshold and move into an alternative standard that China wants to set in East Asia as well as in 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 Explorers, and Cisco's network equipment? In reality, it happened that South Korea was dissuaded by the United States when South Korea attempted to introduce network equipment provided by Huawei, a Chinese telecommunications company, in early 2014.

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 "connecting and disconnecting" that might build new relationships on the one hand, and break existing ties on the other hand. It is usually accompanied by the process of "asymmetric coordination of relationships," belonging to the realm of strategic choices relating to the risk of opportunity cost. This process of integrating or destroying ties lies at the heart of brokerage in the sense

that brokerage may alter network structures, leaving actors with a fundamentally different set of network ties, and changing the agenda in a network. 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.

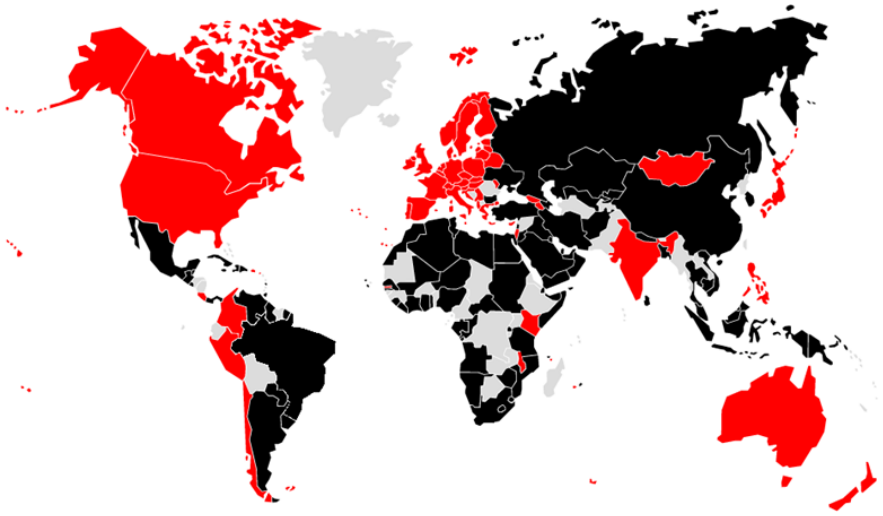
Second, along with technical standard issues, those opportunities or difficulties imposing on middle power's brokerage are also detected in the issues with regard to Internet policies and regulatory institutions. In building the Internet policy and governance models, South Korea's choice is placed between 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 the middle power's role as a broker has an affinity with the strategies of combining or mixing existing models, rather than creating entirely new models. I would call it the strategy of "meta-model" or "meta-programming," comparing to that of "substantial programming." Brokers have more capacity for blending than other actors in world politics although they cannot introduce entirely new inventions. Whether or not a broker's ideas are attractive to others is not so much a matter of content as it is context; it depends on how brokers incorporate various contents found in existing networks.

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 I would call "Seoul Consensus," is likely to combine the concerns of developing countries as well as those of advanced countries. Indeed, although the South Korean model began with the authoritarian model pursuing economic growth, which is recently conceptualized "Beijing Consensus," it has come to achieve the goal of democracy after remarkable economic development, which is usually called "Washington Consensus," as prescribed by advanced countries—especially the United State (Sohn, ed., 2007). In this context, it is a plausible scenario to develop a model of "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.

Finally, South Korea has opportunities and difficulties between two different positions with regard to global Internet governance. Indeed, 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 supports 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 UN, ITU, OECD, and ICANN. The approach could be called the complex strategy of Internet governance, combining the two competing visions.

<Figure 1> Country Positions on ITR Proposed at WCIT 2012



Source: *Dong-A Ilbo*, 2012-12-17

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 ITRs at WCIT in 2012. At last, South Korea voted for the ITRs so that it joined the group of 89 developing countries (Black in Figure-1), and thus took an opposite position to the 55 countries that publicly opposed the ITRs (Red in Figure-1); non-member states of ITU are in grey. 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 (*Dong-A Ilbo*, December 17, 2012). Although the government released that the updated ITRs did not contradict with domestic regulations and national interests, the newspaper was worried that South Korea, which a member of OECD and a host country of G20 in 2010, took a different position from Western countries that believed in the democratic political system and the free trade system. It is uncertain what consequences South Korea's decision at WICIT will cause in the future. However, it is not difficult to imagine that South Korea will be positioned in a very similar situation at the coming conferences.

