SEWPS

SPRU Electronic Working Paper Series

Paper No. 130

Intellectual Property and Inter-organizational Collaborative Networks: Navigating the Maze

Puay Tang and Jordi Molas-Gallart
(SPRU)

February 2005

SPRU Science and Technology Policy Research

The Freeman Centre, University of Sussex,
Falmer, Brighton BN1 9QE, UK
Tel: +44 (0) 1273 877078
E-mail: p.tang@sussex.ac.uk
http://www.sussex.ac.uk/spru/

Intellectual Property and Inter-organizational collaborative networks: navigating the maze

February 2005

Puay Tang and Jordi Molas-Gallart

Abstract

Intellectual Property (IP) is a key intangible asset influencing corporate performance and its management is increasingly recognized as a central element of corporate strategy. This article is concerned with the management of IP in *inter-firm collaborative* projects mediated through the use of advanced IT tools. Here, groups of firms, often competitors, and sometimes their customer organizations, collaborate in the design, development, manufacture and maintenance of complex products, exchanging large amounts of proprietary technical data through IT tools. How can organizations exploit the capabilities offered by these tools without increasing the vulnerability of IP assets to misappropriation, unauthorized use or leakage? We explore the case of the UK defence market, where an extensive set of formal contractual tools is being developed to support IP management in collaborative projects. Through an in-depth study of IP management practice in UK defence projects we analyse the extent to which contractual tools can combine with technical solutions to provide answers to the problems posed by IP management in complex, long-term collaborative projects. We conclude that contractual and technical tools must be underpinned by managerial changes bringing together functions that remain separated in most large corporations: Information Technology management, legal and commercial departments.

Keywords

Intellectual Property management; Information Technology; Shared Data Environments; inter-organisational networks; defence sector; collaborative projects. IPR.

Intellectual Property and Inter-organizational collaborative networks: navigating the maze[1]

Introduction

Until recently, the management of Intellectual Property (IP) and its associated Rights (IPR – formally protected IP) was treated as a specialized 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 deal with patents and other forms of formal IP protection as needed. Similarly, IT (Information Technology) managers who dealt with corporate systems for data access control rarely consulted with the legal or commercial departments on IP issues such as the potential data leakage inherent in the treatment and transfer of electronic data. 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 (Teece, Pisano, and Shuen 1997; Teece 1998; Ruggles and Holtshouse 1999; Shapiro and Varian 1999; Reitzig 2004). IP is now seen as a strategic intangible asset influencing corporate performance (Buigues, Jacquemin, and Marchipont 2000; Nonaka and Takeuchi 1995; Quinn 1992; Davenport and Prusak 1998).

Important as IP is for the modern corporation, scholars have found it a difficult concept to define accurately.[2] The American Heritage Dictionary defines IP as a product of the intellect that has commercial value. The Oxford English Dictionary defines it as property which is the product of invention or creativity, and which does not exist in a tangible physical form. In short, IP refers to intangibles that are commercially valuable. 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 use of IT and electronic networks increases the risk of all these forms of IP to misappropriation or leakage, inadvertent or otherwise.

As the recognition of the commercial value of IP deepens, its protection becomes an increasingly important managerial challenge. Simultaneously, data replication and transmission is becoming easier thanks to rapid development in IT, thus augmenting the risk of data conveying valuable IP leaking to competitors. A US survey estimated that between $53 and $59 billion were lost to 138 responding firms through incidents in which proprietary information was disclosed. Over two thirds of the firms surveyed "strongly agreed" with the statement "The Internet, networks, computers and related technologies have created significant new threats to sensitive proprietary information." This potential threat emerged clearly as the most important source of concern, particularly among large companies (ASIS International, PricewaterhouseCoopers, and American Chamber of Commerce 2002). Similarly, a 2004 survey of 203 companies conducted by the UK National High Tech Crime Unit, reported that 12 per cent of the firms had experienced instances of data theft through the Internet, causing losses amounting to approximately £7 billion (Lyons 2004). Such realization of the risks posed by the growing use of electronic data networks suggests the need for specialized IP and information management strategies addressing 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). The problems and challenges faced are, however, 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 organizations 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 advanced IT tools. The resulting "Shared Digital Environments" (SDEs) involve electronic networks, software platforms, and electronic data management systems used by project partners to manage and share technical data. SDEs are being proposed as a tool to assist large design, engineering and manufacturing projects in a wide variety of sectors, for reasons of efficiency and improved project management, among others. The management of IP in SDEs poses problems that are different in nature and scope to those of IP management within the firm.

