A Different Look at Sticky and Leaky Knowledge: Economic and Industrial Espionage

Jason Ferdinand
The University of Liverpool

and

David Simm
Lancaster University

Paper proposed for the International Conference on Organizational Learning, Knowledge and Capabilities, 20-22nd March, 2006, Warwick, UK.

Stream: Inter-organizational learning and learning across boundaries

A Different Look at Sticky and Leaky Knowledge: Economic and Industrial Espionage

Abstract

The primary objective of this paper is to advance our understanding of inter-organizational learning; in particular, of the concepts of 'sticky' and 'leaky' knowledge. By drawing upon data from, hitherto, a largely unexplored area of management and organization studies, that of economic and industrial espionage, we attempt to demonstrate that contemporary debates could benefit considerably from an exploration of such illegal forms of learning. Three vignettes involving economic and industrial espionage are presented to demonstrate the limitations of both our current conceptualisations of inter-organizational learning and what motivates people to illegally acquire knowledge across organizational boundaries. In direct challenge to the dominant 'black-box' view of organizations presupposed by the sticky and leaky knowledge debate thees vignettes present powerful evidence of external forces encouraging the forced leakage of knowledge. Resultantly our understanding of what constitutes sticky and leaky knowledge has to be adapted. Finally, we conclude with a discussion of the implications for future research

Introduction

In recent years learning across organizational boundaries has received increasing attention. Arguably built upon studies exploring inter-organizational relations in economics (Williamson, 1975), law (Macaulay, 1963) and strategy (Gulati, 1998; Reid et al, 2001), various forms of collaborative inter-organizational activities have been presented as being organizationally beneficial. This orientation can be identified as drawing heavily upon leading proponents of the value of knowledge in contemporary societies (Davenport and Prusak, 2000; Nonaka and Teece, 2001). From studies examining how institutional structures influence inter-organizational relations (Greewood et al 2002; Oliver, 1997), to attempts to improve supply chain efficiencies (Boddy et al, 2000; Harland, 1996), the potential benefits can be summarised in the following three ways. Firstly, inter-organizational collaboration might secure access to complementary assets needed to turn innovations into commercial successes (Hagedoorn, 1993; Teece, 1986). Secondly, inter-organizational

collaboration may allow organizations to spread the substantial cost of research and development (R&D) between collaborators (Hagedoorn, 2002; Veugelers, 1998). Finally, the transfer of codified and tacit knowledge (Ahuja, 2000; Doz and Hamel, 1997; Eisenhardt and Schoonhoven, 1996; Lambe and Spekman, 1997) could be facilitated by such alliances.

In essence, organizational learning is facilitated by inter-organizational collaboration (Dodgson, 1996; Inkpen and Crossan, 1995; Kogut, 1988; Levinson and Asahi, 1995; Lyles, 1988). In some cases, researchers discuss such learning in terms of knowledge sharing and transfer (Dyer and Nobeoka, 2000; Grant and Baden-Fuller, 1995; Kale et al., 2000; Mowery et al., 1996), where, for example, a focal organization learns from a strategic alliance partner (Lei and Slocum, 1992). In others, authors emphasise that through collaboration new knowledge, of which neither collaborating partner was previously aware, can be created (e.g., Gulati, 1999; Mowery et al., 1996; Powel et al, 1996).

In such organizational alliances, the crucial issue to be addressed is the management of learning across boundaries where the concepts of ‘sticky’ and ‘leaky’ knowledge (Brown & Duguid, 2001) are viewed as fundamentally important. Whilst discussions of sticky knowledge (von Hippel, 1994; 1999) have tended to focus upon the difficulty of retaining and disseminating knowledge *within* organizations, ‘leakiness’, by contrast, has generally focused on the external and undesirable flow of knowledge *from* organizations, to competitors (Brown & Duguid, 2001: 199). Here, to prevent knowledge spontaneously overflowing, the emphasis is placed upon the creation and maintenance of boundaries – ‘protective governance structures’ (Williamson, 1981) or ‘regimes of appropriability’ (Teece, 1986).

However, Brown and Duguid also note that focusing solely upon knowledge is somewhat unsatisfactory as ‘exactly the same knowledge can prove both sticky and leaky’ (2001: 199), as studies of ‘fissioning’ (Zeigler, 1985) and second mover advantage (Teece, 1986) demonstrate. As an alternative Brown and Duguid argue that by focusing on social practice, informed by

social and cultural studies of knowledge and learning, the apparent paradox of sticky and leaky knowledge is overcome. Hence, knowledge is re-positioned as intimately related to actual practices within communities of practice. Resultantly, knowledge circulates both internally and externally through networks of associations and is not a property of any particular firm (2001: 209), but rather one that, in part, draws upon much broader structures.

However, we contend that such an account is falsely premised upon a flawed, one-sided and naïve view of 'leakiness'. It is flawed because it fails to acknowledge the considerable difficulties and costs of knowledge protection; it is one sided because it suggests that leakage is primarily of internal origin and it is naïve because of a lack of awareness of an age old and extensive problem which we use to problematize such a perception of 'leakiness' - that of economic espionage.