## 2. Collective Diplomacy in Cyber Security?

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 other words, South Korea has to define the new roles for like-minded groups and continue to attract them as supporters. It is critical for South Korea as a middle power to adopt this strategy of collective and attractive diplomacy, as it will help alleviate the dilemma of being a broker in the cyber security sector (S. Kim, 2014a).

With regard to collecting like-minded countries in the cyber security sector, Maurer and Morgus (2014) conducted research for the Centre for International Governance Innovation (CIGI), identifying some interesting patterns among certain groups of states voting at WCIT 2012. 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" (Maurer and Morgus, 2012: p.4). These 30 swing states are sorted into the four groups of countries as follows (see Table 1).

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 of the 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 (Maurer and Morgus, 2014: p.11).

<Table 1> Top 30 Global Swing States

| Against the ITRs | For the ITRs but... | | |
|---|---|---|---|
| I | II | III | IV |
| | OECD Member | FOC Member | Potential Swing States Based on Indicators |
| Albania | Mexico | Ghana | Argentina |
| Armenia | South Korea | Tunisia | Botswana |
| Belarus* | Turkey | | Brazil |
| Colombia | | | Dominica |
| Costa Rica | | | Indonesia |
| Georgia | | | Jamaica |
| India | | | Malaysia |
| Kenya | | | Namibia |
| Moldova | | | Panama |
| Mongolia | | | Singapore |
| Peru | | | South Africa |
| Philippines | | | Uruguay |
| Serbia | | | |

Source: Maurer and Morgus (2014), p.10; Requoted from Lee (2014).

Maurer and Morgus' groupings 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. 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. Second, it is also probable that South Korea extends the MIKTA coalition to FOC countries, Ghana and Tunisia, which belong to Group III. Third, 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. Finally, it is imaginable that South Korea may form solidarity with another ISBA 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 30 states, is likely to have a similar mind 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?

While South Korea needs to engage in programming the "rule of the game" in the cyber security sector, middle powers' programming diplomacy, if any, should be complementary to the existing system; it is likely and even desirable for them to patch up some subprograms upon the platform designed by world powers. Those complementary programs might target some niches or holes that world powers neglect due to their ontological and epistemological limitations. In particular, its unique position in the existing system requires middle powers to play a complementary role to the existing world order, not to play an exploitive role through challenging world powers' initiatives (S. Kim, 2014a).

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. Both offense and defense take place in cyberspace as an environment of complex networks, in which it is sometimes not possible to identify the subject of offense or the object of retaliation. A wide array of threats to state and business actors are perpetuated by non-state actors. Moreover, cyber threats are continuously evolving, and increasingly blurring distinctions between human and non-human actors, such as computer viruses and malicious codes. In this sense, 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. Indeed, cyber security issues do not belong to the realm of "international politics" between nation-states competing over traditional security issues. In this context, the possibilities of middle power's complementary roles would be emerging.

For example, middle powers are likely to privilege for problematizing normative legitimacy that the existing world order may lack. I would call it the strategy of "normative programming" in the sense that diplomatic concerns are with normative, not with positive, aspects of the sector. 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 (Slagter, 2004). Moreover, if the middle powers pursue collective diplomacy, and mobilize supporters around the world, the authority of normative diplomacy will be reinforced. Considering the normative aspect of middle power diplomacy, is it possible for South Korea to "exploit" the kinds of "structural holes"? In this context, this paper presents three ideas on the complementary and normative approaches, which South Korea needs to develop.

First, 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 (Lawson, 2012). 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.

Second, 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 (Liaropoulos, 2011). 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 dy-

namics 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.

Finally, South Korea could complement the world power's 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.

## VII. Conclusion

As cyber security continues to rise to the front line of world politics, the stakes will increase and tensions and disagreements will become more prevalent. Bearing the rising significance of cyber security in mind, this paper explores the possibilities or constraints of South Korea's middle power diplomacy in the sector. To explain the roles of middle power, this paper relies on the positional approach, which has origins from network theories in natural and social sciences. In this view, it is critical to comprehend the conditions of structure first, not the attributes of actors. Before exploring some details for South Korea's middle power diplomacy, this paper identifies the structural conditions that are unique in the cyber security sector in three aspects.

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 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. 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. Cyber security issues, which are different from traditional security spheres, are evolving in the complex environment that intrinsically contains bugs and holes—i.e., "exploits"—and computer viruses and malwares are actively utilized. In this context, moving beyond the traditional framework of intergovernmental 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.

