Technological Development and Innovation Strategy for Information Security: A Country-Level Analysis

Chun-Yao Tseng[a] and Da Chang Pai [b]

[a] Professor and Chairman, Department of Business Administration, Tunghai University.

e-mail: cytseng@thu.edu.tw, topas1203@gmail.com

[b] Associate Professor, Department of Business Administration, Chungchou Institute of Technology bigwhite0424@yahoo.com.tw

Abstract

The successful management of information security is vital for an organization to keep its survival and establish its competitive advantage. The multidisciplinary nature of information security includes information security policy, access control, monitoring or scanning of software or data, prevention of unauthorized use or data and protection of hardware. Based on patent and citation data from USPTO during 1976-2007, this study investigates four main related to technological development and innovation strategy for information security at a country-level analysis. First, aggregate technological development of information security is examined to compare technological innovation capability of different countries. Secondly, this study demonstrates six sub-technological development of information security, and absolute and relative innovation strengths of different countries in six sub-technological fields are compared. Thirdly, this study investigates knowledge flow of information security technology and manifests knowledge diffusion among different countries. Finally, innovation strategies of information security are demonstrated by a country-level analysis.

Introduction

The successful management of information security is vital for an organization to keep its survival and establish its competitive advantage. Information security can make a positive contribution by helping a business comply with laws, regulations and guidance on governance and on e-commerce by adding value (Sundt, 2006). Information security is a multidisciplinary concept, most of the times cutting horizontally across an organization. This multidisciplinary nature of information security includes personnel security, user access control, network security and regulatory aspects (Eloff and Eloff, 2005). Kim and Leem(2004) try to develop strategy plans for information security by providing a methodology framework, process model and essential tools. Although some studies focus on technical issues of information security,

study related to technological development and innovation strategy for information security based on a country-level analysis is not found.

The most common measures for technological innovation can be categorized as measures of R&D, patents and new products. This study employs patents as a major measure to elucidate technological innovation (Ernst, 2001; Tseng, 2009) for the following three reasons. First, patent data are accurately recorded, readily accessible, quantifiable and easily manipulated for more detailed analysis by technological field, product or patent holder. Second, analysis of patent grants within a single country provides an objective and consistent measure of technological innovation since patents are examined and eventually granted by a single national patent office. Finally, in comparison with other sources, patents are often the only timely measure of rapid technological change, particularly in the context of global competition.

Technological innovation depends on the knowledge linkages of an entity with other entities (Almeida and Phene, 2004). Knowledge diffusion can be beneficial to technological innovation, because the entity can take advantage of both internal and external knowledge to strengthen its innovational capability. That is, the creation and absorption of knowledge are important parts of innovation capability. Because the spillovers arising from technological innovation can cross national boundaries, the effect of innovation on national comparative advantage depends on the geographic scope of its diffusion (MacGarvie, 2005). Therefore, technological innovate capability can be enhanced by merging their own knowledge with acquired knowledge. Due to the importance of interactions between different national innovation systems, understanding knowledge flow is necessary for increasing innovation capability of information security.

Innovation is far more important than land, physical capital, or labor in a knowledge-based economy and the primary factor affecting differential economic growth and development in nations. Effective innovation management is thus a key to corporate success, technological prowess and economic development (Quinn, 1996). Innovation strategy determines to what degree and in what way an entity attempts to use innovation to execute its strategy and improve its performance. Innovations strategy can be characterized in a variety of ways(Gilbert, 1994; Tseng, 2008; Tseng, 2009): fundamental/applied innovation, incremental/radical innovation, internal/external innovation, imitative/inventive innovation and etc. Investigating innovation strategies of information security among different countries is helpful to understand different technlogical development of information security.

This study investigates four main issues related to technological development and innovation strategy for information security. First, aggregate technological development of information security is examined to compare technological innovation capability of different countries. Secondly, this study demonstrates sub-technological development of information security, and relative innovation strengths of different countries in sub-technological fields of

information security are compared. Thirdly, this study investigates knowledge flow of information security technology and manifests knowledge diffusion among different countries. Finally, innovation strategies of information security are compared by analysis of country-level.