The Problems of Protecting Knowledge

The practical problems of knowledge protection have already been well documented by Liebeskind (1996). They are two-fold (for a more detailed review of the issues see e.g. Cheung, 1982; Friedman et al., 1991). Firstly, the obvious protections, the recourse to law and the use of property rights, are fraught with difficulties: patents, copyrights and trade secrets are all narrowly defined, expensive to initiate and administer, and even more expensive to enforce (see e.g. Mansfield, 1985). Secondly, even when recourse to law can be sought such action is premised upon the fact that an infringement has taken place. Unlike other organisational assets, knowledge can be made mobile (the objective of the much of the 'stickiness' literature) and requires deliberate action to prevent such mobility or 'leakiness' (Liebeskind, 1996). However, it is difficult to detect such expropriation or imitation as a result of the very nature of knowledge.

'Leakiness': Osmosis or Theft?

The metaphor of ‘leak’ may well be one that was conjured up from plumbing origins. Here knowledge is regarded as flowing (ideally) merely within the social network of pipes that make up the organization. Leakage is regarded as being primarily the function of an internal ‘blockage’ (of ideas) e.g. in the case of ‘fissioning’ (Zeigler, 1985), However, in the case of second mover advantage (Teece, 1986), which Brown and Duguid employ in their discussion, the metaphor does, admittedly, break-down. Nevertheless, it does serve to illustrate the point that leakage is regarded as being internally generated.

The point that we make here is that these authors are themselves guilty of the very same error that they attribute to those who adopt a socio-cultural perspective of knowledge. Proponents are accused of adopting a ‘black-box model of organizations, where the inside is somehow free of all the forces at work on the outside’ (Brown & Duguid, 2001: 200). More recent studies have served to problematize the degree to which organizations are not impacted by such exogenous forces. In particular, this ‘black-box’ mindset has been challenged by drawing attention to the liminality of temporary workers (Tempest and Starkey, 2004), the tensions surrounding intersecting group affiliations (Lehrer and Asakawa, 2003), and the creation of learning boundaries in project-based learning (Scarbrough et al, 2004). What these studies indicate is that, given the increasing mobility of workers and the diversity of contemporary working practices, external factors do significantly influence learning both within and between organizations.

However improved our knowledge of learning across boundaries has become, such contemporary debates are still afflicted by an intellectual myopia – namely that studies focus on positive, legitimate forms of collaborative activity and thereby neglect *illegitimate* learning across boundaries. In an attempt to address this lacuna this paper explores illegitimate learning across boundaries, specifically that of economic and industrial espionage. In subsequent sections we demonstrate that the debate surrounding sticky and leaky knowledge can be greatly enhanced by the acknowledgement and addressing of such knowledge theft.

Before exploring the incidence, cost and history of knowledge theft as espionage we need to clarify a distinction. Following Nasheri (2005) this paper presents economic espionage as involving a government's efforts to collect information, appropriate trade secrets, and steal knowledge. Industrial espionage is thus viewed as an organizational phenomenon, with the same objectives as economic espionage, yet without direct governmental involvement.

Economic Espionage

When we think of espionage many of us will recall memories of the trashy spy thrillers and tacky Bond films of our halcyon youth. Few of us will give the subject any serious attention, especially in consideration of the more serious business of 'Business'. Yet economic espionage, as we shall subsequently see, has a very long history and pedigree.

More currently, however, in the US economic espionage is deemed so important that the President is compelled by law[1] to annually submit to Congress updated information on the threat to domestic industry from foreign economic data collection and industrial espionage. The President's report to Congress is informed by ongoing work conducted by the US Federal Bureau of Investigation (FBI), who estimated that in 1997 the theft of formulas, process information, blueprints, business plans, and customer lists cost US industries approximately $250 billion per year (Shanley & Crabb, 1998).

A subsequent study, conducted by the American Society for Industrial Security (ASIS) and consulting firm PricewaterhouseCoopers, concluded that during 1999 Fortune 1000 companies sustained losses in excess of $45 billion as a result of the theft of proprietary information (ASIS, 2000)[2]. This

[1] The President is legally compelled to report to Congress by the 'Intelligence Authorization Act for Fiscal Year 1995', Section 809(b), Public Law 103-359.

[2] In the follow up survey, conducted in 2001, this figure was estimated to have risen to between $53 and $59 billion.

investigation further revealed that 44 of the 97 survey participants reported a total of more than 1,000 separate instances of such theft, resulting in an estimated loss per incident in excess of $500,000. Although considerable, these figures pale into insignificance when compared to the average of $15 million in lost business reported by high technology firms in the same survey (Hemphill, 2002).