These structural conditions in the cyber security sector are continuously evolving toward an unprecedented modality of world politics. It is critical for South Korea as a middle power to understand the structure and dynamics of the cyber security sector, to find out any cleavages of who is in which camp in the process of global Internet governance, and to recognize whether the United States and China will have a basically cooperative or antagonistic relationship over the coming several decades. Even more, South Korea has to realize that the potentially poisoning effect of cyber security is occurring at a time when there is genuine uncertainty about the future of cyberspace. 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 this circumstance, South Korea should figure out what kinds of specific roles are expected of its middle power diplomacy. Here, it is most important for South Korea as a middle power 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 network structure and position offers the directions of networking strategies that a middle power has to pursue. Applying these theoretical resources, this paper identifies three elements of middle power diplomacy in the cyber security sector, which South

Korea should consider. This paper suggests to three strategic pillars of middle power diplomacy—brokerage diplomacy, collective diplomacy, and complementary diplomacy.

To summarize, South Korea should be able to manage asymmetric relationships among the world powers and global governance. South Korea would act as a broker, more than a mere connector, providing the mode of transition, switching, transforming and translation between different actors of networks. To fulfill the brokerage roles, South Korea has to learn how to bring together like-minded countries in the sector, and to attract supportive forces in world politics. By questing for networking strategies, 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. In short, being equipped with the ability, it would be more likely to define middle power's roles corresponding to the structural conditions of the cyber security sector. ■

## 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

*Aju Business Daily.* 2014. "Chinese President Xi Jinping's Address in the Brazilian Assembly." July 17. http://www.ajunews.com/view/20140717151605782 (accessed August 10, 2014) (in Korean).

*Asia Economy.* 2014. "US IT Giants, Checked by China's Offense." July 29. http://www.asiae.co.kr/news/view.htm?idxno=2014072908235745851 (accessed August 10, 2014) (in Korean).

Barboza, David. 2010. "Hacking for Fun and Profit in China's Underworld." *New York Times* February 2.

Burt, Ronald S. 1992. *Structural Holes: The Social Structure of Competition.* Cambridge, MA: Harvard University Press.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis.* Boulder: Lynne Rienner.

Cai, CuiHong. 2012. "Sino-U.S. Relations in Cyberspace: Competition, Conflict, and Cooperation." *American Studies Quarterly,* (3), pp.107-121 (in Chinese).

*Cankaoxiaoxi*. 2011. "China, Russia VS. U.S. EU: Struggle for cyberspace preeminence." November, 2. http://world.cankaoxiaoxi.com/2011/1102/4962.shtml (accessed August 9, 2014) (in Chinese).

Castells, Manuel. 2009. *Communication Power.* Oxford and New York: Oxford University Press.

Chang, Dukjin. 2009. "Sociological Anatomy of Political Power: Resource Power and Network Power," in Sangbae Kim, ed., *Soft Power and Network Power.* Paju: Hanul Academy, pp.197-241 (in Korean).

Clark, Richard. 2011. "China's Cyberassault on America." *Wall Street Journa*l, June 15.

Clinton, Hillary. 2010. "Remarks on Internet Freedom." A Speech delivered at The Newseum, Washington, DC. January 21, 2010. http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm (accessed August 10, 2014).

Cooper, Andrew F. ed. 1997. *Niche Diplomacy: Middle Powers After the Cold War.* London: Macmillan.

Cooper, Andrew F., Richard A. Higgott, and Kim Richard Nossal. 1993. *Relocating Middle Powers: Australia and Canada in a Changing World Order.* Vancouver: UBC Press.

Dahong, Min. 2005. "The Passionate Time of Chinese Hackers." *Chinascope.* May, pp.14-25.

Deibert, Ronald J. 2002. "Circuits of Power: Security in the Internet Environment," in James N. Rosenau and J.P. Singh. eds. *Information Technologies and Global Politics:*

*The Changing Scope of Power and Governance.* Albany, NY: SUNY Press, pp.115-142.

Deibert, Ronald J. 2013. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet.* Toronto, Ontario: Signal.

DeNardis, Laura. 2013. *The Global War for Internet Governance.* Yale University Press.

*Dong-A Ilbo.* 2012. "U.S.-Europe Opposed Internet Regulation, South Korea with China and Russia Singed for Internet Regulation." December 17. http://news.donga.com/Economy/mobile/3/0122/20121216/51644147/1?rec=1 (accessed August 10, 2014) (in Korean).

