Asian Research Policy

Volume 8 Issue 1
June 2017

Contents

Science, Technology and Innovation Policy in Tajikistan: Present Status and Highlights

Mamadsho Ilolov[1,*] and Karimova Sakina[1]

Abstract

The system of research organizations in the Republic of Tajikistan (RT) includes academic and branch research institutions and as well as institutions of higher education. This science structure was established in the 1950s and reflects a division of research fields into the following sectors: academic, applied research and universities. During the transition into independence, economic necessity gave rise to new kinds and systems of research organizations besides the existing rigid centralized system. Furthermore, new private-public and non-government research structures emerged. It should be noted, however, that these new kinds and systems currently pose little competition to the traditional structures.

Keywords: research organization, innovation performance review, science indicators, science financing, new technologies

1. Introduction

It has passed 25 years from the date of acquisition of the state independence of the Republic of Tajikistan. The decade following Tajikistan`s independence was very turbulent and dominated by a bloody civil war. In 1997 when the war was over, it took several more years for society to concentrate on policies of peaceful state-building. Naturally, the policy priorities in these years were dominated by the efforts to establish constitutional order and functioning public institutions. In this context, it was only in the late 2000s when entrepreneurship, development and innovation issues started to surface and materialize in the public policy agenda. In the first half of the 2010s, the authorities started to assign an increasing priority to entrepreneurship and innovative development in their policy efforts.

It should be noted that the collapse of the Soviet Union brings the former Soviet republics, including Tajikistan, to find their own sources of funding for research institutions in connection with the liquidation of the Academy of Sciences of the USSR –the world’s largest scientific organization. Moreover, leading universities of Tajikistan have also lost their main funding sources—ministries and agencies of the Soviet Union. Over the past 25 years, the Government of the Republic of Tajikistan has done a lot to ensure the effective functioning of the system of research organizations. At the same time it established the National Innovation System with the new approaches to the organization of research activities. It provides a comprehensive legal

1 Center of Innovative Development of Science and New Technologies, Academy of Sciences of the Republic of Tajikistan, 33 Rudaki Ave., 734025, Dushanbe, Republic of Tajikistan

* Corresponding author: ilolov.mamadsho@gmail.com

framework on the basis of international agreements and treaties, national laws and regulations. The Government has reformed branch ministries and departments in order to improve management and organizational functions. So in 2011, the main scientific organization of the country—Academy of Sciences of the Republic of Tajikistan (ASRT) has conducted managerial and organizational reform. The number of employees of the Central Executive Office of ASRT has been shortened, profile Institutes and Research Centers have been combined. In 2014 Ministry of Science and Education of the Republic of Tajikistan on the basis of the former Ministry of Education was established. The Government adopted the Strategy of the Republic of Tajikistan in the field of Science and Technology (2007), Programme for Innovative Development of the Republic of Tajikistan (2012). At this stage, we can say that the transition period is complete and the current system of research organizations is already gathering pace under the new conditions and rules. However, there is still a lot of uncertainties, and therefore it is required comprehensive understanding of the new challenges.

Tajikistan has achieved strong economic and social development over recent years, and has made important steps in moving away from a controlled to an efficiently controlled model of growth.

This article is an attempt to comprehend new terms on the example of the Republic of Tajikistan. In the first section we present a structural analysis of the system of research organizations in the country, the principles of selection of personnel for these organizations, ways and means of searching new sources of funding. The second section presents the main ideas of the Programme for Innovative Development of the Republic of Tajikistan. Finally, the third section is dedicated to public policy in the field of research and innovation.

The main conclusion of this work is that the newly independent state occurring after the collapse of the Soviet Union, have their own way of development in science, technology and innovation. The way is not similar to the one in the developed and developing countries.

Additionally, we will stress that Innovation will be in the governmental level to move towards to the next level of economic prosperity, and the right policy measures will play a decisive role.

2. Materials and Methods

Narrative documents which we used in this paper are divided in four parts:

I. a) Article 40 of the Constitution of the Republic of Tajikistan

"Everyone shall have the right freely to take part in the cultural life of society, artistic, scientific, and technical creation and to use their achievements. The state shall protect cultural and spiritual values. Law shall protect intellectual property."

b) Article 41 of the Constitution of the Republic of Tajikistan

"Everyone shall have the right to education. The basic general education shall be compulsory. The state shall guarantee the free of charge general basic compulsory education in the state educational establishments. Everyone shall get free of charge general vocational, primary specialized, vocational specialized and higher specialized education in the state educational establishments, within the framework determined by law. Other forms of education shall be determined by law."

II. International regulations (bilateral and multilateral agreements and treaties).

III. Legislation of the Republic of Tajikistan in the fields of science, technology and innovation (more than 30 laws approved by the Parliament and signed by President of the Republic of Tajikistan).

IV. Regulations (decrees and orders of the President of the Republic of Tajikistan, decisions

Table 1. Distribution of research organizations across sectors and directions of science (January, 2014)

Sectors \ Directions	Number of organizations	Natural sciences	Social sciences	Applied and technical sciences	University based research
Academic	23	15	8	-	-
Applied research	40	16	4	20	-
University	37	-	-	-	37
Total	100	31	12	20	37

Source: Statistical Collection of the Ministry of Education and Science RT, 2016

and orders of Government of the Republic of Tajikistan, decisions of the Board of Ministry of Science and Education, decisions of the Presidium of Academy of sciences of the Republic of Tajikistan). Data used in the paper are taken from sources listed in the references [1-3]. Basic research methods are scientometrics and complexity system analysis [4].

3. Research Structure

The system of research organizations in the Republic of Tajikistan (RT) includes academic and branch research institutions and as well as institutions of higher education. This science structure was established in the 1950s and reflects a division of research fields into three sectors: academic, applied research and universities.

During the transition to an independent state, economic necessity gave rise to new forms and systems of research organizations besides the existing rigid centralized system. Furthermore, new private-public and non-government research structures emerged. It should be noted, however, that these new forms and systems currently constitute little competition to the traditional structures.

According to Table 1, the ASRT remains the main scientific center of the country despite the managerial and organizational reform implemented in 2011. ASRT organizes research activities in the various institutes and centers and at the same time carries out the work in the realization of the country’s scientific-technical, technological and innovation policies. ASRT is also responsible for implementing the legislation in the field of science, technology and innovation issued by the Parliament of the country. In addition, ASRT composes project resolutions for the Government of RT and other normative and legal documents in the above mentioned field.

The total number of institutions involved in research and development amounts to 100 (January, 2014) with more than 18000 employees (Table 2). This is a low figure compared with the developed countries. Accordingly, the total number of patents applied by Tajik scholars amounted to only 76 in 2015.

Table 2. Number of personnel of research organizations by category (January 2014)

Scientific sector	General staff	Researchers				Support personnel
		General	PhD	PhD candidates	No degree	
Academic	1560	781	152	271	358	779
Applied research	2033	1102	114	359	629	931
University	14445	8495	529	2486	5480	5950
Total	18038	10378	795	3116	6467	7660

Source: Statistical Yearbook, Dushanbe, 2015.

Table 3. Scientific and technical work funded by state budget, institutional resources, and investments (thousands somoni)

	2008	2009	2010	2011	2012	2013	2014
Total volume of executed works from the beginning of the years	12452.1	19775.0	22027.0	36530.1	41342.1	47699.2	52275.5
including: scientific-technical	12210.4	19664.4	21887.3	35746.3	41238.4	47631.7	52099.5
from them: scientific research	11223.4	14858.9	17987.3	32065.9	39090.7	44339.1	51526.5
fundamental	4017.4	7397.0	8508.7	8968.2	10014.8	14254.0	15836.4
research-developmental and technological	59.2	419	22.8	51.9	112.7	194.1	24.8
making experimental samples (series)	-	-	-	-	-	43.9	-
building projects	169	10.3	10.0	-	-	45.9	54.2
scientific-technical services	758.8	4405.5	3867.2	3628.5	1942.6	2948.7	314.3

Source: Statistical Yearbook, Dushanbe, 2015.

The structure of execution of scientific-technical works funded by both State budget and own resources, and investments is shown in Table 3.

Currently, there are three funding mechanisms of scientific organizations in Tajikistan. Each of these mechanisms has advantages and disadvantages. For instance, thematic funding has made it possible to essentially reduce the duplication of scientific research work and helped to improve the general democratization of the national scientific system.

At the same time it should be noted that funds are mostly spent on salaries rather than on strengthening the material-technical basis of the organizations. Core funding is allocated to the main research areas of Institutes or Centers and to support research infrastructures. Targeted funding is directed to major innovative large-scale research with the participation of industry and SMEs. There is a huge need to attract funds from the private sector. Unfortunately, private sectors in Tajikistan still remain undeveloped and have no capacity to allocate funds for science and technology.

In 2014, the volume of research work performed amounted to 46,483,900 somoni (5,217,721 EUR).

The proportion of funding of research work from the budget in relation to the GDP for the period 2008-2014 continues to remain low (Figure 1).

Figure 1. Dynamic volume of research work relative to GDP in Tajikistan (2008-2014)

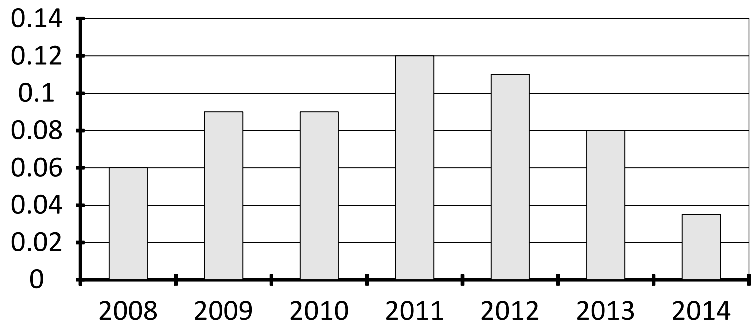
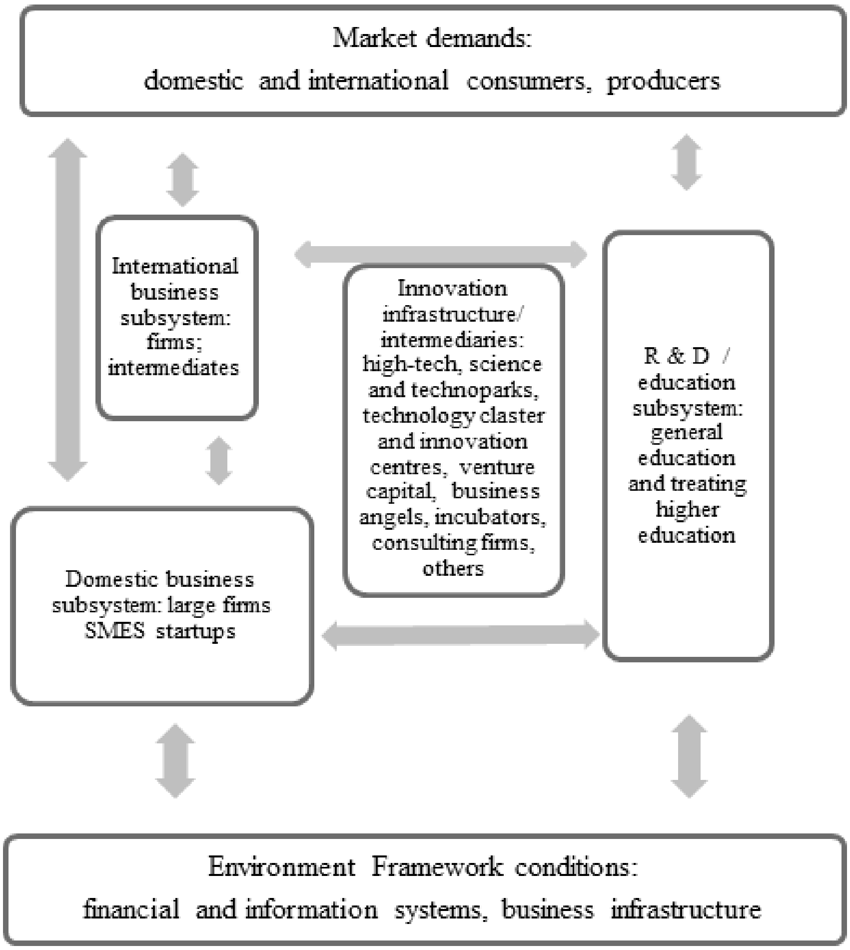


Figure 2. The National Innovation System of a small open economy



4. The National Innovation System of the Republic of Tajikistan

National Innovation System of Tajikistan (NIST) is the network of institutions in the public and private sectors, activities and interactions of which initiate a dissemination of new technologies (Figure 2). The system of approach to innovation helps to identify strengths, weaknesses, driving forces of the innovation process and to identify possible policy actions and measures that could lead to improvements in innovative performance. Generally, innovation is a complex process, involving interactions of a whole range of innovation stakeholders: innovative entrepreneurs, academic and research development institutions, the business sector (as source and target of innovation), innovation intermediaries and support institutions, public bodies with the responsibility to support innovation, financial institutions, national policies in the area of innovation, the framework conditions for innovation, consumers (more generally the market for innovation) etc.

The way from idea to market requires the mobilization and application of many various capabilities and skills. At the beginning an individual entrepreneur can suggest some know-how and he must attract folks with good knowledge in appropriate technology. Therefore, there is a need to bring together relevant actors and stakeholders who can launch the process. Stakeholder cooperation is another important feature of the modern innovation process and is also integrated into of the methodological approach of this paper.

NIST has a number of specific specifications. First, limited local markets call for a high degree of innovation in the global economy and fully-fledged participation in the international division of labor. Well-functioning bidirectional linkages to large international markets are one of preconditions for local firms to grow and necessary conditions for the inflow of the modern technologies and new ideas. These linkages are important for the connection of local innovation stakeholders to international partners and, eventually, for the establishment of stable partnership relations well in global supply value chains.

The second specification is a systemic process of public policy choices and changes that can evolve division of competencies and responsibilities among the various branches of government. Until 2010, most of the legislative and normative acts were adopted without having a clear reference to their main implementing agencies. The decisions regarding the responsibilities for the actual implementation were left to the discretion of the executive power, to be decided at a later phase. However, these practices began to change in the 2010s when policy documents became more elaborate and included references to the responsibilities of concrete branches of government.

The process of dividing competencies and responsibilities among the bodies assigned with responsibilities in implementing public policy is quite advanced in Tajikistan. This refers also to the functional responsibilities for the conduct of innovation for development policies.

5. Science, Technology and Innovation Policy

Today, research and innovation have become the main factors for social development, economic growth and the achievement of a high standard of living. Innovations created through new technologies, production and equipment, the rendering of services, new approaches to organizations and through raising the skill levels of staff, ensure a highly competitive economy. Unfortunately, in the first years of independence Tajikistan was deeply entangled in a civil war and, as a consequence, issues related to the development of science and innovations were put aside for the whole decade. From 2000 onwards, appropriate measures were taken by the Government to support scientific potential, to reform and re-orientate the science sector, and to solve socio-economic problems. Tajikistan strived to strengthen scientific-technological potential as a necessary factor for the modernization of its economy and the gradual transition towards increased innovation.

A number of national laws and government resolutions were passed that defined state policy in the field of science and innovation directed to support scientific potential, the development of scientific research, new technology development and their implementation in production.

A special section “Forming innovative infrastructure and supporting innovative activity” was dedicated to these problems in particular in the Strategy of RT in the field of Science and Technologies for 2007-2015. Laws were passed “On the Academy of Sciences of the Republic of Tajikistan” (2002), “On Industrial Samples” (2004), “On Invention” (2004), “On Rights Protection for the Topology of Integrated Microcircuits” (2006), “On Trademark and Service Marks” (2007), “On Geographical Indicators” (2007), “On Scientific and Scientific-technical Expertise” (2010), and “On Innovative Activity in the Republic of Tajikistan” (2012). A section on “Intellectual Property” was included in the third part of Civil Code of RT (2005).

In 2007, the Government of RT approved the National Development Strategy of Tajikistan 2007-2015. Part of this document is the Science Development Strategy which foresees the updating of the legislative basis of S&T and finding measures to ensure its proper execution. In this strategy, science is described as a national priority. The strategy also aims at further strengthening the collaboration between research organizations and the different ministries, and outlines an ambitious Programme for developing scientific cooperation with other countries, including fellow members of CIS, as well as with international organizations, via intergovernmental agreements and partnerships to be concluded by the Academy of Sciences, research institutes, and universities.

Tajikistan’s Science Development Strategy identifies several weaknesses in the national S&T system such as lack of funding and insufficient research infrastructures, many of which were destroyed during the years of civil war from 1992-1997. The strategy underlines the need to build adequate information infrastructures in order to improve the institutes’ connection to modern information technologies and to make additional scientific literature available to the libraries. There is also lack of highly educated scientific staff due to the very low funding of the research area. To improve the situation, Tajikistan seeks to better integrate its higher education and S&T systems. Moreover, the strategy points out the need to establish comprehensive national S&T programs to tackle the important scientific and socio-economic problems of the country. It also points out that international research collaboration is insufficient despite a high number of signed S&T agreements.

In 2011, the Programme of Innovative Development of the Republic of Tajikistan for 2011-2020 was adopted by the Government. The Programme is to be implemented in two stages:

First stage (2011-2014): Preparation and organization;

Second stage (2015-2020): Development of innovations.

Based on the new national innovative system created, a thorough effort to realize the Programme is to be made during the second stage in order to steadily increase the innovation component in the country’s economy year by year. The national innovation system shall provide the following main components:

1. Creation and development of innovation infrastructure (technical and technological);
2. Forming and improving the system of retraining and professional training of specialists in the field of innovation activity;
3. Organization of the information system in the field of innovation activity;
4. International cooperation in the field of innovation activity;
5. Involving scientific potential in the innovative processes;
6. Tasks related to the innovative development of the fields of economy, education and health.

In 2011, during the realization of the Programme, the Government approved a resolution regarding the foundation of the Center for Innovative Development of Science and New Technologies of the Academy of Sciences of the Republic of Tajikistan. The main task of the Center is to develop scientific bases to implement the main components of the Programme.

6. Conclusion

Currently, Tajikistan is still in the very early stages of establishing a national research, technology and innovation system and the range of recommendations for enhancement is broad. In 2014, Tajikistan moved from being a low income to a lower-middle income model according to the World Bank classification. The approach of this paper is to focus on issues that are critical for the functioning of the STI system in Tajikistan and which would produce visible results without requiring substantial financial and human resources.

In this connection, the following measures have a priority:

1. Increase investment in STI, which is focused on improving absorptive and adaptive capacities. This kind of reforms should be aligned with and support the implementation of international quality standards. This may require financing from international donors because the resource requirements will be significant given the young and growing population of the country. Possible conduits of foreign knowledge are the import of the machinery and equipment, knowledge transferred from multinational companies to their subsidiaries in Tajikistan.
2. Reduce bureaucratic obstacles to business activity and improve the general business environment. Improve the legal provisions aimed at reducing the number of permissive documents required for the establishment of private firms and companies. Such measures can provide rapid results at low cost. It is also necessary to improve the energy and transport infrastructures. This obviously requires a big investment and financial support from international institutions.
3. Coordinate executing innovation policies in order to reduce waste and improve effectiveness (in terms of budgetary resources and policy implementation capacity). Facilitate improvements and innovations in business processes, management and marketing that support greater quality in products and services.
4. Focus policy support on exalting industries, particularly on tradable goods and labor-intensive industries, with a view to supporting productivity improvements in these sectors which can then form the basis for additional investment and economic diversification into related activities. Moving from agriculture to food processing is one of such example.

References

Statistical Agency under President of the Republic of Tajikistan. Statistic Yearbook of the Republic of Tajikistan, 2015

Statistical Agency under President of the Republic of Tajikistan. Educational Statistical Yearbook of the Republic of Tajikistan, 2016

United Nations Economic Comission for Europe. Innovation Performance Review of Tajikistan, Series: ECE Innovative Performance Review 25 Apr 2016

Porter, Alan L., et al. On the Future of Technological Forecasting, Technological Forecasting and Social Change. 67, 1–17 (2001)

The Effects of Intellectual Property Capability of Regions on R&D Performance of Individual Firms†

Young-hoon Kim

Abstract

This research observes, through empirical analysis, the effects of the intellectual property capability of regions on the R&D performance of individual firms, which in detail refers to the firms' growth, profitability, innovativeness, and productivity in comparison with the industrial average. The Korean Institute of Intellectual Property's 2015 Intellectual Property Capability Assessment of Regions and Korea Investor's Service's Database on Firms' Financial Performance Index was used for the analysis.

The IP capability of regions were categorized into IP input, infrastructure, activity, and performance. The findings can be summarized as follows. First, a firm's (sales) growth rate was higher in regions with active IP and education services. Second, in terms of a firm's profitability, the industry's innovation (IP) system was found to be more influential than that of the region. Third, the ratio of R&D investment of firms to total sales was higher in regions with active IP input and excellent IP performance. However, IP performance was found to contribute to private R&D growth when both IP creation and commercialization were active. Fourth, the firm's Total Factor Productivity growth was found to be highly correlated with the region's IP system when the IP activities of both public and private sectors were active.

Despite these results, considering the 16 administrative areas of Korea, none of the areas were found to be active in both public and private sector IP activities, obtain a good score in both IP creation and IP services, or have an active IP service market. This leads us to believe that a thorough reconsideration of the IP systems of the various regions is necessary.

Keywords: national innovation system, regional innovation system, regional intellectual property system

1. Background and Purpose of Research

When we consider an innovation system, a firm's performance is influenced not only by the internal, but also by the external competence, which includes the relationship with the consumer; the network effect of business, education, and research institutes; the usefulness of the financial system; and government support and restrictions. This means that when a firm performs beyond the industry average, it is difficult to interpret this without considering the environment in which the firm exists, such as the nation, the industry, or the region. This statement is also valid in explaining the relationship between a regional firm's performance and the regional innovation system.

POSCO Research Institute, POSRI Building, 514 Bongeunsa-ro (147 Samseong-dong), Gangnam-gu, Seoul, 06163, Rep. of Korea
E-mail: golyong@posri.re.kr

† This paper was funded by KISTEP through the 2016 Creative KISTEP Fellowship Program

The purpose of this study was to observe which internal and external competencies, and in particular which capabilities in the region’s innovation system, are influential when a firm performs beyond the industry average. In considering a firm’s internal competence, the study was focused on its intangible capital; for its external competence, the focus was on the region’s innovation system. In particular, in relation to the innovation system, it was proposed that the scope be restricted to the region’s intellectual property system, which was classified into the four categories of IP input, IP infrastructure, IP activities, and IP performance in order to perform the analysis. In other words, the objective of the study is to observe how individual categories of the region’s IP system influence a firm’s superior performance, measured from the perspective of growth, profitability, innovativeness, and productivity.

The study consists of the following sections. Chapter 2 summarizes the previous research in this area, and Chapter 3 explains the dataset and variables, and provides quantitative models. Chapters 4 and 5 provide the results of basic statistics and model estimation, respectively, while Chapter 6 concludes the study and suggests implications.

2. Previous Research on the Capability and Effects of a Region’s Intellectual Property

2.1. Definition of a Regional Innovation System

Regions are being considered as the new unit of competition defining a nation's competitiveness (Scott and Storper, 2003). This means that the region is not only a physical, geographical space, but is also a social and institutional environment which promotes innovation (Kim and Choi, 2007). There are numerous definitions of the concept of a regional innovation system, but the consensus is that it can be defined using a model that combines the Systems of Innovation approach and the Innovative Environment approach. According to Cooke et al. (1997), a Regional Innovation System refers to the networks and institutions in which firms, research institutes, academies, regional governments, and financial institutions participate, interact and study under the institutional milieu of a region, in order to maximize the innovation potential of the regional economy. While Braczyk et al. (1998) and Asheim and Coenen (2004) define it as a system that triggers methodical interactive learning between the firm’s production structure (knowledge utilization system) and the support infrastructures (knowledge creation system) of research institutes, universities, and technology transfer organizations, Evangelista et al. (2002) defines the system as the unique local network that creates, enhances, and diffuses new technologies through interactions between the public and the private sector. Jeong-hong Kim (2003) defines a regional innovation system as the policy through which the clusters of each region’s strategic industry, innovative firms in the region, research institutes and universities, and other supporting agencies such as Regional Development Agencies establish interactive networks, and effectively cooperate to develop the region. Seok-jin Kim (2005) refers it to a cyclical process, in which the technology created through interactive study between the firms, research institutes, universities, residents, local governments, and other innovative subjects become industrial assets through the connection mechanism of regional finance, which in turn contributes to industrial development, and ultimately feeds back to the innovative subjects. There are minor differences in how the concept of the system can be defined, but the consensus on the regional innovation system is that it is an important factor that explains the networking between the region's innovative subjects and supportive regional environments of which leads to the excellent performance of a firm.

2.2. Measurement of a Region's Intellectual Property Capability

Many previous studies have aimed to effectively measure a region's innovation system or capability. Fratesi (2004) suggested that the scale of a region's resources and R&D investment is a crucial factor in measuring the region's competence. Schiuma and Lerro (2008) categorized the knowledge-based elements which can be used to differentiate the innovative capabilities of regions: human capital, relational capital, structural capital, and social capital. Here, they emphasize that human capital is the know-how and competence the personnel in the region possess, which are important components of an innovative system that determines a region's competitive advantage, as they are important resources for sustainable innovation and can be increased by training and education. Relational capital is the index which represents the linkage between the region's knowledge capital, and includes not only the competence accumulated in the region, but also the connection with the subjects outside the region. Structural capital refers to the assets which promote the development, acquisition, management, and diffusion of knowledge in the region. This includes not only the innovation infrastructure of the region, but also the intellectual properties the stakeholders in the region possess. Lastly, social capital usually refers to the value, culture, and network identity of the region, or in other words the components of competence which were capitalized as the interactions between the innovative subjects accumulated.

Looking at previous studies conducted in Korea, Sung-jong Kim (2006) utilized the region's innovation foundation, innovative activities, and the region's innovativeness in order to analyze the innovation potential of 16 Korean administrative areas. The innovation foundation consists of a region's industrial, research, and information foundation, while the innovation performance consists of the number of venture firms, innovation exhibitions, total software sales, total software exports, and number of IPs in the region. Jin-su Kim and Myeong-shin Choi (2007) compared the innovation capabilities of local administrations, categorizing the capabilities as level of knowledge, economic power, human resource, and infrastructure. For the level of knowledge, the number of patent applications was used, while fiscal self-sufficiency ratio, number of workers in manufacturing and service industry, and the number of registered vehicles were used for the economic power, and the population and aging index were used for human resource. For infrastructure, total road length, number of medical personnel, urban land use, and the number of cultural facilities were used. Dong-sook Heo's recent study (2014) demonstrated that a region's innovation system can be evaluated using the existing statistics under the categories of Innovation input and resource (R&D expenditure, number of researchers and research institutes, number of incubation centers, etc.), Innovation environment and infrastructure (internet usage ratio, financial status of local administration, IT budget, etc.), economic and industrial foundation (Gross Regional Domestic Product (GRDP) per capita, income level, etc.), innovation calculation and performance (patent application and registration, percentage of venture firms, number of workers in knowledge-based manufacturing and service industry, etc.), and innovation process and linkage (number of firms' innovative activities, etc.).

2.3. *Effect Assessment of Regional Intellectual Property System*

The effect of a region's intellectual property system on the firms in the region can be explained by the agglomeration effect in cluster theory. The agglomeration effect is the functional synergy deriving from large-sized enterprise management, vertical integration of value chain, or concentration of diverse industries, academies, and research institutes in a nearby area.

Numerous studies have used the agglomeration effect to provide explanations on the performance of a regional innovation system. According to Cooke and Morgan (1998), a region's innovation system is not only the preconditions of technological innovations of firms, but also the aggregated system of institutions, knowledge structures, production structures, demand and competition, and trust and collaboration. Anselin et al. (2000), Bathelt et al. (2004), and Jaffe (1989) all suggested that a region's innovative behaviors and knowledge creation were found to be more vigorous when there were comparably more universities and research institutes. Lim (2004) argued that the specialization and diversity indices of a region's high-tech industry have a significant impact on the number of patents. Feldman and Audretsch (1999) analyzed the specialization, diversity, and competence indices of American science-based manufacturing industry in each region, and found a correlation between an industry's structural characteristics and the region's IP creation.

This agglomeration effect is maximized when various subjects of innovation concentrated in an area interact to produce, distribute, and reproduce tacit knowledge. Marshall (1920) emphasized through his Industrial District approach that spatial agglomeration establishes a decent pool of specialists, which in turn effectively spread knowledge among personnel, and ultimately recreate new knowledge through interactions. Furthering his argument, it can be said that the agglomeration effect explains the reason why a firm's performance increases when many firms in the same industry become concentrated in the same area. Patel and Pavitt (1994) suggested that the subjects of innovation reside in spatial and cultural proximity in order for them to minimize the uncertainty and danger that accompany the process of innovation, and emphasized the importance of geographic adjacency as the basic resource of success in innovation activities. Jaffe (1989) and Anselin, et al. (1997) both demonstrated how networks of inventors are arising in large cities, based on patent citation information. Exchange of tacit knowledge leads to the elimination of uncertainty, resulting in the success of innovation activities, and this unofficial face-to-face contact is more likely to occur in large cities with dense populations. Putnam (2000) addressed the agglomerate effect from the perspective of social capital, which includes trust, norms, and networks. The underlying idea was that communication and cooperation between innovative subjects are crucial for the knowledge to be created, and that the cities with abundant social capital are ideal locations for the interaction. According to Stern (2000), the innovation capabilities of regions rely on how ideally the research personnel and facilities are arranged in universities and research institutes, how agglomerated they are, and how well they are utilized.

There have also been numerous empirical studies on how regional IP capabilities influence the performance of the economy, industry, and a firm's performance in the region. Jae-jin Chung & Chae-hong Lim (2006) conducted an empirical analysis of the effects of a region's innovation capability on an innovation firm's location and performance, based on 27 national industry innovation complexes. The regional innovation capabilities were categorized into four categories of economy (financial self-sufficiency), welfare (number of hospitals and social welfare facilities), industry's spatial competence (potential innovation capabilities, number of communication firms and manufacturers), and administrative competence (number of processed licenses and registers), and the factors the firms take into consideration when relocating to specific industry complexes were analyzed, from the perspective of regional innovation systems. It was found that innovation firms preferred regions with higher financial self-sufficiency, a higher potential innovation capability index, and more communication firms and manufacturers, while the correlation between the firm's location and the number of hospitals was relatively weak. It was also discovered that the region's financial self-reliance and the number of processed licences have a positive impact on the productive capacity and job creation of firms in the region. Hee-yeon Lee (2010) demonstrated how the number of postgraduate students in the region, the percentage of large companies in the region, the location quotient of leading manufacturers and knowledge-based manufacturers, and the diversity index of knowledge-based manufacturers had a statistically significant effect on regions' knowledge creation (patent application) differentials. Hong-joo Kim (2006) conducted a periodic analysis on the effects of a region's industry and technology structure, human resources, and social proximity on patent creation. The results showed that while in the 1990s the total number of firms, IT specialization, and adjacent social connection were the decisive factors, in the early 2000s, the percentage of specialists in the workforce arose as an additional significant factor.

3. Data and Analysis Model

3.1. Data

Two datasets are mainly used in the study's analysis. For regional IP capability, the Korea Institute of Intellectual Property's "2015 Intellectual Property Capacity Assessment of Regions" was used. Korea Institute of Intellectual Property began to measure the IP capacities of 16 administrative areas in Korea in four categories of input, infrastructure, activity, and performance, and announced the composite scores. The four categories consist of 9 types and 20 items. The RIPC assessment item in the IP infrastructure category was excluded from the study, as the performance evaluation on institutions that support a certain ministry may distort the interpretation of the study's analysis. The firm's productivity item in the IP performance category was also ruled out, as it is already included in the analysis as a performance variable, and using the same value as one of the explanatory variables may result in causality issues.

IP input indices fall into one of the two categories of IP stock and financial investment, and are used to assess the essential input factors of regions in order to achieve IP creation. IP infrastructure indices consist of local administrations and services, and are used to assess the basis of a region's IP activities. IP activity indices are divided into the public and the private sector, and each are again segmented into the size of R&D organizations, and IP management and university-industry cooperation performance. IP performance indices are categorized into IP creation performance and economic performance. The detailed items of each index are explained in Table 1.

