Paper to be presented at the DRUID Summer Conference 2007

on

APPROPRIABILITY, PROXIMITY, ROUTINES AND INNOVATION

Copenhagen, CBS, Denmark, June 18 - 20, 2007

INTELLECTUAL PROPERTY IN COLLABORATIVE PROJECTS: NAVIGATING THE MAZE

Jordi Molas-gallart
INGENIO (CSIC-UPV)
jormoga@ingenio.upv.es

Puay Tang
SPRU, University of Sussex
p.tang@sussex.ac.uk

Abstract:
This article analyses the use of IT tools in the management of Intellectual Property in collaborative projects involving groups of firms and their customer organisations in the design, development, manufacture and maintenance of complex products. Through an in-depth study of IP management practice in collaborative defence projects we identify two contrasting approaches to the implementation of inter-organisational networks for the exchange of technical information. We find that, in both approaches, the IP management capacities offered by IT tools have not been fully utilised. The slow diffusion of available technological solutions can be attributed to organisational and regulatory factors.

JEL - codes: Z00, M00, -

Intellectual Property in collaborative projects: navigating the maze

Introduction

Until recently, the management of Intellectual Property (IP) and its associated Rights (IPR – formally protected IP) was treated as a specialised function within a company. Corporate strategy would concern itself mainly with the management of tangible and financial assets, and IP management would be left to specialist lawyers who dealt with patents and other forms of formal IP protection as needed. This situation is changing. Toward the late 1990s, analysts were underlining the importance of IP and IPR management as a key element of corporate policy (1997; Teece 1998; Ruggles and Holtshouse 1999; Shapiro and Varian 1999; Reitzig 2004; Chesbrough 2003; Rivette and Kline 2000; Davis 2004), and as a strategic intangible asset influencing corporate performance (Buigues, Jacquemin, and Marchipont 2000; Nonaka and H Takeuchi 1995; Quinn 1992; Davenport and Prusak 1998; Chesbrough 2003; Rivette and Kline 2000).

Important as IP is for the modern corporation, scholars have found it a difficult concept to define accurately.[1] Dictionaries define IP as a product of the intellect that has commercial value and is intangible[2]. Yet, IP can be expressed in many different tangible forms: books, blueprints, designs, trademarks are all expressions of IP, which can be made available to other parties. The increasing use of Information Technology

[1] For a clear discussion of the IP concept and the different forms of IP see for instance (Weil and Snapper 1989).

[2] The American Heritage Dictionary and the Oxford English Dictionary, respectively.

(IT) and electronic networks increases the risk of all these forms of IP to leakage, inadvertent or otherwise, and misappropriation. Different sources have estimated that the losses to firms from IP theft and corporate information leaks run into the billions of dollars per year, often through data theft through the Internet (Business Wire 2005; Lyons 2004). The potential threat posed to sensitive proprietary information by the Internet and other computer networks has emerged as an important source of concern, particularly among large companies (ASIS International, PricewaterhouseCoopers, and American Chamber of Commerce 2002). Such realisation of the risks posed by the growing use of electronic data networks for business operations suggests the need for coherent IP and information management strategies that address data control and access issues.

So far, corporate responses and academic analyses have focused on IP management *within* the firm (Reitzig 2004; Grindley and Teece 1997; Tang 1998; Chesbrough 2003). Similarly, analysts who have studied the role of digital technologies in collaboration, also address knowledge management *within* the firm (McAfee 2006). However, the problems and challenges faced are likely to be different when managing IP in the context of *inter-firm collaborative* projects in which groups of firms, often competitors, and sometimes their customer organisations share in the design, development, manufacture and operation of complex products. In these cases large amounts of technical data (including designs, product specifications, manufacturing processes, etc.) can be shared through the use of innovative advanced IT tools, with the aim of increasing efficiency and reducing time for the delivery of the asset/system. The resulting “Shared Digital Environments” (SDEs) involve data networks and data management systems used by project partners to manage and share technical data across organisations. SDEs are being proposed by leading customers, such as the UK

Ministry of Defence, as a tool to assist in the design, engineering and manufacturing of large complex products in a wide variety of sectors. The management of IP in SDEs, as discussed below, poses problems that are different in nature and scope to those of IP management within the firm.

This article analyses the nature of the problems posed by IP management in SDEs and discusses how organisations have, in practice, tried to devise solutions. Our main concern is the management of information and data whose disclosure or unauthorised use can generate a loss of commercial advantage to its owner. Although, strictly speaking not all IP falls within this category,[3] we retain the use of the term IP for convenience, as it is commonly used to refer to departments, groups and experts dealing with the formal (IPR) and informal protection of commercially sensitive and proprietary information.

The article is based on an in-depth analysis of the use of SDEs in the UK defence industries. In this area an exceptional effort is taking place to develop precise codes of practice and procedures affecting all aspects of the contractual process and project management *including* IP management. In collaboration with industry, the UK Ministry of Defence (MoD) has developed extensive guidelines and sets of contractual conditions for the management of IP in SDEs. Further, existing MoD procurement policies emphasise the use of inter-organisational IT networks to improve project performance and have introduced detailed IP regulations to develop and implement large SDEs. This situation provides a unique test bed for analysing the

[3] Some IP, like brands and designs, need to be “disclosed” to be valuable. On the other hand, tacit knowledge embedded in workers can also be regarded as IP. In this article, we refer mainly to codfied knowledge.

impact of formal regulations and processes on, and the challenges for the management of IP in collaborative projects employing inter-organisational digital networks and systems.

The article is structured as follows. We first discuss our approach. We then introduce the main relevant traits of present UK defence procurement practice, in particular the way it deals with IP, and analyse the specific IP management problems encountered when conducting collaborative ventures in the defence industries. We follow with a discussion of the strategies for responding to these challenges, and an analysis of the ways in which two specific SDEs have been implemented. We find that they have adopted different implementation models. We conclude with generic lessons for IP management in collaborative ventures.