This article analyzes the nature of the problems posed by IP management in SDEs and discusses a range of approaches to their solution. Our main concern is the management of information and data whose disclosure or unauthorized use can generate a loss of commercial advantage to its owner. Although, strictly speaking not all IP falls within this category,[1] we retain the use of the term IP for convenience, as it is the term 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

[1] Some IP, like brands and designs, need to be "disclosed" to be of commercial value.

contractual conditions for the management of IP in SDEs. This situation provides a unique test bed for analyzing the impact of formal regulations and processes on the management of IP, and the challenges faced when explicitly addressing IP management issues in inter-organizational networks and systems. Further, existing MoD procurement policies emphasize the use of inter-organizational IT networks to improve project performance. A context of detailed IP regulations is thus set against an effort to develop and implement large SDEs.

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 analyze 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 Ministry of Defence (MoD). This choice is justifiable and does not limit the relevance of our study to the UK defence industries. 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). This situation provides a unique test bed for analyzing the impact of formal regulations and processes on the management of IPR. Further, the “Smart Acquisition” initiative

launched by the UK MoD emphasizes the use of e-commerce and advanced IT to improve project performance. A catalogue of detailed IPR regulations is thus set against an effort to develop and implement sophisticated IT systems in support of product development, manufacture and maintenance. The experience that the UK defence sector is developing is significant for other sectors. Although there are unique aspects to the regulatory environment of the defence sector, there is nothing inherently unique 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. It could be argued that the IP environment in which defence customer agencies and their industrial suppliers operate is characterized 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. In particular, we have explored elsewhere the mistrust between defence suppliers and the MoD generated by the way in which IPR have been handled in the privatization process of the British defence research establishments (Molas-Gallart and Tang 2004). The UK defence sector is therefore becoming more open and akin to other commercial environments where trust between suppliers and clients is either lacking or fragile.

The first step in our study was 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 programmes.

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). 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.

We then carried out interviews with all major UK defence systems producers. Between November 2003 and July 2004 we conducted detailed interviews with 20 relevant executives; involving IP Directors, Commercial executives, IT systems directors, programme directors and lead engineers. In addition, we held several meetings with other officials from industry, the DPA and a defence industrial association. In total we carried out 66 hours of meetings and interviews with 33 senior officials and executives. Except for six telephone interviews, the rest were all face-to-face interviews and meetings carried out by both of us.

Within each participating company most of the interviewees were self-selected by their organizations based on their work on IP management and IPR issues both within

the company, and in collaborative projects and defence contracts. Because of the commercial sensitivity of the issues explored we will not attribute the information collected and used in this article to any name and affiliation of the individuals interviewed.

The case: Managing IP in the UK defence market

All the firms and organizations involved in this study are simultaneously using different network technologies and inter-organizational systems (Volkoff, Chan, and Newson 1999).[3] These are usually for large complex projects involving a number of suppliers, coordinated through a prime contractor, to provide a system 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 organization, final users and industrial producers, and play a complex interface role between suppliers, the MoD client and military users. From an MoD perspective the IPT is seen as its internal "supplier," in charge of delivering a system to frontline users. From the industry perspective the IPT plays the role of customer. Each IPT has a "Leader" who is the line manager for most core members of the IPT, and the formal point of contact with the MoD representative (final customer), and is responsible for meeting the agreed cost, and performance targets and milestones.

In the British approach, IPTs are the key organizational mechanism for the management of defence procurement projects, and an avenue to facilitate constant communication among all main project stakeholders throughout the project's life cycle, from conception, through research and development, production, operation,

maintenance and upgrading and, ultimately disposal. In practice, every project establishes its own set of network technologies and inter-organizational systems, and its contractual conditions and procedures. The responsibility rests on the IPT and ultimately on its Leader: 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 of the firms interviewed 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. Such a situation engenders not only additional costs but also a situation in which it is difficult to control and monitor the information flows through the variety of inter-organizational 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: it is common for large firms, including those in this study, to employ patent attorneys, copyright specialists, etc. within an IP department. 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. A corporate IPR audit could reveal where formally protected IP is yielding direct economic

benefits, both 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 which parts of its IP are valuable. Second, enforcement practices and monitoring of infringement could also be part of company-wide processes and procedures for the treatment and use of corporate IP, *whether they be formally protected or not*.