Other studies have indicated that economic espionage is a global problem. In 1998 the FBI identified 23 nation-states as hijacking sensitive trade secrets to gain competitive advantage (FBI, 1998)[3]. More recently, the US identified foreign individuals, from both the private and public sectors, in almost 100 countries and how they have attempted to acquire sensitive US technologies in the fiscal year 2004 (ONCIX, 2005: ix). According to these official sources this has:

> *Resulted in an erosion of US military advantage, and a degradation of the US Intelligence Community's ability to provide information to policymakers, and undercut US industry.*

Although the United States claims to have suffered most as a result of trade secret and technology theft, 2004 saw a number of other countries suffering similarly in consequence of foreign economic espionage. ONCIX (2005: 15) examples include the following incidents:

> *China: In April 2004, a court in China sentenced a former engineer from a Wuhan Iron & Steel Company to 18 years in jail for taking bribes and industrial espionage, according to press reports. The individual was found guilty of selling sensitive corporate information to an unidentified foreign company bidding for the project to produce high-end steel products and cold-rolled steel sheet. The foreign company accused of receiving the information reportedly pulled out of the bidding process after the individual was arrested.*
>
> *Russia: In April 2004, Russia's Federal Security Service claimed to have uncovered an industrial espionage network that was preparing to pass information on Russia's*

[3] Ironically, the vast majority of these nations identified were previously trained by U.S. intelligence services (Frauman 1997).

satellite program to the Chinese. The theft would have enabled China to close the gap with Russia in satellite production and delivery, according to press reports.

South Korea: In mid-2004, a South Korean employee of a Hong Kong based cell phone distributor was arrested on charges of espionage for attempting to give 75,000 internal computer files from a South Korean handset maker to a Hong Kong firm. The computer files contained secret information about the South Korean company's technology for making mobile phones. Prosecutors estimated that if the information had leaked, it would have cost the company $3.8 billion in lost exports.

Given the extent of the problem, and the cost to individuals, organizations, and nation states, one would expect economic espionage to merit serious academic study. Yet critical, and for that matter, even mainstream orthodox accounts of business and management appear to be virtually oblivious to the existence and range of economic espionage. Apart from the difficulty in conducting empirical research into such practices (Punch, 1996), one reason for this paucity of interest could be that economic espionage is a new phenomenon, perhaps a consequence of rediscovering the value of knowledge in today's societies.

Historical evidence of economic and industrial espionage

The claim of espionage being a new phenomenon can be swiftly discounted. It has been claimed that the history of this phenomena could extend back to pre-historic times with the quest for the secret of fire between competing nomadic tribes (Rosny, 1967). Bergier (1977) even cites an example from the Old Testament (Numbers, ch. XIII) in which God commanded Moses to send the leaders of the twelve tribes of Israel to spy upon the land of Canaan.

More factually, perhaps, Jeremy (1981) notes that as early as the 1780's Britain had passed rigorous patent laws and banned the exportation of cotton-making technology. As a result of this legislation skilled technicians convicted of taking such knowledge abroad had their property summarily confiscated by the crown (Jeremy, 1981: 36). At the same time France made the export of lace-making expertise a capital crime punishable by death (Davenport and

Prusak, 2000: 16). Even the American Constitution provides an example of the early recognition of the value of knowledge, as Article I (Section 8) authorizes Congress to enact suitable patent legislation (Nonaka and Teece, 2001: 1). The reason such measures were created is obvious. Even at this early stage of development in Western societies economic espionage existed.

Evidence of the incidence of economic espionage activity can be found throughout history. For example, Landes (1999: 276) observes that in early eighteenth century France explorers were sent out to acquire British technologies, including in 1718 a systematic pursuit of British technicians specializing in clock and watchmakers, woollen workers, glassmakers, and shipbuilders. This looting of British technology was, according to Fialka (1997: xi), taken up in 1811 by Francis Cabot Lowell (after whom the city of Lowell. Massachusetts was named in recognition of such efforts). This 'enterprising' American visited Scotland and England specifically to surreptitiously acquire knowledge of water-powered mills and cotton-making technology: an expropriation of knowledge without recompense. Many similar examples can be found in the many and various literatures dealing with the diffusion of technological innovations, particularly those that could be defined contemporarily as 'leading edge' (Harris, 1998). The porcelain industry, in particular, regularly engaged in such illegal knowledge acquisition activities (see e.g. Savage, 1961 for a detailed discussion of examples from the 17th and 18th centuries).

What these contemporary (ONCIX, 2005) and historical examples (Fialka, 1997; Jeremy, 1981; Landes, 1999) demonstrate is deliberate strategic knowledge acquisition, by learning across organizational and nation state boundaries, has been around for centuries and continues today. As yet management scholars have failed to address this gap in our understanding of inter-organizational learning.

Where some evidence exists of the exploration of the issues relating to espionage, both industrial and economic, is in the area of white collar crime within the sociology and criminology literatures and, as we have already

remarked, within those dealing with the diffusion of technological innovations. Here, however, economic espionage, or Trade Secret theft as it is often referred to, is seen as occurring in consequence of one or both of two particular motivations: either a disgruntled employee misappropriates the company's trade secrets for his/her own financial benefit or to harm their employer or else a competitor of the company or a foreign nation misappropriates the trade secret to advance its own financial interests (Nasheri, 2005: 7).