Our approach

Our analysis has followed a case study methodology addressing the IP corporate management practices in the main British defence-related corporations and the way they relate to the IP practices of their main customer: the UK MoD. This choice of sector, however, does not limit the relevance of our study as the management of IP when using electronic networks has generic implications and applications for non-defence sectors. Although there are distinctive aspects to the regulatory environment of the defence sector, there is nothing inherently typical in the contractual procedures and guidelines for IP management that the sector has developed. For instance, the guidelines on how to develop a contractual structure for a “shared data environment” discussed below are equally applicable to any other industry. Still, some argue that the IP environment in which defence customer agencies and their industrial suppliers operate is characterised by a cosy relationship derived from a long-term customer-supplier relationship in what is a comparatively closed and trusted environment. If this was ever the case it is no longer now. New suppliers are entering the defence market, the defence industrial structure is in the midst of potentially profound changes (Gholz 2003), and changes in procurement practices have heightened the tension between large defence suppliers and their customers.[4] The UK defence sector is therefore becoming more open and akin to other commercial environments where trust between suppliers and clients can be lacking, fragile or in need of nurturing.

As noted above, the UK defence sector has invested a special effort to develop precise codes of practice and procedures affecting all aspects of the contractual process and project management including IPR procedures (see below). Further, the "Smart Acquisition" initiative launched by the MoD emphasises the use of e-commerce and advanced IT applications to improve project performance. The MoD's establishment of a Defence Information Infrastructure, which is part of the Defence Change Programme, also aims to replace a large assortment of individual information systems throughout the MoD with a single more efficient information infrastructure. These measures are part of MoD's modernising effort, which will result in the complex integration of technical data and business processes throughout a system's life-cycle. A catalogue of detailed IPR regulations has been thus set against an effort to develop and implement sophisticated IT systems in support of product development, manufacture and maintenance.

[4] We have explored elsewhere the mistrust between defence suppliers and the MoD generated by the way in which IPR have been handled in the privatisation process of the British defence research establishments (******)

We first undertook a documentary study of the IP practices and regulations used in defence contracting laid out in the "contractual conditions" used by the MoD procurement agency (the Defence Procurement Agency –DPA). We followed with a programme of semi-structured interviews using two different interview protocols, one addressing corporate policies and activities, and another oriented to the analysis of IP management practices within specific projects. The main objective of the interview programme was to determine the ways in which firms addressed IP management in a digital environment both within the corporation and in collaborative programs.

To guide the interviews we designed a protocol structured according to a list of IP management topics with potential effects on firm and corporate performance. We based the list on IP management issues identified by the extant literature on IP management within specific sectors and firms (Granstrand 2004; Guilhon, Attia, and Rizoulieres 2004; Hall and Ziedonis 2001; Tang and Paré 2003; Shapiro 2001; Tang 1998; Grindley and Teece 1997; Arora, Fosfuri, and Gambardella 2000). A panel of academic, industrial and government IPR experts validated the interview protocol, which we then piloted through a 6-hour long interview with two IPR and commercial managers of a major UK defence corporation. Following the pilot we adapted the protocol and used the two different formats, as noted above in an interview programme consisting of formal interviews and informal meetings with UK defence manufacturers, industrial associations and the Defence Procurement Agency. During a period of 9 months, ending in July 2004 we carried out interviews with 33 senior official and executives, covering, among others, the largest UK defence systems manufacturers.[5] The participating companies selected interviewees with direct

[5] Except for six telephone interviews, the rest were all face-to-face interviews carried out by both of us.

experience in IP management, IPR and contractual issues, and the implementation of IT tools, either at corporate level, or within the context of specific collaborative projects. Finally, we organised a conference in March 2005 in which the results of our study were validated. The event was attended by some 50 IP management experts, lawyers and executives from the defence industries, the MoD and the Department of Trade and Industry. Because of the sensitivity of the issues explored we will not attribute the information used in this article to any individual or organisation.

The case: Managing IP in the UK defence market

All the firms and organisations involved in this study are simultaneously using different network technologies and inter-organisational systems (Volkoff, Chan, and Newson 1999).[6] These are usually for large complex projects involving a number of suppliers, coordinated through a prime contractor, to provide a system, asset or a service for use by the UK armed forces. Under the current UK defence procurement approach, most of the above stakeholders participate in Integrated Project Teams (IPTs) set up by the DPA (Ministry of Defence Smart Procurement Implementation Team 1999). The IPTs bring together representatives from the client organisation, final users and industrial producers, and play a complex interface role between suppliers, the MoD client and military users. Every project establishes its own set of network technologies and inter-organisational systems, and its contractual conditions and procedures. The responsibility rests on the IPT and ultimately on its Leader:

[6] Here we use the term “network” to refer to a group of organisations collaborating within a specific large project. “Network technology” is the technical information and communications infrastructure that supports the network, and an “inter-organisational system” refers to the applications shared by the network through its network technology.

different projects will adopt different contractual clauses, different IT systems and different approaches to the management of IP. This means high set up costs for every project (there is an element of reinventing the wheel and limited cross-project learning). Consequently, defence firms work with a wide variety of network environments and under varying contractual conditions. For instance, one interviewed firm is running 300 separate projects supported by different IT networking arrangements and contractual conditions to manage and share data with, often the same, customers and suppliers. Furthermore, the same engineering staff maybe involved in several projects. Such a situation engenders not only additional costs but also a situation in which it is difficult to control and monitor the information flows, and the kind of information through the variety of inter-organisational systems.

That every project sets up its own IT system and IP rules and practices is also explained by the “alarming” lack of detailed corporate IP policies, a finding also reported by a study commissioned by DLA, a London-based law firm (Tait 2004; Nunan 2004). Companies are familiar with the process of formally protecting their IP: For instance, the firms interviewed for this project either focused their IP management approaches on patenting strategies or relied on trade secrets. Yet a concentration on formally protecting firm IP does not amount to a fully-fledged corporate IP management policy. First, not all formally protected IP yields economic rewards and the costs of building a patent portfolio can be substantial. Instead, a corporate IPR audit could reveal where formally protected IP is yielding direct economic benefits, in terms of licensing income and, more importantly, protecting key technologies (“crown jewels”) that underpin the competitiveness of the firm. An audit should record where the company’s IPRs are used and who uses them and could also help a corporation identify its valuable IP. Second, enforcement practices and monitoring of infringement could also be part of a company-wide processes and procedures for the treatment and use of corporate IP, *whether they be formally protected or not*.[7]

Instead, we have observed that the IP management "ethos" is biased, in the main, toward the formal protection processes – deciding whether or not to patent. The often-informal practices that determine, for instance, when and how to share proprietary information with clients and partners are not instituted as part of a corporate IP policy.[8] The rest of this section discusses some of the problems that the defence companies and their customers have encountered when addressing IP issues in this context.