Table 1. IP capability indices for regions

Category	Type	Item	Sub-item
Input	IP Stock	IP Size	- Patent rights/design rights/trademark per 10,000 people - Region's territorial asset trademark
		IP Quality	- Patent's qualitative assessment grades, trademark registration & renewal rate
	Financial Investment	IP Investment	- IP budget amount, percentage of local gov't investment on IP budget
		R&D Investment	- Public sector R&D budget, private sector R&D budget
Infrastructure	Local Gov't & Institutions	IP-related Organizations & Institutions	- Presence of IP organization and IP specialist - Administrative efficiency of IP organizations, number of IP-related ordinances
		SME Supporting Organizations	- Personnel expertise, RIPC budget and activity - Technoparks, Creative Economy Centers personnel and budget management
	Service	IP Specialists	- IP service personnel, number of patent agents
		Education	- Credits in university and postgraduate courses, invention classes
Activity	Public Sector	R&D Organizations	- No. of R&D organizations/researchers per 10,000 people - Average number of researchers per R&D organization
		IP Management & University-industrial Cooperation	- Ratio of Technology Licensing Organizations, IP organizations and regulations
	Private Sector	R&D Organizations	- Number of R&D organizations/researchers per 10,000 people - Average number of researchers per R&D organization
		IP Management	- Ratio of firms with patented technology - IP organizations and regulations, technology valuation, IP financing
Performance	IP Creation	Quantitative Performance	- Number of patent/design/trademark applications per 10,000 people - Territorial asset trademark applications per 10,000 people
		Qualitative Performance	- Percentage of annual PCT applications among total applications - Applied patent's scope of protection and ratio of joint application
		Activity Performance	- Percentage of patent applied firms
	Economic Performance	IP Transfer Performance	- Technology transfer, national R&D engineering fee
		IP Commercialization Performance	- Commercialization of national and firm's R&D performance

Source: Korea Institute of Intellectual Property (2015), Intellectual Property Capacity Assessment of Regions, Amended

In order to measure a firm's performance and internal competence, the financial data of 24,990 firms were collected from Korea Investor's Service. Since the KIIP's Intellectual Property Capacity Assessment of Regions first commenced in 2014, Korea Investor's Services financial data from 2013 to 2015 was used.

Firm performance was measured in four categories: growth, profitability, innovativeness, and productivity. In order to measure the performance created by the intangible assets and innovative capabilities of the firm, the industry average performance was calculated from Korean Standard Industrial Classification's Division 2, and deducted from the performance of individual firms. The result was named "excess performance," and served as the basis for analysis.

Table 2. Excess performance indices of individual firms

Category	Indices
Growth	- Sales Growth: Compound Annual Growth Rate (CAGR) between 2013 and 2015, industry average deducted - Employment Growth: CAGR between 2013 and 2015, industry average deducted
Profitability	- Rate of Operating Profit: Operating income to sales in 2015, industry average deducted - ROA: Net profit to gross asset in 2015, industry average deducted
Innovativeness	- R&D Concentration: R&D Investment to sales in 2015, industry average deducted - R&D Expenditure Growth: CAGR between 2013 and 2015, industry average deducted
Productivity	- Total Factor Productivity Growth: CAGR between 2013 and 2015, industry average deducted - Labor Productivity: Sales per employee in 2015, industry average deducted

Table 3. Indices of internal competence of intellectual property

	Definition	Indices
Expenditure on Human Capital	- Employees' expertise, experience, skills, problem solving, leadership, entrepreneurship, business management know-how, innovativeness, etc.	- Personnel expenses, severance pay - Training expenses
Expenditure on Structural Capital	- Infrastructure, organizational process and structure, and information systems to support the personnel - Innovation, IP (Industrial Property, trade secrets, know-how) etc.	- R&D expenses - Welfare benefits, book and printing budget
Expenditure on Customer Capital	- Brand, relationship with clients and suppliers, industrial network, distribution channels, etc.	- PR expenses, sales promotion expenses - Export expenses, overseas marketing expenses

Source: Korea Institute of Intellectual Property (2015), Intellectual Property Capacity Assessment of Regions

A firm's internal IP competence is accumulated in the form of human capital, structural capital, and customer capital. However, it was impossible to identify the accumulative amount of capital due to the restrictions in the firms' financial dataset, and thus the expenditures on human, structural, and customer capital were used as proxy variables. For instance, the sum of firms' expenditure on personnel, severance, training, and education was used as the proxy variable, as it is highly correlated with human capital. For structural capital, the sum of R&D and welfare expenditure was used as the proxy variable, while for customer capital the sum of PR, promotion, exporting, and overseas marketing expenditures were used.

3.2. Basic Statistics

The composite scores of IP input, IP infrastructure, IP activity, and IP performance for 16 Korean administrative areas are as follows.

Table 4. IP input, infrastructure, activity, and performance scores of regions

Region	IP Input	IP Infrastructure	IP Activity	IP Performance
Seoul	49.7	39.9	57.7	42.4
Busan	25.6	44.3	28.2	26.9
Daegu	30.2	27.3	19.6	26.0
Incheon	24.2	26.2	41.6	35.9
Gwangju	17.7	26.4	30.8	33.7
Daejeon	64.4	56.9	78.9	41.6
Ulsan	37.5	24.6	37.5	31.8
Gyeonggi	48.5	21.7	63.8	57.0
Gangwon	16.8	26.8	21.0	37.1
Chungbuk	23.1	43.4	41.0	37.9
Chungnam	30.3	29.1	51.2	41.0
Jeonbuk	13.9	32.8	29.1	40.8
Jeonnam	15.7	28.4	24.6	27.3
Gyeongbuk	28.8	27.1	33.3	23.8
Gyeongnam	20.2	24.3	28.6	26.0
Jeju	11.4	40.1	7.2	30.9
Mean	28.6	32.5	37.1	35.0

Source: Korea Institute of Intellectual Property (2015), Intellectual Property Capacity Assessment of Regions

First, for IP input, Daejeon was ranked the highest with 64, followed by Seoul and Gyeonggi. Since Daeduck Research Complex and other public research institutes are located in Daejeon, the city's cumulative number of patents is high and the government R&D investment is active. This is also the case for Seoul and Gyeonggi, as many venture firms and corporate research institutes are located in this area, and private sector R&D investments are active.

Daejeon was also ranked the highest in IP infrastructure indices, followed by Chungbuk and Busan. Since the core indices of IP infrastructure are the presence and size of IP organizations in local governments, the administrative efficiency of local administrations, and small and medium-sized enterprise support activities, Daejeon, where these public services are concentrated, was able to get a good score on this as well.

For IP activity, Daejeon was also ranked the highest, with Gyeonggi and Seoul in second and third place, respectively. This is because the number of researchers in public and private sector research institutes is the core index of IP activity score.

For IP performance, Gyeonggi was ranked first, while Daejeon was in the middle of the table. Judging by the results, it can be assumed that the reason why Daejeon's IP performance score is low, despite the fact that IP performance is influenced by the number of patent applications, is that the city lacks technology transfer and commercialization performance, as the city's IP system is focused more on public research institutes.

Then, the human, structural, and customer capital were measured, based on the firms' investment on enhancement of internal competence. The results are as follows.

Table 5. Firm's internal competence of Intellectual Property (Percentage of expenditure on sales, %)

Regions	Expenditure on Human Capital	Expenditure on Structural Capital	Expenditure on Customer Capital
Seoul	11.64	0.66	3.31
Busan	6.80	0.36	1.38
Daegu	7.11	0.69	1.58
Incheon	6.28	0.74	1.72
Gwangju	6.50	0.60	1.61
Daejeon	9.98	1.97	2.27
Ulsan	5.94	0.48	1.12
Gyeonggi	7.20	1.11	1.82
Gangwon	9.51	1.00	3.34
Chungbuk	6.19	0.87	2.10
Chungnam	5.80	0.75	1.86
Jeonbuk	5.22	0.88	1.68
Jeonnam	4.92	0.43	1.31
Gyeongbuk	5.23	0.50	1.49
Gyeongnam	5.34	0.44	1.43
Jeju	11.31	0.67	3.01
Mean	8.04	0.77	2.17

The firms were found to spend 8.04% of total sales on human capital. In Seoul and Jeju, the numbers go up to more than 10%. In Seoul, where high wage personnel are abundant and a diverse educational infrastructure is in place, employee education and training are active. In contrast, Jeju's economy is less focused on manufacturing and more in the service industry, which accounts for the high personnel expenses.

Structural capital refers to the ratio of R&D investment to total sales, and the national average was a mere 0.77%. Daejeon was ranked the highest at 1.97%, followed by Gyeonggi's 1.11%, where the infrastructure for venture firms is well established in towns like Pangyo. However, even the highly ranked areas only invest a small amount in this type of capital.

Firms were found to spend 2.17% of total sales on customer capital, which include promotion and PR expenses. Seoul, Gangwon and Jeju were on the top of the table, with their spending on customer capital exceeding 3% of total sales.

The study measured the excess performance in terms of a firm's growth, profitability, innovativeness, and productivity, as a firm's performance indices. The absolute performance indices, without deducting the industry average, are as follows.

Table 6. Firm performance in regions

Regions	Growth		Profitability		Innovativeness		Productivity	
	Sales Growth (%)	Employment Growth (%)	Rate of Operating Profit (%)	Net Income Ratio (%)	R&D Intensity (%)	R&D Growth (%)	TFP Growth (%)	Labor Productivity Growth (%)
Seoul	0.81	-2.86	1.61	3.98	0.25	-21.88	-0.78	-0.40
Busan	-0.40	1.51	2.13	2.94	0.18	-21.86	-1.08	-0.56
Daegu	-1.60	-0.88	2.27	3.83	0.40	10.10	-1.41	-0.66
Incheon	0.84	-2.38	1.76	2.92	0.49	15.29	-0.77	-0.27
Gwangju	11.21	-0.43	2.57	4.76	0.17	-10.97	0.11	-0.16
Daejeon	-6.55	-0.22	0.95	5.25	1.28	-16.17	-1.13	-0.68
Ulsan	0.63	-0.21	1.76	3.81	0.23	-37.94	-0.70	-0.31
Gyeonggi	-0.45	-0.61	1.46	2.31	0.73	-9.24	-0.75	-0.34
Gangwon	4.34	-3.01	-0.34	-0.73	0.37	4.59	-0.09	-0.07
Chungbuk	4.75	0.53	2.18	2.19	0.59	25.29	-0.39	-0.20
Chungnam	-0.68	-3.18	1.99	2.42	0.45	-5.25	-0.66	-0.39
Jeonbuk	3.88	1.30	0.54	1.01	0.30	28.98	-0.63	-0.41
Jeonnam	5.99	2.42	1.53	4.47	0.20	-23.86	-0.42	-0.16
Gyeongbuk	-3.87	-3.09	0.37	1.33	0.36	-1.87	-1.02	-0.50
Gyeongnam	-1.46	0.59	0.55	0.96	0.25	-0.88	-1.02	-0.59
Jeju	10.82	-4.28	0.78	1.25	0.13	-31.49	-0.54	0.01
Mean	0.35	-1.30	1.50	2.86	0.42	-10.48	-0.79	-0.39

The national average sales growth of Korean firms was only 0.35%, and employment decreased by 1.3% in 2015. In terms of profitability, the average ratio of operating profits to sales was 1.5%, while the average net profit ratio was 2.8%. In terms of innovativeness, the average ratio of R&D investment to total sales was only 0.42%, which was down by 10.4%. On productivity, the total factor productivity and labor productivity are both decreasing. All 8 indices show the slow growth of the Korean economy overall.

On the regional scale, Gwangju, Jeonbuk, and Jeonnam were regions with comparably higher growth in terms of sales and employment. These regions also showed comparably brisk statistics in terms of profitability. Although Daejeon was ranked the highest in terms of innovation factor input, infrastructure, and activity, the firms' average sales and employment was showing a decline. Considering that the region's R&D investment growth is rapidly declining despite its comparably higher ratio of R&D intensity to total sales, the high R&D intensity is considered to have been influenced by the decrease in total sales, rather than the increase in R&D expenditure. In terms of productivity, all regions except for Gwangju are experiencing a decline. The decline in productivity all over the country, despite the general decline in employment and investment in facilities, is caused by the structural abyss of slow growth.

3.3. Analysis Model

Excess performance, which is derived by taking the 8 indices of a firm's performance, as suggested in Table 1, and subtracting the industry average, was used as the dependent variable, while the three internal innovation capabilities (human, structural, and customer capital), and four categories of regional innovation systems (IP input, IP infrastructure, IP activity, IP performance) were used as the independent variable. The quantitative model which assesses the effect of region j's IP system on the performance of firm i which is located in region j is then established as follows:

$$
\begin{aligned}
&Firm's\,Performance_{ij} - Industry average_{j} \\
&= \phi control variables_{ij} + \alpha \cdot Internal competence_{ij} + \beta \cdot regional competence_{j} + \epsilon_{ij}
\end{aligned}
$$

The control variables included to rule out the effect of scale and political support are firm age, gross assets, and whether or not the firm is considered a small and medium-sized enterprise.

The four categories of regional capabilities were used in the analysis for the study, along with 8 items in order to analyze the results in different dimensions. Each of the variables are natural logarithms of composite scores for each capabilities. In order to check the error deriving from interrelationship between explanatory variables in quantitative models using the least squares method, the correlativities between 8 independent variables on a region's innovative capabilities, 3 independent variables on a firm's internal competence, and 2 control variables excluding the dummy variable, were calculated. The correlations between variables were low.

4. Results of Analysis

4.1. Growth

Table 7 shows the effect of a region's IP capability on a firms' sales and employment growth.

Among the internal competencies of firms, expenditure on structural capital was found to contribute to the firms' sales and employment growth. This reflects the fact that expenditures on R&D have bigger effects on a firm's growth than spending on human or customer capital, because unlike other types of capital, investment in R&D expenditures is accompanied by investments in facilities, which leads to the employment of professionals, and ultimately results in short-term sales growth due to the promotion of new facilities.

Table 7. Effects of regions' IP capability on growth

Independent Variables		Model I (Based on IP capability categories)				Model II (Based on IP capability types)			
		Sales Growth		Employment Growth		Sales Growth		Employment Growth	
		Estimated Coefficient	Standard Deviation	Estimated Coefficient	Standard Deviation	Estimated Coefficient	Standard Deviation	Estimated Coefficient	Standard Deviation
Control Variable	Firm Age	-0.070***	0.011	-0.027***	0.009	-0.070***	0.011	-0.027***	0.009
	Gross Assets	-0.055***	0.010	-0.034***	0.008	-0.055***	0.010	-0.035***	0.008
	Small and Medium Enterprises	-0.038*	0.022	0.011	0.017	-0.038*	0.022	0.011	0.017
Firm's Competence	Human Capital	0.015	0.011	0.010	0.008	0.012	0.011	0.011	0.008
	Customer Capital	-0.006	0.005	-0.001	0.004	-0.006	0.005	0.000	0.004
	Structural Capital	0.008**	0.004	0.010***	0.003	0.008**	0.004	0.010***	0.003
Regional Competence	IP Input	-0.055	0.035	0.005	0.027				
	IP Stock					-0.054	0.044	-0.023	0.034
	Financial Investment					-0.018	0.022	0.012	0.017
	IP Infrastructure	0.088***	0.028	0.031	0.022				
	Local Gov't					-0.017	0.027	0.034	0.021
	Service					0.085**	0.039	0.055*	0.030
	IP Activity	0.044	0.047	-0.018	0.036				
	Public Sector					0.012	0.045	-0.044	0.035
	Private Sector					0.024	0.028	0.020	0.022
	IP Performance	0.041	0.047	0.022	0.036				
	IP Creation					0.037	0.028	-0.004	0.022
	Econnomic Performance					0.093	0.058	0.044	0.045
Constant Variable		0.899***	0.287	0.499**	0.228	0.805**	0.370	0.342	0.292
Industry Dummy Variables		Included		Included		Included		Included	
No. of Observations		6,216		5,384		6,216		5,384	
R^2		0.029		0.023		0.031		0.024	

1) Asterisks ***,**,* each refer to 1%, 5%, 10% significance level, respectively.
2) The upper and bottom 2.5^{th} percentile dependent variables are excluded as outliers.

Among regional IP capabilities, the firms' sales growth was bigger in regions with higher IP infrastructure scores. For a 1% increase in IP infrastructure scores, the sales growth rate compared to the industry average increased by 0.08%p.

To identify this mechanism in greater detail, the regional innovation capabilities were further segmented into the units of types (see Table 1), and were used as independent variables (Model II of Table 7). The results showed that the statistics related to the specialists in the private sector, such as the density and activity of IP service-related workers or patent agents, or the excellence of relevant education infrastructures, were influential on the firm's sales growth or job creation, rather than the local government's competence. Since the IP-related personnel mainly contribute to the commercialization process, rather than the R&D phase, the analytic results of Model II are in accordance with the expectation.

However, these IP-related personnel tend to reside in large cities, due to agglomeration effects. If the service-concentrated large cities act as hub cities which diffuse benefits to other nearby cities, the shortage of IP-related personnel in rural administrative areas is not a cause for concern. However, as seen in Table 5, while Seoul scored 70 on IP service, Busan scored 32, and other large cities such as Daegu, Incheon, Gwangju, Daejeon, and Ulsan scored 19, 16, 27, 33, and 15, respectively. Incheon is adjacent to Seoul, and is less likely to be able to supply IP service personnel. However, Daegu and Ulsan, which are cities far away from Seoul, do suffer from a shortage in personnel, and cannot function as hub cities of IP services. Therefore, the roles of metropolitan cities as hub cities of IP service markets must be reevaluated in consideration of local universities.

4.2. Profitability

Table 8 shows the effects of a region's IP capability on the firm's ratio of operating profit to sales and net profit.

Of the internal competencies of firms, increased expenditure on customer capital was found to contribute to an increase in a firm's profitability. This means that investing in market encounters, which include efforts to enhance the relationship with customers and marketing, leads to an actual increase in profitability of the firm.

However, among the IP capabilities of regions, none were found to enhance the profitability of firms.

Similar results were found using Model II, which indicates that industry effects such as the performance and the competition of the industry are what influences the firm's profitability, not the regional effects.

4.3. Innovativeness

Table 9 shows the effects of a region's IP capability on the firm's R&D investment to total sales, and the R&D investment growth.

First, of the internal competencies of firms, the growth of expenditure on structural capital was found to contribute to the firm's improvement in innovativeness. However, this correlativity is presumed to have been due to the fact that the variable on structural capital is based on the R&D investment statistics of 2013, while the performance variable is based on the statistics of 2015. In general, firms that continuously invest in R&D tend to maintain the same level or increase investment over the previous year.

In contrast, a firm's ratio of R&D investment to total sales was higher in regions with higher IP input and IP performance.

Table 8. Effects of regions' IP capability on profitability

Independent Variables		Model I (Based on IP capability categories)				Model II (Based on IP capability types)			
		Operating Profit to Sales Ratio		Net Profit Ratio		Operating Profit to Sales Ratio		Net Profit Ratio	
		Estimated Coefficient	Standard Deviation	Estimated Coefficient	Standard Deviation	Estimated Coefficient	Standard Deviation	Estimated Coefficient	Standard Deviation
Control Variable	Firm Age	0.431	0.379	1.214***	0.326	0.431	0.379	1.201***	0.327
	Gross Assets	-0.116	0.332	-1.412***	0.288	-0.159	0.332	-1.437***	0.289
	Small and Medium Enterprises	0.873	0.734	1.466**	0.640	0.843	0.734	1.452**	0.640
Firm's Competence	Human Capital	0.389	0.353	0.928***	0.305	0.495	0.355	0.964***	0.307
	Customer Capital	0.522***	0.181	0.668***	0.157	0.536***	0.181	0.679***	0.157
	Structural Capital	0.217*	0.122	0.319***	0.107	0.203*	0.122	0.317***	0.107
Regional Competence	IP Input	-2.052*	1.177	-0.026	1.013				
	IP Stock					-0.387	1.471	-0.953	1.281
	Financial Investment					-0.688	0.751	0.373	0.653
	IP Infrastructure	-0.560	0.954	0.736	0.833				
	Local Gov't					0.876	0.913	0.385	0.802
	Service					-1.724	1.307	0.194	1.138
	IP Activity	2.283	1.587	-0.407	1.360				
	Public Sector					1.897	1.525	0.395	1.338
	Private Sector					1.245	0.957	0.292	0.829
	IP Performance	0.305	1.585	1.021	1.375				
	IP Creation					-0.621	0.955	0.215	0.835
	Econ. Performance					-0.462	1.957	0.007	1.692
Constant Variable		-17.910	9.528	-6.697	8.272	-19.201	12.345	-4.790	10.660
Industry Dummy Variables		Included		Included		Included		Included	
No. of Observations		6,243		6,331		6,243		6,331	
R^2		0.014		0.021		0.016		0.022	

1) Asterisks ***,**,* each refer to 1%, 5%, 10% significance level, respectively.
2) The upper and bottom 2.5th percentile dependent variables are excluded as outliers.

Table 9. Effects of regions' IP capability on innovativeness

Independent Variables		Model I (Based on IP capability categories)				Model II (Based on IP capability types)			
		R&D Investment to Total Sales		R&D Growth		R&D Investment to Total Sales		R&D Growth	
		Estimated Coefficient	Standard Deviation	Estimated Coefficient	Standard Deviation	Estimated Coefficient	Standard Deviation	Estimated Coefficient	Standard Deviation
Control Variable	Firm Age	-0.144***	0.039	0.046*	0.024	-0.1378**	0.039	0.046*	0.024
	Gross Assets	-0.252***	0.035	-0.038*	0.021	-0.264***	0.034	-0.043*	0.021
	Small and Medium Enterprises	0.274***	0.074	0.085*	0.045	0.264***	0.073	0.082*	0.045
Firm's Competence	Human Capital	-0.099***	0.036	0.039*	0.022	-0.066*	0.036	0.046**	0.022
	Customer Capital	-0.050***	0.019	0.023**	0.012	-0.045**	0.019	0.024**	0.012
	Structural Capital	0.457***	0.013	0.009	0.010	0.452***	0.013	0.008	0.010
Regional Competence	IP Input	0.352***	0.119	-0.003	0.070				
	IP Stock					0.483***	0.146	-0.044	0.089
	Financial Investment					0.349***	0.076	0.039	0.046
	IP Infrastructure	0.143	0.097	-0.081	0.059				
	Local Gov't					0.444***	0.095	0.021	0.057
	Service					-0.490***	0.132	-0.156*	0.080
	IP Activity	0.032	0.164	0.062	0.097				
	Public Sector					0.461***	0.156	0.148	0.095
	Private Sector					-0.171*	0.101	0.060	0.060
	IP Performance	0.446***	0.163	-0.007	0.097				
	IP Creation					-0.105	0.096	-0.040	0.058
	Econ. Performance					-0.228	0.195	-0.149	0.117
Constant Variable		-0.972	0.988	-2.286	0.812	-0.504	1.252	0.777	-0.360
Industry Dummy Variables		Included		Included		Included		Included	
No. of Observations		4,212		4,294		4.212		4,294	
R^2		0.268		0.008		0.286		0.012	

1) Asterisks ***,**,* each refer to 1%, 5%, 10% significance level, respectively.
2) The upper and bottom 2.5th percentile dependent variables are excluded as outliers.

When Model II was used for the analysis, a firm's R&D investment was higher in regions with IP stocks of higher quality, and with stronger financial investment from the central government. In terms of IP infrastructure, regions with a solid structure and vigorous activities contributed to the firm's R&D performance. In contrast, the ratio of a firm's R&D investment to total sales was lower in regions with active IP services. This is basically due to the increase in total sales, rather than the decline in R&D investment, as shown in Table 7. The sales growth is likely to be high in regions with active IP service infrastructures in the private sector, and this speed of growth may exceed the growth of R&D investment, thus decreasing the ratio of R&D investment to total sales. In terms of IP activity, the firm's investment in R&D was strengthened in regions with more abundant research personnel and vigorous industry, education, and research collaboration in the public sector. However, this correlation was not found to be statistically significant in the private sector.

Table 9 shows that a firm's R&D investment tended to strengthen in regions with excellent IP performance, as reflected in a higher number of patent applications and vigorous technology transfer and commercialization. However, such correlation is not found when using Model II, and this means that IP creation and economic performance should take place in parallel, in order for the IP performance to contribute to the firm's R&D investment. Regions without IP commercialization, or without a decent stock of IP will not be able to link their strength toward firms' actual investment on R&D, failing to establish a successful virtuous mechanism.

4.4. Productivity

Table 10 shows the effects of a region's IP capability on firms' total factor productivity and labor productivity growth.

First, the productivity of firms was lower in regions with more IP input, while the productivity of firms in regions with vigorous IP activities was comparably higher.

Under the analysis using Model II, financial investment was found to be correlated to a firm's productivity. However, it would be hasty to jump to the conclusion that bigger financial investment from governments for local administrations leads to a decline in productivity for firms. Rather, the central government invests more in regions with low GRDP and low productivity, as the composite score for financial investment is calculated based on the percentage of government financing on GRDP. This causality issue derives from the limits of the quantitative models and datasets used in this study.

Critically, the significance of the IP activity found using Model I disappeared when Model II was used, a similar result to the innovativeness analysis shown in Table 9. This means that the IP activities of both the public and private sector should seek synergy through interactions in order to enhance the productivity of firms in the region. A great example of this assumption is the low productivity of Daejeon, despite strong public sector activities, and of Seoul and Gyeonggi, despite strong private sector activities, as the asymmetric status of public and private sector activities cannot work in synergy to benefit the productivity of firms in the region.

Table 10. Effects of regions’ IP capability on productivity

Independent Variables		Model I (Based on IP capability categories)				Model II (Based on IP capability types)			
		TFP Growth		Labor Productivity		TFP Growth		Labor Productivity	
		Estimated Coefficient	Standard Deviation	Estimated Coefficient	Standard Deviation	Estimated Coefficient	Standard Deviation	Estimated Coefficient	Standard Deviation
Control Variable	Firm Age	0.000	0.001	0.000	0.001	0.000	0.001	0.000	0.001
	Gross Assets	0.001	0.001	-0.001**	0.000	0.001	0.001	-0.001**	0.000
	Small and Medium Enterprises	-0.001	0.002	-0.001	0.001	-0.001	0.002	-0.001	0.001
Firm’s Competence	Human Capital	0.000	0.001	0.001	0.001	0.000	0.001	0.001	0.001
	Customer Capital	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	Structural Capital	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Regional Competence	IP Input	-0.010***	0.003	-0.004**	0.002				
	IP Stock					0.000	0.003	0.000	0.002
	Financial Investment					-0.005***	0.002	-0.002**	0.001
	IP Infrastructure	0.002	0.002	0.001	0.001				
	Local Gov't					-0.003	0.002	-0.001	0.001
	Service					0.005*	0.003	0.001	0.002
	IP Activity	0.008**	0.003	0.003	0.002				
	Public Sector					-0.001	0.003	0.002	0.002
	Private Sector					0.002	0.002	0.000	0.001
	IP Performance	0.003	0.003	0.001	0.002				
	IP Creation					0.002	0.002	0.001	0.001
	Econ. Performance					0.012***	0.004	0.003	0.003
Constant Variable		-0.056***	0.021	-0.008	0.014	-0.084***	0.027	-0.012	0.018
Industry Dummy Variables		Included		Included		Included		Included	
No. of Observations		5,382		5,396		5,382		5,396	
R^2		0.019		0.015		0.022		0.016	

1) Asterisks ***,**,* each refer to 1%, 5%, 10% significance level, respectively.
2) The upper and bottom 2.5th percentile dependent variables are excluded as outliers.

5. Conclusion and Implications

This study explains the correlation between firms' excess performance and the region's innovation system. A firm's high performance in comparison with the industry average was found to be highly related not only to the efforts of individual firms, but also to the capability of the industry's or the region's innovation system. The study aimed to focus specifically on the IP capability in explaining a firm's performance above the market average.

Table 11 summarizes the results of this research. A firm's investment in R&D is related with each and every aspect of a region's IP capability. If a region's IP input is high, its IP infrastructure is solid, it is active in IP activities, and achieves excellent IP performance, a firm in the region will strengthen its R&D investment, thereby creating a virtuous cycle. However, the IP service market and private R&D system were found to not contribute much during this process compared to their public counterparts. Moreover, in order for a region's IP performance to influence a firm's excess performance, the region's IP creation and commercialization must be simultaneously invigorated. The fact that the average R&D concentration rate among firms was below 1%, as shown in Table 2, indicates that the contributions of the public sector are insufficient to continuously attract an intensification of R&D investment from the private sector.

The invigoration of the IP service market and education services was found to contribute to firms' growth. This stresses the need for the current system, which focuses only on market opening, to be strengthened in order to contribute not only to the R&D phase, but also to an overall enhancement in the productivity and industrial structure of a firm. But by its nature, the IP service market is one of the aspects most influenced by the agglomeration effect, and thus it is inevitable for this market to be concentrated on Seoul and five other metropolitan cities. A thorough planning which would provide services to other regions, while metropolitan cities act as market hubs, is therefore required.

Table 2 shows the slow growth of Korean Firms' productivity. It can be seen that IP activities contribute to a firm's productivity only when the public and the private sector work in synergy. In Daejeon, where IP activities of the public sector are vigorous, the private sector IP activities were poor, while in regions with strong private IP activities such as Seoul and Gyeonggi, the public sector's IP activities were poor. If the government seeks to support regional IP systems in regard to market down, the effects of the support policy may not trickle down onto individual firms. These results stress the need to reconsider the effectiveness of government policies, and to select and concentrate public and private resources on a single definite goal.

Table 11. Effects of region's IP capability on a firm's overall performance

	Growth	Profitability	Innovativeness	Productivity
IP Input			Contribution (Gov't financing, IP registration, etc.)	
IP Infrastructure	Partial Contribution (IP service market & education service)		Partial Contribution (Competence of local administrations)	
IP Activity			Partial Contribution (Public sector activities)	Conditional Contribution (Under the precondition of synergy between the public and private sector)
IP Performance			Conditional Contribution (Under the precondition of both IP creation and commercialization)	

However, it is still too early to overtrust the findings of this study, as there exist methodological and data restrictions in empirically assessing a region's innovation capacity in linkage with the performance of individual firms. Including detailed indices of regional IP capabilities as explanatory variables for multilateral interpretation may cause errors in interrelationship of variables. Also, in the methodological sense, this study considers the regional variables and firm variables as explanatory variables at an equal level, but these variables are in fact hierarchical data, as firms are located in a specific region. This calls for the need to apply a Multi-level model in the analysis, but due to certain restrictions the study utilized the least squares model. The empirical results of this study, which focused on the one-way effect of the regional IP capability on a firm's excess performance, neglected the mutual influence between the two variables, and therefore restricts us from extending the interpretation beyond statistic significance.

In further studies, it is necessary to enhance the methodology of the study, to modify the analysis model through reconstruction of the IP capacity indices, to collect the specialist's thoughts on the results, and to calibrate and systemize the mechanism related to how the IP capabilities influence a firm's performance.

References

Anselin, L., Varga, A. and Acs, Z. (1997) "Local Geographic Spillovers between University Research and High Technology Innovations", Journal of Urban Economics, Vol. 42, pp. 422-448.

Anselin, L., Varga, A. and Acs, Z. (2000) "Geographical Spillovers and University Research: a Spatial Econometric Perspective", Growth and Change, Vol. 31, pp. 501-515.

Bathelt, H., Malmberg, A. and Maskell, P. (2004) "Clusters and Knowledge: Local Buzz, Global Pipelines and the Process of Knowledge Creation", Progress in Human Geography, Vol. 28, pp. 31-56.

Braczyk, H., Cooke, P. and Heidenreich, M. (1998) "Regional Innovation Systems", Routledge, UCL Press.

Cooke, P., Gomez, M. and Etxebarria, G. (1997), "Regional innovation systems: institutional and organisational dimensions", Research Policy, Vol. 26, pp. 475-491.

Cooke, P. and Morgan, K. (1998), "The associational economy: firms, regions, and innovation". Oxford: Oxford University Press.