In order to address the gap in our knowledge of inter-organizational learning, and to connect management research with sociological insights, the remainder of this paper explores three vignettes to indicate what could be discovered about learning across boundaries from focused investigation of industrial and economic espionage. Given the distinctions introduced by Nasheri (2005) we concentrate our considerations on the motivation of individuals to commit acts of espionage, the inter-organizational learning facilitated by the act of espionage, and the degree of company and/or State involvement. By exploring these aspects we discover a different perspective of sticky and leaky knowledge.

Stealing DNA

Our first vignette concerns a medical research project, undertaken in Cleveland Ohio, into Alzheimer's disease. Watts (2001) reports a series of events involving two Japanese clinical researchers, one a 40-year-old neuroscience researcher from the Japan Institute of Physical and Chemical Research (known in Tokyo as Riken), the other a 39-year-old clinical researcher at the Kansas University Medical College.

> *After an investigation by the Federal Bureau of Investigation, law authorities in the USA filed charges in May against two Japanese scientists for the alleged theft of DNA samples from an Alzheimer's disease research project. At the centre of the "DNA spy" controversy is Takashi Okamoto — a graduate of Tokyo University and a scholar at*

Harvard — who worked at the Cleveland Clinic in the USA from January, 1997, to July, 1999.

Okamoto is alleged to have secretly sent DNA samples and cell-line reagents to Riken, a quasi-governmental Japanese body, shortly before returning to his home country. According to an indictment filed by Ohio State prosecutors, Okamoto attempted to cover his tracks by destroying research material and by switching the stolen samples with test tubes filled with tap water. The change was noticed by junior researchers at the Cleveland laboratory, who reported their suspicions to the US authorities.

According to the indictment, in or about April 1999, Riken offered Okamoto a position to commence in the autumn of 1999. Okamoto accepted. On or about the 8th and 9th of July 1999 Okamoto and a third person misappropriate DNA and cell line reagents and constructs from the Cleveland Clinic. Okamoto stored four boxes containing the stolen DNA with a colleague in Kansas. Okamoto resigned from the Cleveland clinic on the 26th July 1999 and started his new position in Japan with Riken. In August 1999 Okamoto returned to the US to retrieve the stolen DNA. Okamoto left the US later that month with the stolen DNA and cell line reagents

An FBI investigation found that the espionage carried out by Okamoto and his alleged accomplice, Hiroaki Serizawa had caused US$2 million worth of damage to the Cleveland Clinic. On the 8th of May 2001 a grand jury in Cleveland, Ohio returned a four-count indictment against Okamoto.

(Adapted from Watts, 2001: 2111; Nasheri, 2005: 143-5)

Motivation of individuals to commit acts of espionage

Discerning the motivation for Okamoto is a complex matter because a number of aspects could be equally important. Firstly, as Lehrer and Asakawa (2003) note, members of intersecting groups with different affiliations can suffer great tension. Okamoto is simultaneously a member of a scientific community, has allegiance to his Japanese employers, and allegiance to the research project. As a scientist Okamoto is used to sharing knowledge with the broader scientific community, and as such practice is arguably the basis of scientific endeavour, community membership encourages the leakage of communal

knowledge. Merton (1968: 601) clarifies this communal understanding of knowledge in science thus:

> *The substantive findings of science are a product of social collaboration and are assigned to the community. They constitute a common heritage in which the equity of the individual producer is severely limited. An eponymous law or theory does not enter into the exclusive possession of the discoverer and his heir, nor do the muses bestow on him special rights of use and disposition*.

It could therefore be argued that Okamoto was acting in the public interest by attempting to deliberately 'leak' knowledge of the research to prevent exclusive ownership claims by the Cleveland Clinic. What Okamoto could be experiencing is the tension resulting from the increasing encroachment of market relations into scientific communities (O'Neill, 1998). In such circumstances Nelkin (1984) notes that conflicts of interest are bound to arise because "the academic responsibility of open communication inevitably conflicts with the commercial responsibility to maintain secrecy" (Nelkin, 1984: 25).

In addition to the considerable tensions associated with scientific community membership, Okamoto is also faced with the dilemma of opposing loyalties. Although temporarily employed in America, Okamoto is a Japanese national, most recently employed by a quasi-governmental agency. It appears that his loyalty to Japan outweighed his loyalty to his previous employers. This is perhaps to be expected, if not condoned, if we consider the influence of Japanese government agencies on espionage activity.

Fialka (1997: 44) draws our attention to JETRO, the Japan External Trade Organization, which uses partial funding from the Japanese government to train people how and where to look for new technology. This Japanese 'technology lust' (Sammuels, 1994: 170) has seen huge numbers of Japanese students being trained in US universities to become the researchers of the future. During 1990, for example, 29,840 Japanese students attended US institutions, whereas only 1,485 American students studies in Japan (Fialka,

1997: 151). Okamoto is the product of this experience, and could feasibly have been briefed to secure prior research samples for Riken.