IP issues in collaborative environments

The protection of information within SDEs

The first key problem with an SDE is the protection of "background information." Background information refers to the wide range of pre-existing proprietary information that a company brings to a collaborative project, from technical data and components and subsystems, to manufacturing processes and design techniques. These will need to be integrated with technology brought by other firms or developed for this project, and therefore other firms may need to have access to such "background information." By sharing background information through SDEs companies run the risk of (inadvertent) leakage of commercially sensitive

[7] An audit should also ideally involve processes for managing knowledge/IP of employees leaving the company (Parise, Cross, and Davenport 2006).

[8] Only one firm interviewed had a clearly articulated IP management policy supported by an IT system. This is used to track which patents were used in each of the firm's products, so that the firm can monitor where and how patents are used and also to identify infringements.

information; such as technical data about specific components, designs, design techniques or other processes that are not usually patented, but rather kept secret.

The second potential problem relates to the *early* release of “foreground information,” information developed during the course of the project. Although the MoD will have rights of use over such foreground information where it has funded its development, contractors worry about the possibility that, through an SDE, the customer may access data that is still being worked upon. This is because work-in-progress foreground information, often privately ventured, may include commercially sensitive information on company techniques and processes that will *not* be included in the final data packs delivered to the customer. Furthermore, firms are concerned about liability issues that may be derived from the customer accessing and using data that are still in draft form and not ready, or not intended, for delivery to the customer.

Both these problems are inherent in SDEs. Because digital data is easy to replicate, systems to monitor and track the information shared through the SDE and strict procedures on data sharing must be established. The establishment of such systems and procedures is more than a technical problem. Although there are known approaches for strict data access control, there is a palpable fear among the IP policy staff in all the companies interviewed that engineers do not adequately appreciate the importance that misappropriation of “background information” may have for their firm. Anecdotes abound of engineers who have been only too happy to share proprietary and commercially sensitive technical details with their peers in other companies. An example of this is an incident in which an engineer blithely shared the software architecture of the firm’s proprietary process with an engineer of a collaborating firm. Interviewees attributed such behaviour to “cultural” traits within the engineering community that drive individuals to share their work with their partners across organisational divides, much in the same way that academics are widely known to do. Although several of the anecdotes involved instances in which such exchanges were not always facilitated by electronic networks (sometimes in conversations and data exchanges in paper form) concerns were expressed about what would happen when the digital systems for collaboration are in place and its use enforced that could allow a loquacious engineer to send reams of technical information across to project partners at the click of a button.

All companies were concerned about this problem, albeit in different degrees, depending on the extent to which they saw their competitive advantage as depending upon codified technologies that could be transferred to potential competitors, or on being “first to market.” They all agreed, however, that there is a need to “educate” their engineering staff about the importance of protecting their IP appropriately, particularly as inter-organisational collaboration is increasingly being supported by advanced IT.

Convergence of product and process data

An effect of the use of IT in systems design is the confluence of product and process data within the same data sets. This is the case, for instance, in the manufacture of specialised components for aero-engines or for aero-structures, which is driven by unique software-based processes. Naturally companies do not wish to reveal these processes to third parties, but sharing product data in electronic format could imply sharing also software-based processes when product and processes data are inextricably linked. Companies that base their competitive advantage on the uniqueness of their manufacturing processes fear that an SDE could make them vulnerable to disclosure of their trade secrets.

Divergent approaches to IP management and data control among collaborators

To complicate matters even further, defence projects will often involve foreign partners operating within different legal and regulatory environments. This means, for instance, that an SDE will require data control access systems able to cope with the export and technology control regulations in each of the participating countries. As technical data, hence IP is covered under the export control regime of most NATO countries, sharing of some IP invariably would come under export control considerations. Collaborating companies have to ensure that data mounted in an SDE do not violate each collaborating partner's national export control regime. IP management methods will have to be coupled with the technical and regulatory structure emanating from the need to adhere to different export control regulations.

Equally, coping with different approaches to IP management across countries is problematic. Firms may not be able to trust the practices of their foreign partners and may decide to withhold information. We were offered examples of firms involved in international collaborative *research* programmes that were not contributing their best IP to the project, thus resulting in the joint research project performing at a suboptimal level.[9] A related problem is the lack of consistency in the meaning of the terms used by firms and governments to class the different levels of information protection and access. For instance, terms like "restricted" are interpreted differently among firms. Although we found no cases in which these differences led to identifiable financial losses or leakage of vital IP, our interviewees were adamant

[9] The practice of holding back one's best technology when contributing to international collaborative programmes has long been pointed out as a main problem in international arms collaboration.

about the need for consistency and common use of terms, particularly when structuring an SDE for collaborative projects.

Addressing the issues: what solutions?

The issues and difficulties presented above may not pose an insurmountable barrier to the introduction of SDEs in collaborative defence projects. In fact, defence customers and their industrial suppliers have been seeking solutions to address the afore-mentioned problems through four different but interrelated areas:

1. the definition of codified procedures to assure proper identification of all individuals accessing the system, together with their rights of use across all stakeholders;
2. the establishment of procedures and rules regarding the management of the SDE, and the marking and segregation of the data the SDE contains;
3. the network technologies and inter-organisational systems they support;
4. the underlying *training* necessary to raise awareness of the importance of IP management among stakeholders and to explain the nature and implications of the tools and procedures in place.

The first two aspects, can, in principle, be addressed through *contractual conditions* and associated commitments.

Contractual conditions

Buyers may try to address the uncertainty on the use and sharing of IP and IPRs through the inclusion of detailed contractual provisions. In the UK defence sector, a wide choice of DEFCONs (“Defence Conditions”) and DEFFORMS (templates for annexes that can be appended to contracts) are available for contract officers to include in contracts (Ministry of Defence 2004). These provide detailed contractual clauses and provisions applicable to a wide set of situations.

Although it is not mandatory for IPTs to include specific DEFCONs within a contract, or to follow rigidly to a specific DEFCON, explicit guidance documents recommend the adoption of some DEFCONs in specific contractual conditions. For instance, DEFCON 14 is commonly included in contracts for work that is likely to generate new IP. This and other generally used DEFCONs provide, in practice, an established contractual framework that defines the MoD negotiation policy for key aspects of defence procurement, including IPR. Yet it is ultimately the responsibility of the specific contracting team to decide which DEFCONs to include and whether or not to modify them.

While some DEFCONs are relatively straightforward and often applied, there are others that have given rise to serious contention between the MoD and defence suppliers. In part, the differences emerge from the difficulties of covering all possible future events through generic contractual provisions. For instance, the long life cycle of many defence systems which extend over three or more decades during which they will be subjected to several planned and unplanned upgrades and changes to improve the capabilities of the system. Managing these complex systems over such long life spans engender difficult IP problems. We distinguish two main sets of difficulties.