Aggregate Technological Development of Information Security in the World

Many studies typically examined patent count as a measure of technological innovation. Patents granted are assigned a higher value than mere patent applications because patents are only granted when they contain technological innovations which exceed a certain level of newness (Sherry and Teece, 2004). This study selected patents granted form USA (United States Patent and Trademark Office; USPTO) as most reliable proxy of measuring technological innovation. USPTO provides full text for patents issued from 1976 to the present, so research period is restricted from 1976 to 2007. Each patent application is assigned by patent examiners to one main technology code and one (or more) secondary technology codes, based upon the US Patent Classification (UPC). Information Security is classified by U.S. patents subclasses for class 726. This class provides, within a computer or digital data processing system, for processes or apparatus for increasing a system s extension of protection of system hardware, software, or data from maliciously caused destruction, unauthorized modification, or unauthorized disclosure (USPTO, 2007).

Based on USPTO database, the whole world had a low level of patent count in information security before the 1996 year, and it had increased incrementally over time after the 2003 year, peaking in 2007 year. Patent count in information security indices over 1976-2007 totaled 4,133. Patent count of information security during 2007 was nearly fourteen times that of information security during 1997. Aggregate technological innovation of Information security has made great progress year by year. Table 1 displays the comparison of patents in information security technology among different countries from 1976 to 2007. USA, Japan, Canada, France, Germany, United Kingdom, Israel, South Korea, Finland and Holland are top 10 countries in patent analysis of information security technology. USA is the No. 1 information security technology patentee (2,970), taking more than 71 of total patents in the USPTO. Japan has the second highest patents in the world, and accounts for 13.81% of total patents. Canada takes only 1.91% listing as the third in the world. Every country have a markedly growth tendency during 2002-2007. Finland owns the ninth highest patents, but it has the highest growth rate in patents of information security technology. Table 1 indicates the divergent technological development of information security in different country.

Table 1 Comparison of patents in information security technology from 1976 to 2007

Country	1976-2007		1976-1995		1996-2001		2002-2007	
	Patents	Percent	Patents	Percent	Patents	Percent	Patents	Percent
USA	2970	71.09%	111	68.52%	772	73.66%	2087	70.32%
Japan	577	13.81%	21	12.96%	134	12.79%	422	14.22%

Canada	80	1.91%	2	1.23%	20	1.91%	58	1.95%
France	64	1.53%	3	1.85%	16	1.53%	45	1.52%
Germany	64	1.53%	4	2.47%	10	0.95%	50	1.68%
United Kingdom	45	1.08%	6	3.70%	15	1.43%	24	0.81%
Israel	44	1.05%	0	0.00%	15	1.43%	29	0.98%
South Korea	44	1.05%	1	0.62%	18	1.72%	25	0.84%
Finland	43	1.03%	0	0.00%	2	0.19%	41	1.38%
Holland	33	0.79%	1	0.62%	3	0.29%	29	0.98%
Other country	214	5.12%	13	8.02%	43	4.10%	158	5.32%
Total	4178	100.00%	162	100.00%	1048	100.00%	2968	100.00%

Note: A patent possibly belongs to assignee countries of two and upward.

Sub-technological development of information security among Different Countries

USPTO divided information security class into five subclasses, including *information security policy*, *access control*, *monitoring or scanning of software or data*, *prevention of unauthorized use or data* and *protection of hardware* (USPTO, 2007). Furthermore, access control subclass is partitioned off into two subclasses, comprising *access control-network* and *access control-standalone*. Finally, this study adopts this classification and assigns patents of any of six sub-technological fields of information security, as follows

Information Security Policy

This sub-technological field includes systems, methods, and apparatus that provide for the administration and management of rules or regulations governing the protection of information, services and other data processing resources involving coordination of more than one security mechanisms among a plurality of entities, resources, or processes.