Evangelista R., Iammarino, S., Mastrostefano, V. and Silvani, A. (2002) "Looking for regional systems of innovation: evidence from the Italian innovation survey," Regional Studies, Vol. 36, pp. 173-186.

Feldman, M. P. and Audretsch, D. (1999), "Innovation in cities: science-based diversity, specialization and localized competition", European Economic Review Vol. 43, pp. 409-429.

Fratesi, U. (2004) "Regional Economies, "Innovation and Competitiveness in A system Dynamics representation", QUADERNI DI RICERCA (Universita Politechnica delle Marche, Dipartimento di Economia), pp. 204-210.

Jaffe, A. (1989), "Real Effects of Academic Research", American Economic Review, Vol. 79, pp. 957-970.

Lim, U. (2004) " Knowledge spillovers, agglomeration economics, and the geography of innovative activity; a spatial econometric analysis", The Review of Regional Studies, Vol. 34(1), pp. 11-36.

Marshall, A. (1919) "Industry and Trade", Macmillan.

Patel, P. and Pavitt, K. (1994) "National innovation system: When they are important, and how they might be measured and compared", Economics of Innovation and New technology.

Putnam, R. (2000). Bowling Alone: The collapse and Revival of community. Touchstone Books.

Schiuma, G. and Lerro, A. (2008) "Knowledge-based capital based in building regional innovation capacity", Journal of Knowledge Management, Vol. 12(5), pp. 121-136.

Scott, A. and Storper, M. (2003) "Regions, Globalization, Development," Regional Studies, Vol. 37(6-7), pp. 579-593.

Stern, S., Michael, E., Poter, J. and Furman, L. (2000) "The determinants of national innovative capacity", National Bureau of economic research, pp. 1-56.

Kim, Seok-jin (2005) "Regional Innovation and the Tasks of Regional Finance", Daegu Bank Economic Review, pp.50-73.

Kim, Seong-jong, Ko, Seok-chan, Ko, Kim, Hak-min (2006) "Analysis on Regional Innovation Potential for the

Establishment of Regional Innovation System", Korea Academia-Industrial Cooperation Society, Vol. 7. pp. 80-88.

Kim, Jeong-hong (2003) "An Empirical Analysis between Regional Innovative Capabilities and Regional Industrial Performances in Korea", The Korean Economic Association, pp. 99-121.

Kim, Jin-su, Choi, Myeong-shin (2007) "An Empirical Investigation of the Upper and the Lower Local Governments Innovation Capability in Korea“, Financial Knowledge Research, Vol. 5(2), pp. 29-57.

Kim, Hong-joo (2006) "Determinants of Regional Knowledge Production Based on Korean Patent Data", Korean Journal of Regional Science Vol. 22(3), pp. 95-115.

Lee, Hee-yeon (2010) “The Spatial Clustering of Knowledge Production Activities and Its Determinants of Regional Disparity based on Korean Patent Data”, Korea Intellectual Property Society, Vol. 5(1), pp. 115-149.

Jeong, Jae-jin, Lim, Chae-hong (2006) “Empirical Analysis on RIC (Regional Innovation Capacity) and LPIE (Location and Performance of Innovational Enterprises)”, Korea University Institute of Governmental Studies, Governmental Studies, pp. 171-201.

Heo, Dong-sook (2014) “The Influence of Innovative Capacity on Regional Economic Performance”, Journal of the Korean Geography Society, Vol. 49(6), pp. 884-896.

Korea Institute of Intellectual Property (2014), Developing a Model for Measuring the Intellectual Property Capacity of Regions.

Selection of 10 Emerging Technologies in 2017: Pollution & Contamination Response Technologies for Sustainable Development of Korea†

Jonghwa Park[1,*], Yoon A Kim[1], and Seung Ryong Lee[1]

Abstract
In 2017, KISTEP selected 10 emerging technologies, based on the issue of 'Environmental Pollution in Daily Life'. The issue of 'Environmental Pollution in Daily Life' was subdivided into 10 pollutants for further study, and detailed research was conducted to identify public needs through literature review, social data analysis, public polls, and review by specialists. Candidate emerging technologies were identified based on the database of future technologies, news clippings, and the recommendations by specialists. The final list of 10 emerging technologies were selected from the candidate pool through priority assessment by specialists and researchers, followed by social and economic impact assessment.
The selection for this year was focused on emerging technologies to counter environmental pollution in daily life, and support Korea's sustainable development. Environmental pollution has been intensified by past government policies prioritizing economic growth over environment. Damage from sensory and information pollution, which were not recognized as pollution in the past, has been increasing. Selection of public goods-related technologies as emerging technologies is expected to have significant implications.

Keywords: environmental pollution, 10 emerging technologies, sustainable development

1. Introduction

The increased influence and rapid development of science and technology have led to higher expectations regarding the social roles of emerging technologies. Nowadays, technologies are not only considered as the growth engine for new industries, but also as the means by which to address important issues faced by society, such as social stratification, low fertility and population aging, and climate change. National projects such as Research & Solution Development and public benefit programs are currently being operated. For effective utilization of limited resources, strategic selection of core technologies is needed. In this regard, research on the methodology to effectively assess core technologies based on thorough assessment of societal changes and public needs.

KISTEP has annually selected and announced 10 emerging technologies since 2009, and since 2013, has incorporated the betterment of future Korea as a focal perspective. KISTEP's selection process

Division of Technology Foresight, Korea Institute of S&T Evaluation and Planning (KISTEP), 12F Dongwon Industry Bldg., 68 Mabang-ro, Seocho-gu, Seoul, 06775, Korea
* Corresponding author: parkjh@kistep.re.kr

† This paper is based on the study for annual selection of KISTEP 10 Emerging Technologies as summarized in Issue Paper 2017-01 published by KISTEP.

emphasizes the social role of technologies, by first selecting the core issues of future Korean society, and then selecting emerging technologies with both technological and economic impacts, and the capacity to address these issues. The issues considered thus far include the aging of society, increasing safety hazards, increasing inequality, and the need to enhance the quality of life and social trust.

Among the numerous issues arising as side-effects of technological development prioritizing economic growth, the emergence of new types of pollutions has been attracting public attention to the role science and technology can play in sustainable growth. Despite technological developments, environmental pollution is still a serious issue. Especially over the last decade, new pollutants such as particulate matters have emerged, which have high impacts on human health. Light, noise, and odor, which were originally not considered as pollutants, are becoming bigger concerns due to industrialization and urbanization, further emphasizing the role of science and technology in providing solutions to social issues.

Table 1 shows an overview of the selection process of KISTEP Emerging Technologies. The selection process consists of two stages: analysis of future needs and selection of emerging technologies. The analysis of future needs was conducted in five stages: selection of target issues, literature review on pollution, big data analysis, identification of detailed issues & needs, and public survey. The selection of emerging technologies was conducted in four stages: compilation of technology pool, identification of candidate technologies, selection of emerging technologies, and in-depth analysis for each technology.

Table 1. Selection process of KISTEP Emerging Technologies

Stages	Steps	Methods
Analysis of Future Needs	Selection of target issues	- Review of domestic and international research
	⇩ Identification of issues and future needs	- Survey and analysis of current trends - Expert reviews - Big data analysis on social media
	⇩ Survey of public needs	- Public poll on mobile platform
Selection of Emerging Technologies	⇩ Candidate pool of future technologies	- Utilization of diverse data sets and internal DB - Analysis of means of addressing each future need through science and technology
	⇩ Selection of 10 emerging technologies	- Review by internal research staff and technological experts - Technology prioritization evaluation
	⇩ In-depth analysis of emerging technologies	- Trend analysis of research, industries, and markets of each technology - Economic and social impact analysis of technology

2. Analysis of Future Needs

2.1. Issues for the Selection of 2017 Emerging Technologies

‘Enviornmental Pollution in Daily Life’ was selected as a core issue in Korean society in 2017, through a comprehensive review of news, media, and major domestic and international future issue reports by internal and external experts. At a summit held during the 70th United Nations General Assembly in September 2015, the Sustainable Development Goals (SDGs) of the “The Agenda 2030 for Sustainable Development” was ratified and has been in effect since January 2016. The SDGs propose 17 goals and 169 tasks to bring concerted actions of the international society for next 15 years, for humanity and the Earth. (UN, 2016) The three pillars of economy, society and environment were adopted as the main agendas, and the SDGs were proposed as a means to resolve socioeconomic issues including poverty and human rights, and environmental issues regarding climate change, depletion of ozone layer, and loss of biodiversity. Many of the goals closely relate to the issue of environment, for example, 6. Clean Water and Sanitation, 7. Affordable and Clean Energy, 11. Sustainable Cities and Communities, 12. Responsible Consumption and Production, 13. Climate Action, 14. Life Below Water, and 15. Life on Land.

The Global Risks Report 2016 by the World Economic Forum (WEF) categorized risks to the global economy into economic, environmental, geopolitical, societal, and technological risks, and identified 29 risk factors. The report recognized the adverse effects from daily life pollution and environmental pollution including climate change, biodiversity loss and ecosystem collapse, man-made environmental catastrophes, failure in urban planning, food crises, and water scarcity as major environmental and social risks, and included information issues including critical information infrastructure/network breakdown, cyberattacks, data fraud and theft) as technological risks.

In the 2016 Environmental Performance Index (EPI), which is biannually reported by Yale University and Columbia University, Korea was ranked the 80th out of 178 countries. In particular, Korea was ranked 173rd in air quality due to the impact of particulate matters, and was also found to be vulnerable in fields of public health, climate, and energy. Korea’s relatively low EPI relative to GDP reflects its emphasis on economic growth without sufficient measures to manage pollution.

Based on the aforementioned results of literature review and internal workshops, various pollution and contamination caused by human activities were selected as target issues. This includes not only conventional forms of environmental pollution such as air, water, and soil pollution, but also includes recently emerging issues such as sensory pollution[2], chemicals in daily life, and mismanagement of invasive species. The topic also encompasses the concerns related to nuclear power plant incidents intensified by the earthquake which occurred in Gyeongju region in September 2016, and includes issues regarding radiation exposure in daily life. It also covers information pollution issues caused by unnecessary or erroneous information on the Internet, which tends to intensify with progressive informatization. The responsibility of resolving these manmade pollution and contamination occurring as side effects of industrialization lies with humankind. It aims to emphasize the role of science and technology in resolving these issues.

2.2. Analysis of Pollution and Contamination

Types of pollution from industrialization can be categorized into daily life pollution, radiation risk, and environmental pollution. Pollution in daily life

2 Seonsory Pollution refers to 3 major types caused by light, noise and odor, which distrupts vision, audibility, and sense of smell

includes sensory pollution from light, noise and odor, information pollution, and chemicals in daily life. Radiation risk refers to issues related to nuclear power plant incidents and radiation to which people are exposed in daily lives. Environmental pollution includes pollution of air, water, and soil, and disruption by invasive species.

2.2.1. Sensory Pollution

Korea's light pollution severity is ranked the second highest among G20 countries, following Italy (90.3%) (Falchi, F. et al., 2016). Of 125,000 total civil complaints over sensory pollution reported and registered in 2015, the majority were related to noise and vibration. Floor impact noises in apartments sometimes develop into conflicts between neighbors; in Hanam, Gyeonggi, complaints over floor noise escalated to the murder of a couple in their 60s who lived in the upper floor in 2016. During the last decade, civil complaints regarding odor increased 3.4-fold, and in particular, complaints from outdoor workplaces located in designated odor management zones were dramatically increased. Regarding the source of odors, 65% originated from eateries, agricultural manure, and sewers, and approximately 13.2% of total civil complaints regarding odor concerned residential facilities and small businesses, including printing services and laundry facilities. The increased ambiguity of the boundary between residential and commercial areas has been intensifying noise and odor pollution issues. Public concern over the adverse effects of sensory pollution on the human body is rising. Human exposure to light exceeding a certain level of luminosity suppresses the secretion of melatonin, a biorhythm controlling hormone, which results in increased fatigue, a weakened immune system, and growth impairment for children. Exposure to excessive noise results in an increased heart rate, contraction of peripheral blood vessels, and digestive disorder, and can lead to the long-term effects of blood circulation disorder from hormone secretion at the endocrine glands, and excessive stress.

2.2.2. Chemicals in Daily Life

Risks of products with substances which may induce endocrine disruptors, nanomaterials, and hazardous chemical substances were increased. Endocrine disruptors have emerged as one of the top 3 environmental issues, along with ozone layer depletion and global warming, raising concerns over the possible worldwide threat to the ecosystem. According to the UNEP report *Marine Plastic Debris and Microplastics*, it is estimated that 4.8 million to 12.7 million tons of plastic washed into the oceans in 2010 alone. Public anxiety regarding exposure to chemicals in daily life has increased following the lethal humidifier sterilizer issue of 2016 [3], as illustrated by massive refund incident of Median toothpaste. Insufficient education and information on chemicals in daily life has intensified public anxiety.

The adverse effects of endocrine disruptors and nanomaterials on the human body and environment are severe and difficult to detect. During the humidifier sterilizer incident, there was a great deal of conflict in terms of proving the sterilizer's impact on the human body, and the majority of reproductive system disorders induced by endocrine disruptors require a long time before symptoms occur. Nanomaterials may be absorbed into the human body through the use of nanomaterial products, and cause brain or cardiovascular disease (Kim, E., 2010). There are reports of decreased fertility, feminized male reproductive organs, thyroid malfunction, and immune system issues in wildlife caused by

3 Oxy humidifier sterilizer incident caused 239 deaths and 1,528 cases of serious fibrosis in lung tissue (Asian Citizen's Center for Environment and Health).

contamination from endocrine disruptors (Kang, C., 2007), which may lead to a decrease in the population and ecosystem collapse in the long-term. Microplastics may accumulate in the food chain, as predators ingest contaminated prey (Greenpeace, 2016). Residual nanoplastics may discharge toxic chemicals into seawater, or may adsorb marine chemicals, both resulting in the induction of toxic materials in the marine ecosystem (Greenpeace, 2016).

2.2.3. Information Pollution

Information pollution refers to the adverse effects of information overflow as society becomes informatized.

The present study focuses on adverse social phenomena originating from information exchange through SNS and the Internet. Information pollution was categorized into information overload, harmful information, information behavior, and associated negative social phenomena were classified accordingly to examine their respective causes. Excessive provision of information due to developments in SNS leads to a decline in perception, decrease in work efficiency, and psychological damage. Information fatigue syndrome causes symptoms such as impaired judgement, anxiety, increased self-doubt, and scapegoatism. According to the SNS Usage Statistics of Korea in 2011, 40% of SNS users answered that their stress was increased by using social media (Dong-A Ilbo, 2011), and some even avoid using SNS due to various reasons including feelings of relative deprivation. Diversification of SNS and Internet media leads to an increase in malicious posts (comments), false information, and spam email. Damage from the proliferation of false information through SNS is characterized by the uncertainty of responsible parties due to the process of proliferation and exaggeration. "Post-truth," which was selected as the word of the year by Oxford Dictionary in 2016, means "relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief." The issue of school violence and bullying has extended from physical violence to the emotional violence of cyber-bullying, and in particular, closed SNSs (instant messaging such as Kakaotalk) are usually the forum for cyber-bullying.

Differences in individual behavioral tendencies (fact-checking) exist when faced with information overload, and serves as the source of various social conflicts. Neglecting to fact-check results in the proliferation of harmful information. Recently introduced systems of SNS, including autocomplete suggestions or automatic adapted information provision, leads to exposure to biased information, if individuals do not make an effort to seek out diverse opinions. Repeated exposure to biased information may lead to the increase in mutually slanderous posts. Lack of individual and social awareness has also lead to rampant violations of copyrights and privacy.

2.2.4. Radiation Risk

Exposure to radiation can occur in our daily lives. Laborers who handle radioactive materials are at risk of repeated exposure. Contaminated food and products may lead to internal exposure. High level radioactive waste from nuclear power plants and industrial facilities increases risk of radiation accidents. Terrorism activity using radioactive material from industrial, medical and experimental equipment can also pose a threat.

Due to the increased risk of earthquakes on the Korean Peninsula, risks of nuclear power plant accidents has increased. Following the Gyeongju earthquakes of September 2016, fears that Korea is no longer safe from earthquakes arose, which led to concerns over nuclear reactors designed to withstand earthquakes up to magnitude 6.0 on the Richter scale. Kori Nuclear Power Plant in Busan is the largest nuclear power plant complex in the world, and if an accident were to occur, the number of casualties is estimated to be approximately 20 times that of the Fukushima accident due to the high population density (Greenpeace, 2012).

Emergency response is also needed for possible nuclear power plant accidents in neighboring countries. On February 2, 2017, Tokyo Electric Power reported that the highest radiation level of 530 sieverts (sv) per hour was measured at the containment vessel of reactor 2 in Fukushima Daiichi Nuclear Power Plant. Thus, the anxiety over Japanese radiation continues, especially after the Fukushima Daiichi nuclear accident in 2011 (The Hankyoreh, 2017.2.3.). This level of radiation is 7 times higher than 73 sieverts, which was measured one year after the incident in 2011. Human exposure to 73 sieverts can lead to death in less than a minute. Currently, there are 13 nuclear power plants on the Chinese shores near the Korean Peninsula, and more than 100 plants are under construction or in the planning process. Therefore, international measures to mitigate the damage in the event of possible accidents involving Chinese nuclear power plants are required.

2.2.5. Invasive Species

Korea's EPI ranking for Biodiversity and Habitat has continued to fall for the last 4 years, and Korea was ranked the lowest compared to other countries in 2016. Many non-indigenous species that were imported without review as pets are already classified as invasive species by other countries or have the potential to turn invasive. Problems arise as these species are frequently abandoned. There are cases in which certain species were imported for a specific purpose, but later failed to achieve their intended purpose and became an invasive species. Giant apple snails were adopted for eco-friendly farming, but their high reproduction rate and appetite led to damage to agricultural produce, and the deterioration of the ecosystem.

The annual loss to the global economy caused by invasive species has reached approximately 1.67 trillion KRW (Institute for European Environmental Policy (IEEP). 2016). There has been an increase in invasive species due to advancements in vessel and aircraft technology, increased immigration and travel, trade liberalization, and increased international trade. According to "Global Exchange and Accumulation of Non-native Plants," a paper published in the journal Nature, 13,168 invasive plant species have been spread outside their native habitat due to human intervention. This number accounts for 3.9% of the world's plant species, and is almost equal to the total number of indigenous plants found in Europe. In 2008, damage in Europe caused by invasive foreign species amounted to approximately 16 trillion KRW (The Kukmin Daily, 2015), and damage to agriculture caused by insects amounts to 30 to 40% of the global yield, with which 1 billion persons could be fed (The Segye Times, 2016). Some alien species can act as carriers of certain diseases (mainly insects), and a number of them are reported to be physically hazardous to humans. Examples include yellow fever, Japanese encephalitis, malaria, Zika fever, and African sleeping sickness. Global health costs caused by invasive insects, including mosquitoes which carry dengue fever, are estimated as 6 billion USD (The Segye Ilbo, 2016).

2.2.6. Air Pollution

The annual number of days on which particulate matter warnings were issued is increasing every year (Seoul Air Quality Information), and measures to monitor and mitigate PM2.5 are insufficient. International air pollution indices report that Korea's air pollution is quite severe. In the Better Life Index

(BLI) of 2016, Korea was ranked the lowest among 38 countries regarding air quality. Korea was also ranked 160th in the EPI regarding air quality. According to the OECD report "The Economic Consequences of Outdoor Air Pollution," Korea will face the highest premature mortality rate and the biggest economic damage from air pollution among member states in 2060. It is predicted that if Korea does not take additional measures to mitigate air pollution, the premature mortality rate in Korea will steeply increase by 3.1-fold, from 359 deaths per one million population in 2010, to 1,109 deaths per one million population in 2060. Korea is the only country among the major OECD member states with a premature mortality rate forecast exceeding 1,000 deaths. Korea would also suffer from the largest economic damage, reaching up to 0.63% of the GDP. It is predicted that annual worldwide GDP loss, from increased medical costs, decreased labor productivity, and decline in agricultural yield, due to diseases caused by air pollution would reach 1.6 trillion USD (3,015 trillion KRW) in 2060.

While larger particulate matters (PM10) entering through the nose and the mouth only reach up to bronchial tubes and lungs, ultrafine particulate matters (PM2.5) may reach the alveoli, where gas exchange takes place, and affect blood vessels and other organs. Thus the impact of ultrafine particulate matters needs to be assessed continually. According to WHO, a $10\mu g/m^3$ increase of PM2.5 will lead to an 0.9% increase in the mortality rate, an 1.3% increase in the mortality rate from respiratory diseases, and an 1.1% increase in the mortality rate from cardiovascular diseases. Ultrafine particulate matters were classified as Grade 1 carcinogens in 2013. According to a Taiwanese study on 23,000 subjects, long-term exposure to PM2.5 increased the chance of liver cancer (Pan, W. C., 2015). Air pollution may not only directly affect organisms, but also have impacts on soil and water pollution through meteorological phenomena. Air pollutants may move through air and accumulate in coastal waters, damaging the marine environment. Sedimentation of nitrogenous pollutants has been linked to the steady increase of nitrate concentration in the East Sea, Yellow Sea, and East China Sea (Kim, I. N. et al., 2014).

2.2.7. Water Pollution

The numbers of days in which algal blooms appear in Nakdong River is increasing, from 100 days in 2013, to 143 days in 2014, and to 171 days in 2015. Eutrophication caused by organic matters in domestic sewage and manure is the cause of algal bloom, which turns the water into "dead zones" uninhabitable to fish and other aquatic organisms. Water pollution may impact the human body and give rise to social issues. Heavy metals and organic compounds from synthetic detergents and agricultural pesticides do not degrade and pollute the water, threatening the aquatic ecosystem. These chemical compounds may also accumulate in the human body through consumption of water or marine products. Such adverse effects may also lead to insufficient clean drinking water, and a lack of water resources. The Ministry of Environmental Protection of the People's Republic of China’s considerable spending on the prevention of water pollution suggests a potential boom in the water quality management business. Due to the greater demand of sewage treatment expected, China's sewage treatment market is expected to grow to reach CNY 69.6-86.7 billion within the next three years (Xinhua News Network, 2015).

2.2.8. Soil Pollution

Urban expansion leads to the development of former industrial, army base, and mining areas, turning soil pollution which took place in the past into serious socioeconomic concerns. Following the large-scale relocation of the US armed forces in Korea, serious soil pollution was found in areas formerly used as bases by for more than 50 years. Reported cases include oil contamination in Gimje US missile base, oil and benzene contamination in Noksapyeong station near Yongsan base, and detection of dioxin in Camp Market of Bupyeong (Ecomedia, 2015). Numerous cases of soil pollution being detected in former industrial areas, after multiple changes of ownership, have led to conflicts over attribution of responsibility. Because the soil is immobile, large amounts of contaminants may not be visually apparent, and even pollution tests of nearby regions mostly show clean results (Park, Y. H., 2002). Although soil pollution is contained a limited area, the contamination persists even after eliminating its source. there is also the possibility of additional pollution through the spread of pollutants to other media, including nearby subterranean water, rivers, and air (Park, G., 2012). Recently, contamination near livestock burial grounds has been identified as another cause of soil pollution (Ryu, J. G., 2014). Because burial grounds offer suitable conditions for pathogenic microorganisms, there is high possibility of zoonotic viruses existing in leachate. If the leachate is not treated in the early stage, there is a risk of secondary environmental pollution in nearby groundwater and rivers, as well as in surrounding soil. Because excavation is legally allowed after 3 years from the livestock burial, the implementation of measures to treat the leachate is urgent. Increase in loss of soil is also caused by urbanization. Net value of Korean surface soil is approximately 26 trillion KRW, and the average volume of annual loss of soil is 32 tons per 100 ha, which is almost 3 times the average of 11 tons among OECD countries.

2.3. Identification of Issues and Needs Related to Pollution

Specific issues and needs closely related to pollution in daily life and environmental pollution in Korean society were identified, through literature reviews, and professional consultation. A total of 33 environmental issues and 58 needs from 10 types of pollution were identified. The four phases of the disaster management process, which are Prevention, Preparedness, Response, and Recovery, were reinterpreted and applied to addressing pollution in daily life and environmental pollution.

- Prevention: Activities designed to eliminate or reduce the possibility of pollution by eradicating or reducing its causative substance. Such activities include diagnosis, preventive measures, and mitigative measures.
- Preparedness: Activities designed to reduce the damages and negative impacts of pollution. Such activities include establishing an early warning system, prediction measures, real-time diagnosis, managing harmful factors, physical and environmental risk analysis and ·assessment.
- Response: Short-term measures designed to stop the dispersion of and reduce the impact of damage, and reduce the possibility of secondary damage by rapidly responding to pollution. Such activities include purification, elimination, dispersion preventing measures, and the use of personal hygienic items.
- Recovery: Long-term measures designed to recover the damaged environment to the original state, and includes recovery, waste processing, and resource recovery.

Table 2. Identified issues and needs related to pollution

Pollution	Major Issues	Needs	Process
Light Pollution	- Concerns over harmfulness of light pollution on the human body - Lack of specific standards for Korea - Lack of proper recognition and regulation on light pollution	- Automatic control of excessive lighting (depending on time, place, situation, etc.)	Prevention /Preparedness
		- Reform of regulations on lighting of public facilities (upward light, lighting time, etc.)	Prevention /Preparedness
		- Development of products that help the recovery of personal biorhythm	Response
		- Risk assessment system and standards that consider individual (age, gender, etc.) and environmental differences	Response
Noise Pollution	- Increasing conflicts from noise in residential areas (Floor impact noise, and noise from community facilities, etc.) - Increase in noise and vibration pollution near construction sites and traffic facilities - Lack of specific standards on sound quality	- Active noise control and reduction	Response
		- Inexpensive and lightweight soundproofing materials and facilities for households	Preparedness
		- Effective education on noise-related etiquette	Preparedness
		- Price reduction and longevity improvement of noise reduction technology (in household appliances, transportation, etc.)	Prevention /Preparedness
		- Personalized noise standards (based on gender, age, experience, etc.)	Preparedness
Odor Pollution	- Lack of laws related to odor in residential and urban areas - Difficulty in control (Difficult to assign responsibility as odors arise from multiple causes, and difficult to record as odors disperse)	- Establishment of system for living odor control (Establishment of living odor standards and related guidelines that fit domestic situation)	Prevention /Preparedness
		- Monitoring of odor sources in daily life	Preparedness
		- Installation and maintenance of customized odor reduction facility based on the odor source	Prevention /Preparedness
Chemicals in Daily Life	- Insufficient information on chemicals in daily life - Rising concerns over the harmfulness of chemicals in daily life (fake products, endocrine disruptors, nanomaterials, etc.)	- Setting customized chemical material safety guidelines based on use method (inhalation, ingestion, skin penetration, etc.) and users (particularly vulnerable groups such as elderly people) and providing information	Prevention /Preparedness
		- Development of substitute materials for hazardous chemicals (endocrine disrupters, etc.) in consumer chemical products	Prevention
		- Securing the safety of consumer chemical products in a complete cycle of production, distribution, consumption and disposal	Prevention /Preparedness
		- Simple and accurate method to identify fake products	Preparedness
Information Pollution	- Privacy invasion - Infringement of copyright - Spread of malevolent posts - Lack of critical judgement regarding information - Spread of polarized opinions	- Automatic identification of malicious comments (development of algorithm and UI)	Prevention /Preparedness /Response
		- Educating the public through media (in ethical/functional aspect)	Prevention

Pollution	Major Issues	Needs	Process
		- Information source tracking and fact-checking	Preparedness /Response
		- Providing opportunity to be exposed to various information	Prevention /Preparedness
		- Filtering excessive information (based on personal information)	Preparedness
		- Copyrighting, identifying, and tracking of posts and content in all forms	Prevention /Preparedness /Response
		- Enhancing security and awareness of personal information	Prevention
Radiation Risk	- Safety concerns due to natural disasters - Safety concerns on food and beverages contaminated by radiation - Concerns over the influence of environmental radiation on the human body - Possibility of accidents from careless handling of industrial/medical radiation sources	- Closure of aged nuclear power plants	Recovery
		- Safe management of radioactive waste	Recovery
		- Prevention of nuclear plant accidents caused by accidents and disasters	Prevention /Preparedness
		- Provision of accurate information on presence of radioactive contamination in daily life such as in food ingredients and building materials	Preparedness
		- Real-time monitoring of radioactive contamination in neighboring countries	Preparedness
		- Replacement for industrial use of radioactivity such as in nondestructive testing equipment	Prevention
		- Safe management of medical radiation devices and radiation sources and scientific management for human safety	Preparedness
		- Accurate verification of effects of radiation on human body	Preparedness
		- Rapid decontamination in the event of radiation exposure	Response
		- Development of therapeutic agents for patients with radiation exposure	Response
Invasive Species	- Increase in invasive species due to abandonment and release of foreign species and pets - Increasing risk of extinction for indigenous animals and plants, and increasing damages to farm produce due to invasive species (spotted lanternfly, etc.) - Lack of social system related to invasive species (sanctions, monitoring, alert, education, etc.) - Lack of scientific, economic, and quantitative assessment of the damages caused by invasive species	- Improving the efficiency of invasive species monitoring	Preparedness
		- Finding measures to effectively remove invasive species without harming the ecosystem	Response /Recovery
		- Strengthening quarantine to prevent unintentional introduction of invasive species (particularly organic matter, plants and insects that can cause disease)	Prevention /Preparedness
		- Strengthening regulations on dangerous invasive species sold as pets, and strengthening the social system to prevent abandoning of pets (pet registration system, etc.)	Prevention /Preparedness

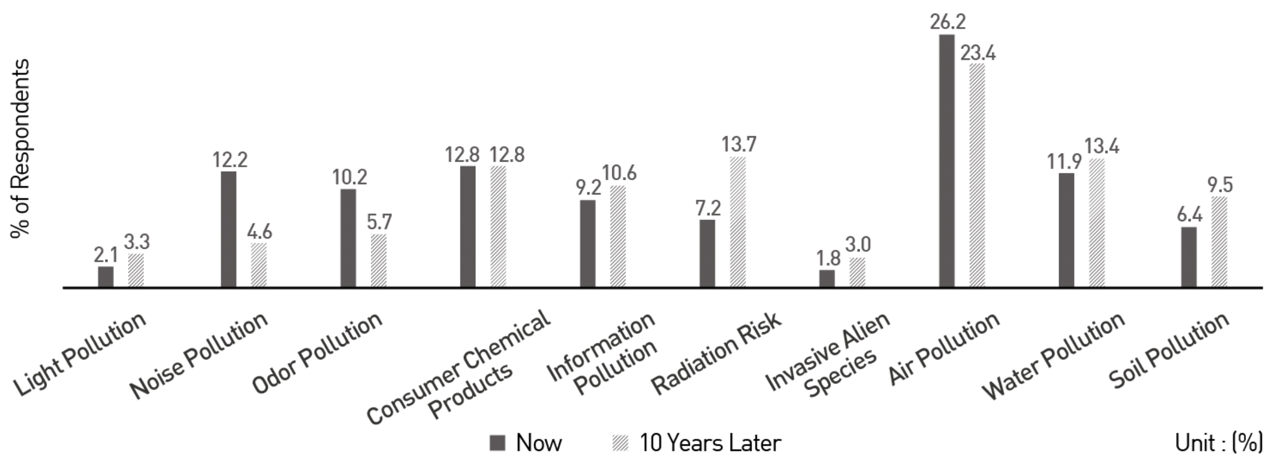
Pollution	Major Issues	Needs	Process
		- Education and promotion of the dangers of invasive species	Prevention /Preparedness
		- Database systematization for ecosystem management	Preparedness
Air Pollution	- Lack of verification on the influence of ultrafine particulate matters on human body and ecosystem - Increased occurrence of ultrafine particles - Continued emission of exhaust gas from the use of fossil fuel	- Understanding the cause of ultrafine particulate pollution	Prevention
		- Improving efficiencies related to purifying and removing ultrafine particles (Regional/National)	Response /Recovery
		- Expanding the real-time ultrafine particle monitoring system to the national level	Prevention
		- Improving the accuracy of ultrafine particles forecasting	Preparedness
		- Assessing influence of ultrafine particles on human body and ecosystem	Preparedness
		- Researching and developing products that prevent the absorption of ultrafine particles by the human body, and that helps to release ultrafine particles from human body	Response
		- Supplying low-cost exhaust gas filters for deteriorated automobiles	Preparedness
Water Pollution	- Increased occurrence of green & red tide - Health risk to aquatic ecosystem - Lack of water resources	- Accurately analyzing the cause of the increased occurrence of green & red tide and prediction of massive outbreak of them	Prevention /Preparedness
		- Reducing the cause of green & red tide (wastewater treatment, non-point pollutant management, etc.)	Prevention /Preparedness
		- Researching and developing methods for removing green & red tide in an eco-friendly way	Response
		- Preparing environmental standards for the protection of the aquatic ecosystem	Preparedness
		- Expanding the reuse of wastewater and the recovery of reusable substances and energy	Recovery
		- Efficiently distributing water resources	Recovery
Soil Pollution	- Deterioration of soil quality (vulnerable soil, improper management of landfill and burial sites) - Increase in disputes regarding soil near pollution source - Threat to soil ecosystem - Increase in soil loss	- Expanding the reuse of soil	Recovery
		- Continuously monitoring soil pollution near landfill and burial sites	Prevention /Preparedness
		- Improving the accuracy of tracking soil pollution and ground-water contamination	Response
		- Reducing the costs of purifying polluted soil	Response
		- Preparing environmental standards for the protection of the soil ecosystem	Preparedness
		- Engaging in eco-friendly urbanization that minimizes soil loss	Preparedness

Table 3. Survey respondents information (Area/Age)

Area	Number of People	Age Group	Number of People
Seoul/Gyeonggi area	90	10s	90
Gangwon area	90	20s	90
Chungcheong area	90	30s	90
Jeolla area	90	40s	104
Gyeongsang area	90	50s	89
Jeju area	90	60s	77

Note : The number of respondents in their 40s was increased, as there was a limited number of respondents in their 50s and 60s in Gangwon and Jeju area.