Inter-organizational learning facilitated by the act of espionage

If Okamoto had been successful in removing DNA samples a quasi-governmental Japanese body would have learned everything that an American research centre had taken time and money to discover. The DNA samples and cell line reagents represent the product of substantial research and development investment by the Cleveland Clinic. By employing Okamoto, Riken not only reduced the research costs involved in producing the DNA and cell line reagents, but also had access to the tacit and codified knowledge associated with the original research. If seen as an exercise in learning across organizational boundaries alone, thereby ignoring the illegality of the actions, Riken has secured the advantages of collaboration without any of the costs.

Degree of company and/or State involvement.

The theft of DNA samples itself raises real concerns regarding commercial competition between nation states. In this particular case Okamoto's actions indicate that scientific collaboration for the good of human kind could sometimes be relegated by commercial interest. The implications of this are wide ranging, and question the future of scientific work in commercial arenas where market mechanisms apply. If it could be demonstrated that the Japanese Government took overt steps to encourage the theft of materials then we could argue, given the US research data presented earlier, that the economic prosperity of nations is seriously affected by espionage. What this means is that 'knowledge stickiness' is a matter of national security. The issue of national security is taken up by our second example.

Rocket launchers

Our second vignette concerns the practice of competitive tendering for government contracts reported by Swartz (2003). In this particular case the US Air Force put out to tender contracts for rocket-launchers valued at $2 billion. What follows is an example of what can happen when employees feel wrongfully dismissed.

> *Krishnan Raghavan, a former employee of Boeing, alleged he was wrongfully fired after he told Boeing managers that a colleague – Dean Farmer, a former Lockheed employee, had propriety documents. Farmer reportedly brought the documents – 8,800 pages – with him to Boeing from Lockheed. According to letters from Boeing lawyers to Lockheed lawyers, Boeing fired Farmer in 2001 after an internal investigation found that he had sent propriety Lockheed documents to eight Boeing employees, including Raghavan. Raghavan claimed to have alerted Boeing's ethics office after receiving 40 Lockheed slides from Farmer that contained secret Lockheed financial and bidding information.*
>
> *In an investigation the US Air Force found that Boeing had acquired 25,000 Lockheed documents during the 1998 competition. The Air Force said it would shift seven rocket launch contracts valued at $1 billion from Boeing to Lockheed and suspend three former employees and three Business units of Boeing Integrated Defence Systems from further government work until corrective action is taken.*
>
> (Adapted from Swartz, 2003: 16)

Motivation of individuals to commit acts of espionage

Dean Farmer's actions can be seen as premeditated because the confidential documents he sent to colleagues in Boeing were already in his possession when he joined the organization. The central question here is why Farmer chose to take propriety information regarding his former employer's financial and tendering plans with him when he left. One possible explanation is that Farmer recognised the value of such knowledge and used this for internal self-promotion. It is possible, if highly unlikely, that Farmer did not fully appreciate the situation and was merely trying to be helpful. Given the value of the contracts involved this is implausible. Consequently we have to explore

the possibility that Boeing sought to discover Lockheed's plans for the tender and took the opportunity to hire an ex-employee, hoping that Farmer would bring with him inside knowledge of the tenders. The discovery of codified knowledge in his possession could have been seen as a bonus, and may even have constituted part of his employment deal. Either way, our understanding of sticky knowledge has to be adapted. When we think about employee mobility we may accept that tacit knowledge sticks with an individual. This vignette demonstrates that sometimes codified knowledge also sticks to individuals when they shift employment.

Inter-organizational learning facilitated by the act of espionage

This vignette emphasises a different facet of competition in knowledge-driven economies, and a different type of inter-organizational learning. *Contra* the emphasis placed on 'know-how' by practice-based theorists (), this example vividly demonstrates the importance and value of 'know-what'. In situations where a number of organizations possess the requisite 'know-how', 'know-what' become vitally important. By 'know-what' we mean that organizations can make strategically informed choices to undercut competitors when placing tenders for lucrative contracts if they know competitors plans, and make adjustments to their own bids accordingly. The value of knowing what a competitor is going to do in most cases is hard to quantify, but in this case it be suggested by the US Air Force's reaction upon discovering the espionage - $1 billion.

Degree of company and/or State involvement.