*Economy Insight.* 2014. "A bolt from the blue hit Cisco." January 1. http://www.economyinsight.co.kr/news/articleView.html?idxno=2123 (accessed August 10, 2014) (in Korean).

Evron, Gadi. 2008. "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War." *Georgetown Journal of International Affairs.* 9(1) pp.121-126.

Galloway, Alexander R. and Eugene Thacker. 2007. *The Exploit: A Theory of Networks.* Minneapolis and London: University of Minnesota Press.

Goddard, Stacie E. 2009. "Brokering Change: Networks and Entrepreneurs in International Politics." *International Theory.* 1(2), pp.249-281.

Gordon, J. King. 1966. "Canada's Role as a Middle Power." *Contemporary Affairs,* 35. The Canadian Institute of International Affairs, Toronto.

Gould, Roger V. and Roberto M. Fernandez. 1989. "Structures of Mediation: A Formal Approach to Brokerage in Transaction Networks." *Sociological Methodology,* 19, pp.89-126.

Grewal, David Singh. 2008. *Network Power: The Social Dynamics of Globalization.* New Haven and London: Yale University Press.

*Guardian.* 2014. "China reacts furiously to US cyber-espionage charges." May 20. http://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges (accessed August 10, 2014).

Ha, Young-Sun and Sangbae Kim, eds., 2010. *World Politics of Networks: From Metaphor to Analysis,* Seoul: Seoul National University Press (in Korean).

Hafner-Burton, Emilie M. and Alexander H. Montgomery. 2006. "Power Positions: International Organizations, Social Networks, and Conflict." *Journal of Conflict Resolution,* 2006; 50(1), pp.3-27.

Hafner-Burton, Emilie M., Miles Kahler, and Alexander H. Montgomery. 2009. "Network Analysis for International Relations." *International Organization,* 63, pp.559–592.

Hansen, Lene and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the

Copenhagen School." *International Studies Quarterly,* 53(4), pp.1155-1175.

Holbraad, Carsten. 1971. "The Role of Middle Powers." *Cooperation and Conflict.* CA: Sage Publication.

*Huamqiu*. 2014. "Escalate cyber security war between China and America, lead the early spring to China science and technology enterprises." May 29, http://tech.huanqiu.com/it/2014-05/5007875.html (accessed August 10, 2014) (in Chinese).

Hughes, Rex. 2010. "A Treaty for Cyberspace." *International Affairs,* 86(2), pp.523–541.

Hvistendahl, Mara. 2010. "China's Hacker Army." *Foreign Policy.* March 3, 2010.

Kahler, Miles. ed. 2009. *Networked Politics: Agency, Power, and Governance.* Ithaca and London: Cornell University Press.

Kim, Sangbae. 2012. "U.S-China Standard Competition in the Information Age: A Perspective of the Network Theory of World Politics." *Korean Political Science Review,* 46(1), pp.383-410 (in Korean).

Kim, Sangbae. 2014a. "Roles of Middle Power in East Asia: A Korean Perspective." *EAI Middle Power Diplomacy Initiative Working Paper-02,* East Asia Institute.

Kim, Sangbae. 2014b. *International Relations of Arachne: Challenge of the Network Theory of World Politics.* Paju: Hanul Academy (in Korean).

Lawson, Sean. 2012. "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States." *First Monday,* 17(2). http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270.

Lee, Young-eum. 2014. "Establishing and Applying of the Concept of *Multistakeholder* in the Global Internet Governance." Workshop on Non-traditional Security and Middle Power Diplomacy (in Korean).

Levy, Pierre. 1999. *Collective Intelligence: Mankind's Emerging World in Cyberspace,* Basic Books.

Liaropoulos, Andrew. 2011. "Cyber-Security and the Law of War: The Legal and Ethical Aspects of Cyber-Conflict." Greek Politics Specialist Group Working Paper, no.7.

Lieberthal, Kenneth and Peter W. Singer. 2012. *Cyber security and U.S.-China Relations.* China Center at Brookings.

Lu, ChuanYing. 2013. "Analysis of the dilemma of the current global governance of cyberspace." *Contemporary International Relations*, 11 (in Chinese).

Manson, George Patterson, 2011. "Cyberwar: The United States and China Prepare For the Next Generation of Conflict." *Comparative Strategy,* 30(2), pp.121-133.