Figure 1. Comparisons of answers from respondents on pollution & contamination (Present/10 Years Later)



2.4. General Survey on Pollution

A survey was conducted to understand the general public's awareness on pollution and contamination, with the purpose of using the survey data in selecting emerging technologies. A survey was conducted on 540 respondents via mobile devices, classified by area and age.

2.4.1. Critical Analysis of Top 10 Types of Pollution

Air pollution was considered the top priority, both for the present and for 10 years from now.

Radiation risks, water pollution, and soil pollution were expected to worsen 10 years from now.

Noise pollution and odor pollution were considered important now, but their importance was expected to decrease drastically in 10 years.

2.4.2. Critical Analysis on Top 10 Pollution Issues

A comparison on the selection rates by item revealed that there are issues considered as difficult to solve even in a ten-year time period.

Issues regarding insufficient water resources and radiation risks due to accidents or natural disasters were expected to gain bigger recognition in 10 years.

3. Selection of Emerging Technologies

3.1. Identifying Candidates of Emerging Technologies

The candidate technology pool was formed through an expert review of potential candidate technologies using diverse research paths that reflect recent trends in technology development and social needs for new technologies. Technologies that satisfy social and technological needs were chosen from those registered in KISTEP's internal database and the database of future technologies selected and announced by domestic and overseas institutions. Future technology related contents of 'KISTEP News Clipping (Domestic press / Online news DB, Nov 2015 ~ Oct 2015)' was analyzed. Future technologies reflecting social needs in Korea were identified. In addition to reviewing potential emerging technologies selected through the above processes, technological experts also suggested the inclusion of technologies related to domestic and environmental pollution issues in order to address the related needs. The final candidate technology pool was formed after reviewing the relevance with future needs.

Figure 2. Top 10 items with the highest rates of changing issues in 10 years

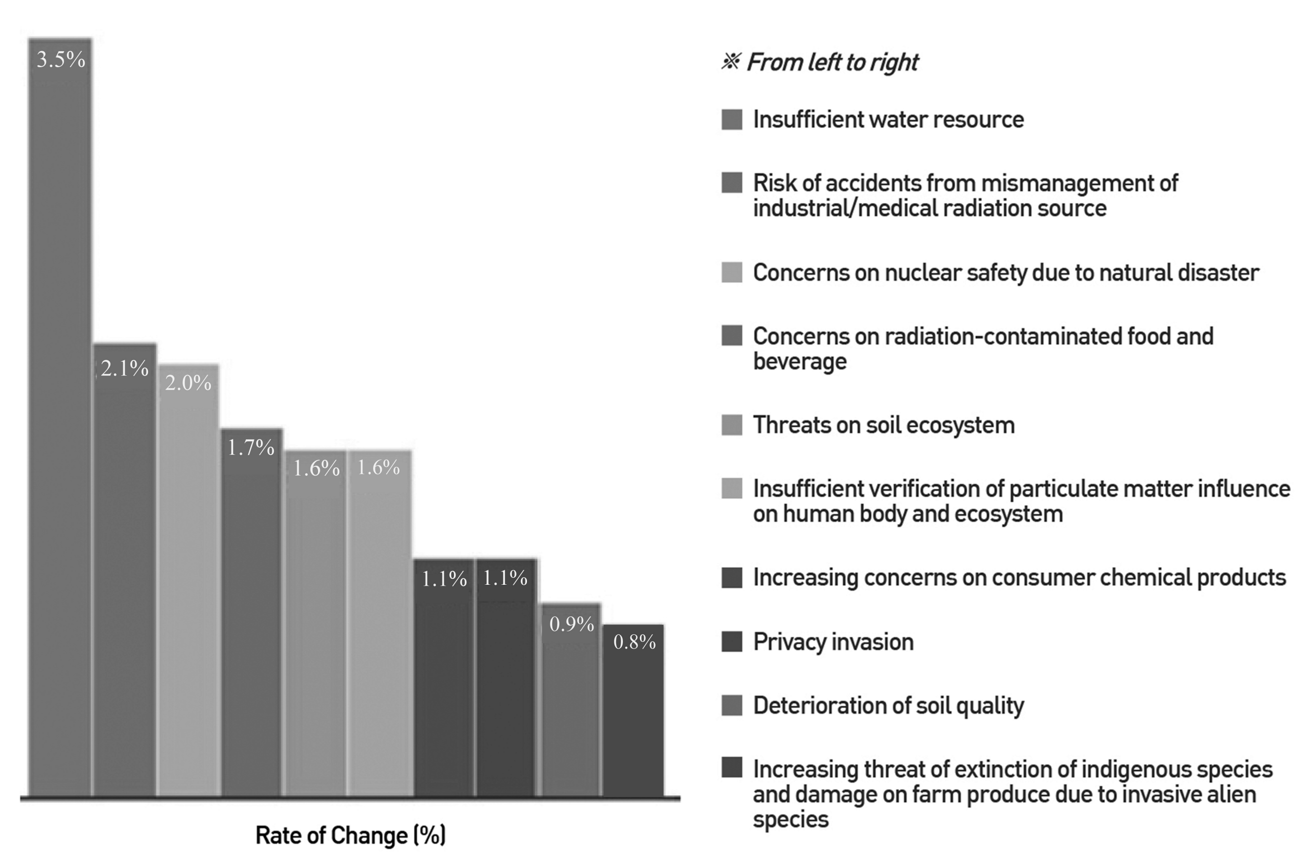


Table 4. Candidate technologies

Pollution	Candidate Technologies
Light Pollution	- IoT-based context-aware dimming technology - Biorhythm customized dimming technology - Light pollution risk assessment technology using model animals
Noise Pollution	- Active Noise Control & Reduction Technology - Ultra directional speaker - Inexpensive and durable noise reduction construction material technology
Odor Pollution	- Real-time odor monitoring and abatement technology - Septic tank / sewerage odor reduction technology - Combined treatment system for odor elimination
Consumer Chemical Products	- Real-time monitoring sensor for endocrine disrupters - Biological and environmental suitability assessment technology for nanomaterials - Environmentally friendly, nontoxic alternative technology for hazardous chemicals - Biocide risk assessment technology
Information Pollution	- Automatic screening technology for malicious posts - Digital watermarking technology - AI based fact-checking technology - Model-based collaborative filtering algorithm - Electronic fingerprint technology
Radiation Risk	- Technology for decommissioning of aged nuclear power plants - Nuclear power plant accident response system - Non-radioactive non-destructive testing technology - Pyro processing - Real-time monitoring system for radioactive contamination - Integrated management system for information on radiation exposure in daily life - Technology for discharging radioactive substances within human body
Invasive Species	- Navigation robot for ecosystem monitoring - Technology for remote monitoring of invasive species - Environmentally friendly technology for elimination of invasive species
Air Pollution	- Eco-friendly artificial rainfall technology using laser - Ultrafine particles monitoring technology - AI-based Korea customized fine dust prediction system - Ultrafine particles removal technology - Vehicle mounted non-powered dust collector - Technology for tracking path and evaluating volume of ultrafine dust generation - Technology for assessing impact of ultrafine dust on the human body
Water Pollution	- Biosensor technology for real-time monitoring of harmful algal tides - Harmful algae removal robot - Environment-friendly green & red tide removal technology - Smart Water Grid - Waste water recycling technology - Marine environmental restoration technology using microorganisms - Technology for real-time monitoring of water quality using satellites
Soil Pollution	- Advanced Domestic Waste Sorting System - City mines - Bio charcoal - Technology for treatment of Soil hazardous heavy metal - Natural material for plant protection - Soil Ecosystem Health Assessment Technology

Table 5. Criteria for evaluation of appropriateness as emerging technologies

Criterion	Contents
Concreteness	• Excluded products and services for which no specific technology can be derived
Novelty	• Excluded products or services that can be produced or provided with the current level of technology, given sufficient capital and political or systemic support
Social and Technological Realization Possibility	• Excluded technologies with significantly low realization possibility within the next 10 years from a technological and/or social perspective

3.2. Results of 2017 KISTEP Selection of 10 Emerging Technologies

After examining the candidate technology pools for appropriateness as emerging technologies, 20 technologies were selected. Evaluation was based on three criteria: concreteness, novelty, and realization possibility. KISTEP's internal research team and experts in each field of future needs participated in the evaluation.

Priority evaluation was conducted by KISTEP researchers and experts in each field on the 20 candidate technologies selected. Priority evaluation was conducted based on four criteria: possibility of actualization within 10 years, capability to respond to future issues, economic impacts, and technological impacts. The evaluation was performed in two-stages by KISTEP researchers and technological experts of relevant fields. Each of the 20 technologies were evaluated and given a score out of 5 for 4 different criteria, and each criteria was assigned weights. Response certainty was also surveyed and reflected in the analysis of survey results. The composite scores for each technology (maximum: 20) were calculated based on weights of each of the four criteria. Two-stage evaluation was performed, with the first stage based on information regarding future needs and technologies, and the second stage based on trend analysis with experts.

Table 6. Evaluation criteria for selection of Emerging Technologies

Criteria	Standards	Weight based on survey
Realization Possibility in 10 years	The possibility of complete development and commercialization of technology, enabling practical use by the public in 10 years	24.3
Capability to Respond to Future Issues	The expected scale of impact from the realization of the technology in terms of the resolution of key issues in the future	31.3
Economic Impacts	The potential of creating added value expected from the realization of the technology	21.3
Technological Impacts	The expected contribution to leading innovative development in the same or other fields of technology	23.1

Table 7. Results of survey for 20 candidate technologies

Rank	Candidate Technologies	Realization Possibility	Responsiveness to Future Issues	Impacts		Overall*
				Economic	Technological	
1	Nuclear Power Plant Accident Response System	3.63	4.25	3.50	3.72	15.27
2	Particulate Matter Reduction Technology	3.69	4.09	3.64	3.66	15.19
3	Real-time 3D Environmental Change Observation Technology	3.59	3.96	3.61	3.82	15.05
4	IoT-based Context-aware Dimming Technology	4.15	3.51	3.38	3.43	14.47
5	AI-Based Prediction System for Particulate Matter	3.41	4.02	3.34	3.41	14.34
6	Advanced Domestic Waste Sorting and Recycling System	3.76	3.63	3.52	3.34	14.28
7	Ecological Restoration Technology using Microorganisms	3.45	3.66	3.60	3.54	14.28
8	Eco-friendly Green & Red Tide Elimination Technology	3.32	3.96	3.53	3.33	14.27
9	Active Noise Control & Reduction Technology	3.48	3.64	3.48	3.53	14.16
10	Non-radioactive Non-destructive Testing Technology	3.45	3.42	3.42	3.61	13.88
11	Real-time Odor Management and Reduction Technology	3.57	3.56	3.28	3.39	13.86
12	Nanomaterial Bio- and Eco-compatibility Assessment Technology	3.49	3.58	3.18	3.49	13.81
13	Sewage & Wastewater Recycling Technology	3.50	3.37	3.49	3.48	13.81
14	Plant Protectant using Natural Substances	3.52	3.43	3.35	3.40	13.72
15	AI Fact-checking Assistive Technology	3.69	3.54	2.97	3.35	13.64
16	Ultra Directional Speakers	3.55	3.56	3.12	3.28	13.60
17	Automatic Online Posting Screening System	3.99	3.55	2.74	2.90	13.35
18	Biorhythm Customized Dimming Technology	3.89	3.06	3.10	3.09	13.11
19	Smart Water Grid	3.47	3.19	3.39	3.07	13.10
20	Risk Assessment Technology using Animal Models	3.36	3.33	2.93	3.10	12.79

* Calculated based on weights determined through survey

The 10 Emerging Technologies were selected based on a priority evaluation of 20 candidates, and specialist/researcher review on the technologies' impact and responsiveness to future issues. Priority evaluation results were considered in conjunction with the technologies' strategic importance to the nation. Multiple technologies were merged based on their similarity, and some of them were renamed to enable easier comprehension. The distribution of technologies was considered based on detailed categorization of pollutants, and technologies applicable to multiple forms of pollution were selected as a priority.

3.3. Social and Economic Impacts of Emerging Technologies

The economic and social impacts that are likely to follow the adoption of the 10 emerging technologies were analyzed, focusing on the individuals and the industries that the implementation of each technology will affect.

Table 8. KISTEP 10 Emerging Technologies in 2017

Technology	Details
IoT-based Context-aware Dimming Technology	[Definition] Dimming technology which enhances utilization and energy efficiency through automatic control of the direction and brightness of lighting, by recognizing outdoor conditions; or, which mimics sunlight indoors, enabling customized lighting for personal health care [Applicability] When applied outdoors, saves energy, and prevents crime and light pollution by automatically controlling the lighting's brightness, hue, and angle based on environmental changes (season, climate, etc.) and surroundings (sounds, human movements, etc.). When applied indoors in conjunction with IoT, enables effective biorhythm control, health management and treatment by having the effect of natural light exposure, providing particular benefits for night shift workers, and critically ill patients in intensive care wards
Active Noise Control & Reduction Technology	[Definition] Active noise reduction technology which predicts the occurrence of noise in real-time and generates sound waves of the inverted phase [Applicability] Applicable on public facilities (subway tunnels, airports, expressways, etc.) where noise occurs repeatedly; enables active noise control based on human movement in a home environment
AI Fact-checking Assistive Technology	[Definition] AI-based software which fact-checks in real time during speeches or debates [Applicability] Helps fact-check speeches of politicians, and enables a transparent information service which can prevent false or misleading rumors from spreading
Nuclear Power Plant Accident Response System	[Definition] Integrated nuclear power plant accident response system, which encompasses all technologies needed for different scenarios [Applicability] Plans emergency response against nuclear power plant accidents, such as simulating major accident scenarios, evacuation technologies, information security, physical protection, integrated real-time risk assessment, monitoring and quantification technologies, nuclear accident management robots, AI-based remote surveillance, and automatic responses
Non-radioactive Non-destructive Testing Technology	[Definition] Non-destructive testing technology using non-radioactive substances or devices which can replace the radioisotopes currently used for testing [Applicability] Ensures safe use and fundamentally prevents the risk of misuse for nuclear terrorism by eliminating the risk of radiation

Technology	Details
Particulate Matter Reduction Technology	[Definition] High-efficiency, low cost particulate matter collection and reduction system, which eliminates particulate matters (PM2.5) and causative agents [Applicability] Initially eliminates particulate matters from the source of pollution before diffusion into the air, and effectively reduces particulate matters indoors and outdoors
Eco-friendly Green & Red Tide Elimination Technology	[Definition] Eco-friendly technology which effectively eliminates harmful algae and nutrient salts without environmental side effects [Applicability] Effectively eases green and red tides by selectively eliminating specific harmful algae using algae coagulants made from natural substances
Advanced Domestic Waste Sorting and Recycling System	[Definition] Recycling technology which categorizes waste materials into metal, plastic, paper, etc., maximizing recycling and waste-to-energy recovery [Applicability] Reduces public burden of sorting waste into different categories, and enhanced precision of waste management will dramatically increase the recycling rate of waste materials
Real-time 3D Environmental Change Observation Technology	[Definition] Integrated technology which monitors and analyzes real-time changes in the environment and the ecosystem, using IoT, satellites, and unmanned aerial vehicles [Applicability] Enables real-time monitoring of diverse forms of pollution and contamination, including red and green tides, soil contamination, air pollution, and proliferation of invasive species
Ecological Restoration Technology using Microorganisms	[Definition] Ecological restoration technology using microorganisms to decompose toxic or recalcitrant chemicals [Applicability] Enables oil removal in oil spill situations using microorganisms, eco-friendly processing of food waste using marine protists, production of bio-diesel and other chemicals from biomass, and effective and eco-friendly extraction of valuable metals from waste resources

Table 9. Social and economic impacts of selected technologies

Emerging Technology	Social Impacts	Economic Impacts
IoT-based Context-aware Dimming Technology	• Context-aware lighting can be applied to workplace illumination, the main culprit of light pollution and trespass, and enable night lighting practices and enhances public safety, environmental protection and energy savings. • The development of an active lighting technology for personal biorhythms enables automatic lighting control according to individual physiological conditions, contributing to the promotion of public health.	• European market for lighting control and management systems: USD 1.188 billion ('20) • European market for human-centered lighting: USD 2.42 billion ('20)
Active Noise Control & Reduction Technology	• The development of active noise control and reduction technology can reduce disputes and civil complaints, which not only reduces social costs but also improves the quality of life for the general public	• Global market for automobile noise control devices: USD 1.7 billion ('18)

Emerging Technology	Social Impacts	Economic Impacts
	• The development of active noise control and reduction technology can reduce aperiodic impulse noise generated from construction sites, providing protection for workers' hearing, enhanced work safety and a calm surrounding environment.	
AI Fact-checking Assistive Technology	• The technology will enable immediate fact-checking on speeches in real-time, allowing listeners to differentiate between credible and non-credible speakers, and greatly help in making many political decisions. • The costs previously involved in fact-checking may be reduced, and the technology could also aid media spokespersons and judicial personnel in making just decisions for the society. • The introduction of fact-checking technology will greatly increase media credibility and the general credibility of information in society.	• Global market for media-related AI: USD 1.161 billion ('22) • Global market for natural language processing: USD 18.65 billion ('22)
Nuclear Power Plant Accident Response System	• Nuclear power plant accident-decision making process and citizen evacuation aid systems could be applied to other types of disasters. Casualty numbers and economic damage will be significantly reduced. • Securing the safety of citizens near nuclear power plants and creating a technological emergency response guideline will contribute to relieving the anxiety of citizens and increasing nuclear power plant credibility. • When there are nuclear power plant accidents in nearby states, the technology will help establish a mid- to long-term response to radioactive contamination in the domestic environment (eliminating contaminants, limiting outdoor activities, etc.), and aid in minimizing social disorder and damage.	• Global market for radiation monitoring and detection: KRW 7.2 trillion ('22) • Global market for nuclear accident management robots: KRW 1.8 trillion ('20)
Non-radioactive Non-destructive Testing Technology	• The utilization of non-radioactive non-destructive testing technology can prevent radiation exposure at the source, and greatly increase safety for workers. Also, issues such as difficulties in isotope management, risks of contamination, and limited penetration depth (to minimize radiation exposure) can be overcome. • Development of technologies such as terahertz non-destructive testing will enable material-specific testing and contribute to increasing structural safety, and material/equipment/product reliability, as well as public safety.	• Global market for non-destructive testing: USD 24.23 billion ('22)

Emerging Technology	Social Impacts	Economic Impacts
	• The use of non-destructive testing technology in particular will be expanded, in areas such as identifying foreign substances in food, detecting harmful chemical substances such as drugs and explosives in the mail, testing plastic structures for body cracks in planes, automobiles, ships and structural soundness, as well as new areas such as medical use.	
Particulate Matter Reduction Technology	• Particulate matter generation will be significantly reduced with the development of technologies that reduces particulate matter pollution itself, and secondary damage-inducing gases. • Even when particulate matter pollution occurs, indoor air cleaning and purifying technologies will minimize damage from exposure and provide a safe air environment.	• Global market for indoor air quality control: USD 24.84 billion ('20) • Global market for air pollution management systems: USD 13.8 billion ('16)
Eco-friendly Green & Red Tide Elimination Technology	• This technology is a fusion of biotechnology and environmental technology for the eco-friendly control of green and red tides. Broad mobility, reduced processing time, increased processing volume and other effects will greatly contribute to watershed management and water quality control. • A collaboration with technology that can reuse collected green and red tides as energy, feed and compost will lead to development in zero-energy and non-CO_2 technology. • The dissemination of diverse tide elimination technology available for immediate application will secure the safety and well-being of the public. Clear water resources management will lead to pleasant waterfront areas, increasing ecological value.	• Global market for water and wastewater management: USD 625 billion ('16)
Advanced Domestic Waste Sorting and Recycling System	• Maximized reuse of recyclables as new material and usage of non-recyclables as energy sources will become possible. Such waste sorting system is critical in preparation for resource exhaustion, and securing new energy sources. • The application of domestic waste sorting and recycling technology will redirect the traditional waste disposal systems (such as incineration or landfill) to a more recycling-centered system. • Individual emission sources and intermediate and final disposal plants will be directly connected through underground plumbing. Individual and public housing recycling dumps and street trash disposal cans will be unnecessary, improving the aesthetic value of a city.	• Global market for domestic solid waste management: USD 296 billion ('20)

Emerging Technology	Social Impacts	Economic Impacts
Real-time 3D Environmental Change Observation Technology	• Monitoring massive, long-term, gradual and slow environmental and ecological changes will become possible. Understanding the mechanisms of these changes will also facilitate addressing the causes or preparing for the effects. • The development of a real-time 3D observation technology over the general earth environment will continuously reduce the scale of damage, both casualties and economic losses, from natural disasters. • Increased overall real-time 3D monitoring ability across the general ecosystem will lead to scientific, system-based general ecosystem management including contamination tracing. Environmental pollution will be significantly reduced.	• Global market for environment monitoring: USD 20.5 billion ('20) • Global market for environmental testing equipment: USD 1.32 billion ('22)
Ecological Restoration System Using Microorganisms	• Ecological restoration using microorganisms does not require ground excavation using heavy equipment. Pollution levels are contained, and it is economical as well as convenient. • Immediate detection and treatment of contamination in its early stages will be enabled through the development of biosensors and the establishment of a real-time contamination monitoring system. • The chemical industry paradigm of the 21^{st} century will be changed, from a fossil fuel based system to a biomass system, while biotechnology-based and environmentally friendly processes will be advanced.	• Global market for industrial waste management service: USD 750.1 billion ('20) • North American market for microorganism-based ecological restoration: USD 106 million ('19)

4. Conclusions and Implications

KISTEP 10 Emerging Technologies were selected with the goal of constructing a desirable future society, which distinguishes this list from other selections of emerging technologies in Korea. The selection of emerging technologies in Korea is performed mostly by public institutions, and focus on technologies that are more likely to have bigger economic and social effects. However, KISTEP 10 Emerging Technologies is the only assessment that presents a balanced reflections of the ability to cope with needs in the future society and the economic and social impacts. KISTEP 10 Emerging Technologies is significant in that the changes of the future are forecasted based on a different issue every year. The perspectives and methods are adjusted and newly developed accordingly to select emerging technologies, contributing to enhancing diversity and advancing research methodology.

KISTEP 10 Emerging Technologies in 2017 has the following characteristics in issue analysis and technology identification: The discussion of 'Enviornmental Pollution in Daily Life', which is both a public and technological issue, maximizes the issue responsiveness of the 10 emerging technologies. The key issues and needs of citizens were identified through a survey on the public. Mass media (press) and blogs were differentiated during social data analysis for more accurate assessment of implications and incorporation into issue analysis. Future technologies announced by the media were analyzed and utilized during the selection process to identify technologies addressing Korea's social needs. When analyzing 10 emerging technologies in details, combining analysis of the existing literature and quantitative analysis of patent is expected to provide rich data and improve utilization.

The selection for this year was conducted based on future technologies which can counteract environmental pollution in daily life, and enable the sustainable development of Korean society. Of the Sustainable Development Goals (SDGs) announced by the United Nations in 2015, a fair number are related to the environment. Moreover, the adverse effects of environmental pollution in daily life and problems of an information society were included in the WEF Global Risks Report 2016 as key issues. The effects of environmental pollution are intensifying due to government policies that have prioritized economic growth over environment, and damage from sensory and information pollution, which were not recognized as pollution in the past, is increasing. In particular, the severity of light and air pollution in Korea is among the worst in the world, and urgent solutions are needed. Developing technologies to counteract pollution in daily life and environmental pollution would prevent the costs from further damage, ultimately benefiting the country economically, and enhancing the ecosystem and the quality of life for the public.

It is true that Korea has been lacking in research and development for solving social problems because it has focused on technology development with economic growth as a top priority. This has also resulted in the adverse effects of technology development causing various pollution and pollution. Now that Korea has world-wide scientific and technological leadership, we must focus on sustainability for the prosperity of the whole of humanity. 2017 KISTEP 10 Emerging Technologies provides a new direction for the role of science and technology in building a desirable future for Korea. The research aimed to emphasize the role of science and technology in resolving threats to the ecosystem and the environment that have caused by technological development focusing on economic growth alone. The research stresses the need to break away from the notion of a producer-centered and performance-centered national R&D policy, in which the primary objective is to develop profitable technology and pursue economic growth. The research is expected to serve as an important example where technologies that promote public interest can be emerging technologies of high potential.

References

Asian Citizen's Center for Environment and Health <http://www.eco-health.org/>

Environmental Performance Index <http://epi.yale.edu/>

Falchi, F., Cinzano, P., Duriscoe, D., Kyba, C., Elvidge, C., Baugh, K., Portnov, B., Rybnikova, N., Furgoni, R. (2016). The new world atlas of artificial night sky brightness. Science Advances, 2(6), e1600377

Greenpeace (2016), Plastics in Seafood

Greenpeace (2012), Lessons from Fukushima

Kang, C. G., Lee, S. H., Kim, E. K. (2007), Endocrine Disruptor, Journal of the Korean Medical Association, 50(4), 359-368

Kim, E.(2010), Risk Assessment of Nanomaterials: Issues and Perspectives. Environment Review, 12, 193-206

Kim, I. N., Lee, K., Gruber, N., Karl, D., Bullister, John., Yang, S., Kim, T. W. (2014), Increasing anthropogenic nitrogen in the North Pacific Ocean, Science, 346(6213), 1102-1106

OECD (2016), The economic consequences of outdoor air pollution

OECD Better Life Index <http://www.oecdbetterlifeindex.org/>

Pan, W. C., Wu, C. D., Chen, M. J., Huang, Y. T., Chen, C. J., Su, H. J., Yang, H. I. (2015), Fine Particle Pollution, Alanine Transaminase, and Liver Cancer: A Taiwanese Prospective Cohort Study, Journal Of The National Cancer Institute, 108(3), djv341

Park, G. (2012), Study on the improvement of soil pollution management, Konkuk University

Park, J. and Kim, Y. A. (2017), KISTEP 10 Emerging Technologies, Issue Paper 2017-01, Korea Institute of S&T Evaluation and Planning

Park, Y. H. (2002), Management and Remediation Policy of Contaminated Lands in Korea Ⅰ, Korea Environment Institute

Ryu, J. G. (2014), "Korea should be prepared for soil and groundwater contamination from livestock burial", Water Journal

Seoul Air Quality Information. <http://www.airkorea.or.kr/index>

United Nations (UN) (2016). The Sustainable Development Goals Report 2016

United Nations Environment Programme (UNEP) (2016), Marine Litter and Microplastics

Science and Technology Trends
Governance Systems for Cybersecurity

Cybersecurity Policy and Governance in Korea: A Close Look at "Authentication" †

Hyeon-Suk Lyu

1. Introduction

In the past few years, a number of incidents involving large-scale disclosure of personal information have occurred in telecommunication companies, as well as in public departments and agencies in Korea. These incidents have raised people's awareness of personal information protection and caused social anxiety and distrust. As a representative case, the personal information of over 100 million people, which belonged to three major credit card corporations, was inadvertently disclosed in January 2014 (Financial Supervisory Service, 2014: 31). According to the report (2014), "Current State of Personal Information Leakage in 2010-2014," published by the Korea Communications Commission, the personal profiles of 106.2 million people were leaked over a four-year period.

It is well-known that most cyber infringement incidents involve the disclosure of personal information, which is related to the process of authentication (Otto, P. N. et al., 2007). The identity theft occurred while collecting citizens' resident registration numbers, which is similar to a Social Security Number in U.S., in order for websites to identify users online. As a result, the ban on collecting resident registration numbers online was included in the Privacy Protection Act of August 2014. No corporation, including one-man companies and public companies, is permitted to gather the resident registration number except in exceptional situations as defined by the law.

The public's awareness of the significance of personal information protection, however, is still lacking; they believe that their personal information has already been leaked to varying degrees, and that policies for cybersecurity would not work properly (Malandrino, D. et al., 2013: 280). This distrust is attributed to the current status of cyberspace, which remains vulnerable to attack and manipulation from ever-evolving malicious threats. Cyber-attacks and crimes are currently the fastest growing threats to almost every aspect of modern life, from the government to the private sector. New cyber-attacks such as DDoS, malicious apps, pharming, smishing, APT, etc. are also rapidly expanding across the world. In addition, with technological advancement and convergence such as ICBM (Internet of Things, Cloud, Big Data, and Mobile), complexity, uncertainty,

Korea Institute of Public Administration, 235, Jinheung-ro, Eunpyeong-gu, Seoul 03367, Korea
E-mail: hslyu@kipa.re.kr

† This article is a modified version of an excerpt from Lyu, H.S. et al. (2015). A Study on Cybersecurity Policy and Governance in the ICT Convergence Environment: Focused on "Authentification". KIPA Research Report 2015-24.

and risk in the cybersecurity environment are ever increasing. As stated above, it is well-known that the majority of cybersecurity incidents take place due to personal information disclosure. According to FIDO alliance (2015), 76% of cyber incidents occur in the process of authentication.

However, South Korea’s cybersecurity institutional arrangements and corresponding government policies do not seem to address these issues and challenges in a timely and appropriate manner. This is due to a lack of inclusive legislation, an effective governance system, budget, etc. More specifically, the existing legislative system pertaining to cybersecurity includes the “Digital Signature Act,” “Electronic Government Act,” ‘Framework Act on National Informatization,” “Act on the Protection of Information and Communications Infrastructure,” “Act on Promotion of Information and Communication Network Use and Protection of Information,” “Framework Act on Electronic Commerce,” and “National Cybersecurity Management Regulation (Korea Communications Commission, 2011).” These laws show that various roles in protecting personal information are scattered across multiple departments (see Table 1). For instance, “Digital Signature Act” pertaining to authentication certificate authorizes the Ministry of Science, ICT and Future Planning. “Electronic Government Act” and “Electronic Financial Transaction Act” authorize the Ministry of Government Administration and Home Affairs and Financial Services Commission respectively.