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.[4] 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 information;

not only technical data about specific components, but also 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, the concern for contractors relates to the possibility that, through an SDE, the customer may access data that is still being worked upon. First, work-in-progress foreground information may include commercially sensitive information on company techniques and processes that will not be included in the final data packs delivered to the customer. Not all information in the foreground information is necessarily funded by the MoD as it could be privately ventured, a situation which is not uncommon in defence projects. 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 for delivery to the customer or as noted above, not to be used by the customer.

SDEs generate concerns in relation to both of these problems. 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 approaches exist or have been suggested for strict data access control, there is a palpable fear among the staff responsible for IP policy 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 that were 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 organizational divides, much in the same way that academics are widely known to do. Although most of the anecdotes involved instances in which such exchanges were not 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 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-organizational 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 specialized 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 IP invariably would come under export control considerations. Collaborating companies have to ensure that data mounted in an SDE does 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 sub-optimal level.[5]

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

The responses

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

1. the definition of codified procedures to enable the assured 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-organizational 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 areas or 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 that follows from the collaboration of diverse partners in the development and production of large complex systems through the inclusion of detailed contractual provisions. In the UK, 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 to the letter the text within 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 and its use is recommended whenever the contracted work is likely to generate 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 contractual team to decide which DEFCONs to include and whether or not to modify them.

While some DEFCONs are relatively straightforward and are applauded by the defence companies for their necessity, 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, many defence systems are used for long periods, extending over three or more decades during which they will be subjected to several planned and unplanned upgrades and changes, for instance, the customer may require improvements in system capabilities to meet new challenges. Managing these complex systems over such long periods of time gives rise to difficult IP problems.

We can distinguish two main sets of difficulties.

First, when there are several units of such systems operating side-by-side (for instance, a squadron of fighter aircraft), it is common that the individual system will have slightly different configurations although they may be formally identified as 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, as well as the components that, being part of the initial system, have been superseded by new ones. 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. [6]

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 be the result of private investment, that is not funded by the MoD. They are therefore anxious not "to give away" data that could be and is likely to be commercially sensitive, particularly if the support and maintenance of the system is not to be undertaken by the prime contractor, but by a third party.

Furthermore, there is a cost to the provision of a data manufacturing pack that the DEFCON does not appear to contemplate. As product components and subsystems are constantly updated, keeping a manufacturing data pack updated entails refreshing

the data over the life cycle of the system to take account of the changes introduced by the prime contractor *and* its supply chain. This cost, coupled with the IP problem addressed above, does not appear to be thoroughly recognized by the MoD, according to the interviewed companies.

The preceding examples show some emerging tensions in the application of IP conditions by the UK MoD. The root of the problem here is that it is almost impossible to foresee and track all the contributions, changes, and new requirements that will take place during a complex system's long life. Nonetheless, there was a consensus among our interviewees, shared by the responsible officials at the DPA, 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.

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 as well as user rights and obligations. DEFFORM 687c was finalized in 2001, after about 18 months of 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, who formally endorse their use. Yet despite their genesis and wide support basis "Type 45" (more below) is the only fully-fledged development and production programme to implement some of the contractual tools in the "687 family."

UK defence prime contractors see the use of 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.

To sum up, the relationship between the UK defence customer and its suppliers when dealing with the development of a contractual system to deal with IP management issues is in a state of dynamic tension and one characterized by a mixture of collaboration and conflict. A continually evolving defence procurement policy, which, in turn, is driving changes in the content and application of contractual conditions, is perceptibly stirring up tensions within the main defence contractors. 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-organizational systems

The technological foundations and the strategic rationale to deploy IT systems enabling the sharing of technical data information and collaborative working across geographically dispersed sites have been in place for some time. From the early 1990s communities of practice 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 developing guiding principles and associated standard and technology developing activities aiming 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.[7] During the 1990s, the civilian Boeing 777 became the best-publicized case of collaborative design and production across different locations for an aircraft system. Not only was this example heralded as an innovative programme for its team management approaches, but was also lauded for representing the first use of digital computers to design and electronically pre-assemble an entire plane.[8] Further, joint design was achieved 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 centralized product database available online to project partners under various access control conditions, 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 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 contractor 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 project participants' "design deadlines," for instance, to be delayed 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.