Given the findings of the US Air Force investigation, and the fact that 25,000 Lockheed documents were discovered in Boeing, we can assume that the Farmer case is not an isolated incident. This raises serious questions as to the nature of Boeing's organizational culture. In the case of organizational culture contributing to illegal acts Stone (1975) suggests the following factors may be involved:

> *A desire for profits, expansion, power; desire for security (at corporate as well as individual levels); fear of failure (particularly in connection with shortcomings in corporate innovativeness); group loyalty identification (particularly in connection with citizenship violations and the various failures to 'come forward' with internal information); feelings of omniscience (in connection with inadequate testing); organizational diffusion of responsibility (in connection with the buffering of public criticism); corporate ethnocentricism (in connection with limits in concern for public's wants and desires)*
> (Stone, 1975: 236 as cited in Punch, 1996: 225)

Clearly Boeing demonstrates a number of these characteristics in the evidence provided, and yet there is the larger question of the impact of such activity on national security. Given that the espionage is industrial rather than state sponsored, it may initially appear odd to talk about national security, and yet we have to consider the implications of Lockheed's actions. If sensitive information was so readily available as this vignette suggests, then we have to question how easy it would be for foreign organizations to acquire such knowledge. Lockheed, a regular governmental contractor, clearly has serious security issues to deal with. If one of its main US rivals could obtain 25, 000 internal documents containing sensitive information, then how easy is it to obtain and transfer knowledge across organizational boundaries? The final vignette provides an indication to the relative ease of such knowledge transfer, and provides us with a final insight into internal espionage.

The Glue Man

The third vignette focuses on perhaps the most famous case of economic espionage - Four Pillars and Avery Dennison. The full features of the case are discussed in relation to risk and crisis management by Fink (2002). What is most striking about this case is the extent of the espionage conducted.

> *Tenhong 'Victor' Lee (PhD), a Taiwan-born US educated chemical engineer, was employed as a Senior Research Engineer at Avery Dennison in Concord Ohio for 11 years. Although Dr. Lee was a highly valued and trusted expert, working for a Fortune 500 listed company specialising in self-adhesive products, Lee was a spy. For eight*

years, between 1989 and 1997, Dr. Lee conducted extensive espionage activities for his other employer – Four Pillars Enterprise Co. of Taipei Taiwan. During this period Four Pillars grew to become Avery Dennison's leading competitor in Asia, despite Avery Dennison spending $200 million on research and development.

Once discovered, the extent of Dr. Lee's activities became apparent. In eight years Dr. Lee stole 12,000 research documents, 71 adhesive formulas, trade secret information relating to 37 speciality adhesive tapes and 20 label primers, Avery Dennison new products, and even gave seminars to Four Pillar scientists in 1990, 1991, 1992, 1994 and 1996. Dr. Lee was finally discovered by chance, as a result of an employee of Four Pillars being legitimately hired by Avery Dennison. This 'new hire' instantly recognised Dr. Lee and alerted his new employer. During criminal and civil proceedings it was discovered that Dr. Lee had received $160,000 over eight years for his extensive work.

(Adapted from Fink, 2002: 5, 86)

Motivation of individuals to commit acts of espionage

Given that Dr. Lee spent six months confessing to his crimes, and six days giving court testimony, we can examine what drove this massive espionage effort. Dr. Lee maintained that he did not commit the crimes for financial benefit, and in support of this claim no evidence was ever found that Dr. Lee asked for payment of any kind. Dr. Lee had taken what had been offered. Dr. Lee claimed that he saw the Head of Four Pillars, a P.Y. Yang, like 'a father he never had' (Fink, 2002: 23), and that this was one of the main reasons for his activities. In addition to this, Dr. Lee claimed that in his native Taiwan the title of 'consultant' carried tremendous esteem, and that he had decided to act on the behalf of Four Pillars because of this kudos. Irrespective of the cultural pressure placed upon Dr. Lee, the claim that the title was a motivating factor is unlikely because only a handful of Four Pillars' employees knew of Dr. Lee's role. Fink (2002: 25) argues that ego and power made Dr. Lee do it, and we are inclined to agree.

Inter-organizational learning facilitated by the act of espionage

The extent of espionage conducted by Dr. Lee, summarised by Fink (2002: 87-99), provides us with great detail. Dr. Lee started his espionage spree by sending a confidential training guide for pressure-sensitive adhesive technology. This was followed by technical details of mastercurves and accompanying formula, enabling Four Pillars to clone some of Avery Dennison's most successful products. Not only could Four Pillars clone products, but with a slight change to the templates, could create unique products without having spent anything on research and development. Later that same year Dr. Lee sent internal software, market test reports, sales data, and test samples. Effectively Four Pillars spent $160, 000 in eight years, and received $200 million worth of information.

Degree of company and/or State involvement.

Four Pillars recruited Dr. Lee specifically to supply as much technical information as possible. Four Pillars encouraged and financed Dr. Lee to acquire virtually every aspect associated with Avery Dennison's products. Again we discover the same motivational forces at work with this particular organization as we have found with our two prior vignettes. The organizational culture is clearly conducive to illegal activity, provided it directly benefits the organizational goals. The implication of this is that we can suggest that industrial espionage could be a deliberate organizational strategy. If this is the case with one organization, it logically follows that other similar organizations could adopt this position.