Table 1. Agency and law related to authentication

<table>
<tr><th>Sector</th><th colspan="2">Public Sector</th><th colspan="2">Private Sector</th></tr>
<tr><td>Establishment of Policies for Personal Information Protection</td><td colspan="4">• “Framework Act on National Informatization”: Information Security Professional Committee
• “‘Act on Promotion of Information and Communication Network Use and Protection of Information”: Establishment of information protection policy</td></tr>
<tr><td>Protection of Information & Communication</td><td colspan="4">• “Act on the Protection of Information and Communications Infrastructure”: Protection of Information in public/financial/IC sectors. Information Communications Infrastructure Protection Committee</td></tr>
<tr><td>Response against Infringement</td><td colspan="2">• “National Cybersecurity Management Regulation”: Response against infringement in the public sector, National cybersecurity center</td><td rowspan="3">“Act on Promotion of Information and Communication Network Use and Protection of Information”</td><td>• Response against infringement in the private sector
• Center for Response against infringement</td></tr>
<tr><td>Cybersecurity Policies and Initiatives</td><td rowspan="2">“Electronic Government Act”</td><td>• Establishment and implementation of cybersecurity policies such as communication network of information</td><td>• Information protection for users
• Prohibition on network infringement</td></tr>
<tr><td rowspan="2">Assessment, Authentication, and Examination</td><td>• Security of electronic document
• The Common Criteria Evaluation and Validation System in public sector</td><td>• Safety Inspections for Information Protection
• Information Security Management System Certification</td></tr>
<tr><td colspan="4">“Framework Act on National Informatization”: information security system evaluation and validation system</td></tr>
<tr><td>Digital Signature</td><td colspan="2">“Electronic Government Act”: Administration electronic signature</td><td colspan="2">“Digital Signature Act”: official electronic signature</td></tr>
<tr><td rowspan="2">Personal Information Protection</td><td colspan="4">“Act on the Protection of Personal Information”</td></tr>
<tr><td colspan="2">• “Protection of Personal Information in a Public Institution”
• “Resident Registration Act”</td><td colspan="2">• “Act on Promotion of Information and Communication Network Use and Protection of Information“
• “Protection of Credit Information Act”</td></tr>
</table>

Source: Korea Communications Commission, 2011:12 cited in Lyu, et al. 2015:10

Table 1 indicates that there are many laws related to cybersecurity and a number of departments managing them, which has led to negative effects in establishing and implementing cybersecurity policies in a consistent and systematic manner. Particularly with regards to the policies of authentication, there have been challenges in cooperating with each other among agencies and implementing policies in a reliable way because of conflicting interests and the differing direction of policy for each agency. For instance, the Ministry of Government Administration and Home Affairs tends to consolidate security of cyberspace, while the Ministry of Science, ICT and Future Planning as well as the Financial Services Commission tend to mitigate related regulations to enhance usability. This situation could cause interagency conflicts and confusion to the public.

Meanwhile, there has been little budget allocated to cybersecurity. For example, the amount of budget the Ministry of Government Administration and Home Affairs allotted to personal information protection was 9.8 billion won in 2015, of which only 1.3 billion won was used for cybersecurity such as maintenance of Public i-PIN (Ministry of Government Administration and Home Affairs, 2015). Many specialists evaluated that this budget would be inadequate to meet the cost of upgrading i-PIN after spending personnel expenses.

In this milieu, this study attempted to cover all aspects of cybersecurity including the current legal arrangement, governance structure, and public finance, human resources and so on by taking a “holistic and integrated approach.”

2. Research Design

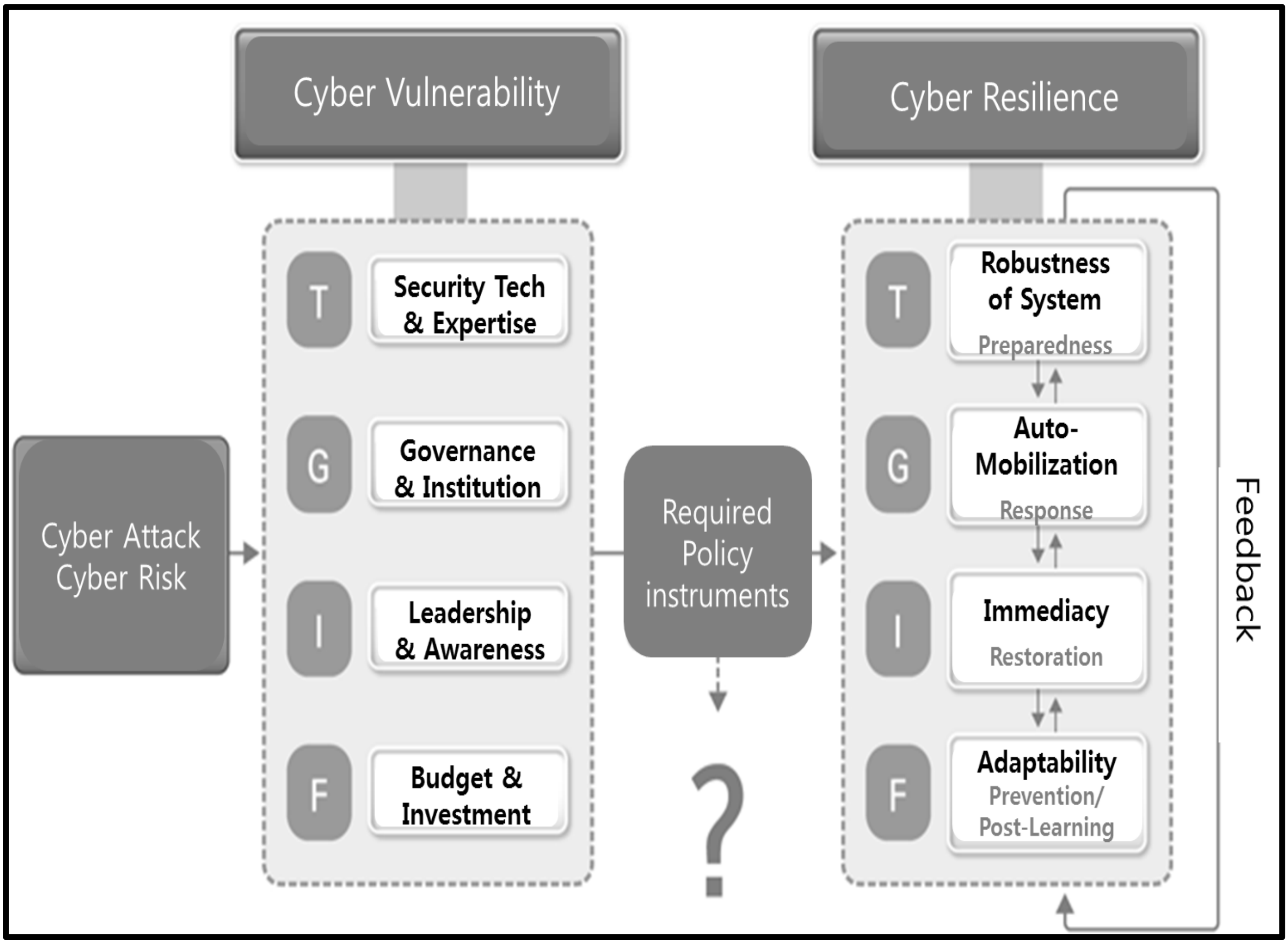
This study is divided into five steps; this study attempted 1) to explore different types of cyber threats and the current state of cyber breaches; 2) to examine the changing paradigm of authentication security systems and diversified authentication along with the advent of new technology; 3) to establish a theoretical framework, based upon the concept of resilience as well as vulnerability of cyberspace; 4) to examine domestic personal authentication technology, the pattern of usage by individuals and corporations, and budget, policies, and governance system related to authentication; 5) and to conduct an AHP (Analytic Hierarchy Process) survey in order to prioritize national cybersecurity policy.

More specifically, this study aspired to identify and compare the key cyber vulnerability and cyber resilient factors in both domestic and foreign cybersecurity environments. Based upon the “cyber resilience analytical framework” (see Figure 1), this study categorized cyber resilience into four dimensions; robustness, resourcefulness, rapidity, and adoptability. Then it further developed a new national cybersecurity, “TGIF.” T (Technology) stands for technology & expertise, G (Governance) stands for governance and institution, I (Insights) stands for leadership and awareness, and finally F (Finance) stands for government budget for cybersecurity.

The key cyber vulnerability and resilience factors were drawn from the literature review, domestic and foreign case studies, and interviews with experts and practitioners in cybersecurity, and expert brainstorming. Then, an AHP (Analytic Hierarchy Process) survey was conducted so as to prioritize national cybersecurity policy.

In brief, through integrating findings from theoretical reviews, case studies, interviews and the AHP survey, specific policy implications and policy suggestions were drawn reflecting the aforementioned TGIF index.

Figure 1. Research model based on cyber resilience



Source: Lyu, et al. 2015:85

3. Domestic Cybersecurity Environment and Governance

3.1. Domestic Security Environment and Risk

Internet technology has developed rapidly in recent years. With the increase in mobile device usage changing the fundamental qualitative nature of Internet usage, data is being utilized in more ways than ever before. This trend is called "Technological Advancement and Convergence based on ICBM (Internet of Things, Cloud, Big Data, Mobile)," which has accelerated complexity, uncertainty, and risk in the cybersecurity environment (Friess, P., 2013: 9). In addition, ICBM frequently deals with a large amount of information and a majority of cybersecurity incidents typically occur due to personal information disclosure. The cybersecurity incidents could be categorized according to various fields of internet usage.

Table 2. Cybersecurity incidents in various fields

	Details
Privacy	(CCTV) CCTV made by Trendnet, a security camera company, could be tapped easily. In fact, about 700 videos recorded by the company's cameras were leaked.
	(Smart TV) Cameras in smart TVs were hacked in LA on August 2013.
	(Google Glass) Through Google Glass, people could collect personal information regardless of place or time; it was proved that the PIN number of bank account could be disclosed.
Smart Home	(Smart Home) Poofpoint, a security corporation in U.S., made public cases of cybercrimes that a hacker sent about 750,000 spoof emails by utilizing routers of home networks, smart TVs, and refrigerators.
	(Robot cleaner) Black Pearl Security gave a trial performance in terms of possibility that the camera embedded in a robot cleaner could be hacked and monitored in real time at ISEC 2014, Seoul.
	(Temperature controller) In the Black Hat USA 2014, a team from Florida demonstrated a temperature controller in the house could be controlled by a hacker.
	(Printer) At 44Con, an information security conference held in London on September 2015, showed that the Doom, which is a PC game, could be hacked through the LED screen of the printer. This indicates that any document in print requests could be stolen by hacking the printer.
	(Hotel) In the Black Hat USA 2014, a blinder, temperature, TV on-off, etc. of a hotel in China were controlled remotely through an IPadⅡ based on KNX protocol.
Network	(Car network) A hacker team from Spain made public circuit boards (20 dollars) which could invade car networks. This circuit board can approach the Control Area Network (CAN) which are installed in order for car corporations to check the system of computers in the car.
	(Home network) Kaspersky, a security corporation, reported that it invaded the home network through the home DSL router and spent less than 20 minutes in searching 14 weak spots.
	(Line Sharer) Team Cymru, a security consulting company, warned that about 300,000 line sharers made by D-Link, Tenda, Micronet, TP-Link, etc., were hacked.
Control System	(Industrial Control System) The United States Department of Homeland Security warned that the industrial control system which could be targets by hackers, because it has an internet connection without using firewall or authentication access control.
	(Air Control System) Korea Internet and Security Agency announced that the set-top box used for controlling air-conditional systems was abused through DDos attacks in Korea.
Medical Service	(Insulin pump) It was proved at the Black Hat Security conference in 2012 that an insulin pump could be manipulated by a hacker away from 800m and inject a fatal dose of insulin.
Transportation	IOActive Labs, a security company, inspected remote sensing technique of cars made by Sensys Networks. As a result of investigation, it found defects in the aspects of design and security, which meant a hacker could transmit fake data to the traffic management system and control the infrastructure such as traffic lights.
Cyber Crime	Europol asked the government to suggest countermeasures in order to respond to cybercrimes involving cars, medical equipment, wearable devices, other IoTs, etc.
	IID, a security corporation in U.S., projected that there could be cyber murder incidents using IoT technology in a few years. In fact, it is known that there might be a black market where people transact information with regard to security vulnerability of IoT equipment.
Broadcasting	(TVshing) The Black Hat USA made public the TVshing using 'Man In The Middle (MITM) in 2013.

Source: Institute for Information & Communications Technology Promotion (IITP), 2014:19 cited in Lyu et al (2015: 96)

3.2. Domestic Authentication Policy and Digital Governance

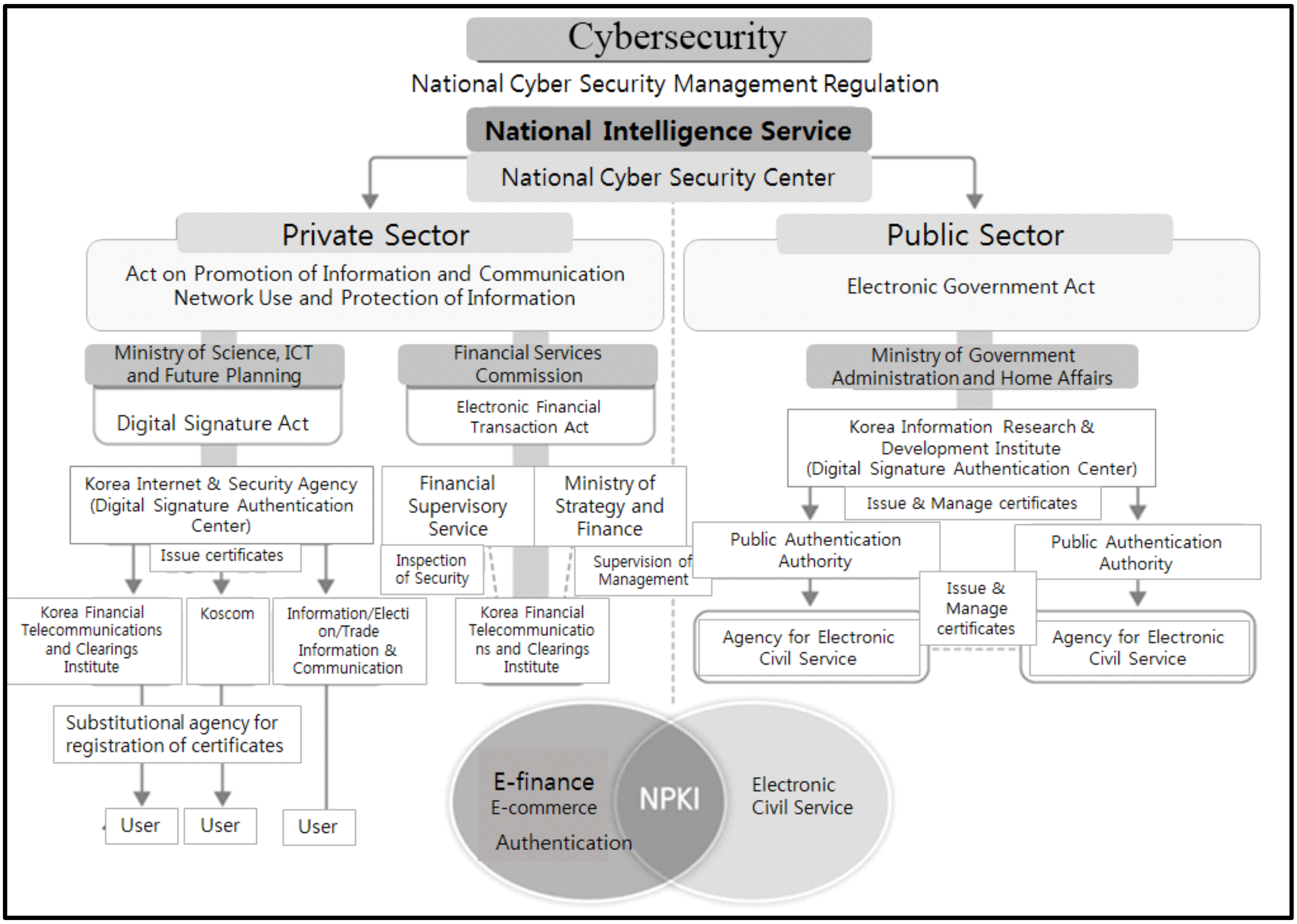
Various government departments, such as the Ministry of Government Administration and Home Affairs, Korea Communications Commission, the Ministry of Science, ICT and Future Planning, Financial Services Commission, etc., are being charged with tasks related to personal information protection. Each department has its own mandates, manpower, and organizational instruments, based on several laws and regulations. In the alternative, the central government announced the "Policy for Normalizing Personal Information Protection," which organizes the related laws and systems which extend across the agencies involved, through the "National Council for Policy Coordination" since 2014. Yet, there still exist issues pertaining to decentralized works of personal information.

Table 3. Mandates of agencies related to authentication

Ministry of Science, ICT and Future Planning	Korea Internet and Security Agency	Korea Financial Telecommunications and Clearings Institute
• Management and operation of "Public Key Infrastructure (PKI)" • Establishing policies for operating the PKI in a safe and reliable way. • Appointing authentication authorities, inspection, and request of correction order, work suspension, and cancellation of appointment • Implementing supervision of Korea Internet and Security Agency and authentication authorities based on laws and regulations related to the PKI • Conducting mutual agreement regarding the PKI with foreign governments	• Implementation of mandates grounded on the Article 25 of Digital Signature Act • Supporting examination of candidates for authentication authorities, according to the Article 4. • Supporting inspection of the authentication authorities, based on the Article 14-1. • Supporting evaluation and technology, based on the Article 18-3. • Implementing inspection of facilities and equipment for operation and management, according to the Article 19-2. • Working on various authentication tasks such as issuing and managing certificates • Conducting research in terms of developing technology and standardization pertaining to digital signature. • Supporting international cooperation such as mutual recognition and conducting research including system of digital signature. • Taking over members or certificates from authorities which are abolished or cancelled • Forwarding cases of the loss of authentication certificates to the authorities • Other duties in terms of digital signature	• Implementation of mandates according to the Article 4 and the Article 8 of Digital Signature Act • Accepting and processing application of authentication certificates • Verifying an enterer's identity • Issuing, reissuing, renewing, suspending, and abolishing authentication certificates. • Publishing information about authentication such as certificates and CRL • Operating substitutional agency for registration of certificates • Other duties required for the purpose of authentication authorities

Source: Homepage of each department (Ministry of Science, ICT and Future Planning <www.msip.go.kr>, Korea Internet and Security Agency <www.kisa.or.kr>, Korea Financial Telecommunications and Clearings Institute <www.kftc.or.kr>)

Figure 2. Governance for protection of information on cyber space



Source: Lyu, et al. 2015:133

The Table 3 and Figure 2 show that the Korean authentication system is a dual system, which is divided into both the private sector and the public sector. The private authentication system includes e-commerce and electronic financial transactions, while the public authentication includes e-government civil affairs. In this dual system, it is often pointed out that there might be a loophole or a blind spot regarding authentication, caused by having different agencies that supervise their own system security in different ways (Jung, 2013:30). Therefore, the current status of governance for protecting information on cyber space implies that an integrated system, which could manage and supervise personal information security such as management of I-PIN, is required.

4. Vulnerability and Resilience of Cybersecurity and Authentication

The vulnerability factors of cybersecurity were frequently found in domestic environment, compared with those of foreign environment, in various aspects of technology, institution, leadership, and perception (Von Solms, R., & Van Niekerk, J., 2013: 100). The most significant difference is to change the perception of public officials in terms of cybersecurity. This is attributed to the fact that the change of perception and leadership could be followed by secondary factors such as standardization and advancement of technology, increased budgets, improved professionality of manpower, and other policy instruments.

Most vulnerability factors have an influence on resilience factors of cybersecurity. These two factors could be divided into two areas; technical and political. To begin with, vulnerability factors of cybersecurity are involved with technology, such as prevention-centered, under-developed, and isolated technology. It might have a positive effect on addressing these issues to adopt international standards of cybersecurity and apply technology in diversified ways including prevention, transaction, and post-response. In the political area, the vulnerability factors might be alleviated by reorganizing the system in order to secure enough budget and manpower as well as reduce redundant costs and time.

Table 4. Vulnerability and resilience factors of cybersecurity

	Vulnerability Factor	Resilience Factor
Domestic Environment	• Prevention-centered technology • Outdated security technology • Unorganized system of management (lack of governance and/or decentralized security system) • Different ways of authentication • Lack of budget • Lack of professional manpower • Insufficient regulations and laws regarding violations and crimes related to authentication • Unstandardized and isolated security technology • Low level of awareness about the importance of cybersecurity (especially in upper management)	• Application of new technology for prevention, exploration, and resilience • Training and acquisition of professional security personnel • Clarifying accountability and mandates across related agencies • Improving the status of office in charge of cybersecurity • International cooperation • Quantification of investment, such as cost-benefit analysis • Balanced budgeting for pre- and post-response • Enhancing multi-layer verification of identity (telephone, mail, message) • Reinforcement of security • Enhancing usability of authentication • Securing a sufficient budget • Introduction and adoption of standardized technology • Increasing awareness of public officers about cybersecurity
Foreign Environment	• Reluctance towards budgeting and investment because of uncertainty of cybercrime occurrence • Low understanding of information and communication compared to domestic environment • Low level of awareness by the public about cybersecurity • Less responsibility of public agencies with regard to cyber breach, compared with that of private organization • Little interest in the public sector	• Establishing a security framework with aims such as reducing crime rates, enhancing resilience, protecting interests, making cyberspace safe, and constructing knowledge (UK) • Proactive international cooperation (UK) • Repeated testing of resilience (UK)

Source: Lyu, et, al. 2015:182～183

In addition, with regards to the technical aspect, application of new technology and international cooperation are the key resilience factors of cybersecurity. With regards to the political aspect, it is important to clarify accountability and mandates among the various departments managing cybersecurity. Moreover, the perception of public officials about cybersecurity could be the vial factor for raising resilience, in that they might put more efforts in projecting cost and benefit analysis and allotting reasonable budget into cybersecurity (Shafqat, N., & Masood, A., 2016: 133).

Table 5. Vulnerability and resilience factors of authentication

	Vulnerability Factor	Resilience Factor
Domestic Environment	• Requiring excessive information • (After enforcement of ban on collecting resident registration numbers) Complex process of authentication (I-PIN, My-PIN) • Low awareness about the process of authentication • Low trust in the process of authentication • Complexity of the process of authentication • Only checks whether passwords are matching • Overreliance on website security systems • Mandatory certificate use • Multiple ways of authentication due to the advent of new technology • Insufficient investment for establishing security in electronic finance and payment • Possibility of replication without any permission • A single data terminal processing every step of authentication	• Application of international standardized cryptographic techniques • Development of mobile-based technology for authentication • Reinforcement of network security • Development of system reflecting user intent • Establishment of legislations and institutions regarding new authentication methods • Suggestion of binary or diversified steps of digital signature and governance of authentication • Simplification of authentication process • Increased investment in research about current vulnerability and development of alternative technology
Foreign Environment	• Inclusive definition of digital signature (EU, Germany) • Centralized operation of the authentication system (North Europe)	• Clarification of binary steps for digital signature to allow more flexible operation (EU) • Application of various ways for authentication (EU) • Expanding private autonomy, rather than government regulation (US) • Providing authentication by individual authorities, rather than by permission of the government (US) • Reducing usage areas of Social Security Numbers (US) • Inclusive and specific identification of digital signature (US) • Acceptance of both limited technical conditions and experimental technical conditions (German) • Autonomy of operation (UK) • Operation of accreditation systems rather than permission systems (Japan) • Introduction of voluntary authentication system (Japan) • Operation of actual examinations by organizations appointed as investigation agencies (Japan) • Minimizing risks by regulating frequency of exposing identification numbers (AU) • No designation of universal personal identification numbers (AU) • Acceptance of voluntary accreditation systems (Singapore)

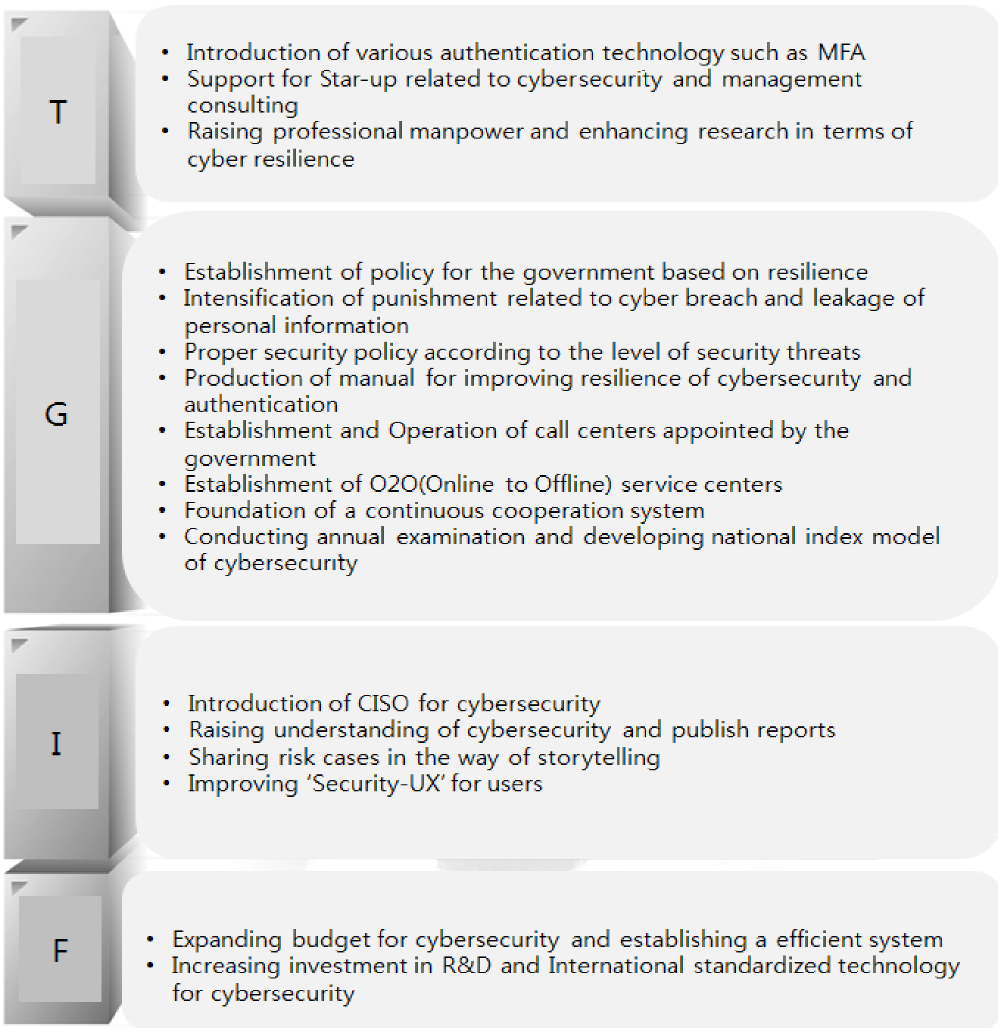
Source: Lyu, et al. 2015:182～183

The domestic environment related to authentication implies that the process of authentication is complicated and frequently requires users to send excessive information. The low level of trust in the process of authentication, a web-based authentication system, and a relatively low investment also were raised as vulnerability factors of authentication.

5. Policy Recommendation and Conclusion

This study conducted a policy workshop on both October 7th and 9th 2015, based upon the results of three iterations of the AHP survey, after drawing the key cyber vulnerability and resilience factors. A total of ten cybersecurity experts participated in this workshop so as to prioritize national cybersecurity policy in Korea. This study suggests new governance for improving resilience of cybersecurity. This governance is composed of four factors, technology, governance, insight, and finance (see below Figure 3).

Figure 3. New governance system for improvement of resilience



Source: Lyu, et al. 2015:271

In conclusion, this study suggests a number of policy implications for a better cybersecurity governance in Korea. First of all, the domestic cybersecurity system ought to be more enhanced by embedding high technology to predict and prevent cyber breach. Thus, the technology neutrality could be the key element for developing various technologies pertaining to security and authentication.

Secondly, the government should establish cooperative governance and an interchangeable system in order for the government to promote responsibility, to identify mandates, and to response various cybercrimes timely and efficiently.

Moreover, the government needs to recruit professional manpower to have expertise in terms of cybersecurity and to further raise awareness about it. It could have a positive influence on improving both the quality and quantity of policies related to cybersecurity to change the perception of chief administrators in the department. Job training and education also might be the key elements for changing the culture of organizations with regard to the importance of cybersecurity.

For the final point, budget is an important factor for the new governance system. The government should conduct strategic planning and establish integrating pre- and post-response by expanding budget related to the cybersecurity.

References

Fast IDentity Online (FIDO) Alliance. (2015). Federal Gov't Near 100% 2Factor Authentication, Retrieved from <https://goo.gl/F936TD.>

Financial Supervisory Service. (2014). Financial Supervisory Information. 2014-3:764.

Friess, P. (2013). Internet of things: converging technologies for smart environments and integrated ecosystems. River Publishers.

Institute for Information & communications Technology Promotion (IITP). 2014. Current State of IoT and Major Issues. 2014:19.

Jung, Gi Seok. (2013). Study on improvement of authentication systems for electronic financial transactions. Convergence Security, 13(6), 25-33.

Korea Communications Commission. (2011). A Study on Solutions for the Advancement of Security Legislation.

Korea Communications Commission. (2014). Current State of Personal Information Leakage in 2010-2014.

Lyu, H.S. et, al. (2015). A Study on Cybersecurity Policy and Governance in the ICT Convergence Environment: Focused on "Authentification". KIPA Research Report 2015-24. Korea Institute of Public Administration.

Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R., & Krishnamurthy, B. (2013, November). Privacy awareness about information leakage: Who knows what about me?. In Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society (pp. 279-284). ACM.

Ministry of Government Administration and Home Affairs, 2015, Annual Budget Report FY2015.

Otto, P. N., Antón, A. I., & Baumer, D. L. (2007). The choice point dilemma: How data brokers should handle the privacy of personal information. IEEE Security & Privacy, 5(5).

Shafqat, N., & Masood, A. (2016). Comparative Analysis of Various National Cybersecurity Strategies. International Journal of Computer Science and Information Security, 14(1), 129.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. Computers & Security, 38, 97-102.

Science and Technology Trends
Governance Systems for Cybersecurity

Cybersecurity in India: Regulations, Governance, Institutional Capacity and Market Mechanisms

Nir Kshetri

1. Introduction

The meteoric rise in cybercrime has been an issue of pressing concern to businesses and consumers in India. Among the Indian organizations, which responded to KPMG's (2014) Cybercrime Survey report 2014, 89% considered cybercrime as a "major threat" (p, 3). One estimate suggested that 42 million Indians were victimized online in 2011 (indolink.com, 2012).

As early as in 2009, it was reported in some Indian cities such as Mumbai in India, there had been more cybercrime cases were registered with the police than conventional crimes (Hindustan Times, 2009). According to a 2016 report of the National Crime Records Bureau (NCRB) 11,592 cases of cybercrime cases were registered in India in 2015 (Das, 2017). This is more than 300% increase of the 2009 level when there were 2,866 reported cybercrime incidents (Economictimes, 2012).

India also generates cybercrimes that affect Internet users worldwide. For instance, according to the U.S.-based Internet Crime Control Centre, India ranked fifth in the number of complaints received by the agency (Internet Crime Complaint Center, 2011). As an example, in 2012, the U.S. Federal Trade Commission (FTC) sued the California-based American Credit Crunchers. According to the FTC, an Indian company associated with American Credit Crunchers made threatening calls to U.S. consumers with histories of applying for payday loans, which are short-term, high-interest loans that are typically applied online. Agents in India with massive amount of personal data allegedly called potential victims and threatened dire consequences if the fictitious loans of up to US$2,000 were not repaid. U.S. consumers had lost over US$5 million to the scam, which had been in operation for two years (Shaftel and Narayan, 2012). Likewise, India was the top origin country for spam in 2011 and 2012. Similarly, a phishing survey released by the Anti-Phishing Working Group (APWG) in April 2012 found that India had the highest phishing top-level domain (TLD) by domain score (calculated as phish per 10,000 domains) in the second half (H2) of 2011 (Kshetri, 2015b).

Factors such as cybercrime's relative newness in the country and resource constraints have led to a poor cybersecurity orientation and weak defense measures among consumers, businesses and government agencies (Kshetri, 2013). According to a study of the Security

Bryan School of Business and Economics, The University of North Carolina at Greensboro
Bryan Building, Room: 368, P. O. Box 26165, Greensboro, NC 27402-6165, USA
E-mail: nbkshetr@uncg.edu

and Defense Agenda, a Brussels-based think-tank, India is among countries most vulnerable to cyberattacks due to a lack of systems and procedures to defend among the public and private sector (Blitz, 2011).