Access Control- Network

This sub-technological field comprises systems, methods, and apparatus for the prevention of unauthorized access to resources of a system or information system, including the manner of identifying and verifying the entity, process, or mechanism requesting access to the resource. These means of limiting access to the resources of a system are based on a network level.

Access Control- Standalone

Subject matter wherein the access control or authentication includes the means of limiting access to the resources of a system based on a single computer or end user level.

Monitoring or Scanning of Software or Data

This sub-technological field includes systems, methods, and apparatus for ensuring data integrity by scanning of software or data or otherwise monitoring data to prevent or detect attacks.

Prevention of Unauthorized Use or Data

Systems, methods, and apparatus for prohibiting any impersonation, unauthorized browsing, falsification or theft of data, or alteration of data not consistent with defined security policy are included in this sub-technological field.

Protection of Hardware

Subject matter comprises systems, methods, and apparatus for prohibiting any impersonation, unauthorized browsing, falsification or theft of data, or alteration of data not consistent with defined security policy.

Figure 1 illustrates the comparison of six sub-technological fields of information security during 1976-2007. Patent count of *Access control-network* indices over 1976-2007 totaled 2,843 and it is the largest sub-technology in six sub-technological fieldS. *Prevention of Unauthorized Use or Data* has the second highest patent count (1,259). *Access control-standalone* is the third (882) and *monitoring or scanning of software or data* is the fourth (833). Six sub-technological fields of information security have a low level of patent count before the 1997 year. Patent count of *Access control-network* has increased incrementally over time after 2003, peaking in 2007 year. Patent count of *Prevention of Unauthorized Use or Data* is less than that of *Access control-standalone* before 1997, but the former patents were more two times the latter patents in 2007 year. That is, annually growth rates of patents in both *Access control-network* and *Prevention of Unauthorized Use or Data* are more than other four sub-technological fields of information security. Both *information security policy* and *protection of hardware* have a low level of patent count during 1976-2007.

Figure 1 Comparison of six sub-technological fields of information security

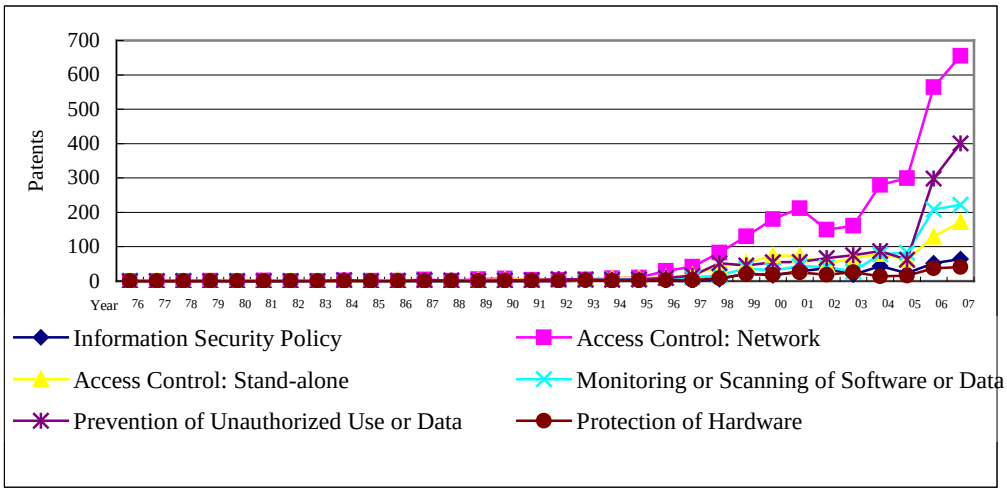


Table 2 presents innovation strengths of top 10 countries in six sub-technological fields of information security. Analysis of innovation strength included absolute innovation strength and relative innovation strength. Absolute innovation strength is measured by number of