Although there is no suggestion of state involvement in this example, we still have to recognise the impact of Four Pillars espionage at nation state level. Four Pillars developed to become Avery Dennison's main competitors in Asia, and as a result of this increased profitability would have increased national wealth, and may even have been heralded as an organization to emulate. If this were to happen it is feasible to suggest that national policy may follow this route. Given the USTR watch lists produced every year monitoring nation

state infringements of the international TRIPs agreement (http: usinfo.state.gov), and the consistent lack of action undertaken by countries like Ukraine to address these infringements, the plausibility of this is affirmed.

Analysis of vignettes

As noted earlier, Nasheri (2005) suggests that three different units of analysis can be used to understand espionage activities. Espionage is conducted by individuals, organizations and nation states. The central motivation for all of these entities is presented as the desire to advance their own financial interests. Beyond this basic unitary understanding, the case of individuals' personal dissatisfaction is additionally offered as a motivating force. When we look at the three vignettes presented not only do we discover that Nasheri's position is less than clearly supported, we discover a different perspective on the sticky and leaky knowledge debate.

From the espionage perspective we learn that valuable 'know-how', associated with inter-organizational collaboration, and valuable 'know-what' is made to leak. Although the information on espionage presented in the three vignettes is very limited we can still suggest a number of factors that affect the stickiness and leakiness of knowledge at work both within and beyond organizational boundaries.

Motivation to force leaks

What is most striking about the examples presented is the suggestion that, at the individual level, financial gain may not be the main motivation for conducting espionage. We can suggest different, non-financial, motivating factors for Dr. Okamoto, Mr. Farmer and Dr. Lee. This is not to discount the external influence of payment for espionage, because it may be one of the external forces at work, as the Glueman case indicates.

However *contra* Nasheri (2005) there is no evidence to suggest that Okamoto, Farmer and Lee were disgruntled employees. In the DNA and Glueman cases

we can suggest that the perpetrators may have suffered divided loyalties, and in all three vignettes evidence suggests that each individual may have had pressure to commit espionage applied by organizations. This insight repositions the notion of leaky knowledge because we are forced to accept that some organizations engage in activities to force leaks.

At the organizational level the evidence suggests that all of the potential benefits of collaborative inter-organizational learning can be achieved by illegal means. In the Glueman case Four Pillars had access to the complementary assets needed to turn innovation into commercial success, reduced the R&D cost by paying a pittance direct to the thief, and through Dr. Lee had created a conduit for the transfer of tacit and explicit knowledge. In this particular case the benefits of 'know-how' can clearly be achieved.

In addition to the benefits associated with 'know-how' being available through espionage, the evidence presented also suggests the following benefits of inter-organizational learning by focusing on 'know-what'.

The return of 'know-what'

With the preoccupation with 'practice' so evident in contemporary research conducted in inter-organizational learning the commercial value of knowing what competitors are planning to do, what new products and technologies are being developed, and what scientific research may offer business appears to have slipped off the research agenda. Yet espionage activity demonstrates that the old English adage that 'forewarned is forearmed' still has relevance. This is most explicitly demonstrated by Boeing's preoccupation with Lockheed's financial and technical information relating to government tender applications.

Organizational pressures

In each of the three vignettes organizational forces could be suggested as a reason why perpetrators committed espionage. Although the evidence is questionable in the case of Riken, both Boeing and Four Pillars sought and acted upon knowledge obtained through espionage activities. This observation suggests that certain organizational cultures could contribute to, or even encourage, illegal activity by employees.

Although the notion of organizational culture is notoriously diffuse (Punch, 1996: 225) there may be something about certain environments that make them conducive to illegal activity (Stone, 1975). This suggestion could be extended to include nation states, as the evidence provided by the FBI (1998; ONCIX, 2005: ix) indicates concerted efforts have been made to acquire knowledge via economic espionage by over 100 countries.

Discussion

The aim of this paper has been to develop our understanding of sticky and leaky knowledge in the context of inter-organizational learning. By drawing on data from economic and industrial espionage we attempt to offset the myopic focus on legitimate organizational activity to illustrate that contemporary debate could benefit from exploring understanding the illegal forms of inter-organizational learning.

Three vignettes capturing different aspects of economic and industrial espionage were presented to demonstrate the limitations of both our current conceptualisations of inter-organizational learning and what motivates people to illegally acquire knowledge across organizational boundaries.

Marchington and Vincent (2004) note that much of the strategic management and economics literature tends to focus at the organizational level, thereby neglecting wider institutional forces that help to shape inter-organizational relations. The vignettes presented here demonstrate that economic and industrial espionage are multi-level phenomena, with different aspects forming

linkages across levels. By focusing on the different levels of analysis this paper seeks to overcome the limitations of mono-level readings to address sticky and leaky knowledge in inter-organizational learning.

In direct challenge to the ‘black-box’ view of organizations presupposed by the sticky and leaky knowledge debate the vignettes present powerful evidence of external forces encouraging the forced leakage of knowledge. Resultantly our understanding of what constitutes sticky and leaky knowledge has to be adapted. Although we are aware that tacit knowledge sticks with the individual, the evidence suggests that sometimes codified knowledge also sticks to individuals when they shift employment. Rather than leaking knowledge the evidence provided suggests a third dimension - knowledge theft.