Due partly to the above trends, many initiatives and efforts of the government and private sector actors have emerged to strengthen cybersecurity in the country. Table 1 presents some of the key initiatives on the cybersecurity front. As a major recent regulatory initiative, in July 2013, the government of India (GOI) released the National Cyber Security Policy (NCSP), which had 14 objectives that included enhancing the protection of critical infrastructure and developing 500,000 skilled cybersecurity professionals in the next five years. The NCSP was formulated in response to domestic and international pressure to enhance cybersecurity measures.

Private sector actors such as the National Association of Software and Services Companies (NASSCOM) have also taken measures to strengthen India's cybersecurity standards. For example, the Data Security Council of India—a self-regulatory member organization set up by NASSCOM—imposes a fine of up to US$1 million for member companies that fail to secure data (Kshetri, 2016b).

Public–private partnerships (PPPs) are probably the most notable feature of the Indian cybersecurity landscape and an appropriate institutional means of dealing with underdeveloped cybersecurity-related institutions. For instance, a key component of NCSP is the development of PPP efforts to enhance the cybersecurity landscape. Note that PPPs are especially well-suited for areas that require diverse types of expertise and knowledge to address complex problems, including cybersecurity (Yu and Qu, 2012).

In light of the above observations, our goal in this paper is aimed at providing an overview of current cybersecurity landscape in India. We examine regulations and enforcement, governance mechanisms, functions of relevant actors as well as challenges and opportunities facing India on the cybersecurity front.

The paper is structured as follows. We proceed by first examining the regulatory environment related to cybersecurity in India. Next, we discuss private sector initiatives and market mechanisms in India in this evolving phenomenon. Then, we look at the public–private partnership in cybersecurity. It is followed by a section on discussion and implications. The final section provides concluding comments

Table 1. The evolution of cybersecurity-related initiatives in India: Major events

Time	Event
October 2000	Information Technology Act, 2000 came into force.
2006	Cyber Appellate Tribunal (CAT) started functioning.
2008	NASSCOM established the DSCI.
December 2008	Information Technology (Amendment) Bill 2008 passed by Indian Parliament
February 2009	The IT (Amendment) Act 2008 received the assent of the President
October 2009	The IT (Amendment) Act 2008 came into force.
2011	The central bank, RBI introduced a set of recommendations, which include the formation of separate information security groups within banks and maintenance of adequate cybersecurity resources based on their size and scope of operation.
October 2012	Cybersecurity joint working group (JWG) released its "Engagement with Private Sector on Cyber Security" report.
July 2013	The government released the NCSP, which set forth 14 objectives that included enhancing the protection of critical infrastructure and developing 500,000 skilled cybersecurity professionals in the next five years.
April 2017	The IRDAI issued guideline, which require all insurance companies to appoint a CISO.

Source: Kshetri (2010, 2015a)

2. The Regulatory Environment

India is strengthening cybersecurity-related regulatory and enforcement capacity (Kshetri, 2016a). India is among the first developing countries to criminalize cybercrimes by enacting the IT Act in 2000. India's IT Act 2000, however, did not cover offenses such as phishing, cyberstalking, and cyber-harassment (Hindustan Times, 2006). To address these drawbacks, the IT (Amendment) Act 2008, added specific provisions to deal with and punish cyber-offenses such as publication of sexually explicit material, cyber-terrorism, Wi-Fi hacking, child pornography, identity theft, and spam (Deshpande, 2009).

Privacy is also becoming an increasingly important issue. Recently legal institutions have recognized that citizens have a fundamental right to protect privacy. In September 2013, India's Supreme Court issued an interim order, which ruled that people cannot be required to have the Aadhaar identification in order to collect state subsidies (Ribeiro, 2014). Note that the government of India (GoI) led by the Bharatiya Janata Party (BJP) indicated that it would require residents to have biometric IDs in order to collect government benefits. The project had set a target of 1 billion enrolments by 2015 (cio.de, 2014). The biometric ID assigns a person a 12-digit number, which is called the Aadhaar number. It requires the collection of 10 fingerprints, iris scans and other information such as the name, date of birth and address and will be hosted in the eGovernance cloud platform.

The country's regulatory bodies overseeing various markets have also issued guidelines, best practices and regulations to monitor and control cybersecurity activities. For instance, India does not have data breach disclosure laws. However, the central bank, RBI has asked banks and financial institutions in the country to share information on data breach. The idea is to provide opportunities to learn about cyber-threats. For instance, a database of banking malware "signatures" would allow banks to set up firewalls against known malware types. For instance, the knowledge about breach in a bank would help other banks to look for the signatures of the same type of breach. Likewise, in April 2017, the Insurance Regulatory and Development Authority of India (IRDAI) has issued guideline, which require all insurance companies in the country to appoint a Chief Information Security Officer (CISO) (DNA, 2017).

Despite some enforcement activities, however, there is an enormous gap between laws on the books and the government's capability to enforce laws. India's most daunting challenge lies in overcoming the severe shortage of cybersecurity manpower. For instance, in 2004, of the 4,400 police officers in India's Mumbai city, only five worked in the cybercrime division (Duggal, 2004). Likewise, in 2011, the police cybercrime cell of Delhi had only two inspectors (Nolen, 2012). In 2012, the Delhi High Court noted the Delhi police website's lack of functionality, calling it "completely useless" and "obsolete" (Nolen, 2012).

In the same vein, consider India's only Cyber Appellate Tribunal (CAT), which started functioning since 2006 (catindia.gov.in, 2014). It was reported in June 2014 that the tribunal had not adjudicated a single case during the previous three years due to the non-availability of the chairperson and judicial members (Singh, 2014).

Cybercrime awareness level is very low among the law-enforcement community.

For instance, it was reported that when a police officer was asked to seize the hacker's computer in an investigation of a cybercrime in India, he brought the hacker's monitor. In another cybercrime case, the police seized the CD-ROM drive from a hacker's computer instead of the hard disk (Aggarwal, 2009).

Overall, India is facing a severe shortage of cybersecurity professionals which hampers the country's ability to fight rapidly rising cybercrime (Kshetri, 2016c). For instance, a large number of IT security auditors are needed to evaluate the adequacy of controls in the management of project and business processes and validate whether the controls are effective (Hettigei 2005). An estimate suggested that in 2013, India had only 60 auditors (Doval 2013). Regarding the requirement of government agencies to conduct security auditing of IT infrastructures, websites and applications, it is important to note that most Indian government agencies' websites are hosted by the National Informatics Centre (NIC), which was established by the GoI to promote IT culture among government organizations. It is argued that NIC-hosted websites are vulnerable to cyberattacks due to a shortage of manpower, especially IT security auditors. NIC outsources security audit works due to the lack of manpower. Likewise, in 2011, India's central bank, Reserve Bank of India (RBI) introduced a set of recommendations, which include the formation of separate information security groups within banks and maintenance of adequate cybersecurity resources based on their size and scope of operation. The country is finding it difficult to enforce the RBI guidelines due to the lack of IT security auditors to validate banks' cybersecurity practices (Bradbury 2013).

In India about 10% cybercrimes are reported. Of the reported crimes, about 2% are registered. The conviction rate is as low as 2% (Hindustan Times, 2006). For instance, while most BPOs in Gurgaon had been cybercrime victims about 70% of the respondents did not report to the police (indiatimes.com, 2011). Most organizations reported doubt about competence, professionalism and integrity of the police in handling cybercrime cases. About 50% of the respondents not reporting thought that the cases are not dealt with professionally and 30% noted that they had "no faith" in Gurgaon police (indiatimes.com, 2011).

In one way, there is a vicious circle: a) law enforcement agencies' unwillingness to put efforts for investigating cybercrimes and their technological illiteracy indicate that they lack the skills and capability to address cybercrime related offenses; b) the survey conducted among Gurgaon-based BPOs indicates that there are low cybercrime reporting rates because of the victims' lack of confidence in law enforcement agencies; and c) cybercriminals may become more confident, resourceful and powerful because their offenses are not reported.

As of 2006, no one charged for data fraud in India was convicted (Ribeiro, 2006). As of August 2009, only four people were convicted for cybercrime (Aggarwal, 2009). Until 2010, there was not a single cybercrime related conviction in Bengaluru, the biggest offshoring hub. The total number of convicted cases by 2010 was estimated at less than 10 (Narayan, 2010).

One reason behind the low rate of registration of cybercrime cases concerns the barriers, hurdles and hassles that confront the victims. In some cases, the police show unwillingness to take the extra work needed for the investigations (Narayan, 2010). There are reports that the police do not support the victim when they want to report a cybercrime case. Cybercrime victims have also complained that the police follow a long and inefficient process to build a criminal case (Anand, 2011).

3. Private Sector Initiatives and Market Mechanisms

Due to escalating cyber-threats, cybersecurity has become an area of increasing priority among enterprises in India. Cybersecurity is reported to account for 30-40% of most overall IT budgets in some Indian companies (Goswami, 2017).

Nonetheless, cybersecurity initiatives among

Indian firms have been hampered by insufficient investments. According to Gartner, Indian organizations spent US$882 million in 2013 in cybersecurity, which was expected to increase to US$953 million in 2014 and US$1.06 billion in 2015. Over half of the cybersecurity spending goes to consulting, implementation, support and managed services (TechTarget, 2014). As a point of comparison, China's cybersecurity spending is much higher, which is estimated to amount US$4.9 billion by 2015 (Kshetri, 2016b).

3.1. Hollow Internet Diffusion and Weak Cybersecurity Measures

The concept of "hollow diffusion" of the Internet among firms may help understand weak defense mechanisms (Otis and Evans 2003, p. 49). The basic idea behind "hollow diffusion" is simple: Many organizations digitizing their activities lack organizational, technological and human resources, and other fundamental ingredients needed to secure their system, which is the key for the long-term success of online businesses.

As to organizational resources, on the cybersecurity front, one key global trend in organizational structure involves the tendency to create the position of Chief Information Security Officer (CISO). For instance, a 2014 PwC survey found that only 28% of over 500 companies surveyed had a CISO or Chief Security Officer (Damouni 2014). CEOs and board often consult CISOs to understand cyber risk, implement appropriate security controls and promote a culture of defense. One study suggested that 90% of CISOs are connected directly to their organizations' top leadership team, and half of them were on the leadership team (Sweeney 2016). For instance, in India, except for few firms in banking, financial services and insurance, telecom, and business process outsourcing (BPO) it is rare to have a CISO in organizations (Pandya 2009).

On the human resources front, demand of cybersecurity professionals greatly exceeds supply. According to international data corporation (IDC), only 22,000 security professionals were available in the country by early 2012 whereas the country needed 188,000 (Saraswathy, 2012). An adviser to the Information Systems Audit and Control Association noted that India needs 300,000 cybersecurity professionals but there are about 30,000 such professionals (Gent, 2016). Citing a study by the Indian CERT, an indiatimes.com article reported that Indian organizations faced a shortage of about 400,000 trained cybersecurity professionals in 2013 (PTI, 2014).

On the technological front, unlike some developing countries, India lacks major anti-virus companies. For instance, Moscow-based Kaspersky Labs is among the world's biggest cybersecurity companies. Some other former second world economies also have top cybersecurity companies such as the Czech Republic's AVG Technologies, Romania's BitDefender and the Slovak Republic's ESET (Kshetri, 2011). Likewise, the Belarusian firm VirusBlokAda was the first company to identify the Stuxnet code in June 2010 (Borland, 2010). India's lack of high profile cybersecurity firms is related to the broader problems of the country's low R&D profile. Due to India's poor R&D and innovation performance, some liken economic activities in the Indian IT and offshoring industry to a "hollow ring." An Economist article notes: "India makes drugs, but copies almost all of the compounds; it writes software, but rarely owns the result. ⋯ [it has] flourished, but mostly on the back of other countries' technology" (Economist, 2007).

India's R&D profile is relatively lower compared to other BRIC economies. According to the World Bank, India had 100 researchers in R&D per million people in 2000 (the numbers for other BRIC economies were Brazil, 424; China, 548; and Russia, 3,451). Looking at more recent data, according to a report presented by Science and Technology Minister Kapil Sibal to the Rajya Sabha, the Upper House of the Indian Parliament, India had 156 researchers in R&D per million people in 2008. As a point of comparison, according to the World Bank, the corresponding numbers for other BRIC economies for 2008 were Brazil, 696; China, 1,199; and Russia, 3,152. Sibal suggested that universities in India were characterized by inferior R&D quality and capabilities (rediff.com, 2008). A related point is that much of the R&D in India is geared towards smaller projects that complement other innovation centres in Silicon Valley and other parts of the world (Economictimes, 2005). Moscow-based Kaspersky Lab’s CEO and Chairman Eugene Kaspersky put the issue this way: “ [Engineers in] China or India …are good if you just want something programmed, but if it’s about research, then it has to be Russia” (Robinson, 1998).

The above said, there have been recent initiatives to accelerate startups in cybersecurity related areas. According NASSCOM, as of 2016, there were about 150 cybersecurity companies. A challenge has been limited access to funding for such startups. NASSCOM suggested that only 40% of cybersecurity companies had received funding from investors (Srivastava, 2016).

3.2. Underdeveloped Market for Cyber Insurance.

Market forces and mechanisms are evolving that may enhance firms’ cybersecurity performances. For instance, the cyber liability insurance (data breach insurance) industry and market are are growing fast in industrialized economies (Kshetri, 2016b). A company is required to strengthen cybersecurity in order to buy coverage at a lower rate. A system that requires cybersecurity insurance thus raises cybersecurity S standards. That is, such insurance could help companies improve their cybersecurity S systems and put efforts to help secure policies (Business Insurance, 2014). Cyber liability insurance provides coverage for the theft or loss of first-party and third-party data. For the loss or theft of first-party data, an insurer may cover expenses related to notifying clients regarding the data breach, purchasing credit monitoring services for affected customers and launching a public relations campaign to restore the company’s reputation. Third-party coverage includes claims related to unlawful disclosure of a third-party's information and infringement of intellectual property rights (IPR) (McGrayer, McGinnis, Leslie, and Kirkland, 2014).

India is regarded as an underdeveloped market for cyber liability insurance. Until as late as 2008, there was no insurance company in India that offered an anti-cybercrime policy for a company (Syed and D’monte, 2008). In the early 2017, insurers such as New India, National, ICICI Lombard, Tata AIG, HDFC Ergo and Bajaj Allianz offered cyber liability insurance (PTI, 2017). One estimate put the size of the Indian cyber liability insurance market in the range of US$14-19 million (PTI, 2016). The cyber-Insurance market is thus relatively small and immature.

3.3. The Information Technology-Business Process Management (IT&BPM) Sector

A key characteristic that distinguishes India from other developing countries is the well developing information technology-business process management (IT&BPM) sector. The sector is expected to exceed $155 billion by FY17 (Venkatesh, 2017). The IT&BPM sector is arguably an enclave economy in India. Call centers in India have already spread from big cities to intermediate towns, and even to small towns in rural areas. In this sense, this sector deserves special attention and should be a prominent subject of discussions in the context of cybersecurity.

Before proceeding further, it is important to stress that most high-profile and widely publicized cybercrimes in India are concentrated in the offshoring sector (Kshetri, 2010). The British Tabloid, Sun, reported that an Indian call center employee sold confidential information of 1,000 bank accounts to its reporter working as an undercover (tribuneindia.com, 2005; Hindustan Times, 2006). In another case, call center workers at Pune, India, subsidiary of Mphasis, a provider of outsourcing services, transferred about US $500,000 from four Citibank customers' accounts to their personal accounts (Schwartz, 2005; Fest, 2005). It was reported that in first- and second-tier cities, there are data brokers and data merchants, who buy data from people working in offshoring companies (Aggarwal, 2009). For instance, data frauds have been reported in call centers in Pune, Hyderabad, Bangalore, and Gurgaon. In a more recent case reported in March 2012, two "consultants", who claimed to be workers in Indian offshoring firms, met undercover reporters of The Sunday Times. They came with a laptop full of data and bragged that they had 45 different sets of personal information on about 500,000 UK consumers. The information included credit card holders' names, addresses, phone numbers, start and expiry dates and security verification codes. Data for sale also included information about mortgages, loans, insurance, phone contracts and television subscriptions (Gardner, 2012).

Unsurprisingly firms in the Indian IT&BPM sector are taking strong cybersecurity measures to prevent attacks on computers by current and former employees (Kshetri, 2013). This is due primarily to address their clients' fear that customer data will be stolen and even sold to criminals. For instance, call centre employees are required to undergo security checks which are considered to be "undignified" according to the Indian culture (The Economist, 2005). Firms have established biometric authentication controls for workers and banned cell phones, pens, paper and Internet/email access for employees for a long time (Fest, 2005). Computer terminals of firms in the IT&BPM sector (e.g., Mphasis) lack hard drives, email, CD-ROM drives, or other ways to store, copy or forward data (Engardio et al., 2004). Indian outsourcing firms also extensively monitor and analyze employee logs (Fest, 2005).

India's IT&BPM sector thus manages cybersecurity risk through effective industry self-regulation. A highly visible private-sector actor on this front is the National Association of Software and Services Companies (NASSCOM). NASSCOM was established in 1988 as an industry-funded not-for-profit organization to contribute to the software industry's development. NASSCOM aims to help the IT&BPM sector to be a "trustworthy, respected, innovative and society friendly industry in the world" and to "[e]stablish India as a hub for innovation and professional services" (NASSCOM, 2017).

Owing to the rapid rise in data incidents, addressing cybersecurity issues has become increasingly important for the Indian IT&BPM sector's success and vitality. NASSCOM launched a registry of IT employees, which allows employers to perform background checks on existing or prospective employees (Hindustan Times, 2006). Creation of criminal and public records databases has been a part of the program (Fest, 2005).

In 2008, realizing the importance of an organization with an exclusive focus on data protection, NASSCOM established the Data Security Council of India (DSCI). The DSCI is a self-regulatory member organization. DSCI's mission is to create trust in Indian companies as global outsourcing service providers. Its focus on cybersecurity is to "[h]arness data protection as a lever for economic development of India through global integration of practices and standards conforming to various legal regimes" (https://www.dsci.in/taxonomypage/1). DSCI took over most of NASSCOM's data protection–related activities.

DSCI monitors member companies to ensure they adhere to cybersecurity standards. For instance, it requires members to self-police and provide additional layers of security at the infrastructure, applications and other levels. Companies failing to secure their data may be fined as much as US $1 million. Noncompliant companies might also lose NASSCOM and DSCI membership.

NASSCOM and DSCI also help create awareness of the latest trends in cybercrime and cybersecurity. Security in cloud computing was one of the topics reviewed by the NASSCOM–DSCI Information Security Summit 2009 (http://www.dsci.in/events/about/225) and every annual summit since then. In the DSCI Best Practices meeting held in June 2011, issues related to data protection in cloud computing and compliance were discussed (Haran, 2011). In 2011, the DSCI announced a plan to set up a cloud security advisory group that would develop a policy framework. The group would also advise the government on security and privacy issues in a cloud environment (Das, 2011).

As of 2015, NASSCOM had more than 1,800 members, compared to 485 corporate members of DSCI. Although any company operating in India's IT&BPM sector might have incentive to join NASSCOM, DSCI membership is especially important for companies for which cybersecurity is a key priority. NASSCOM membership fees vary from approximately US$450 to $100,000, depending on organization size. Many of NASSCOM's members are also global firms from the U.S., Europe, Japan, China, South Korea and other countries. NASSCOM thus has a fairly high level of expertise and the financial resources to take various cybersecurity measures.

A trade association's enforcement strategy becomes efficient and powerful if a large number of firms join the association. NASSCOM ex-president Kiran Karnik addressed the importance of DSCI membership: "While it would be voluntary for the members to be part of the body, it would ensure at the same time that market forces make it mandatory for companies to register themselves." (thehindubusinessline.com 2007).

We noted above that India lacks major anti-virus companies. Recently NASSCOM and DSCI have taken various initiatives on this arena. During 2015-2016, the DSCI incubated 80 cybersecurity startups (Goswami, 2017).

4. Public–Private Partnership in Cybersecurity

In the context of developing countries such as India, cybersecurity is in a nascent stage. Like other economic sectors characterized by nascentness, cybersecurity exhibits an underdeveloped regulatory structure. There is no template for policy development, assessment, and analysis. Developing templates, monitoring the behaviors of individuals and organizations, and enforcing regulations require extensive resources and expertise in such areas. However, most governments in developing countries are characterized by weak public administration, inadequate technical competence, and lack of political will in the implementation of economic and social policies (Pughm, 1999).

But there is another point that is perhaps even more important. The way the Indian government is positioned does not allow it to spend state resources to support a new area at the cost of competing sectors. If policymakers allocate disproportionately more resources to develop modern sectors such as IT&BPM, they face stiff opposition from the mass of population that depends on the traditional economy. For instance, in India's Andhra Pradesh state in the late 1990s and the early 2000s, political opponents attacked then–Chief Minister Chandrababu Naidu's decision to raise rice and electricity prices by cutting subsidies, which would worsen the welfare of most people. They also labeled his promotion of offshoring-related sectors and foreign capital as elitist. Naidu was voted out of office in 2004. For most the Indian population, data privacy and security are largely irrelevant.

Due to the above limitations, the resulting regulatory vacuum needs to be addressed by collaborative actions of the public and the private sector actors. A number of such efforts stand out in the context of India.

NASSCOM has engaged in advocacy and lobbying activities. In the mid-2000s, NASSCOM asked the Indian government to create a special court to try people accused of cybercrimes and other violations of the country's Information Technology Act (Ribeiro, 2006). NASSCOM has also established a CyberCop committee and a member of the committee serves as a technical advisor to the Indian CyberCrime Investigation Cell. NASSCOM works with police officers, lawyers, and industry bodies to ensure the enforcement of cybersecurity regulations. NASSCOM meets with bar councils in different cities to educate legal communities. It also educates police officers about cybersecurity and trains them to recognize and prosecute cybercrimes.

NASSCOM started working with Mumbai police since 2003 (Saravade & Saravade, 2007). NASSCOM helped police departments of cities such as Mumbai and Thane in establishing cybercrime units and providing training to officers. In 2005, NASSCOM announced a training initiative for Pune's cybercrime unit, which caught data crime perpetrators from Mphasis (Cone, 2005). A third cybercrime unit established in Bangalore in January 2007 has resources to train more than 1,000 police officers and other law-enforcement personnel annually. NASSCOM also offered to work with authorities in the U.K. and India to investigate cases involving identity theft (tribuneindia.com, 2005).

DSCI helped to establish cyberforensic labs in Mumbai, Bengaluru, Pune and Kolkata. As of the early 2012, DSCI had organized 112 training programmes on cybercrime investigation and awareness, which benefited about 3,700 police officials, judiciary and public prosecutors (Kshetri, 2013). As of 2014, there were eight Cyber Labs in various Indian cities, which provided training to over 28,000 police officers (DSCI, 2014).

Some PPP activities have been initiated by the government. Due to the country's lack of indigenous technology and patents related to cybersecurity, the GoI has announced that it would provide financial incentives to Indian firms to acquire foreign firms with high-end cybersecurity technology (Thomas, 2012). The Ministry of External Affairs would explore possible targets worldwide through Indian embassies and missions. The fact that Indian government agencies have been under cyber-attacks, suspected from foreign governments, has provided a major motivation for such an approach. An Indian company which owns the technology gained through the acquisitions is required to give the government agencies an access to the intellectual property rights (IPR).

5. Discussion and Implications

The Indian government severely lacks the resources to develop and enforce cybersecurity-related regulations, standards, and guidelines. Some have rightly labeled India's cybersecurity policy as "incomplete" and "all words and no action" (Desai, 2013) due to a lack of national cybersecurity action plan document or any guidelines regarding how the policy will be implemented. For instance, there is no clear action plan as to how the various goals proposed by the NCSP are going to be achieved. Overall, the NCSP lacks details of tangible actions and specific guidance, direction and procedures in order to achieve the vision of a secure cyberspace. The director of Israel's Military and Strategic Affairs Program and director of the cyber-warfare program at the Tel Aviv University's Institute for National Security Studies (INSS) noted: "India has published its strategy .., but it is far away from what I call strategy ... It does not have the substance ... (and is) a very generic, high-level paper" (Alawadhi, 2014).

NASSCOM and DSCI have been exemplary self-regulatory bodies, playing key roles in strengthening the IT&BPM sector’s cybersecurity orientation. They have played an equally important role in the PPP cybersecurity initiatives and worked with government and law enforcement agencies to formulate and enforce cybersecurity-related legislation.

Trade associations such as NASSCOM and DSCI influence industry behaviors directly as well as through causal chains. Indirect effects entail mimicking behaviors of other actors that are perceived to be exemplary and have a higher degree of effectiveness ((Dickson et al. 2004; Lawrence et al., 2001). Exemplary firms serve as models for smaller firms to imitate. In such cases, knowledge flow takes place by externalities mainly due to interactions among firms or their employees. Trade associations are likely to accelerate this process by stimulating interaction among member companies.

Regarding the active and influential roles played by NASSCOM and DSCI, it is worth noting that the Indian economy and society are less centralized with more room for trade associations to flourish and to have a strong voice (Frankel, 2006). Since the 1990s, there has been a shift from a state-dominated economic policy framework towards a decentralized one. Religious, social, economic and political associations have offered a viable set of examples encouraging the development of many new trade and professional associations (Frankel, 2006). A strong mutual interdependence between the state and the private economic actors, particularly organized business groups, has developed very quickly.

The initiatives and responses of NASSCOM and DSCI can be considered to be the results of a hollow state and the thin institutions that hamper legislative and law enforcement efforts. For instance, India lacks standard identifiers like the U.S. Social security number making it difficult to check potential employees' backgrounds. It was reported that a thorough background check cost up to $1,000 per employee to (Schwartz, 2005). In response to the lack of such databases, in 2005, NASSCOM announced a plan to launch a pilot employee-screening program called "Fortress India", which would allow employers to screen out potential workers who have criminal records. Subsequently it was developed into the National Skill Registry (NSR), which allows employers to perform background checks on existing or prospective employees. It is a voluntary registry for call center employees.

6. Concluding Comments

Like other developing economies, India faces problems such as ineffective regulation, a lack of poorly trained law enforcement manpower and up-to-date technology. These factors have led to under-resourced and underdeveloped institutional capacity on the cyber front. As is the case of the rest of the world, India faces a severe shortage of cybersecurity professionals. This is among the key obstacle in addressing the growing cybercrimes in the country. A strong civil society has been recognized as a crucial feature of India’s political development. This phenomenon has also allowed private-sector participants such as NASSCOM to play an important role in strengthening cybersecurity. Indeed, Indian offshoring industry provides a remarkable example of industry government collaboration in combating cybercrimes.

References

Aggarwal, V. (2009). Lead: Cyber crime's rampant, Express Computer, 03 August 2009. <http://www.expresscomputeronline. com/20090803/market01.shtml. Accessed 1 October 2009>

Alawadhi, N. (2014). Cyber security policy must be practical: Experts. <http://articles.economictimes.indiatimes.com/2014-10-22/news/55318902_1_cybersecurity-digital-india-national-cyber-security-policy>

Anand, J. (2011). Cybercrime up by 700% in Capital. http://www.hindustantimes.com/India-news/NewDelhi/Cyber-crime-up-by-700-in-Capital/Article1-766172.aspx

Blitz, J. (2011). Security: A Huge Challenge from China, Russia and Organised Crime. <http://www.ft.com/intl/cms/s/0/b43488b0-fe2a-11e0-a1eb-00144feabdc0.html#axzz1dnezI1eF>

Borland, J. (2010). A Four-Day Dive Into Stuxnet's Heart. <http://www.wired.com/threatlevel/2010/12/a-four-day-dive-into-stuxnets-heart/>

Bradbury, D. (2013). India's Cybersecurity challenge. <http://www.infosecurity-magazine.com/view/34549/indias-cybersecurity-challenge/>

Business Insurance. (2014). N.Y. state financial regulator will focus on cyber security. <http://www.businessinsurance.com/article/20140923/NEWS07/140929962?tags=|338|299|69|80|83|302|303>

catindia.gov.in (2014). History, September 22, <http://catindia.gov.in/History.aspx, Cyber Appellate Tribunal, Government of India>

cio.de (2014). India's biometric ID project is back on track, <http://www.cio.de/index.cfm?pid=156&pk=2970283&p=1>

Damouni, N. (2014). Exclusive: U.S. companies seek cyber experts for top jobs, board seats, May 30. Reuters. <http://www.reuters.com/article/us-usa-companies-cybersecurity-exclusive-idUSKBN0EA0BX20140530>

Das, G. (2011). Panel to Advise Govt, IT cos on Cloud Security on the Cards. <http://www.financialexpress.com/news/Panel-to-advise-govt—IT-cos-on-cloud-security-on-the-cards/809960/>

Das, S. (2017). 11,592 cases of cyber crime registered in India in 2015: NCRB. <http://www.livemint.com/Politics/ayV9OMPCiNs60cRD0Jv75I/11592-cases-of-cyber-crime-registered-in-India-in-2015-NCR.html>

Desai, V.V. (2013). Is India's cyber policy all words and no action? <http://searchsecurity.techtarget.in/news/ 2240207148/Is-Indias-cyber-policy-all-words-and-no-action>

Deshpande, S. (2009, October 28) New cyber law casts its net wide. The Economic Times. <http://economictimes.indiatimes.com/infotech/internet/New-cyber-law-casts-its-net-wide-/articleshow/5170897.cms>

Dickson, M., BeShers, R., Gupta, V. (2004). 'The impact of societal culture and industry on organizational culture: Theoretical explanations', Culture, leadership, and organizations: the GLOBE study of 62 societies, Robert J. House, Paul J. Hanges, Mansour Javidan, Peter W. Dorfman, and Vipin Gupta (eds) Thousand Oaks, Calif. : Sage Publications.

DNA (2017). Irdai asks insurers to appoint data security officer by April 30. DNA Daily News & Analysis. <http://www.dnaindia.com/money/report-irdai-asks-insurers-to-appoint-data-security-officer-by-apr-30-2391043>

Doval, P. (2013). Govt orders security audit of IT infrastructure. <http://timesofindia.indiatimes.com/tech/tech-news/Govt-orders-security-audit-of-IT-infrastructure/articleshow/38398644.cms>

DSCI. (2014). Cyber Labs, <http://www.dsci.in/cyber-labs>

Duggal, P. (2004). What's wrong with our cyber laws? <http://www.expresscomputeronline.com/20040705/newsanalysis01.shtml>

Economictimes. (2005). R&D in India: The Curtain Rises, the Play Has Begun. <http://economictimes.indiatimes.com/rd-in-india-the-curtain-rises-the-play-has-begun/articleshow/1207024.cms>

Economictimes. (2012). Cyber Crime Increasing in India at Fast Clip: P. Chidambaram.<http://economictimes.indiatimes. com/tech/internet/cyber-crime-increasing-in-india-at-fast-clip-p-chidambaram/articleshow/11891033.cms>

Economist. (2007). Imitate or Die; Technology in China and India, 385(8554): 9.

Engardio, P., Puliyenthuruthel, J., & Kripalani, M. (2004). Fortress India? Business Week, 3896, 42–43.

Fest, G. (2005). Offshoring: Feds take fresh look at India BPOs; Major theft has raised more than a few eyebrows. Bank Technology News, 18(9), 1.

Frankel, R. (2006). Associations in China and India: An Overview, European Society of Association Executives. <http://www.esae.org/articles/2006_07_004.pdf>

Gardner, T. (2012). Indian Call Centres Selling Your Credit Card Details and Medical Records for Just 2p. <http://www.dailymail.co.uk/news/article-2116649/Indian-centres-selling-YOUR-credit-card-details-medical-records-just-2p.html>

Gent, E. (2016). Lack of cybersecurity expertise could derail 'Digital India' initiative, Tech Wire Asia <http://techwireasia.com/2016/08/lack-cybersecurity-expertise-digital-india/#iyi6YSKdmJ4eeotO.97>

Goswami, S. (2017). India's Cyber Security Startups Are Gaining Traction, Thanks To Demonetization, Forbes. <https://www.forbes.com/sites/suparnagoswami/2017/02/02/indias-cyber-security-startups-are-gaining-traction-thanks-to-demonetization/#e9dc12e58261>

Haran, V. (2011). Insider Threats a Major Concern for India Inc: DSCI–PwC Study.<http://searchsecurity.techtarget. in/news /2240037365/Insider-threats-a-major-concern-for-India-Inc-DSCI-PwC-study>

Hettigei, N.T. (2005). The Auditor's role in IT development projects. <http://www.isaca.org/Journal/Past-Issues/2005/Volume-4/Pages/The-Auditors-Role-in-IT-Development-Projects1.aspx>

Hindustan Times. (2006). Securing the web.