First, although several units of systems operate side-by-side (for instance, a squadron of a same model of fighter aircraft), it is common that the individual aircraft will have a slightly different configuration although together they may be formally belong to the same model. In practice, different sub-classes of each model may be identified ex-post by “working backwards” through the different modifications to which the planes have been subjected. In this situation, it is difficult to identify and monitor the ownership of the IP that may be involved in each small change and the superseded components that were part of the initial system. A line-by-line definition of the different IPR contained within a complex system may not be possible, and therefore it may remain preferable to stipulate IPR conditions in generic terms. [10]

Second, ownership over product data can generate problems with long term system maintenance and repair needs. Contractual conditions try to address this situation. For instance, the application of DEFCON 15 will require from a contractor the supply of a "manufacturing data pack" to which the MoD will have rights of use for the purpose of competitive procurement. DEFCON 15 is only to be applied when the development of a system has been fully funded by the MoD. Yet, today's highly complex defence systems are likely to include subsystems or parts, or involve processes, whose development has been privately funded, a point already discussed above. The leading prime contractors we interviewed pointed out that it is very likely that some of the IP that the client requests to be included as part of the manufacturing data pack will involve technologies from private investment. They are therefore anxious not "to give away" data that could be and is likely to be commercially sensitive, particularly if the

[10] However, there is a debate in the field of relational contractual theory as to the extent to which contracts can and should be written to address all possible eventualities in a complex, long-term project. Contract theorists have argued that contract is not an abstract formalistic mechanism, but one that typically involves development of relationships that go beyond the terms of a contract and evolve through the course of the project (MacNeil 1999, 1980). The practice in defense contracting, however, has tended towards the detailed specification of conditions and deliverables trying to cover for all possible eventualities.

support and maintenance of the system is *not* to be eventually undertaken by the prime contractor, but by a third party.[11]

Furthermore, there is a cost to the provision of a data manufacturing pack that DEFCON 15 does not appear to contemplate. As product components and subsystems are constantly updated, refreshing a manufacturing data pack over the life cycle of the system needs to take into account all changes made by the prime contractor *and* its supply chain. This cost, coupled with the IP problem addressed above, does not appear to be thoroughly recognised by the MoD, according to the interviewed companies.

The preceding examples show some emerging tensions in the application of IP conditions by the MoD. The root of the problem here is that it is very difficult to foresee and track all the contributions, changes and new requirements that will take place during an asset's long life. Nonetheless, there was a consensus among our interviewees, shared by the DPA officials that it is necessary to codify procedures for the protection of IP when dealing with the procurement of complex, long-life cycle systems. In fact some DEFCONS, such as DEFCON 15 referred to above, have been developed in collaboration with industry.

Directly relevant to our article is the "687 family" of DEFCONs and DEFFORMs, which establish how a "shared data environment" should be operated. For instance, DEFFORM 687C provides a detailed "Electronic Information Sharing Agreement." setting out the obligations, responsibilities of the SDE operator, user rights and obligations. DEFFORM 687c was finalised in 2001, after about 18 months of

[11] The complex issues of life cycle support service contracts and the management of IP is currently the basis of another research project.

preparation in which both representatives from industry and from the MoD participated. In addition, the MoD developed a set of guidance notes to these DEFCONs and DEFFORMs at the request and with the collaboration of the Confederation of British Industry. These contractual tools can therefore be seen as the outcome of a consensus-seeking process between industry and the MoD. Yet despite their genesis and wide support "Type 45" (more below) is the only full-fledged development and production programme to implement some of the contractual tools in the "687 family."

To sum up, UK defence prime contractors regard most IPR DEFCONS positively. Most of them have worked well and provided a proven and carefully constructed solution to the needed codification of IP protection procedures. But they also insist that DEFCONS must continue to abide by a principle of equity in which the MoD may not assume ownership of company IP without adequate terms of compensation. The continual development of a contractual system to deal with IP management issues is in a state of dynamic tension and one characterised by a mixture of collaboration and conflict. Still, there is broad agreement on the need to continue with the collaborative approach that has led to the development of some crucial IPR DEFCONs.

Supporting network technologies and inter-organisational systems

The second response to the IP problems lies in the use of IT systems. The technical foundations and the strategic rationale to deploy IT systems enabling technical data sharing and collaborative working across geographically dispersed sites are not new. From the early 1990s communities of practice have developed around concepts like TDI (Technical Data Interchange) and CALS (Continuous Acquisition Life-Cycle

Support) among others. TDI focused on the development of common standards for exchanging the electronic files used by different Computer-Aided Design and Computer-Aided Manufacturing (CAD/CAM) (Donnington 1995).CALS was a more ambitious set of initiatives. It developed guiding principles and associated standard and technology activities that sought to create a new type of customer-supply network relationship that would use advanced IT to integrate the different phases in the procurement of a complex system (design, production, support,...) into a continuous relationship. A key element in the implementation of the CALS vision was the creation of a "Contractor-Integrated Technical Information System": a full technical data set that would accompany a complex system through its life-cycle, from conceptual design to system decommissioning, and would be delivered to the customer together with the system. In an SDE this data set would be available to partners during the system's design and production.

Initial applications of these principles proved problematic.[12] During the 1990s, the civilian Boeing 777 became the best-publicised case of collaborative design and production across different locations for an aircraft system. This example was heralded as an innovative programme for its team management approaches and was also lauded for representing the first use of digital computers to design and electronically pre-assemble an entire plane.[13] Further, joint design was achieved

[12] For an early discussion of their application to the European fighter aircraft project, Eurofighter, see (Spinardi, Graham, and Williams 1995).

[13] Yet a very sophisticated IT system for technical data sharing a across US partners, project design and engineering has been described and analysed for the B-2 Stealth Bomber, an aircraft design and manufacturing project that predated the 777 by several years (Argyres 1999).

through a distributed computer network, consisting of mainframes and workstation installations in Japan, Kansas, Philadelphia, and other locations.

Yet for all its achievements this IT system fell short of constituting a full-blown SDE in the way defined above. Instead of offering a centralised online product database available to project partners, the communication between suppliers and Boeing was often carried out using more rudimentary techniques, which in the opinion of an interviewee was because 777 is "old technology" and thus the prime contractor did not see the need to introduce a more sophisticated IT system for data transmission. According to our interviewees, suppliers would e-mail their designs to the prime contractors' sites and *vice-versa*, a process that was often slow and cumbersome given the size of the file attachments and the low speed of the modem links used. The slowness also caused delayed "design deadlines," for instance, because the IT network could not always cope with the volumes of data being transmitted. This meant that file attachments were left sitting "on hold" until the system could clear the backlog of data transmission.