patents in a specific technological field. Relative innovation strength is measured by number of patents in a specific technological field relative to all patents in a country. USA possesses absolute innovation strengths in every sub-technological fields of information security, and Japan is the next. USA, Canada, France and Finland have all relative innovation strength in *access control-network*. *Access control-network* and *Prevention of Unauthorized Use or Data* are top two technological fields of relative innovation strengths in Japan and Germany. United Kingdom and Holland own relative innovation strengths in fields of *Prevention of Unauthorized Use or Data* and *access control-network*. *Monitoring or Scanning of Software or Data* and *Access control-network* are top two sub-technological fields of relative innovation strengths in Israel. South Korea holds relative innovation strengths in fields of *access control-standalone* and *access control-network*.

Knowledge Diffusion of Information Security Technology among Different Countries

To understand knowledge diffusion of information security technology is necessary to investigate knowledge flow among different countries. Jaffe et al.(1993) pioneered the use of patent citations data to trace the flow of knowledge. They argued that these linkages represent a trace of

Table 2 Absolute and relative innovation strengths of top 10 countries in six sub-technological fields

	Information Security Policy	Access Control: Network	Access Control: Stand-alone	Monitoring or Scanning of Software or Data	Prevention of Unauthorized Use or Data	Protection of Hardware	Total
USA	271 (5.68%)	2208 (46.32%)	590 (12.38%)	701 (14.71%)	838 (17.58%)	159 (3.34%)	4767 (100%)
Japan	28 (3.34%)	327 (39.02%)	141 (16.83%)	44 (5.25%)	274 (32.70%)	24 (2.86%)	838 (100%)
Canada	5 (3.79%)	73 (55.30%)	24 (18.18%)	9 (6.82%)	15 (11.36%)	6 (4.55%)	132 (100%)
France	2 (2.04%)	39 (39.80%)	20 (20.41%)	11 (11.22%)	19 (19.39%)	7 (7.14%)	98 (100%)
Germany	4 (4.35%)	32 (34.78%)	13 (14.13%)	5 (5.43%)	29 (31.52%)	9 (9.78%)	92 (100%)
United Kingdom	1 (1.61%)	18 (29.03%)	16 (25.81%)	5 (8.06%)	21 (33.87%)	1 (1.61%)	62 (100%)
Israel	4 (6.56%)	18 (29.51%)	3 (4.92%)	19 (31.15%)	14 (22.95%)	3 (4.92%)	61 (100%)
South Korea	1 (1.64%)	20 (32.79%)	20 (32.79%)	3 (4.92%)	11 (18.03%)	6 (9.84)	61 (100%)
Finland	1 (1.37%)	36 (49.32%)	11 (15.07%)	14 (19.18%)	10 (13.70%)	1 (1.37%)	73 (100%)
Holland	1 (2.38%)	14 (33.33%)	7 (16.67%)	1 (2.38%)	16 (37.10%)	3 (7.14%)	42 (100%)

knowledge flows since the applicant refers to a piece of previously existing knowledge and its patent builds upon the cited ones. Follow-up studies have adopted this approach of using patent citation to investigate knowledge flow and spillover(Jaffe and Trajtenberg, 1999; Hu & Jaffe, 2003). Consequently, this study uses patent citation data as a proxy for knowledge flow.

Table 3 displays knowledge flow of information security technology among top 10 countries. There are huge knowledge flows among 10 countries. USA is a major knowledge creator in information security technology in the world. Main knowledge sources of other nine countries are the same from USA. On the other hand, Information security technologies of USA also cited patents of other nine countries. That is, ten countries simultaneously play the roles of knowledge creators and knowledge acceptors. If knowledge outflows are greater than knowledge inflows, it implies countries play the role as knowledge creators more than knowledge acceptors, including USA, Canada, France, United Kingdom and Israel. Japan, Germany, South Korea, Finland and Holland play the role as knowledge creators less than knowledge acceptors.