Maoz, Zeev. 2010. *Networks of Nations: The Evolution, Structure and Impact of International Networks, 1816-2001.* Cambridge and New York: Cambridge University Press.

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, http://www.cigionline.org/sites/%20default/files/no7_2.pdf.

McLin. Jon B. 1967. *Canada's Changing Defense Policy, 1957-1963: The Problems of a Middle Power in Alliance.* Baltimore: Johns Hopkins Press.

*MK Business News.* 2014. "Chinese government retaliates against US firms after prosecuting Chinese army for hacking." May, 23. http://news.mk.co.kr/newsRead.php?year=2014&no=800319 (accessed August 10, 2014) (in Korean).

Mueller, Milton L. 2002. *Ruling the Root: Internet Governance and the Taming of Cyberspace.* Cambridge, MA: The MIT Press.

Mueller, Milton L. 2010. *Networks and States: The Global Politics of Internet Governance.* Cambridge and London: MIT Press.

Nexon, Daniel and Thomas Wright. 2007. "What's at Stake in the American Empire Debate?" *American Political Science Review,* 101(2), pp.253-271.

Nexon, Daniel. 2009. *The Struggle for Power in Early Modern Europe: Religious Conflict, Dynamic Empires, and International Change,* Princeton, NJ: Princeton University Press.

Nye, Joseph S. 2011. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly.* Winter, pp.18-38.

Otte, Max. 2000. *A Rising Middle Power?: German Foreign Policy in Transformation, 1989-2000.* New York: St. Martin's Press.

Pratt, Cranford. ed., 1990. *Middle Power Internationalism: The North-South Dimension.* Kingston and Montreal: McGill-Queen's University Press.

Rid, Thomas. 2013. *Cyber War will not take place.* Oxford and New York: Oxford University Press.

Schmitt, Michael N. 2012. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard International Law Journal.* 54, pp.13-37.

Shen, Yi. 2010. "Cognition, Competition and Cooperation of the Digital Space: Cyber Security Relationship under the Framework of Sino-Us Strategic Relations." *Foreign Affairs Review,* 2, pp.38-47 (in Chinese).

Slagter, Tracy Hoffmann. 2004. "International 'Norm entrepreneurs': A Role for Middle Powers." Prepared for presentation at the Annual Meeting of the International Studies Association, March 17-20, 2004.

Sohn, Yul, ed., 2007. *East Asia from the Perspective of Attractive Power: Creating*

*Regionness and Seoul Consensus.* Chisikmadang (in Korean).

Swaine, Michael D. 2013. "Chinese Views on Cybersecurity in Foreign Relations." *China Leadership Monitor*, no. 42, http://carnegieendowment.org/files/CLM42MS.pdf.

*Takong*. 2014. "Deputy Director of the National Internet Information Office Talk About the Cyber Security: Mismanagement Lead The nation is in peril." May 18. http://news.takungpao.com/mainland/focus/2014-05/2481785.html (accessed August 10, 2014) (in Chinese).

Thomas, Timothy L. 2009. "Nation-state Cyber Strategies: Examples from China and Russia." Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. eds. *Cyberpower and National Security.* Washington DC: Center for Technology and National Security Policy, National Defense University, pp.465-488.

Tilly, Charles, 1998. "Contentious Conversation," *Social Research,* 653(3), pp.491–510.

US-China Economic and Security Review Commission. 2009. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. McLean, VA: Northrop Grumann Corporation Information Systems Sector.

Wæver, Ole, Barry Buzan, Morten Kelstrup, and Pierre Lemaitre. 1993. *Identity, Migration and the New Security Agenda in Europe.* London: Pinter.

Wæver, Ole. 1995. "Securitization and Desecuritization." In Ronnie Lipschutz. ed. *On Security.* New York: Columbia University Press.

Waltz, Kenneth N., 1979. *Theory of International Politics,* New York: Random House.

Wang, ZhengPing and Xu TieGuang. 2011. "Western cyber-hegemonism and Internet rights of developing countries," *The Ideological Front*, 2(37) pp.107-121 (in Chinese).

*Xinhua*. 2014. "The ministry of foreign affairs: China is researching the policy to improve the security of network information." May 28. http://news.xinhuanet.com/world/2014-05/28/c1110904778.htm (August 10, 2014) (in Chinese).

*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).

- This article is the result of East Asia Institute's research activity of the Asia Security Initiative Research Center.



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