The diffusion of SDEs using centralised databases accessible to project partners is still very limited. The US-led Joint Strike Fighter (JSF) and the British "Type 45" Destroyer, described in more detail below, are the main examples of involvement by UK defence firms in programmes using an SDE.

Briefly, in Type 45 the prime contractor (who is not the leading manufacturer but is the systems integrator) is responsible for setting up a centralised product database system to which all project collaborators can have access, and to organise and control different levels of access to each of the "folders" in the system. The system is based on Internet architecture, can be accessed through a Wide Area Network or dial-up connections, and uses a suite of off-the-shelf software applications. In some cases the applications have had to be modified in-house to adapt them to the specific needs of the programme; this is the case, for instance, with Windchill, a set of software tools to enable a shared, Web-based configuration and document management system.

The prime contractor for JSF is “Lockheed Martin Aeronautics” (LMA), which is both the final assembler and systems integrator, and also a sub-systems and parts manufacturer for the aircraft. LMA has implemented an SDE, which again rests on Internet standards and a combination of off-the-shelf software tools, including “Metaphase” (a Product Data Management programme enabling access to an extended supply network) and, again, Windchill (providing a Web access to programme management data). LMA controls access to these facilities.

These examples show how Internet standards have been central to the implementation of SDEs in the defence sector. However, the need to tailor these off-the-shelf software technologies for each project represents a difficult challenge for which no ready-made solution exists and that can be addressed using the different implementation models described below.

Training

The third solution to the IP management problems is the need to inculcate in the engineering personnel a staunch sense of the importance of corporate IP. While training is frequently undertaken by corporations in various areas, IP management training does not appear to be widely adopted or considered as a core part of training. As noted above, all the firms interviewed expressed concern about the allegedly casual attitude of engineers towards the protection of company IP; such fears being exacerbated by digital technologies. To combat this laissez-faire attitude toward the appropriate treatment of corporate IP, some companies have issued guidelines about sharing data across companies, and imposing penalties for misappropriation of data, which include dismissal, fines and imprisonment. Others have introduced induction briefings on the management of IP and export control regulations, especially for those who are involved in international collaborative projects. However, these training sessions are conducted on a *project-by-project* basis, rather than as part of a corporate-wide IP management policy, thereby signalling potential ineffectiveness for IP management as a whole.

Interviewees unanimously agreed about the need for systematic training of engineers on the importance of corporate IP and the handling of these assets, as part of a company-wide IP policy. The need for such training was also highlighted by ASIS, whose report also found that there was little evidence of training and awareness of information security in the US (ASIS International, PricewaterhouseCoopers, and American Chamber of Commerce 2002). The report also found that proper labelling/marking and handling of classified information are not the norm among companies, nor are employees typically trained to safeguard proprietary information in the office or while travelling.

Propelled by the assumption that “IT matters”[14] and their use is increasingly critical to their competitive advantage and strategic success, defence companies have made large IT investments, as with businesses in other sectors. However in the innovative use of IT tools and applications for collaborative design work and R&D, the adoption of these technologies for an SDE appear to be less common, despite encouragement

[14] Marco Iansiti, “Why IT Matters,” keynote speech presented at the eBusiness Management School, ISUFI-Universita Degli Studi di Lecce Summer School, July 5-8, Brindisi, Italy. This paper was in

by the MoD in the case of the UK defence sector. The following section analyzes two SDE models that we uncovered in our study.

Two implementation models

As reviewed above, we found few defence programmes with British participation in which an SDE system has been established. Here we show the two main cases of dissimilar implementation models. They are different in the way the two major constituents of an SDE solution are defined and combined. We distinguish them accordingly:

1. A "*regulated approach*" as applied in UK contracts using elements of the 687 series of DEFCONs and DEFFORMs.
2. A "*prime-led*" approach as applied in the US-led JSF transatlantic collaborative programme. Here the prime contractor controls the definition of the inter-organisational system and imposes it, together with its associated IP conditions, to its international supply chain.

Regulated approach: Type 45 and contractual conditions

The Type 45 Anti-Warfare Destroyer is a large 7350-ton ship designed to provide fleet defence. Six platforms have already been contracted out of a total planned requirement of eight. This is the first fully-fledged development and production programme to implement an SDE following the approach laid out by the "687 family" of DEFCONs and DEFFORMs. Type 45 draws upon DEFFORM 687a, which places obligations on the prime contractor to create and manage a database of project

response to the controversial book by Nicholas Carr (Carr 2004) in which the author argues that IT' strategic importance has dissipated because of the wide availability of similar IT tools.

information and make it accessible to users, and DEFFORM 687b, which establishes a “database information agreement” that sets out mutual obligations for all parties accessing it. These forms include IP clauses establishing, *inter alia,* that uploading data into the database does not imply the granting and unauthorised use of any IPR, and an obligation on the contractor to grant a user license to the customer (MoD) to operate and maintain the database system once this is transferred from the contractor.

Although the responsibility for creating and managing the SDE can be vested in a third party, in this case it is the prime contractor, BAE SYSTEMS Electronics Limited,[15] who is in charge of setting up the SDE. This is one of the responsibilities of the “Prime Contract Office” (PCO), but it has involved other partners and stakeholders in the development of the system, such as:

- through the application of DEFFORMs that are themselves the result of a process of negotiation among the industry stakeholders and the MoD.
- the PCO drawing on the input from main stakeholders, which includes five main supplier firms and the programme client, the Defense Procurement Agency. All have access to the SDE through a dedicated Wide Area Network. Defining the SDE, its applications and management, and the user practices were collectively conducted through an “Enterprise Integration User Group,” comprising representatives of all the main stakeholders. This Group is responsible for overseeing the system implementation across stakeholders, and reviewing and updating the enterprise integration strategy. The resulting “Enterprise Integration Implementation Plan” affirms that IPR previously owned by a stakeholder will not “normally” be published in the SDE, and that, if it is, such “background IPR” will

[15] This has now been handed to BAE Systems Naval Ships.

be protected by access controls and made accessible only to the relevant stakeholders.