Table 3 Knowledge flow of information security technologies among transnational regions

Knowledge Inflow / Knowledge outflow	USA	Japan	Canada	France	Germany	United Kingdom	Finland	Israel	South Korea	Holland	Total
USA	—	2164	415	197	311	151	179	330	158	119	4024
Japan	1345	—	12	19	14	20	11	14	45	10	1490
Canada	523	47	—	4	4	4	2	5	5	1	595
France	257	26	7	—	11	18	2	3	3	6	333
Germany	213	19	1	7	—	3	1	1	1	1	247
United Kingdom	299	42	3	3	7	—	5	3	4	8	374
Finland	64	2	4	0	0	0	—	0	3	2	75
Israel	471	42	8	8	6	1	4	—	0	3	543
South Korea	75	56	0	3	2	0	1	9	—	1	147
Holland	42	11	2	3	1	0	0	0	1	—	60
Total	3289	2409	452	244	356	197	205	365	220	151	7888

Comparing Innovation Strategies of Information Security among Different Countries

The following two methods have been employed to examine differences in innovation strategies of information security among different countries.

Fundamental vs Applied Innovation

Distinguishing fundamental and applied innovation is vital. Technology invention is often termed fundamental innovation, and technology adoption is termed applied innovation (Rao et al., 2001*)*. This study employed an index of Science Linkage measure to distinguish between fundamental and applied innovation. Science Linkage indicates the extent to which innovation builds upon cutting-edge scientific research. Science Linkage is calculated based on the average number of citations that a country's patents cite scientific journal papers and

conferences (Bierly and Chakrabarti, 1996). Countries whose patents cite many scientific papers are assumed to be partial to fundamental innovation. Conversely, countries with lower scientific linkage ratios are assumed to focus more on applied innovation.

The left side of Table 4 provides summary of science linkage for 10 countries. Science linkages of Israel (8.7045) and USA (6.6855) are higher than those of other countries in information security technologies. Restated, Israel and USA are partial to fundamental innovation. Comparatively, South Korea, France and Japan have relatively lower science linkage ratios and are assumed to be focused more on applied innovation.

Table 4 Comparison of science linkage and self-citing ratio among top 10 countries

Country	Patent Count	Citing Scientific Journal papers and conferences		Citing its own patents	
		Total citations	*Science Linkage*	Total citations	*Self-citing ratio*
USA	2970	19856	6.6855	26679	8.98283
Japan	577	796	1.3795	663	1.14905
Canada	80	177	2.2125	35	0.43750
France	64	78	1.2188	22	0.34375
Germany	64	117	1.8281	14	0.21875
United Kingdom	45	68	1.5111	2	0.04444
Israel	44	383	8.7045	19	0.43182
South Korea	44	27	0.6136	14	0.31818
Finland	43	102	2.3721	2	0.04651
Holland	33	77	2.3333	3	0.09091