Hindustan Times. (2009). Wired for trouble. <http://www.tmcnet.com/usubmit/2009/10/24/4442635.htm>

indiatimes.com. (2011). Most Gurgaon IT, BPO companies victims of cybercrime: Survey, November 6, <http://timesofindia.indiatimes.com/city/gurgaon/Most-Gurgaon-IT-BPO-companies-victims-of-cybercrime-Survey/articleshow/10626059.cms>

indolink.com. (2012). India Battles Against Cyber Crime. <http://www.indolink.com/displayArticleS.php?id=102112083833>

Internet Crime Complaint Center (2011). 2010 Internet Crime Report. <http://www.ic3.gov/media/annualreport/2010_ic3report.pdf>

KPMG. (2014).Cybercrime survey report 2014, Retrieve from www.kpmg.com/in

Kshetri, N. (2010). The Global Cyber-crime Industry: Economic, Institutional and Strategic Perspectives, Springer-Verlag: New York, Berlin and Heidelberg.

Kshetri, N. (2011). Kaspersky Lab: From Russia with Anti-virus, Emerald Emerging Markets Case Studies, 1(3): 1–10.

Kshetri, N. (2013). Cybercrime and Cybersecurity in the Global South, Palgrave Macmillan: Houndmills, Basingstoke, U.K.,

Kshetri, N. (2015a). India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership. IEEE Security & Privacy, 13(3), 16-23.

Kshetri, N. (2015b). Cybercrime and Cybersecurity Issues in the BRICS Economies. Editorial, Journal of Global Information Technology Management, JGITM, 18(4), 1-5.

Kshetri, N. (2016c). Cybersecurity and Development. Markets, Globalization & Development Review, 1(2), Article 3: <http://digitalcommons.uri.edu/mgdr/vol1/iss2/3>

Kshetri, N. (2016d). Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future. Crime, Law and Social Change, 66 (3), 313–338.

Kshetri, N. (2016a). Big Data's Big Potential in Developing Economies: Impact on Agriculture, Health and Environmental Security. Centre for Agriculture and Biosciences International (CABI) Publishing, Wallingford, Oxon, the U.K.

Kshetri, N. (2016b). The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies, Springer-Verlag: New York, Berlin and Heidelberg.

Lawrence, T. B., Winn, M. I., Jennings, P. D. (2001). 'The Temporal Dynamics of Institutionalization', The Academy of Management Review, 26(4): 624-644.

McGrayer, McGinnis, Leslie, and Kirkland (2014). What is Cyber Liability Insurance? The National Law Review. <http://www.natlawreview.com/article/what-cyber-liability-insurance>

Narayan, V. (2010). Cyber Criminals Hit Esc Key for 10 yrs. <http://timesofindia.indiatimes.com/city/mumbai/Cyber-criminals-hit-Esc-key-for-10-yrs/articleshow/6587847.cms>

NASSCOM (2017). Vision and Mission. <http://www.nasscom .in/vision-and-mission>

Nolen, S. (2012). India's IT Revolution Doesn't Touch a Government That Runs on Paper. The Globe and Mail (Canada), p. A1.

Otis, C. and Evans, P. (2003). The Internet and Asia-Pacific Security: Old Conflicts And New Behavior. Pacific Review, 16 (4), 549–550.

Pandya, D. (2009). CISO reporting to board of directors: Myth or for real? <http://www.computerweekly.com/news/1375176/CISO-reporting-to-board-of-directors-Myth-or-for-real>

PTI (2014). Shortage of over a million cyber security experts globally, The Economic Times.<http://economictimes. indiatimes.com/tech/internet/shortage-of-over-a-million-cyber-security-experts-globally/articleshow/29110114.cms?intenttarget=no>

PTI (2016). Cyber insurance premium rates increase after debit cards hack, BGR. <http://www.bgr.in/news/cyber-insurance-premium-rates-increase-after-debit-cards-hack/>

PTI (2017). Banks rush to buy cyber security cover as digital payments rise, The Times of India. <http://timesofindia.

indiatimes.com/business/india-business/banks-rush-to-buy-cyber-security-cover-as-digital-payments-rise/articleshow/57109647.cms>

Pughm, C. (1999) Getting Good Government: Capacity Building in the Public Sectors of Developing Countries," Urban Studies, 36, 2, pp. 400–402.

rediff.com (2008). Researchers? Only 156 per Million in India. <http://www.rediff.com/money/2008/mar/12rnd.htm>

Ribeiro, J. (2006). India's Nasscom calls for special cybercrimes court. Network World. <http://www.networkworld.com/news/2006/090706-indias-nasscom-calls-forspecial.html>

Ribeiro, V. J. (2014). India's biometric ID project is back on track. CIO. <http://www.cio.de/index.cfm?pid=156&pk=2970283&p=1>

Robinson, G.E. (1998), Elite cohesion, regime succession and political instability. Syria Middle East Policy, 5 (4), 159-79.

Saraswathy, M. (2012). Wanted: Ethical Hackers. <http://www.wsiltv.com/news/three-states/Protect-Yourself-from-Cyber-Crime-139126239.html>

Saravade, P., & Saravade, N. (2007). A public-private partnership in India: Broken windows in cyberspace. The Police Chief, 74(3), 16.

Shaftel, D. and Narayan, K. (2012). Call Centre Fraud Opens New Frontier in Cybercrime. <http://www.livemint.com/2012/02/26225530/Call-centre-fraud-opens-new-fr.html>

Singh, S.R. (2014). India's only cyber appellate tribunal defunct since 2011, Retrieve from <http://www.hindustantimes.com/india-news/india-s-only-cyber-appellate-tribunal-defunct-since-2011/article1-1235073.aspx>

Srivastava, M. (2016). India to promote indigenous expertise in cyber security, to fund start-ups, Business Standard. <http://www.business-standard.com/article/companies/india-to-promote-indigenous-expertise-in-cyber-security-to-fund-start-ups-116101300028_1.html>

Sweeney, B. (2016). Cybersecurity Is Every Executive's Job. Harvard Business Review. September 13. <https://hbr.org/2016/09/cybersecurity-is-every-executives-job>

Syed, F., & D'monte, L. (2008). India lags in cybercrime insurance. <http://www.rediff.com/money/2008/apr/07cyber.htm>

Schwartz, K. D. (2005). The background-check challenge. InformationWeek, 59–61.

TechTarget (2014). Indian businesses wake up to IT security risks, Computer Weekly. <http://www.computerweekly.com/news/2240225781/Indian-businesses-wake-up-to-IT-security-risks>

The Economist. (2005). Business: Busy Signals; Indian Call Centres, The Economist, 376(8443): 66.

thehindubusinessline.com. (2007). Regulator Soon for Monitoring Data Security Standards. 24 Apr. 2007. <www.thehindubusinessline.com/todays-paper/regulator-soon-for-monitoring-data-security-standards/article1656182.ece>

Thomas, T.K. (2012). Govt will help fund buys of foreign firms with high-end cyber security tech, <http://www.thehindubusinessline.com/industry-and-economy/info-tech/article3273658.ece?homepage=true&ref=wl_home>

tribuneindia.com. (2005). Outsourcing crime Call centre expose can wreak havoc. <http://www.tribuneindia.com/2005/20050625/edit.htm>

Venkatesh, S. (2017). Indian IT-BPM industry clocks growth rate of 8.6 percent in FY2017: NASSCOM. Forbes India. <http://www.forbesindia.com/article/special/indian-itbpm-industry-clocks-growth-rate-of-8.6-percent-in-fy2017-nasscom/45951/1>

Yu, J.X. and Z.Y. Qu. (2012) PPPs: Inter-Actor Relationships Two Cases of Home-Based Care Services in China," Public Administration Quarterly., vol. 36, no. 2, pp. 238–264.

Science and Technology Trends
Governance Systems for Cybersecurity

National Cybersecurity Governance and Implementation of Malaysia for the Critical National Information Infrastructure

Mohd Shamir Bin Hashim

1. The Policy on Cybersecurity

1.1. Background

In 2005, the Malaysian Government realized the interdependency of ICT infrastructures, mainly through the Internet, brings great benefits and enables the country to turn knowledge into value for the benefit of the people. However, this same interdependency means that the country's modern industrialized society is now increasingly vulnerable to cyber threats that have potential devastating impacts. The interdependent and borderless nature of the Internet increases the number of attack vectors and makes bringing cyber criminals to justice an ever more challenging task.

The increasing pervasiveness, connectivity and globalization of information technology and the dynamic nature of cyber threats means that countries must adopt an integrated approach to protect their Critical National Information Infrastructures (CNII) including efforts to focus resources, strengthening the law enforcement, improving coordination, enhancing research and development, facilitating information sharing, and encouraging greater public and private cooperation. This approach is in a form of a cybersecurity policy which focuses on protecting the country's CNII.

1.2. Policy Domains

In coming up with a cybersecurity policy, the following domains were considered.

1) Legislation − identify and review the existing laws and regulations governing cybersecurity and to perform analysis to confirm compliance to international laws;
2) Institutional − review existing institutional arrangements and identify the roles and responsibilities that coordinate national security efforts in protecting the CNII against cyber threats;
3) Technology − review existing information security requirement against international standards and best practices and identify deployment of security controls and safeguards to CNII;

CyberSecurity Malaysia, Level 5, Sapura@Mines, No. 7 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia
E-mail: shamir@cybersecurity.my

4) Public and Private Cooperation − review and analyze the current level of coordination of cooperation and partnership arrangements between the public and private sector in mitigating attacks and cyber threats to the CNII;
5) International Engagement − analyze the available international security implementation models and determine the feasibility to implement it locally.

1.3. The Critical National Information Infrastructure

The policy is developed to cater for the protection of the CNII. Therefore, there is a need to have a definition of CNII for the country. A series of discussion sessions were conducted involving the relevant stakeholders from the ministries, academic institutions, the industry, and government agencies to decide on a definition of Malaysian CNII. As a result, the CNII of Malaysia is defined as those information infrastructures that are very important to the nation that significant disruption to which, would have severe impact on the national economic strength, image, defense and security, government capabilities to function, and public health and safety.

In addition to the definition, the CNII of Malaysia is categorized into ten (10) sectors which are:

National Defence & Security	Water
Banking & Finance	Health services
Information & Communication	Government
Energy	Emergency services
Transportation	Food & Agriculture

2. The National Cybersecurity Policy

The proposed cybersecurity policy for Malaysia was presented to the Cabinet of Ministers in 2006. The proposal was accepted for implementation and is named The National Cyber Security Policy (NCSP).

The NCSP seeks to address the cyber threat risks to the CNII of Malaysia. It recognizes the critical and highly interdependent nature of the country's information infrastructure and aims to develop and establish a comprehensive program and a series of frameworks to ensure the effectiveness of information security controls over vital assets and that the CNII are protected to a level that commensurate the risks faced.

2.1. Policy Vision

The vision of the NCSP is:

''Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well-being and wealth creation.''

This vision is in line with the need in reaching a developed nation status and aligned with the culture and values of the Malaysia. Continuous promotion and communication of the vision created short term objectives and encouraged individual entities within the CNII to focus on cybersecurity resources in a manner that is compatible and aligned with the NCSP vision.

Promoting stability means reducing risk of disruption to critical services. A secure, resilient and self reliant CNII will reduce the level of disruption to critical services and will help prevent hostile cyber attacks from outside of Malaysia. Meanwhile, promoting social well-being is about having a greater availability of services through the increased use of new technologies.

2.2. Key Policy Pillars

The NCSP has eight (8) Policy Thrust (PT) that covers the aspect of national cybersecurity, which are as follows.

2.2.1. Effective Governance

The interdependent nature of the CNII means that cybersecurity incidents can cascade to other sectors. The Malaysian Government has made significant progress in securing the CNII since the adoption of the NCSP but there are still challenges to be confronted. Initially, the Ministry of Science, Technology and Innovation Malaysia, the developer of the NCSP, took the task of implementing the policy. At that point, cybersecurity protection programs were not systematically coordinated across the government machineries resulting to confusion and misunderstanding among agencies regarding their roles and responsibilities. In the absence of coordination, ministries and agencies focus on their own missions and not on the overarching national needs.

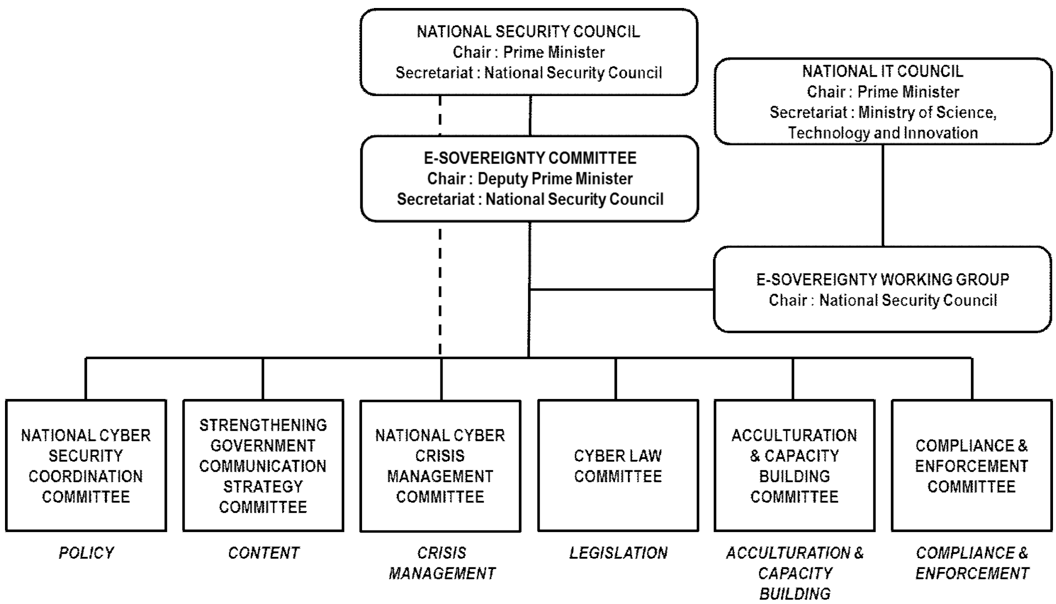
The policy identified the need for a single information security coordination body to be established. CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation, was given this task to provide a strong platform for strengthening the nation's cybersecurity efforts and improving the public and private cooperation across the CNII. To date, the agency has raised the profile of cybersecurity and continued to vigorously promote the 'culture of security' within the country.

In 2011, as cybersecurity grew in importance, the custodian of the NCSP, was transferred from the Ministry of Science, Technology and Innovation Malaysia to the National Security Council Malaysia under the Prime Minister's Department. This further facilitates the coordination in implementing the initiatives of cybersecurity across multiple ministries and agencies. However, CyberSecurity Malaysia remains as the organization implementing the policy.

The CNII organizations in Malaysia are a combination of public and private entities which are governed by their respective regulators. Therefore, under this policy thrust, there is a need for a public-private cooperation framework covering incident response, reporting structure, focal point for cybersecurity protection-related, research and development (R&D) and cybersecurity awareness efforts.

Cybersecurity effective governance for Malaysia is done by the e-sovereignty Committee under the purview of the National Security Council. Figure 1 shows the structure of the committee.

Figure 1. Malaysia e-Sovereignty Committee



2.2.2. Legislative & Regulatory Framework

The NCSP is to ensure the confidentiality, integrity and availability of information and non-repudiation of communication in accordance with its vision. It is intended to create trust and confidence within the Malaysian CNII. The legal system is important and must be adequate and adaptable to ensure the advancement in information technology benefits the people and the country, and to ensure that the CNII is securely protected from cyber attacks. Therefore, the laws and regulations are defined, and categorized to penalized cyber crimes so as to deter future malice and to provide the country with the appropriate level of compliance.

The laws and regulations must be enhanced in order for enforcement agencies to effectively detect and address problems and threats from cyber attacks and interruption to the information systems; both with preventive and corrective measures to effectively address legal challenges surrounding the information security protection. To achieve this, it is imperative for Malaysia to create an enabling environment through continuous reviews and coordination of the country's legislative and regulatory frameworks in line with global standards and approved best practices.

CyberSecurity Malaysia in 2011 conducted 'A Study on the Legal Issues of Cyber Activities in Malaysia', under the guidance of the Attorney's General Chambers, on the existing laws of Malaysia related to the cyber environment such as the Computer Crimes Act, the Communication and Multimedia Act and the Digital Signature Act. These also include some of the conventional laws that also have implication on the cyber environment such as the Penal Code, the Internal Security Act, the Sedition Act, the Defamation Act, and the Evidence Act. The outcome of the study is recommendations on improvement that need to be made to the existing laws. With the recommendations, the Attorney General's Chambers worked with the respective ministries to make the necessary amendments.

However, presently such legislative and regulatory initiatives should not only be a national agenda, but also as part of an international framework in curbing cyber threats to the global community. Crimes in cyber space transcends traditional boundaries that restrict the movement of conventional criminals. In the realm of information and communications technology, criminal action in one country can affect other countries due to the interconnectivity and interdependence of borderless networks.

2.2.3. Cybersecurity Technology Framework

The cybersecurity technology framework defined clear security controls to be implemented and enforced. Security controls such as management, technical and operational controls help to put the necessary measures in place for security implementation. In addition, the security controls applied to a particular information system shall be commensurate with the potential impact on organizational operations, organizational assets, or individuals should there be a breach in security due to the loss of confidentiality, integrity, or availability.

Previously the need for equipment and systems were based on individual requirements and not based on a baseline or standards approved by the government. Thus for most cases, cybersecurity controls were determined at a later stage and had proven to be expensive and damaging to the network.

This policy thrust provides a reference point for formulating the standard cybersecurity baseline for the protection of CNII. The key objectives of formulating the standard cybersecurity baseline are to establish a standard to be used by CNII; and to ensure all procurement or in-house development of CNII cybersecurity-related products and systems comply with the security requirements of the baseline.

Cybersecurity-related products and systems encompasses a broad range of hardware, application software, security practices, security architecture and designs, physical security measures, as well as policies and procedures that protect the confidentiality, integrity, and availability of information residing within and across the CNII elements. This policy thrust defined the security controls that are needed. Security such as management, technical and operational controls provided some assurance that security measures are in place.

Base on the requirement of this thrust, it was recommended that all CNII entities of Malaysia adopt the MS ISO/IEC 27001-2007 Information Security Management System (ISMS) as a security baseline and to obtain the certification. After much deliberation, the Malaysian Government agreed to this proposal and issued an instruction in February 2010 that all Malaysian CNIIs are to be ISMS certified within three years.

Another initiative under this thrust is the establishment of the Malaysia Common Criteria Evaluation and Certification Scheme (MyCC). CyberSecurity Malaysia has become a member of the Common Criteria Recognition Arrangement (CCRA) since 2007. The CC scheme implements a security evaluation/certification program that will enable users to procure technology with greater confidence. This kind of evaluation will reduce the need for the individual CNII entities to perform their own testing. This improved competitiveness, technology deployment and decrease the risk faced by implementers of the technology.

2.2.4. Culture of Security and Capacity Building

The advancement of the wireless and broadband technologies has contributed significantly to the increasing participation of the interconnected community. As a result of this mounting interconnectivity and interdependency, information systems and networks are now exposed to a growing number and variety of threats and vulnerabilities. This raises the need for a greater awareness and understanding of cybersecurity issues and the need to develop a culture of cybersecurity, which encompasses on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within the information systems and networks.

There was a lack of cybersecurity outreach and awareness in both the public and private sectors coupled with the lack of initiatives that can drive and increase the level of cybersecurity awareness through training and education strategies across all elements of the CNII. CyberSecurity Malaysia conducted a study in 2010 titled the National Strategy for Cyber Security Acculturation and Capacity Building that focuses on the key aspect, which is the cybersecurity acculturation and capacity building that takes into consideration the interests of all parties that develop, own, provide, manage, service and use information systems and networks within the CNII.

The effort to promote a culture of security requires leadership and extensive involvement of well-planned and well-managed programs that was reduced into a systematic and strategic roadmaps and plans of action. This makes cybersecurity a concern and responsibility at all levels of government and business and for individuals who are involved in the CNII environment.

In achieving maximum success of the cybersecurity awareness and education programs, the initiatives and coordinated efforts are centralized to specialized organizations to drive and increase the level of cybersecurity awareness across all elements of the CNII. The cybersecurity acculturation programs also target the public by having plans to inculcate best practices, good habits and behaviours, and safe use of the Internet. This includes the development of content, the approach and implementation plan of the acculturation.

The culture of security is promoted by qualified professionals from specialized organizations whom identify minimum requirements and qualifications for those who are involved in the cybersecurity knowledge transfer processes. The CyberSAFE program, which stands for Cyber Security and Awareness for Everyone (www.cybersafe.my) is a CyberSecurity Malaysia's main program in inculcating security awareness in the country. This program provides content for children, youth, parents and organizations.

This is the one thrust that gives focus on the human aspect of cybersecurity. The development of human resources is critical to the success of efforts to improve security. In order to achieve the vision of the policy, the public and private sectors must have personnel that are sufficiently and professionally trained in the technical and non-technical issues of cybersecurity.

2.2.5. Research & Development Towards Self Reliance

To effectively garner the output from research and development, the coordination of the research teams, ideas, thoughts and innovation are consolidated under the 'National R&D Roadmap for Self-reliance in Cyber Security' developed by MIMOS Berhad, another entity under the Ministry of Science, Technology and Innovation of Malaysia. The objective of the roadmap is to overcome the lack of cybersecurity coordination and prioritization at the national level, which caused the research agendas and programs not to be systematically managed. Therefore, together with another 22 organizations representing the academics, government, industry and researchers, a consortium was formed with the goal of aligning and integrating all R&D programs and projects related to cybersecurity. This is to avoid duplication of efforts and to encourage collaboration, where appropriate, between academia, industry and the government.

The R&D roadmap focuses on technologies to protect the country's CNII with the aim of achieving self-reliance in those technologies. It specifies the critical technologies that are essential for the operation of the CNII, which are areas that are deemed vital in times of peace and crisis. Determining the research areas is important to prevent uncoordinated research efforts where individual entities and research institutes focus on individual missions that do not meet the overarching national needs and priorities.

The R&D efforts are aimed at countering threats to the CNII by making improvements to the current capabilities and also by developing new ones. This is achieved by intensifying efforts to promote cybersecurity research at learning institutions and research centres to increase the size of cybersecurity research community, which will churn revolutionary ideas and world class intellectual properties. These home grown intellectual properties provide the environment for future creation and development of the original works and finally stimulate greater economic growth and entrepreneurial activities.

2.2.6. Compliance & Enforcement

Interdependencies across the CNII are complex and pervasive. For example, no telecommunications organization can operate without power, and modern financial services organizations cannot operate effectively without telecommunications. As the ten sectors of the CNII are inter linked and reliant upon each other, a weakness in one of the sectors can be translated into a weakness in all the other sectors.

The NCSP requires that cybersecurity systems across the CNII to be standardized. It was strengthened and monitored, and enforced base on international standards. The policy also required the development of a standard cybersecurity risk assessment framework. It is therefore of vital importance that all the ten CNII sectors achieve a minimum level of cybersecurity and that this achievement is independently verified.

Therefore, there is a need for independent cybersecurity audits and other control mechanisms where the information was used to monitor compliance, set baselines and identify trends. This has assisted in identifying the CNII sectors that need help in meeting the security baseline. For this, a Working Group (WG) consisting of members from multiple ministries and CNII organizations along with CyberSecurity Malaysia, develop a risk assessment framework for the CNII to use in identifying risk within their respective IT systems. This has helped the entities to understand their own risk profile by using similar, acceptable and comparable techniques to identify risk. The uniformity in using the framework allowed the identification of trends, strength and weaknesses. Apart from allowing the identification of critical systems that need to be secured, it also provides assistance, focus resources and drive the research and development initiatives.

The Government of Malaysia has imposed the requirement for all CNII organizations to be ISO/IEC 27001 Information Security Management System (ISMS) certified. The National Security Council of Malaysia has identified about 200 of the country's CNII and spearheads the task of ensuring these organizations get the required certification. The ISO/IEC 27001 ISMS is the cybersecurity baseline for the CNII Malaysia.

The Chief Government Security Office under the Prime Minister's Department of Malaysia has an Inspectorate Team, and together with CyberSecurity Malaysia conduct periodic security audit on the country's vital points which covers the CNII sectors. This is to ensure that the security requirement dictated by NCSP is fulfilled and maintained.

2.2.7. Cybersecurity Emergency Readiness

The cybersecurity incident response, warning and alert systems are critical tools in combating cyber attacks. Although is it difficult to establish with any accuracy the actual loss resulting from these attacks, the trend shows that such attacks are increasing in frequency, sophistication and scale. Therefore, vigilant monitoring and effective incident response is very important.

During the initial stage of implementing the NCSP, effective cybersecurity monitoring is not prevalent among the CNII entities. In addition to incident response and monitoring, the absence of business continuity management was seen as another critical factor hindering the country towards having a resilient and secure CNII.

The Computer Emergency Response Teams (CERT) or the Computer Security Incident Response Team (CSIRT) is an instrumental set up in mitigating cyber threats and incidents. There are a few CERTs in Malaysia but the two prominent ones are the Government CERT (GCERT) and the Malaysian CERT (MyCERT). The GCERT is hosted by the Malaysian Administrative Modernisation and Management Planning Unit of the Prime Minister's Department, and having the public sector as its jurisdiction. Meanwhile, MyCERT is hosted by CyberSecurity Malaysia having jurisdiction over the country and is consider the national CERT.

Previously the CERT's operate effectively within their own sectors, and it was found that there was a lack of coordination between CERTs due to their defined jurisdiction and this resulted in less information sharing and less effective incident response. Therefore, the lack of coordination was improved to ensure effective coordination, standardization and consistency in order to address national cyber threats and attacks, by strengthening the cooperation between CERTs and relevant parties. Proper mechanisms were identified and put in place, and enforced for effective national cyber incident reporting.

The National Security Council of Malaysia has developed the National Cyber Crisis Management Plan (NCCMP) outlining national strategies in mitigating and responding to cyber incidents and attacks emphasising on the public and private collaboration and coordination. Tied to this plan are the national cyber drills co-organized annually by the National Security Council and CyberSecurity Malaysia. The main objective of these drills is to test the procedures and processes stated in the NCCMP. Through these drills, all shortcomings are identified and rectified to ensure continuous improvement to the NCCMP. The drills also observe the reactions of the participating CNIIs and the flow of information. It is critical to ensure that all cybersecurity related information gathered be disseminated to all the relevant CNII sectors as and when needed. Therefore, vulnerability advisories and threat warnings can and should reach everyone in a timely and efficient manner.

Additional to the drills, CNII organizations were strongly requested to develop document on comprehensive business continuity and disaster recovery plans as part of an effective business continuity management strategy. For the continuous efficiency of emergency readiness, periodic vulnerability assessments programs was also conducted to identify security flaws and recommended remedial actions.

2.2.8. International Cooperation

The global community has recognized that cyber threats are not affected by the geographical factors and the physical boundaries of countries. Therefore there is a serious need for international collaboration among countries for information security initiatives such as sharing information, research, best practices, overcoming challenges and formulating international policy. Under this policy thrust, Malaysia, through CyberSecurity Malaysia, maintain active participation on relevant international information security bodies and panels, and also in all relevant international information security events, conferences and forums. In addition, CyberSecurity Malaysia hosted international information security events to enhance the strategic position of the country.

CyberSecurity Malaysia is one of the co-founding members of the Asia Pacific Computer Emergency Response Team (APCERT) and has held the Chair and Secretariat position full term. Now the agency, as a member of the APCERT Steering Committee, holds the Deputy Chair position. On another major international initiative, CyberSecurity Malaysia spearhead the formation of the Organization of the Islamic Cooperation Computer Emergency Response Team (OIC-CERT)[2] holding the Chair and Secretariat position for full term. Just like the APCERT, the OIC-CERT is a collaborative platform of CERTs in mitigating cyber threats. However, while APCERT covers the Asia Pacific region and having members from 20 economies, the OIC-CERT have members from 21 Organization of the Islamic Cooperation (OIC) countries. Presently, CyberSecurity Malaysia has been appointed as the Permanent Secretariat of the OIC-CERT.

International cooperation in information security has strengthened the nation's capability, improves international recognition, highlights the existing achievements, and planned future activities. It has improved competitive advantage and strategic position, direction and initiatives in securing the CNII.

In addition to the mentioned multilateral engagement, Malaysia participated in various global information security platforms such as the Forum of Incident Response and Security Teams (FIRST), Anti-phishing Working Group (APWG), International Telecommunication Union (ITU), Asia-Pacific Economic

2 APCERT <www.apcert.org> , OIC-CERT <www.oic-cert.org>

Cooperation Telecommunications and Information (APEC TEL)[3]. The participation in international information security events, conferences and forums has enable Malaysia to increase the overall knowledge on information security, share best practices and identify common challenges as well as positioning Malaysia to becoming a leader in the field of information security. These events are excellent forums for knowledge sharing and helped increase the capacity of Malaysia's information security professionals.

The hosting of an annual international information security conference has help position Malaysia at the forefront of information security and establishes a reputation of thought leadership in this field. CyberSecurity Malaysia hosted the CyberSecurity Malaysia Award, Conference and Exhibition (CSM-ACE)[4].

This annual international conference hosted locally has increased the reputation, skills and capacity of Malaysia's own information security professionals. This event is also used to showcase home grown organizations and products giving the local information security industry an added advantage.

Increased international cooperation, activity and visibility by Malaysia in the field of information security have provided rapid expansion of local technologies in the security industry.

2.2.9. Lesson Learned

With the dependence on IT infrastructure resulting as the increase of cyber incidents, it is a right move for Malaysia to develop a national cybersecurity policy with a focus on enhancing the security, resilience and self-reliance of the country's CNII to promote stability, social well-being and wealth creation.

In implementing the policy, the keys to success were;

- Effective governance and coordination with the establishment of a single coordination centre which in this case is CyberSecurity Malaysia, which has created organization clarity and accountability;
- Improving the public private cooperation;
- Improving the information security skills and capacity;
- Enhancing the existing research & development initiatives toward self-reliance;
- Mapping out the emergency readiness;
- Dictating the program for compliance and assurance across the whole of CNII; and
- Reaching out to international partners.

References

Ministry of Science, Technology and Innovation, Malaysia, "National Cyber Security Policy: The Way Forward," Federal Government Administrative Centre. July 2006.

UK Office of Cyber Security, "Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space" Office of Public Sector Information, Information Policy Team, June 2009.

United State, Executive Office of the President "Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure," United State, Executive Office of the President, May 2009.

Ministry of Science, Technology and Innovation. "National R&D Roadmap For Self-Reliance in Cyber Security Technologies." Unpublished.

ISACA and the IT Governance Institute. ISACA Overview. Retrieved April12, 2011. From <http://www.isaca.org/About-ISACA/History/Pages/default.aspx>

Hashim, M.S; "Malaysia's National Cyber Security Policy − The Country's Cyber Defence Initiatives'; IEEE; London, UK; June 2011

(ISC)². About (ISC)². Retrieved April 12, 2011. From <https://www.isc2.org/aboutus/default.aspx>

EC-Council. About us. Retrieved April 12, 2011. From <http://www.eccouncil.org/about_us.aspx>

3 FIRST <www.first.org>, APWG <www.antiphishing.org>, ITU <www.itu.int>, APEC TEL <www.apectelwg.org>

4 CSM-ACE <www.csm-ace.my>

Science and Technology Trends
Governance Systems for Cybersecurity

Cybersecurity Governance Framework in Vietnam: State of Play, Progress and Future Prospects

Candice Trân Dai

1. Introduction

Vietnam has made tremendous progress over the past decades in the field of Information and Communication Technology (ICT). The country moved fast and emerged as a dynamic player in the global ICT landscape. It has become an attractive location for IT outsourcing and ICT hardware production as well as one of the fastest growing digital economies in the world. With a total population of 94,93 million, the Internet penetration rate in Vietnam has reached 53% and the E-commerce rate penetration is to date 35% (We are social, 2017), both statistics showing that the country enjoys plenty of scope for further development in this area. Since the country was connected to the global Internet network in 1997, and especially at the turn of the Millennium, it has embarked on the path of an accelerated and relatively comprehensive development of the ICT sector, largely driven and supported by a proactive governmental policy.