The Type 45 SDE is however limited in the extent of the applications and data exchanges it supports. The system carries extensive information on project management tasks, and provides a tool for sharing project information across all stakeholders. Yet the use of the system is limited to information that does not have a classification of “Confidential” or higher national security restriction, a common classification in defence projects (and in civil projects). Technical data published in the SDE includes mainly graphical representations of the “product geometry” and a “product model” that can be used to guide the evolving design within the collaborating firms. Detailed design data, however, as for instance the CAD files used for the design of the different elements are not shared through the SDE.

Despite these limitations the Type 45 SDE presents a new stage in the extent to which collaborative IT-based tools have been implemented to facilitate the collaborative development, production and operation of a complex product, and the management of stakeholders’ IP. The system has now been in place for almost five years, has become a key tool in the management of the programme.

Yet, notably the complexity inherent in setting SDEs is magnified when it involves international partners. For instance, participants in the Type 45 SDE pointed out that one of the reasons why the system operates with relative simplicity is that it is a *domestic* project and that no foreign suppliers may access the system, as international programmes, as noted above, need to deal with complex export control legislation and to accommodate different national regulations on issues like IPR and privacy. Given that Type 45’s SDE is relatively “smaller” size and national in character, it is questionable whether this type of SDE would be “scalable” for larger international projects. On the other hand, the JSF case discussed below provides an example of the challenges faced when international collaboration is organised around an SDE.

Prime-led approach: the case of JSF

As discussed above, LMA, prime contractor for the JSF system has set up an SDE using a number of available digital networking technologies. This is a mandated system, imposed as a condition for collaboration and in which the prime contractor, who manages and controls the SDE, defines and establishes its architecture and procedures. The JSF is the biggest weapon program in history ($276 billion).

The SDE revolves around a Joint Data Library (JDL) that serves as the node for technical data sharing across project participants. Ownership of data in the JDL is indicated by restrictive legends, which are included in the footer of all data and drawings. Access to the JDL is established through formal agreements, so-called Technical Assistance Agreements (TAAs) between LMA and its suppliers. TAAs specify the kind of data that can be accessed and used by the supplier and are complex to operate, particularly when they involve non-US suppliers. Often, several TAAs are signed with each supplier covering different sets of data for which the supplier acquires rights to upload and download. TAAs have to take into account existing US export control regulations and establish the relevant data access control accordingly when signing TAAs with foreign suppliers. On the one hand this has a positive effect: it deals with the nettlesome problem of export controls regulations. On the other hand, the system has become cumbersome to operate. For instance, a British firm participating in the programme has signed over 160 TAAs covering, among other things, different requirements relating to the export and re-export of the technical data in different components and sub-systems.

Furthermore, any data communication between two suppliers has to be approved by LMA, regardless of the TAAs signed between the two suppliers and the prime. Accordingly the JDL is partitioned: suppliers cannot access the project data of other suppliers, only LMA has access to all data and information in the JDL. Moreover, when a supplier is involved in different subsystems it will need to access different and separate folders under different TAAs. This means that different parts of a corporation working on other sections or aircraft sub-systems will not have access to each other's data sets within the JDL. Again this has positive and negative effects: each supplier has its own set of folders containing its own information, which acts as a means of IP protection, avoiding potential confusion as to what information belongs to whom. Yet, the system slows down collaboration across suppliers. If a company needs data from another supplier, it will have to request it from LMA, who will then "post" the information in a common folder available to both companies, after checking that the requested information is available and indicated on the TAAs signed by both companies. Even such controls have not prevented the JSF project from being beset by disputes between the UK and the US over the sharing of sensitive technology.

Finally, the management of the access control at individual level is even more awkward. Any supplier employee wishing to access JDL data will have to request permission from the prime contractor, who then manually checks whether the individual is covered by a TAA and what are the rights that this TAA establishes. Once this information is ascertained the prime contractor provides access to the relevant project folder or folders. Yet the onus is on the individual to ensure that the information or access rights it needs are listed on the relevant TAA. Participating companies have had to train the employees working on this system on the complex operating procedures by which it is regulated.

In an international SDE, the issue of export controls is commingled with that of IP for the simple reason that export-controlled items also contain an array of IP and IPR. In comparison, an SDE with domestic collaborators is less complicated, although as has been noted in the Type 45 case, an assortment of IT-based controls and procedures to manage the participants' IP has been instituted.

Managing IP in collaborative SDEs: some concluding thoughts

Despite the burgeoning literature on the technical development and implementation of IT applications to support business activities, there is a noticeable paucity of studies on how firms *actually* use IT to manage their IP and IPR. This article has analysed the IP issues that arise in inter-organisational collaborative projects using SDEs, extending as well the current literature on corporate management of IP, which has so far focused mainly on IP management *within* the firm.

Our study focused on two defence projects involving development and production of large weapon systems and identified two contrasting examples of the ways in which SDEs can be implemented in collaborative projects and IP managed within them. We have explored how these two models of SDE deal with the issues of IP protection, security, confidentiality, privacy, authenticity and integrity of data, and identity management for access control. We have also illustrated their shortcomings and have argued that the full potential of existing IT-based tools has not been under utilised for a catalogue of reasons, not least of which is a lack of effective corporate IP policy. So how can the scope of an SDE be extended so that the potential offered by IT to organise and co-ordinate complex design and engineering tasks across organisations is fully exploited, while minimising the risks of IP misappropriation and leakage? The problems that our study has unveiled suggest actions that can expand the scope and functionality of future SDEs.

The technical solution

As we have seen, an approach to prevent unauthorised data access is the data segmentation approach used in the JSF SDE. This approach diminishes the chances of data leakage but it can slow down collaboration among suppliers, is operationally cumbersome and could cause data replication across folders. Furthermore, data replication carries with it the risk of data fracture; that is, unless configured appropriately, the data in one folder could be updated without the same data being changed in another folder, thereby ending in two versions of the same document.

The alternative is to administer the system by tagging each data element with information including its origin, security, commercial confidentiality markings, and access restrictions, and then linking the access rights of individuals to the markings. This requires a parallel identity and access management system, in which all individuals must have proof of identity to log on to the system. Access will depend on the individual's organisation, role within the organisation and other factors, like nationality, which will bear on the definition of his or hers access privileges.