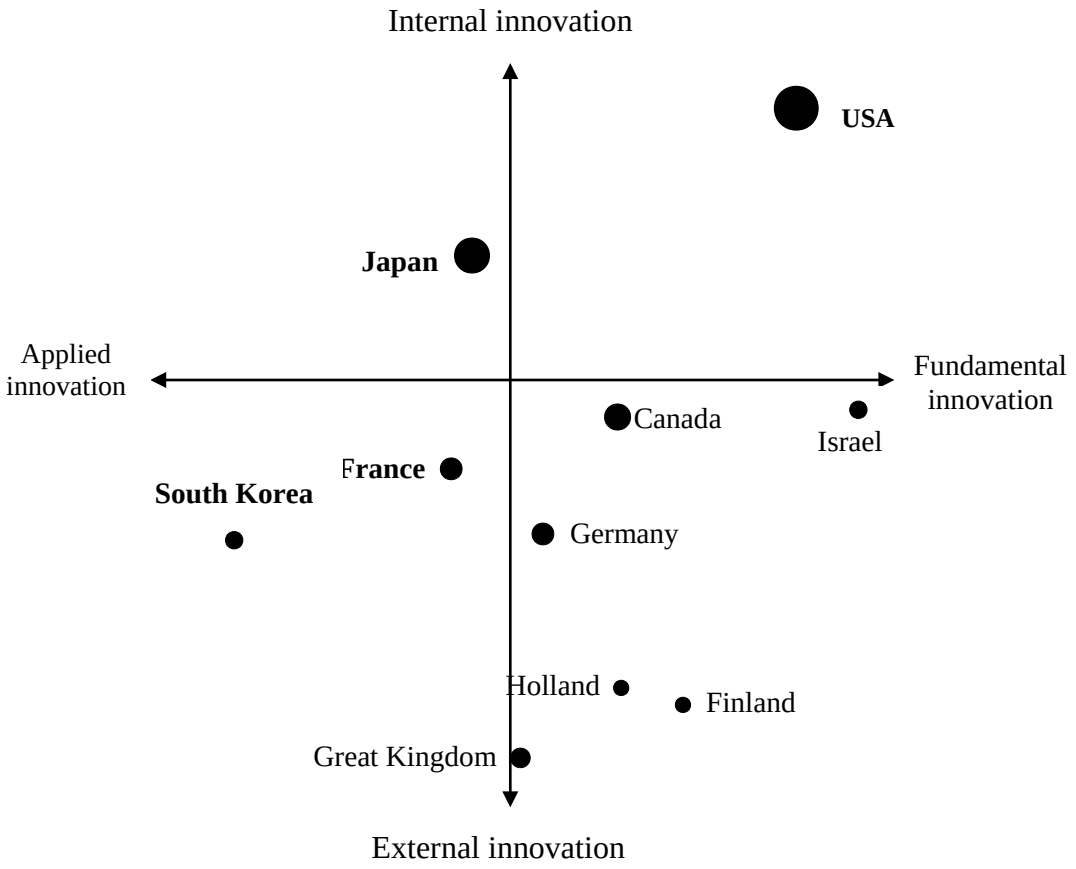
Internal vs External Innovation

The organisation of innovation along the internal versus external sourcing dimension remains a complex issue (Veugelers and Cassiman, 1999). Internal innovation contributes to a firm's economic value-added more than the effects of external innovation (Tseng, 2008), but Hasan (2002) has asserted that less developed countries cannot rely on their internal innovation to increase performance. To enhance technological performance, countries need to external innovation form foreign countries. This study employs a self-citing ratio to distinguish between internal and external innovation. Self-citing ratio is measured by the percentage of citations given by a country citing its own previous patents. A country exhibiting a higher self-citing ratio is presumed to favor internal innovation whereas a country with lower self-citing ratio is assumed to be undergoing external innovation. The right side of Table 4 compares self-citing ratios of information security technologies among 10 countries. USA and Japan tend to favor internal innovation. Conversely, United Kingdom, Finland, Holland, Germany and South Korea tend to engage in external innovation.

Based on data consisting of science linkage and self-citing ratio, through standardization process, comparison of innovation strategies among 10 countries are shown in Figure 2. Obvious differences in innovation strategies are apparent in the 10 countries. USA appears to

be highly focusing on fundamental innovation and internal innovation. Japan is working closely with internal innovation. Israel tends fundamental innovation. United Kingdom favors external innovation. South Korea exhibited a tendency to focus on applied innovation and external innovation.

Figure 2 Innovation strategies of information security in 10 countries



Note: The size of each circle is proportional to patent counts by each country.

Conclusions

Based on patent and citation analysis from USPTO data, this study examined four main issues related to technological development and innovation strategy for information security in different countries from 1976 to 2007. Four empirical findings were shown as follows:

(1) Patents of information security had increased incrementally over time after the 2003 year, peaking in 2007 year. USA owns the most patents of information security and takes more than 71% of total patents in the world. Japan is the next in patents of information security.

(2) Patent count of *Access control-network* is the largest sub-technology in six sub-technological fields of information security. *Prevention of Unauthorized Use or Data* has the second highest patent count. USA possesses absolute innovation strengths in six

sub-technological fields of information security, but differences are apparent in six technological fields of relative innovation strengths among different countries.