Vietnam appears to be a very good example of a country that has chosen a proactive ICT development strategy that is reflected not only by the tangible dynamism of the Vietnamese information society and by the strong enthusiasm of the Vietnamese population for new digital tools, products and services but also consequently by the growing exposure of the country to cyber threats. In the case of Vietnam, cyber threats are internal as well as external in the sense that the country faces malicious acts in cyberspace from its territory but also directed from outside. According to data from collaborative platforms of IT security specialists and reports from companies specializing in information systems security, which monitor and produce statistics on malicious activities in cyberspace on a global scale, Vietnam's situation is as follows: the country belongs to the top ten countries in the world with the highest malware encounter and infection rates (Microsoft, 2016) for January-June 2016 period, it ranks third in the top 25 countries in the world with the highest number of suspected botnet[1] IPs for the year 2016 (Daily Botnet Statistics, 2017), it reaches the fourth place among the top 5 countries for spam sending, and the third place among the top 5 countries for

Asia Center, 59 bis avenue Gabriel Péri 94100 Saint-Maur des Fossés, France
E-mail: C.TranDai@centreasia.eu

1 A botnet is a set of compromised computers, often referred to as "zombies", infected with malicious software, which allows an attacker to control them.

dictionary[2] attacks (Project Honey Pot, 2017). Noteworthy progress has been made regarding the overall cybersecurity situation of Vietnam in recent years, as shown by the results of Vietnam's Information Security Index performed by the Vietnam Information Security Association (VNISA) with the country reaching 59.9 per cent for the year 2016 as compared to 47.4 percent in 2015, 39 percent in 2014 and 37.3 percent in 2013. Nevertheless, Vietnam has to cope with an increasing number of cyber incidents[3].

While Vietnam nurtures strong ambition to reach its digital potential, it faces several obstacles and challenges to achieve its goals. Besides the need for further improvement of overall IT infrastructures to support the growing digital economy, or the need to further expand advancement in reducing the digital divide within the country, one of the important key factors in driving digital advancement lies in digital confidence. How much users trust digital products and services can be either a growth enabler or a significant impediment with regards to the digital economy. The stakes are high because the country remains extremely vulnerable and permeable to cyber attacks and cybercrimes, which could eventually affect the development potential of the ICT sector in the country and contravene the strong ambitions of the Vietnamese government in this field. This is particularly critical as Vietnam considers ICT as a strategic lever for economic development and as the country strives for reaching the next level of digital maturity by leveraging on digital transformation and digital innovation. In the context of great exposure to cyber threats, the Vietnamese authorities have been thriving in recent years to tackle cybersecurity gaps in the country. The issue of cybersecurity has thus become a top priority for the Vietnamese government, which is well aware of the country's weak capacity in this area and the fact that the systems in place, whether organizational, regulatory or technical, do not offer sufficient and adequate protection against malicious acts in cyberspace.

This paper aims at reflecting the progress accomplished by Vietnam in dealing with the issue of cybersecurity by highlighting the formulation of cybersecurity policy and strategy in the making, implementation and work in progress so far, as well as challenges and opportunities.

2. Policy and Strategy

It is only in recent years that Vietnam has undertaken to take better control of the country's vulnerability in cyberspace and to enhance the country's cybersecurity capability. The first landmark initiative regarding cybersecurity in the country dates back to the year 2010 with the release of a dedicated government roadmap, i.e. the Prime Minister's Decision No. 63/QĐ-TTg of January 13, 2010 ratifying the “Digital Information Security Development Project to 2020”, with a planned investment of USD 42 million between 2010 and 2020.

Previous initiatives in this domain were all but scattered and area-focused: they did not encompass a holistic policy and strategy although they did include various cybersecurity aspects. We may for instance refer to the various decrees and laws that were passed at the beginning of the 2000s such as, among others: Decree No. 26/2007/ ND-CP of February 15, 2007 detailing the implementation of the Law on Electronic Transactions regarding digital

2 The attack of passwords by dictionary is a form of attack directed against passwords in clear, not against the encryption of passwords. The attacker is trying words that actually exist in a dictionary. This method is based on the fact that many people use common words for their passwords.

3 According to Vietnam Computer Emergency Response Team (VNCERT), the number of cyberattacks of all sorts in Vietnam for the year 2016 increased four fold as compared to 2015.

signatures and digital signature certification services; Decree No. 90/2008/ND-CP dated August 13, 2008 on Anti-spam ("Decree 90")[4]; Decree No. 64/2007/ND-CP dated April 10, 2007 on the application of information technology in the operation of State agencies; Decree No. 73/2007/ND-CP dated May 8, 2007 on the research, production, trading and use of crypto codes to protect information not falling within the scope of State secrets; the Law No. 51/2005/QH11 of November 29, 2005 on E-transactions, the Law No. 67/2006/QH11 of June 29, 2006 on information technology.

2.1. Digital Information Security Development Project 2010-2020

The "Digital Information Security Development Project to 2020" issued in 2010 sets forth Vietnam's overall objectives in the field of cybersecurity to be achieved by 2020 into a breakdown of four main areas: ensuring network security and information infrastructure so that they are in line with the needs of ICT development; ensuring the safety of data and information technology applications so that they comply with safety standards; training certified cybersecurity specialists and raising public awareness on information security; and improving the legal framework for information security and computer-related crime. The document further details the objectives to be attained during the period 2010-2015 such as: ensuring the security of national information infrastructures, which encompasses security techniques and equipment provision for internal networks of public institutions and national databases; building information security surveillance and alarm systems; ensuring the security of databases and applications of ICT in public institutions from central to local level as well as in the private sector, with the objective of 100% of government websites of all levels having effective solutions against security incidents as well as emergency plans in case of incident and 100% of electronic transactions platforms having taken measures to ensure the security of information; assuring the training of human resources, with the objective of issuing national certificates for 80% of administrators of important information systems of the government and effective training of one thousand cybersecurity professionals according to international standards; and improving the legal environment, especially regarding computer crime and encryption.

The 2010 roadmap also highlights the need to "improve mechanisms and government policies on information security", to "build and strengthen institutions in the field of information security", to "encourage and support the development of local information security products" and to "promote cooperation at home and abroad". Regarding the development of local cybersecurity products, the document focuses on investment and support for R&D of products, solutions and service models to complement imported cybersecurity products together with the support of local cybersecurity businesses as well as R&D and exploitation of open source technologies. As far as international cooperation is concerned, the document stresses the importance of sharing and exchanging information between countries not only at regional level but also at global level. It also calls for the reinforcement of cooperation between the various national institutions involved in cybersecurity.

2.2. Network Information Security Plan 2016-2020

Further to the "Digital Information Security Development Project to 2020", the Prime Minister's Decision No. 898/QĐ-TTg of May 27, 2016 ratifying the "Network Information Security Plan 2016-2020" provides for more specific tasks to be achieved during the period 2016-2020. Compared to the previous

4 This Decree had been amended by Decree No. 77/2012/ND-CP ("Decree 77") issued on October 5, 2012.

intermediate roadmap, which brought out rather basic and broad objectives, this second 5-year roadmap introduces additional features and highlights some current priorities. The new guidelines that have been emphasized revolve primarily around the following areas: reinforcement of the cooperation with the private sector and the role of Vietnamese companies in the domestic information security market; and enhancement of critical information systems security and cyber resilience capacity. There is clearly a call to the private sector, and especially the main associations representing the IT sector in Vietnam, such as the Vietnam Information Security Association, the Vietnam Software and IT Services Association, the Vietnam Association for Information Processing, the Vietnam Internet Association and the Vietnam E-commerce Association, to play an active and leading role in boosting the country's cybersecurity capability. Vietnamese companies, especially ICT and Internet operators, are hence expected to take all appropriate and effective measures to reinforce the protection of critical information infrastructures and to coordinate with the Ministry of Information and Communications (MIC) in this regard. The roadmap advocates the support to investment, training and development of human resources for small and medium enterprises operating in the field of cybersecurity. Moreover, Vietnamese companies are encouraged to foster R&D, production and supply of cybersecurity solutions, products and services. On this point, the Network Information Security Plan 2016-2020 sets out a target of "developing at least five Vietnamese brand name information security products widely used in the domestic market" by 2020. The Ministry of Science and Technology (MOST) shall play a preeminent role in funding and supporting market development of domestic cybersecurity solutions.

The roadmap highlights the task of ensuring the security of national important information systems and information systems of government agencies by insisting on cyber resilience and business continuity. It further emphasizes the objective of upgrading general information security awareness in the country by increasing awareness campaigns, expanding cybersecurity training and drills, as well as enhancing government agencies officials' awareness and training. Further to that, the roadmap introduces the idea of establishing a network of cybersecurity experts to support and advise the competent authorities regarding protection of the national information framework. The stress is also being laid on the need to "update the system of national standards and technical regulations relating to information security" and to "establish a framework model of network information security management system in accordance with international practices". In this domain, evaluation and assessment of information systems security management are to be carried out on a regular basis. It is worth mentioning that the roadmap sets a goal of "putting Vietnam out of the list of 20 countries with the highest rate of malware and spam spreading in the world". As mentioned before, Vietnam belongs to the world top countries for malware encounter and infection rates, suspected botnet IPs, spam sending, and dictionary attacks. Consequently, the country suffers from a bad reputation in this area and this may impact the overall digital attractiveness of the country. There is therefore a need to preserve trust in Vietnam's digital economy. In this respect, we may note that the roadmap highlights the objective of promoting the application of digital signatures. In line with the previous 5-year roadmap, the Network Information Security Plan 2016-2020 additionally reasserts the promotion of national and international cooperation in the field of cybersecurity, including with domestic and foreign enterprises.

2.3. Emergency Response Plan to Secure National Network Information Security

While the "Digital Information Security Development Project 2010-2020" and the "Network information security plan 2016-2020" outline various guidelines and objectives to enhance Vietnam's cybersecurity capability, the Vietnamese policy-makers have also come up with more practical policy and strategy documents which tend to reflect an increasing awareness and stronger engagement regarding cybersecurity issues.

The Prime Minister's Decision No. 05/2017/ QĐ-TTg of March 16, 2017, ratifying the "System of emergency and rescue plan to ensure the safety of the national information network", is a very good example of this evolving policy approach as it provides for an emergency response in case of serious cybersecurity incidents impacting national networks. The plan aims at addressing serious network security issues which fall under specific conditions and meet distinct criteria. Firstly, the information system subject to security incident must have been classified as a level 4 or level 5 information system[5] or it must have been included in the list of national important information systems. Secondly, the information system subject to security incident must have encountered one of the following problems: system services are interrupted; confidential data or State secrets are likely to be disclosed; integrity of important data of the system is not guaranteed and not recoverable; system control is lost; or the incident is likely to occur on a large scale or cause chain effects, compromising other level 4 or level 5 information systems. Thirdly, the management of the information system is not able to control and handle the problem. The emergency response plan further details the procedures for security incidents report, serious cybersecurity incidents remediation as well as initial rescue plan deployment and emergency rescue plan implementation.

Regarding organization and management, a National Steering Committee for Emergency Response will be established with the task of directing the Ministry of Information and Communications, the Ministry of Public Security (MPS), the Ministry of Defense (MOD) and other concerned ministries, branches and localities in emergency rescue work to ensure security of the national network. The Ministry of Information and Communications is the standing body assisting the National Steering Committee for Emergency Response. It is to decide on the rescue options and assume the prime responsibility for, and direct the urgent rescue work to ensure the security of the national information network; to direct the Vietnam Computer Emergency Response Team (VNCERT) to receive, collect and process information and reports on cybersecurity incidents and propose rescue plans. The VNCERT shall remain the National Coordination Unit for Emergency Response and is part of the National Emergency Response Team together with the Authority of Information Security of the Ministry of Information and Communications; the Network Security Department, the High-Tech Police Department for Prevention and Combat against High-tech Crimes of the Ministry of Public Security; the Department of Information Technology, General Staff Department of the Ministry of Defense; as well as with a number of units specialized in responding to network security incidents of ministries, ministerial-level agencies, government-attached agencies, provincial-level People's Committees, telecommunications and Internet enterprises.

Besides the National Emergency Response Team, the emergency plan stresses the compulsory

5 According to Decree No. 85/2016/ND-CP dated July 1, 2016, of the Government on the security of information systems by classification, the classification of the country's information systems comprises 5 levels, of which level 4 and level 5 concern the most critical ones regarding Defense systems, security systems, e-government systems, information infrastructure systems and industrial control systems.

participation of a certain number of organizations to the National network information security rescue network, which comprises notably the Vietnam Internet Network Information Center (VNNIC), the Central Post Office, enterprises providing Internet and telecommunications infrastructure services; organizations and enterprises providing data center services and leasing of digital information storage space; organizations managing and operating national databases; and organizations and enterprises managing and operating important information systems and industrial control systems in the fields of energy, industry, health, natural resources and environment.

The "Emergency response plan to secure national network information security" appears to be very ambitious as it aims at endowing the country with a multidisciplinary incident response team, coordinated at national level and capable of mobilizing various relevant organizations, both in the public and the private sectors, and according to specific procedures and deployment schemes. It shall be noted that additional organizations may join the National network information security rescue network on a voluntary basis, providing they bring out relevant cybersecurity capabilities. It is worth mentioning that the Ministry of Information and Communications is also tasked "to act as the principal body or to designate a coordinating agency acting as the national focal point in coordination with functional units of other countries or international organizations in responding to and handling inter-country incidents". This point is quite important as cyber incidents are very often transnational by nature and require international cooperation and coordination.

3. Implementation and Work in Progress

Vietnam's cybersecurity roadmap implementation is currently based on three main pillars: the first pillar covers the area of institutional framework for cybersecurity, the second pillar concentrates on the legal architecture for cybersecurity and the third pillar focuses on the training and development of human resources specialized in cybersecurity.

3.1. Institutional Framework

Vietnam has embarked in recent years on the reorganization of its institutional framework for cybersecurity, which is reflected not only by the creation of new dedicated organizational units, but also by the search for better coordination of governmental agencies dealing with cybersecurity at national level. The three major governmental agencies in charge of cybersecurity in Vietnam are the Ministry of Information and Communications, the Ministry of Public Security and the Ministry of Defense.

The Ministry of Information and Communications has one dedicated authority, the Authority of Information Security (AIS), and two dedicated units, the Vietnam Computer Emergency Response Team (VNCERT) and the National Electronic Authentication Center (NEAC), which constitute its outpost for cybersecurity. The AIS, which was formally established following the Decision of the Ministry of Information and Communications No. 1281/QĐ-BTTTT of September 9, 2014, officially took office in October 2014. The main functions of the AIS are as follows[6]: "formulation of laws, regulations and policies relating to information security; implementation of technical and procedural measures; guiding and supporting governmental agencies and other organizations to enhance and protect their information systems; giving out early

6 Source: Ministry of Information and Communications.

warning regarding information security; ordinating activities on preventing SPAM in Vietnam; monitoring and inspecting the protection activities regarding information security; evaluating information security level in organizations and critical information infrastructures; raising awareness; improving capacity; cooperating with international organizations”. The Vietnam Computer Emergency Response Team (VNCERT), which was established under the Prime Minister's Decision No. 339/2005/QĐ-TTg of December 20, 2005, has had its functions, tasks and organizational structure redefined by the Decision No.1778/QĐ-BTTTT dated 26 October 2015. As an operational cybersecurity unit, although the VNCERT is primarily in charge of monitoring, warning, coordination and rescue, it has also been playing an active and leading role in the formulation of legal documents relating to cybersecurity, as well as regarding cooperation with foreign CERTs counterparts, promoting and coordinating incident response activities nationwide, or participating to the elaboration of technical standards. VNCERT is a multifaceted operational unit, whose role may be upgraded as its scope of intervention has gained prominence in recent years and as its perimeter of action has expanded. Like the VNCERT, the National Electronic Authentication Center (NEAC) is a specialized unit placed under the supervision of the Ministry of Information and Communications. Following Prime Minister's Decision No. 1592/QĐ-TTg of September 9, 2014, NEAC officially took office in December 2014. It is primarily contributing to the strengthening of the institutional architecture for electronic transactions, including authentication of digital signatures and electronic authentication by building and implementing a national Public Key Infrastructure (PKI) plan in Vietnam that will be the foundation for its National Electronic Authentication Framework (NEAF). The goal is to build a nationwide infrastructure for effectively securing electronic transactions and securing trust in e-commerce and e-government.

The Ministry of Public Security has three main entities dedicated to cybersecurity and information security: the Department of Network Security (referred to as “A68”) and the Department of Information Security and Communications (referred to as “A87”) which both depend on the General Department of Security of the Ministry of Public Security; and the Police Department for Prevention and Fight against High-tech Crime (referred to as “C50”) which is supervised by the General Department of Police. The Department of Network Security, which was officially established rather recently, i.e. after the announcement on August 28, 2014 by the Ministry of Public Security, oversees the management and administration of information systems security and cybersecurity. The Department of Information Security and Communications is focusing on contents control and management, including for instance illegal sale of personal data online. As for the Department for Prevention and Fight against High-tech Crime, it is specialized in the fight against cyber criminality, including for instance online fraud and financial crime.

The Ministry of Defense has two main entities focusing on cybersecurity, the Information Technology Department and the Government Cipher Committee. The Information Technology Department is placed under direct supervision of the Joint General Staff of the People's Army of Vietnam; it oversees IT and secure electronic information management. The Government Cipher Committee is a specialized unit placed under direct supervision of the Minister of Defense. It is responsible for State management of encryption communications and networks; strategy, policies and legal documents regarding encryption; as well as research, development, production, importation and use of encryption solutions and products.

While new institutional entities dedicated to cybersecurity are being created or reorganized, the need for better coordination between the various government agencies responsible for cybersecurity has also been taken into account. On this matter, we may note that the Ministry of Information and Communications introduced in 2014 a proposal related to the coordination of government action on the issue of cybersecurity. The idea was to provide for the modalities and scope of coordination of the action of the Ministry of Information and Communications, the Ministry of Public Security and the Ministry of Defense.

3.2. Legal Framework

Improving the legal framework for data protection, information security and the prevention and punishment of computer-related crime constitute the second pillar of Vietnam's cybersecurity roadmap. While the country's overall regulatory architecture for cybersecurity had long been insufficient, the Vietnamese government has been particularly active on that front in recent years. There has been an abundance of new and re-drafted regulations; several pieces of legislation have already been implemented while other regulations are in the making and being drafted.

Among the main recent texts that ought to have a major impact on the local context of cybersecurity, the Law on Network Information Security is undoubtedly a fundamental text. The Law No. 86/2015/QH13 on Network Information Security was passed on November 19, 2015 by the National Assembly and took effect on July 1, 2016[7]. It is the first dedicated law in Vietnam regarding cybersecurity. In essence, the Law on Network Information Security contains provisions, which address cybersecurity, information systems security, personal data security and contents security. It should be noted that this approach is part of a vision of the issue of cybersecurity from the perspective of information security, meaning that a political distinction is made between the notions of "information security" and "information systems security". For the Vietnamese regime, as for other states in the world, such as China and Russia, cybersecurity policy is inseparable from the concept of information security. It therefore refers to informational content of which information and communication technologies are the vectors and which are envisaged as a source of potential threat to political stability. The apprehension of the issue of cybersecurity thus goes far beyond the purely technological dimension. This policy approach is well reflected by Article 3 of the Law which introduces several definitions such as "network information security" being defined as "the protection of network information and information systems against any illegal access, use, disclosure, interruption, amendment or sabotage in order to ensure the integrity, confidentiality and availability of information". The Law on Network Information Security aims at being a foundational policy and regulatory document for the country's overall cybersecurity strategy. Key aspects of the Law include assurances for four building blocks, i.e. "network information protection", "protection of personal information", "information system protection" and "prevention of network information conflicts"; as well as regulatory frameworks for "civil cryptography", "standards and norms of network information security", "network information security business", "human resource development for network information security" and "state management of network information security".

Among the key new developments brought out by the Law, we may note visible efforts towards

7 English translation of the Law is available on the Ministry of Information and Communications Website: http://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf

the introduction of a unified law regulating data privacy, which was previously addressed within various laws and decrees including the Law on E-Transactions, the Law on Information Technology, the Law on Protection of Consumer Rights, Decree No. 52/2013/NĐ-CP on E-Commerce and Decree No. 72/2013/NĐ-CP on Management, Provision and Use of Internet Services and Online Information, or the Civil Code. Together with the Decree No. 85/2016 / ND-CP of July 1, 2016, on "Safety Information System by Level", which provides details regarding criteria, competence, order and procedures for determining security levels of information systems and for ensuring the security of information systems for each level, we may also note that the Law on Network Information Security recalls the current new existing framework of five distinct levels according to the potential damage and impact on production, public benefits, social order and safety, national defense and security. Additionally, the Law provides for a whole new set of regulatory frameworks regarding civil cryptographic products focusing on trading in civil encryption products, procedures to get business licenses for trading in civil cryptographic products and services, importation and exportation of civil cryptographic products, responsibilities of companies trading in civil cryptographic products and services, responsibility of organizations, individuals using civil cryptographic products and services. Furthermore, the Law details the regulatory framework regarding businesses providing network information security products and services including business license and permit procedures for trading in network information security products and services. Section 4 of the Law entitled "Prevention of Network Information Conflicts" is quite short, very broad and rather vague as compared to other sections of the document, especially as it is mentioned that the government will have to provide further details regarding "responsibilities of organizations and individuals in prevention of network information conflicts" as well as "prevention of network use for the purpose of terrorism". This section is nevertheless quite interesting as it aims at addressing other dimensions of cyberspace which relate more to strategic aspects of cybersecurity. This shows at least that the Vietnamese authorities are considering those aspects as well and that additional output may be expected.

The Law on Network Information Security appears to be a clear engagement towards codifying the regulations on cybersecurity, especially as previous regulations had been scattered throughout different pieces of more general legislation. As it appears throughout the document, additional documents and regulatory inputs are in the making in order to further clarify the scope, applicability and responsibility regarding several aspects of the Law. Apart from the Law on Network Information Security, several regulatory measures have been introduced in recent years, in particular Decree No. 25/2014/NĐ-CP of April 7, 2014, on the "Provisions on preventing and combatting crimes and other violations of the law which use high-tech". The decree provides in particular a whole set of measures applicable in the event of the detection of a high-tech crime and specifically intended for research and investigation. It has to be put in perspective with the ongoing process of reviewing the country's new Penal Code, which was initially scheduled to come into force on July 1, 2016[8], and which shall include criminal penalties for violations relating to cybersecurity and for cybercrime acts. In addition to these specific regulations, it shall be reminded that Vietnam has been continuously working on improving the security of electronic transactions and is conducting further efforts regarding electronic payments and card-based payments.

8 The National Assembly has issued a resolution to delay the implementation of the revised Penal Code.

3.3. Human Resources Development

The third main pillar, which underpins the Vietnamese government's roadmap on digital information security by 2020, focuses on the training and development of human resources specialized in cybersecurity. The Prime Minister's decision No. 99/QĐ-TTg of January,14, 2014, ratifying the plan "Training and development of human resources for information security to 2020", also called "Project 99", constitutes the cornerstone of the Vietnamese government's strategy in this area. By 2020, Vietnam has set out the following objectives: training of 2000 graduates at bachelor's and higher levels; sending 300 teachers and researchers for training abroad, including 100 people at Ph.D. level; sending 1500 cybersecurity personnel for short-term training abroad; organization of short-term cybersecurity training for 10,000 cybersecurity officers in public institutions. It also involves the ongoing training of 2,000 cybersecurity personnel in government agencies of strategic importance. To ensure the training of cybersecurity specialists, Vietnam has decided to encourage the opening of ad hoc specialties in the universities of the country, which is accompanied by a policy of encouragement and incentives for the development of enrollment of students in courses offering specializations in information and communication technologies and cybersecurity. The emphasis is also placed on monitoring the quality of the training provided, in the context of a desire to upgrade the curriculum. Some of the leading institutions in this area include FPT private university (FPT University), which is part of the Vietnamese ICT firm FPT, and the Posts and Telecommunications Institute of Technology (PTIT), which is supervised by the Ministry of Information and Communications. Several Vietnamese universities had previously initiated computer security training courses, but they did not offer full dedicated degree courses, and rather combined them with courses in computer science and information systems. It is expected that no fewer than eight key institutions will integrate "Project 99" to train cybersecurity specialists through dedicated curricula.

Additionally, it is worth mentioning that the Vietnamese authorities have engaged in upgrading the general awareness of the Vietnamese population regarding cybersecurity. The Prime Minister's Decision No. 893/QĐ-TTg of June 19, 2015, on "Approving the project on communication, discipline, awareness and responsibility for information security to 2020" highlights the various means by which the country is expected to raise general cybersecurity awareness, with a particular emphasis on the youth, encompassing for instance educational materials on information security to be integrated into informatics and extracurricular activities from junior to senior high school; information security contests to be organized for different target groups of students of universities, colleges, professional secondary schools; as well as the mobilization of traditional and online media on covering the topic of cybersecurity and developing and broadcasting dedicated awareness programs. This initiative is quite interesting and particularly welcome as it reflects the crucial necessity to raise the Vietnamese population cybersecurity awareness and knowledge level[9]. So far, the objectives of the new cybersecurity awareness roadmap to 2020 appear to be quite ambitious and include notably the following: less than 50% of information security incidents occur because of poor awareness of cybersecurity risks; more than 80% of civil servants, officials and officials of state agencies and organizations are educated about basic habits, responsibilities and skills to ensure information security when using information technology; more than 80% of officials and employees of enterprises

9 According to the ESET Vietnam Cyber-Savviness Report 2015, "When compared with other Asia-Pacific markets, Vietnam comes in last in terms of cyber-savviness behind Malaysia, Singapore, India, Thailand, Hong Kong and Indonesia, in that order."

providing telecommunication and information technology services are educated about cybersecurity risks and procedures for rescue coordinating and troubleshooting; over 50% of users in general, over 60% of high school students and over 70% of university students are educated about the basic risks and skills relating to cybersecurity.

4. Conclusion

As Vietnam has embarked upon the daunting task of revamping and upgrading its cybersecurity policy and strategy with a clear and tangible acceleration in recent years, especially since the last four years, it is facing a challenging work as far as implementation is concerned. As a matter of fact, while strategy and planning documents provide for guidelines and broad outlines, the decisive part of the work concerns the operationalization of the policy framework. In reality, a well-designed policy does not automatically imply successful implementation. This is even more critical when it comes to cybersecurity.

There is no doubt that Vietnam has made positive progress in addressing the issue of cybersecurity by working out the conception of a national cybersecurity governance framework throughout several policy and legal documents. The key determinant of success will rest upon effective coordination of all stakeholders, further clarification on legal aspects and continuous evaluation and assessment of cybersecurity policies. It is worth mentioning that the Vietnamese government tends to have a much more proactive position towards the role of the private sector in the field of cybersecurity and that closer and better coordination with private companies, especially those involved in the ICT and digital sectors, has been emphasized in most recent policy documents. Furthermore, economic and business aspects of cybersecurity are well taken into account as it is shown by support to R&D&I and expansion of the domestic information security market. Regarding legal aspects, the Law on Network Information Security would need further details and sub-legislation guidelines, especially regarding more precise scope of applicability as well as more precise compliance requirements. The issue of civil cryptographic products is bound to pose some challenges for businesses but also for individuals, therefore clear compliance and application requirements ought to be further defined, so as to keep balance between security and privacy. More generally speaking, how new cybersecurity and information security rules may be interpreted or enforced require further developments. As to operationalization of cybersecurity policies, it shall be implemented in a dynamic way that reflects the evolution of the cyber threats landscape. As future cyber risks and threats are evolving, there is a need on the part of policy-makers to focus on regulatory and administrative flexibility together with the design of a set of relevant standards, whether technical or non-technical.

As mentioned before, one very welcome and positive initiative is the Prime Minister's Decision on "Approving the project on communication, discipline, awareness and responsibility for information security to 2020", which shows that cybersecurity-related education and training has become a priority for the Vietnamese government. As far as cybersecurity is concerned, the technology side is indeed only one part of the equation, the human side remains of utmost importance. In any new endeavor, and especially regarding cybersecurity, resistance to change remains a fundamental human characteristic, which may act as a hindrance towards enhancing awareness and responsibility. Beyond cybersecurity awareness, there is also a need for cybersecurity literacy, i.e. an actual and practical understanding of cybersecurity and a culture of information security that becomes part of an organization mindset, whether public or private. Simply put, ICT&D and cybersecurity shall no longer be apprehended as distinct issues.

In the case of Vietnam, the challenge is also that of a developing country, which must combine the promotion of ICT and the development of its digital economy with the security of information systems and the structuring of a cybersecurity policy and strategy, while composing with a lower investment capacity than that of more industrialized countries in this domain and other competing priorities. Vietnam has therefore very clearly chosen an active policy of international cooperation, not only with other countries in the Asia-Pacific region but also with countries in other regions of the world. In this respect, it may be noted that most of the policy and legal documents relating to cybersecurity include a section dedicated to international cooperation. Whether bilateral or multilateral cooperation, Vietnam has been engaged for several years in a collaborative approach to the issue of cybersecurity. There is a clear opportunity for Vietnam to benefit from the experience and expertise of the most advanced countries in this field so as to take advantage of best practices and avoid many pitfalls.

What could be described as a cybersecurity "new deal" in Vietnam has been clearly nurtured by notorious cyber incidents in recent years in the country, which undoubtedly acted as wake-up calls. Additionally, it should be more generally understood as a political will to preserve and consolidate the development potential of the ICT&D sector in the country, the objectives being that "information and communication technologies serve as an important driving force, helping to ensure the country's growth and sustainable development"[10] and that they act as "an important driving force for stimulating the development of the knowledge-based economy and for improving national competitiveness in the process of international integration"[11].

References

Daily Botnet Statistics (2017), Botnet Statistics for the year of 2016. Retrieved from <http://botnet-tracker.blogspot.fr/2017/01/botnet-statistics-for-year-of-2016.html>

ESET (2015), Vietnam Cyber-Savviness Report 2015: Cybersecurity, User Knowledge, Behaviour and Attitudes in Vietnam. Retrieved from <https://static1.esetstatic.com/fileadmin/Images/INT/Press/2015/2015-12-22/ESET_Vietnam_Cyber_Savviness_Report_Dec_2015.pdf>

Microsoft (2016), Microsoft Security Intelligence Report (SIR), Volume 21 | January through June 2016. Retrieved from <https://www.microsoft.com/security/sir/default.aspx>

Ministry of Information and Communications (2014). Vietnam ICT White Book 2014, Information and Communications Publishing House.

Project Honey Pot (2017), Project Statistics. Retrieved from <https://www.projecthoneypot.org/statistics.php>

Tran Dai C. (2014). La cybersécurité : talon d'Achille du Vietnam dans le domaine des TIC, Les Grands Dossiers de Diplomatie n° 23, Géopolitique du cyberespace, enjeux mondiaux, pp.54-57.

Tran Dai C. (2015). La cybersécurité au Vietnam : formulation et mise en œuvre d'une nouvelle stratégie, Hérodote n°157, Les enjeux géopolitiques du Viêt Nam, pp. 126-140.

Vietnam Internet Network Information Center (2014). Report on Vietnam Internet Resources 2014, Vietnam Internet Network Information Center.

We are social (2017), Digital in 2017: Southeast Asia. Retrieved from <https://wearesocial.com /blog/2017/ 02/ digital-southeast-asia-2017>

10 Decision of the Prime Minister No. 1755/QD-TTg of September 22, 2010, on the "Plan to make Vietnam a country strong in information and communication technologies".

11 Resolution No. 36-NQ / TW dated July 1st, 2014 of the Politburo on the "Application and development of IT and communications to 2030".