From the examples of knowledge theft as economic and industrial espionage we have suggested that although financial advantage is often assumed to be the driving force behind illegal activity, the actual motivations of individuals, organizations and nation states are more complex. Drawing on our examples, it is clear that a range of *different* motivations could exist including loyalty, self-promotion, kudos, ego, being valued at work, and perhaps even altruism.

For an organization or a nation state to obtain the potential benefits of collaboration, without having to expose themselves to potential knowledge leaks, what is required is the development an organizational/state culture at ease with espionage as a form of strategic knowledge acquisition, and to recruit employees who are likely to either infiltrate a competitor or pass on secret internal documents of their prior employer. As outrageous as it sounds, the evidence suggests that this is happening in a number of industries. As to the real extent of this, we do not yet know.

Resultantly, we would argue that empirical research is needed to address economic and industrial espionage at the individual, organizational and national levels. At the individual level we need to understand the particular and specific motivations for conducting espionage. At the organizational level

we need to explore the extent of criminogenic organizations (Punch, 1996), organizational cultures that encourage and/or ignore espionage (Stone, 1975), and the degree of institutionalised criminality within superficially legitimate organizations. At the state level we need to explore the relationship between nation states and economic espionage to attempt to understand the extent of the problem. Once we have a clearer understanding of the extent of the problem we would be able to explore the causes and effects of espionage on international trade and the competitive advantage of nations. If knowledge is the source of competitive advantage in the future we had better learn more about knowledge theft to protect ourselves in the future.

References

ASIS. (2000) *Trends in Proprietary Information Loss*. July. Alexandria, VA: American Society for Industrial Security, International and PricewaterhouseCoopers LLP.

Brown, J. S., and Duguid, P. (2001) Knowledge and Organization: A Social-Practice Perspective. *Organization Science,* **12** (2), pp. 198-213.

Cheung, S. (1982) Property Rights in Trade Secrets. *Economic enquiry,* **20**, pp. 40-53.

Fialka, J. (1997) *War by Other Means Economic Espionage in America*. New York: Norton.

Fink, S. (2002) Sticky Fingers: Managing the Global Risk of Economic Espionage, Dearborn: Chicago, Il.

Friedman, D. D., Landes, W. M., and Posner, R. A. (1991) Some Economics of Trade Secret Law. *Journal of Economic Perspectives*, **5**, pp. 61-72.

Hemphill, T. (2002) Electronic Commerce and Consumer Privacy: Establishing Online
Trust in the U.S. Digital Economy. *Business and Society Review,* **107** (2), pp. 221-39.

Jeremy, D. J. (1981) *Transatlantic Industrial Revolution : The Diffusion of Textile Technologies between Britain and America, 1790-1830s*. Cambridge, Mass.: MIT Press.

Landes, D. S. (1999) *The Wealth and Poverty of Nations : Why Some Are So Rich and Some So Poor*. London: Abacus.

Liebeskind, J. P. (1996) Knowledge, Strategy, and the Theory of the Firm. *Strategic Management Journal,* **17** (Winter Special Issue), pp. 93-107.

Mansfield, E. (1985) How Rapidly Does New Technology Leak Out? *Journal of Industrial Economics,* **34**, pp. 217-24.

Marchington, M. and Vincent, S. (2004) Analysing the Influence of Institutional, Organizational and Interpersonal Forces in Shaping Inter-Organizational Relations, *Journal of Management Studies* **41**:6

ONCIX. (2005) *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage - 2004*. April. Washington, DC: Office of the National Counterintelligence Executive (ONCIX).

Punch, M. (1996) *Dirty Business. Exploring Corporate Misconduct: Analysis and Cases*. London: Sage.

Shanley, A., and Crabb, C. (1998) Corporate Espionage: No Longer a Hidden Threat. *Chemical Engineering*, **105** (13), pp. 83.

Swartz, N. (2003) Boeing acknowledges stolen documents, *Information Management Journal*; Sep/Oct, **37** (5); pp. 16

Teece, D. J. (1986) Profiting from Technological Innovation: Implications for Integration, Collaboration, Licensing and Public Policy. *Research Policy*, **15** (6), pp. 285-305.

von Hippel, E. (1994) 'Sticky Information' and the Locus of Problem Solving: Implications for Innovation. *Management Science*, **40** (4), pp. 429-39.

von Hippel, E. (1999) Economics of Product Development by Users: Impact of 'Sticky' Local Information. *Management Science*, **45** (5), pp. 629-44.

Watts, J. (2001) Alleged biotech espionage rocks Japan, *The Lancet*, June 30, pp. 2111

Williamson, O. E. (1981) The Economics of Organization: The Transaction Cost Approach. *American Journal of Sociology*, **87** (3), pp. 548-77.

Zeigler, C. A. (1985) Innovation and the Imitative Entrepreneur. *Journal of Economic Behavior and Organization*(6), pp. 103-21.