(3) Main knowledge sources of other nine countries are the same from USA. There are high inter-relationships among top 10 countries in information security technologies. They simultaneously play the roles of knowledge creators and knowledge acceptors, but relative importance of both roles is different in every country.

(4) USA appears to be highly focusing on fundamental innovation and internal innovation. South Korea exhibited a tendency to focus on applied innovation and external innovation. Japan is working closely with internal innovation. Israel tends fundamental innovation. United Kingdom favors external innovation.

This study has four economical implications. First, Major countries place more importance on technological innovation of information security year after year and information security technology is expected to become a larger force in the world economy. Secondly, analyzing absolute and relative innovation strengths in different sub-technological fields would enhance understanding technological development of information security in different counties. Thirdly, knowledge diffusion serves as an effective linkage and catalyst in enhancing national innovation capability in information security. Tracing knowledge flow is helpful to understand the process of technological development of information security. Finally, obvious differences in innovation strategies of information security are shown in different countries.

References

Almeida, P. & Phene, A. 2004. Subsidiaries and Knowledge Creation: the Influence of the MNC and Host Country on Innovation. *Strategic Management Journal*, 25(8/9): 847-865.

Bierly, P. & Chakrabarti, A. 1996. Generic knowledge strategies in the U.S pharmaceutical industry. *Strategic Management Journal*, 17: 123-135.

Eloff, J.H.P. & Eloff, M.M. 2005. Information Security Architecture. *Computer Fraud & Security*, 11: 10-16.

Ernst, H. 2001. Patent applications and subsequent changes of performance: evidence from time-series cross-section analyses on the firm level. *Research Policy*, 30: 143-157.

Gilbert, J.T. 1994. Choosing an innovation strategy: theory and practice. *Business Horizons*, 37(6): 16-22.

Hu, G. Z. & Jaffe, A. 2003. Patent citations and international knowledge flow : the cases of Korea and Taiwan. *International Journal of Industrial Organization*, 21: 849–880.

Jaffe, A. & Trajtenberg, M. 1999. International knowledge flows: evidence from patent citations. *Economics of Innovation & New Technology*, 8: 105-136.

Jaffe, A., Trajtenberg, M. & Henderson, R. 1993. Geographic localization of knowledge spillovers as evidenced by patent citations. *Quarterly Journal of Economic*, 108: 577-598.

Kim, S. & Leem, C.S. 2004. An Information Engineering Methodology for the Security Strategy Planning. *Lecture Notes in Computer Science*, 3043: 597-607.

MacGarvie, M. 2005. The determinants of international knowledge diffusion as measured by patent citations. *Economic letters*, 87: 121–126.

Quinn, J. B., Anderson, P. and Finkelstein, S. 1996. Leveraging Intellect. *Academy of Management Executive*, 10: 7-27.

Rao, S., Ahmad, A., Horsman, W. & Kaptein-Russell, P. 2001. The Importance of Innovation for Productivity. *International Productivity Monitor*, 2: 11-18.

Sherry, E. F. & Teece, D. J. 2004. Royalties, evolving patent rights, and the value of innovation. *Research Policy*, 33: 179-191.

Sundt, C. 2006. Information security and the law. *Information Security Technical Report*, 11(1): 2-9.

Tseng, C. 2008. Internal R&D effort, external imported technology and economic value added: empirical study of Taiwan's electronic industry. *Applied Economics*, 40(8): 1073-1082.

Tseng, C. 2009. Technological Innovation in BRIC Economies: a Comparative Study Based on Patent Citation Data. *Research-Technology Management*, 52(2): 29-35.

USPTO. 2007. *Class Schedule for Class 726 Information Security*. United States Patent and Trademark Office.

Veugelers, R. & Cassiman, B. 1999. Make and buy in innovation strategies: evidence from Belgian manufacturing firms. *Research Policy*, 28: 63–80.