In practice, the diffusion of SDEs using centralized 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 in which an SDE is being used.

In Type 45 the prime contractor (who is not the leading manufacturer but is the systems integrator) is responsible for setting up a centralized product database system to which all project collaborators can have access, and to organize 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. Yet there is a need to tailor the combination of off-the-shelf software technologies and Internet access to the specific needs of each complex project. As we will see in the cases in the next section this still represents a difficult challenge for which no ready-made solution exists and that can be addressed using different implementation models (more below).

Training

The third response to the problems arising from the management of IP in collaborative projects is the need to inculcate in the engineering personnel a staunch sense of the importance of corporate IP. As noted above, all the firms interviewed expressed concern about the allegedly casual attitude of engineers towards the protection of company IP. The ease by which data can be transferred electronically makes this concern more pressing, especially as the Internet is conventionally regarded as one giant copying machine. To combat this laissez-faire attitude toward the appropriate treatment of corporate IP, some companies have issued guidelines about sharing data across companies, warning employees about inappropriate sharing of data. Penalties for misappropriation of data can include dismissal, fines and even 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 IP management policy. 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.

Two implementation models

As already discussed above, we found few defence programmes with British participation in which an SDE system has been put in place. Here we show that the two main cases responded with dissimilar implementation models. They are different in the way the two major constituents of an SDE solution as discussed in the previous section (the contractual framework and inter-organizational systems) are defined and combined. We can distinguish them accordingly:

1. A "*regulated approach*" as applied in UK contracts using elements of the 687 series of DEFCONs and DEFFORMs. These contractual conditions were defined by a group of experts from defence suppliers and the DPA and relate to the way in which the SDE will work.
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-organizational 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 defence contractual conditions (DEFCONs) and forms (DEFFORMs). Type 45 draws upon DEFFORM 687a, which places obligations on the prime contractor to create, and manage a database of project 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 unauthorized 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, 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:

- through the application of DEFFORMs that are themselves the result of a process of negotiation among many industry stakeholders and Government.
- the PCO has drawn on the input from main stakeholders, which include five main supplier firms and the programme client, the Defence Procurement Agency. These six organizations, which have access to the SDE through a dedicated Wide Area Network, were involved in defining the SDE, its applications and management, and the user practices. This process is conducted through an "Enterprise Integration User Group," which comprises representatives of all the main stakeholders, who 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 be protected by access controls and made accessible only to the required 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 several participating firms and the client representatives. Yet the use of the system is limited to information that does not have a classification of “Confidential” or higher national security restriction, a classification of which is not unusual in defence projects. Technical data published in the SDE includes graphical representations of the “product geometry” and results in a “product model” that can be used to guide the evolving design within the collaborating firms. However, detailed design data, 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 tools based on IT have been implemented to facilitate the collaboration across organizations involved in the 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, and is delivering the services to the PCO and its client.

It must be noted that 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. The main reasons for the added complexity when dealing with international programmes, as noted above, are the need to deal with complex export control legislation and to accommodate different national regulations on issues like IPR and privacy. The JSF case discussed below provides an example of the challenges faced when international collaboration is organized 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. For the suppliers 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 architecture and procedures.

The SDE revolves around a Joint Data Library (JDL) that serves as the node for the sharing of technical data across project participants. Ownership of data in the JDL is indicated by restrictive agreed 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 provide the formal approval mechanism enabling stakeholders to post and access data in the SDE and specify the kind of data that can be accessed and used by the supplier. TAAs have become a very complex tool to operate, particularly when they involve foreign (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. In particular, when the suppliers are foreign nationals such TAAs have to take into account existing US export control regulations and establish the relevant data access control accordingly. On the one hand this has a positive effect: as access

to the JDL requires a TAA it therefore takes into account export control regulations. Data accessible by a partner through the JDL is, in practice, approved for transfer abroad in accordance with existing US export control 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 the prime contractor, 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 as prime contractor has access to all data and information in the JDL. Further, when a supplier is involved in different subsystems it will 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. On the one hand, 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. On the other hand, the system slows down collaboration across suppliers. If a company needs data from another supplier, it will have to request it from the prime contractor, 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.

Last but not least, the management of the access control at individual level is even more cumbersome. 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.