Such "data level" management system would allocate access rights automatically, thus eliminating the need for a manual management of access privileges. The technologies and procedures to set up such a system exist. Experts interviewed for this project believe that the technological capabilities to set up sophisticated SDEs based on "data level" access management have existed for some time. An example of this is the current work undertaken by the Transatlantic Collaboration Program (TCSP), an initiative of a group of US and UK firms to develop frameworks and detailed procedures to tackle security concerns and export control regulations in transatlantic arms collaboration programmes. The Program commissioned Booz Allen Hamilton to produce a Framework and a Design for building secure IT collaborative environments, including the required processes, mechanisms and technologies for collaborating partners (Booz Allen Hamilton 2004, 2003).

The TCSP system essentially departs from a centralized data library of the SDEs and moves toward a "federated trust structure" in which technical data is held by each collaborating partner. Access to such data by any partner is underpinned by a robst identity management system in which all project participants have a unique identity. The identity will be established through commonly agreed methods (between project collaborators and the customer) for proofing and vetting, before a credential is issued. This concept is now being tested by TCSP.

The managerial solution

The main challenge for the establishment of an SDE or a federated trust system is of a managerial nature. Specifically, an SDE able to deal adequately with IP issues has to rest on five key foundations:

(1) a commitment by participant companies to a corporate IP policy laying out guidelines and codes of practice on the treatment of corporate IP, including training of research personnel;

(2) a recognition that a corporate IP management policy entails integration of input from the IT, legal and commercial departments into its definition;

(3) a commitment to allocate the necessary resources for managing the SDE system throughout the collaborative partnership;

(4) an agreement on the ICT tools to monitor and track the information shared through the SDE;

(5) the establishment of procedures to ensure continual robustness, security and functionality of the SDE system to ensure that all IP is "appropriately respected."

Most of these foundations relate to non-technical issues. Our study revealed that commercial and IP managers were particularly concerned about those aspects of IP management that are more difficult to control through contractual or technical measures. Under these circumstances the lack of guidelines on the treatment of information assets can emerge as a barrier to the establishment of an SDE. Corporate-wide IP management policies and procedures can be seen as a precondition to the establishment of project-specific SDEs.

Furthermore, although technical approaches to deal with this problem exist, such as those described above,, there is a need for a corporate IP management policy to address training and raise awareness of the importance of blithe sharing of data. Equally importantly, a corporate policy has to consider instituting company wide processes and procedures for the treatment of company IP that is not formally protected and not focus mainly on formal protection mechanisms.

Moreover, as different SDEs are created for different projects, there is a possibility that in the future, the same company will be involved in several SDEs using different systems, contractual conditions and IP sharing rules. Such complexity also calls for better training of research personnel in the treatment and management of IP, lest it results in incoherent IP management practices, in much the same way that employee training in and buy-in of corporate IT investments is necessary to generate premium returns from such investments (Weill and Aral 2006). Therefore, training on IP management in digital collaborative environments needs to rise above its current project-by-project approach to an all encompassing corporate IP management policy with well articulated procedures and behavioural guidelines for the treatment of IP and information.

Our research revealed that an effective corporate IP management policy ideally should sit at the interface of IT strategy, commercial and contractual policies, and engineering and design practices. While it is necessary for commercial and legal personnel to “steer” the policy, it is the engineers and technical personnel who will, eventually, be responsible for their implementation. We found a tenuous interaction between these two groups of people. For instance, the Type 45 Enterprise Integration Plan establishes mechanisms to request the opinions of SDE users on the operation of the system. This is an example of a good management principle: such a policy provides an information channel between engineers using the SDE and those in charge of its management. Yet, despite following “good practice” Type 45 SDE falls short of bringing together engineering, IT personnel, commercial and legal communities in the *definition* of an IP management policy approach. It must be noted that in ensuring that IP is properly protected and used, and data access effectively controlled in an SDE, contractual obligations, IP practices and IT architecture are inevitably inextricably linked. This requires close collaboration between the commercial/legal and IT departments, and therefore needs to be led from the corporate executive level. Lapses in this collaboration would likely lead to an inadequate IP management policy.

In more general terms the establishment of inter-organisational networks needs to account for the legal and regulatory environment within which SDEs operate. As noted above, experts that had participated in the development and, now, operation of the Type 45 SDE believed that its implementation had been made easier because of the national character of the programme. An international project would be much more difficult to manage and would probably result in more modest functionality or require a larger suite of software-based applications and procedures, and more complex configuration, which have been discussed. In particular, the requirements imposed by export control regulations will affect the architecture of an international SDE. It is important to note that these constraints are not unique to defence projects; many high technology programmes will deal with controlled technologies and will be subject to the same constraints regardless of their military or civilian character. The influence of regulatory constraints on the nature and structure of SDEs is crucial although it is often overlooked in the literature on inter-organisational networks.

In sum, we draw from our study two central themes. First, in this knowledge economy in which globalization of multiple business operations including R&D is a growing trend which greatly emphasises collaboration, the management of IP has moved deeper into the centre stage. As companies extend their enterprise outwards to third party access, such as suppliers, the line between the internal and external network becomes fuzzy, and securing the network and the information it is designed to hold and transmit from a plethora of users becomes correspondingly more difficult.

Second, advances in IT and networking technologies allow the materialization of interactive and flexible management practices, design and production, and distribution processes. Such technologies offer the opportunity to share costs and risks, but as we have seen, there is a real potential of knowledge-loss. Hence the way that executives manage and respond to IT’s transforming role will much determine the benefits that they may reap from IT and IT-enabled collaboration (Carr 2004). We have argued that the nature of the IP management challenges posed by the implementation of SDEs requires the commitment and support at the corporate executive level. Yet, we found that IT implementations are viewed by project directors as additional costs rather than investment for the future, as it is often difficult to attribute specific monetary benefits to the introduction of these technologies. When in 1995 one of us carried out a study on the diffusion of CALS principles in the UK, an expert in a major firm stated that the industry displayed “a file transfer rather than an open database mindset” (*****, 1996).

This state of affairs appears to continue today. Not because it is impossible to protect IP within collaborative IT networks or there are technical difficulties in establishing such open database architectures. The procedures and underlying technologies to establish the networks and protect IP exist. Their slow diffusion could be ascribed to the detachment with which corporate executives deal with the details of IT systems. A clearly defined corporate IP management strategy, countenanced by input from the commercial, IP and IT functions is instrumental for effective and successful IP management throughout the organisation, within and beyond SDEs, regardless of the sector.

References

Argyres, N. S. 1999. The impact of information technology on coordination: Evidence from the B-2 "Stealth" bomber. *Organization Science* 10 (2):162-180.

Arora, Ashish, Andrea Fosfuri, and Alfonso Gambardella. 2000. Markets for Technology and their Implications for Corporate Strategy.