Summary

The need-to-know data access controls, the TAAs and the physical checking by the prime contractor for releasing information and data to each project participant, and the segmented folder structure in the JSF SDE represent the collective means for managing the IP of participating collaborators. Unwieldy as they may appear to be, it becomes apparent that in international collaborative projects, the issues of export controls and IP are co-mingled and that an SDE to support such collaboration will need to consider these dimensions, bearing in mind that export-controlled items also contain an array of IP and IPR. These considerations return us to the observation that an international collaborative SDE will be complex, but one whose difficulties may not be insurmountable. In this, however, apart from the construction of a robust IT system, the procurement authorities may jointly need to "harmonize" their treatment of IP used in and resulting from the collaborative project. Alternatively, industry can also try to establish guidelines for the management of future joint projects. An example of this is the Transatlantic Collaboration Program, an initiative of a group of US and UK firms to develop frameworks for secure transatlantic collaboration. The Program commissioned Booz Allen Hamilton to produce a Framework and then a Design for building secure IT collaborative environments, including the required

processes, mechanisms and technologies for collaborating partners (Booz Allen Hamilton 2004, 2003).

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. However, given its relatively "smaller" size and national character, it is questionable whether this type of SDE would be "scalable" for larger international projects.

Managing IP in collaborative SDEs: some lessons

Despite the burgeoning literature on the development and implementation of IT applications to support business activities, there is a noticeable paucity of studies on how firms use IT to manage their IP. This article has analyzed the IP issues that arise in inter-organizational 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 defence projects typically involving the development and production of large weapon systems that consist of thousands of components and sub-systems delivered by large supplier networks. This environment increases the complexity of managing IP and of setting up an SDE affording protection, security, confidentiality, privacy, authenticity and integrity of data, and identity management for access control.

The two cases we have discussed present two contrasting examples of the ways in which SDEs can be implemented in collaborative projects and IP managed within them.

- JSF represents a more complex programme as it involves a large supplier network distributed across several countries. Its SDE is led, top-down, by the prime contractor; for the British suppliers participation in the SDE is more of a contractual imposition from their client than a tool to help them in their tasks. They have had no participation in the definition of the system, taking as a given the conditions for participation. The SDE provides an avenue for communication with the prime contractor (LMA), but communication with other suppliers through the SDE has to be explicitly allowed by the prime.
- In comparison Type 45 has a much smaller number of partners (only six directly linked to the Wide Area Network), all of them located in Britain. In comparison with the JSF's hierarchical structure, the Type 45 SDE has developed a more collaborative environment, although responsibility for the SDE design and management remains with the prime contractor.

The restricted nature of the JSF SDE reduces the chances for leakage of IP through the electronic network and simplifies the IP management process. In the Type 45 SDE the threat of leakage is minimized as only information generated by the project (foreground information) is shared while background IP is kept outside the SDE.

So how can the scope of an SDE be extended so that the potential offered by IT to organize and co-ordinate complex design and engineering tasks across organizations is fully exploited, while minimizing 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.

As we have seen, an approach to prevent unauthorized data access is the data segmentation approach used in the JSF SDE. Each participating organization has

access only to its own set of folders and any request for data from another supplier needs to be requested from the prime contractor. This approach diminishes the chances of data leakage but, as discussed, 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 organization, role within the organization and any other factors, like nationality, with a bearing 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. For instance, proposals have been put forward establishing detailed procedures to tackle security concerns and export control regulations in transatlantic arms collaboration programmes. Further, 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.

However, as we have seen, present implementations have established modest objectives for themselves and operate at levels of functionality lower than those

allowed by existing technologies. The main challenge for the establishment of an SDE is of a managerial nature, a point that has also been highlighted in discussions on information security (Dutta and McCrohan 2002; Ernst & Young 2004). 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 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.

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. For instance, disquiet was evident among all firms interviewed about the way in which engineers and designers were believed to be treating the information they were working on and the results of their work. Almost all interviewees worried that engineers did not fully appreciate the value of IP and were ready to share all types of technical data and information with their colleagues in other firms. The capacity to copy and transmit data afforded by IT amplified the ability of careless employees to transfer commercially sensitive data outside the firm. 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 the incorporation of “data level” access management controls to prevent unauthorized access, there is a need for a corporate IP management policy to address training and raise awareness of the importance of blithe sharing of data. A corporate policy needs also to consider company wide processes and procedures for the treatment of company IP that is not formally protected, and not focus on the protection mechanisms themselves, for instance, to patent or to keep a particular IP a trade secret.

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 result in incoherent IP management practices. Therefore, training on IP management in digital collaborative environments needs to rise above its current project-by-project approach. A corporate IP management policy should systematically address these issues and establish procedures and behavioural guidelines with respect to the treatment of IP and information.

Importantly, a corporate IP management policy sits 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 have often found the interaction tenuous 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 must be 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-organizational networks needs to account for the legal and regulatory environment within which SDEs operate. 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 more complex configuration.

The requirements imposed by export control regulations will also 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-organizational networks.

In sum, our study has 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” (Molas-Gallart 1996).

This state of affairs appears to continue today. We cannot ascribe this situation to the impossibility of protecting IP management within collaborative IT networks neither can we attribute it to technological difficulties in establishing open database architectures to underpin collaboration. 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 to be used in specific projects. A clearly defined corporate IP strategy, therefore, is instrumental for effective and successful IP management throughout the organization, within and beyond SDEs, regardless of the sector. Importantly, to bring together the commercial, IP and IT functions within the company and across the different partners in a collaborative project, and to support the establishment of “shared data environments”, so that the corporate IP strategy can ably function within and beyond collaborative projects, requires a strong executive drive.

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.

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 Defence: UK Council for Electronic Business.

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

Buigues, P., A. Jacquemin, and J-F. Marchipont, eds. 2000. *Competitiveness and the Value of Intangible Assets*. Cheltenham: Edward Elgar.

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

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

Dutta, A., and K. McCrohan. 2002. Management's role in information security in a cyber economy. *California Management Review* 45 (1):67-87.

Ernst & Young. 2004. Global Information Security Survey 2004: Ernst & Young.

Gholz, E. 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, pp. 279-306.

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, P. C., and D. 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, B. H., and R. H. 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, J. 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, I. R. 1980. *The Social Contract*. London: Yale University Press.

———. 1999. Relational contract theory: Challenges and queries. *Northwestern University Law Review* 94 (3):877-907.

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.
Molas-Gallart, J. 1996. Telematics in life-cycle management. International Conference on Management and New Technologies. Madrid.
Molas-Gallart, J., and P. Tang. 2004. Privatisation and the management of Intellectual Property Rights: the case of British defence research establishments. Paper read at J.K. Galbraith International Symposium, 21-25 September, at Paris.
Nonaka, I., and H. Takeuchi. 1995. *The Knowledge-Creating Company*. Oxford: Oxford University Press.
Nunan, J. 2004. Strategy? What strategy? *Copyright World* 146 (December 2004/January 2005):9-10.
Quinn, J. B. 1992. *Intelligent Enterprise*. New York: Free Press.
Reitzig, M. 2004. Strategic management of Intellectual Property. *Sloan Management Review* 45 (Spring):35-39.
Ruggles, R., and D. Holtshouse. 1999. *The Knowledge Advantage*. Oxford: Capstone Publishing.
Shapiro, C. S. *Navigating the Patent Thicket: Cross Licenses, Patent Pools and Standard Setting* 2001 [cited. Available from http://faculty.haas.berkeley/edu/shapiro/thicket.pdf.
Shapiro, C., and H. Varian. 1999. *Information Rules: A Strategic Guide to the Network Economy*. Boston, MA: Harvard Business School Press.
Spinardi, G., I. Graham, and R. Williams. 1995. Technical data interchange in the Eurofighter project. *Science and Public Policy* 22 (1):29-38.
Tait, N. 2004. 'Alarming' findings on Intellectual Property. *Financial Times*, 2004, 5.
Tang, P. 1998. How electronic publishers are protecting against piracy: Doubts about technical systems of protection. *The Information Society* 14 (1):19-31.
Tang, P., and D. 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, D. 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, D. 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, V., and J. H. Snapper. 1989. *Owning Scientific and Technical Information. Value and Ethical Issues*. New Brunswick and London: Rutgers University Press.

---

[1] The research for this paper has been jointly funded by the UK Economic Social Research Council "E-Society Programme", and the UK Ministry of Defence under the Joint Grants Scheme (ESRC Award Reference RES-335-25-0017). Authors gratefully acknowledge the comments of the executives of the

defence companies interviewed, Prof. J. Adams and Robert Shields. Responsibility for errors is solely ours.

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

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

[4] 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.

[5] 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.

[6] 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 defence contracting, however, has tended towards the detailed specification of conditions and deliverables trying to cover for all possible eventualities.

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

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