ASIS International, PricewaterhouseCoopers, and American Chamber of Commerce. 2002. Trends in Proprietary Information Loss. Survey Report. Alexandria, VA: ASIS International.

Booz Allen Hamilton. 2003. A Framework for Secure Collaboration across US/UK Defense: UK Council for Electronic Business.

———. 2004. Transatlantic Secure Collaboration Program (TSCP). How-To-Guide: UK Council for Electronic Business.

Buigues, Pierre, Alexis Jacquemin, and Jean-Francois Marchipont, eds. 2000. *Competitiveness and the Value of Intangible Assets*. Cheltenham: Edward Elgar.

Business Wire. 2005. *Intellectual Property Still Remains a Huge Difficulty for US Companies* 2005 [cited November 28 2005]. Available from http://uk.biz.yahoo.com/051111/183/fwo5j.html.

Carr, Nicholas G. 2004. *Does IT Matter: Information Technology andthe Corrosion of Competitive Advantage*. Boston, MA: Harvard Business School.

Chesbrough, H. 2003. The logic of open innovation: Managing Intellectual Property. *California Management Review* 45 (3):33-58.

Davenport, Thomas H, and Laurence Prusak. 1998. *Working Knowledge: How Organizations Manage What They Know*. Boston: Harvard Business School Press.

Davis, Lee. 2004. Intellectual Property Rights: Strategy and Policy. *Economics of Innovation and New Technology* 13 (5):399-416.

Donnington, Jerrold. 1995. *Electronic Data Interchange in the Automotive Industry. Managing information flows for greater profitability*, *Financial Times Management Reports*. London: Pearson Professional.

Gholz, Eugene. 2003. Systems Integration in the US Defense Industry. In *The Business of Systems Integration*, edited by A. Prencipe, A. Davies and M. Hobday. Oxford: Oxford University Press.

Granstrand, O. 2004. The economics and management of technology trade: towards a pro-licensing era? *International Journal of Technology Management* 27 (2-3):209-240.

Grindley, Peter C, and David J Teece. 1997. Managing Intellectual Capital: Licensing and Cross-licensing semiconductors and electronics. *California Management Review* 39 (2):8-41.

Guilhon, B., R. Attia, and R. Rizoulieres. 2004. Markets for technology and firms' strategies: the case of the semiconductor industry. *International Journal of Technology Management* 27 (2-3):123-142.

Hall, Bronwyn H, and Rosemarie Ham Ziedonis. 2001. The Patent Paradox Revisited: An Empirical Study of Patenting in the U.S. Semiconductor Industry, 1979-1995. *Rand Journal of Economics* 20 (1):101-128.

Lyons, John. 2004. Internet Investigations - International Standards and Co-operation. Paper read at UN/ECE Advisory Group for the Protection and Implementation of Intellectual Property Rights for Investment, 1-2 April, at Warsaw.

MacNeil, Ian R. 1980. *The social contract*. London: Yale University Press.

———. 1999. Relational Contract Theory: Challenges and Queries. *Northwestern University Law Review* 94 (3):877-907.

McAfee, Andrew P. 2006. Enterprise 2.0: The Dawn of Emergent Collaboration. *Sloan Management Review* 47 (3, Spring):21-28.

Ministry of Defence. July 2004. *Guidelines for Industry. 10 The Intellectual Property Rights (IPR) DEFCONs. Part B*. Defence Procurement Agency 2004 [cited July 2004]. Available from http://www.ams.mod.uk/ams/content/docs/toolkit/ams/policy/gfi/sect10_part_b.htm.

Ministry of Defence Smart Procurement Implementation Team. 1999. *The Acquisition Handbook. A guide to Smart Procurement "Faster, Cheaper, Better"*. First ed. Bristol.

Nonaka, I, and H Takeuchi. 1995. *The Knowledge-Creating Company*. Oxford: Oxford University Press.

Nunan, J. 2004. Strategy? What strategy? *Copyright World* (146):9-10.

Parise, S., R. Cross, and T. H. Davenport. 2006. Strategies for Preventing Knowledge Loss Crisis. *Sloan Management Review* 49 (4):31-38.

Quinn, J B. 1992. *Intelligent Enterprise*. New York: Free Press.

Reitzig, Markus. 2004. Strategic Management of Intellectual Property. *Sloan Management Review* (Spring):35-39.

Rivette, Kevin, and David Kline. 2000. Discovering New Value in Intllectual Property. *Harvard Business Review* 78 (1):59-64.

Ruggles, Rudy, and Dan Holtshouse. 1999. *The Knowledge Advantage*. Oxford: Capstone Publishing.

Shapiro, Carl. *Navigating the Patent Thicket: Cross-Licenses, Patent Pools and Standard Setting* 2001 [cited. Available from http://faculty.haas.berkeley/edu/shapiro/thicket.pdf.

Shapiro, Carl, and Hal Varian. 1999. *Information Rules: A Strategic Guide to the Network Economy*. Boston, Ma: Harvard Business School Press.

Spinardi, Graham, Ian Graham, and Robin Williams. 1995. Technical data interchange in the Eurofighter project. *Science and Public Policy* 22 (1):29-38.

Tait, Nikki. 2004. 'Alarming' findings on intellectual property. *Financial Times*, 2004, 5.

Tang, Puay. 1998. How electronic publishers are protecting against piracy: Doubts about technical systems of protection. *The Information Society* 14 (1):19-31.

Tang, Puay, and Dan Paré. 2003. Gathering the Foam: Are Business Method Patents a Deterrent to Software Innovation and Commercialization? *International Review of Law Computers & Technology* 17 (2):127-162.

Teece, David J. 1998. Capturing Value from Knowledge Assets: The New Economy, Markets for Know-How and Intangible Assets. *California Management Review* 40 (No. 3):55-79.

Teece, David J, G Pisano, and A Shuen. 1997. Dynamic capabilities and strategic management. *Strategic Management Journal* 18:509-533.

Volkoff, O., Y. E. Chan, and E. F. P. Newson. 1999. Leading the development and implementation of collaborative interorganizational systems. *Information & Management* 35 (2):63-75.

Weil, Vivian, and John H. Snapper. 1989. *Owning Scientific and Technical Information. Value and Ethical Issues*. New Brunswick and London: Rutgers University Press.

Weill, Peter, and Sinan Aral. 2006. Generating Premium Returns on Your IT Investments. *Sloan Management Review* Winter 47 (2):39-48.