Multinational Enterprises’ Governance Frameworks

*The Normative Fight against CyberCrime*

Paul Marc Collins

Georgia Tech Center for International Business Education and Research
Working Paper 008-07/08
http://www.ciber.gatech.edu
For further information: email: ciber@mgt.gatech.edu

October 2006

(c) 2006
Introduction

One of the most striking phenomena of the past decade has been the internationalisation of service firms (Tersen and Bricout, 1996). Previously considered “un-exportable” (Segal-Horn, 1993), they have proven day after day that they have the necessary characteristics to undertake an international development, and even a globalization of their offering systems (Vandermerwe, 1989; Campbell and Verbeke, 1994; Gadrey, 1994;). Retail banking and financial services are remarkable illustrations of this phenomenon (Michalet, 1985; Andreff, 1995). And bank cards in the first place. However, management scholars have been slow in reacting to this challenge. Focused on industry (and surprisingly enough on the automotive industry), the scholars have rather neglected the emerging field of international service firms. This Research gap has motivated our project on the international deployment of services. The field study we have selected is relative to the bank card organizations. This industry illustrates the functioning of service firms as political institutions. A striking example relates to the emergence and development of international standards bodies, specifically in the area of Internet payments. We are faced here with the construction of a transnational regulation.

The detailed case study we present and interpret is the SET scheme of Internet security and its localizations in multiple countries of operation. Interoperability is questioned in the context of industry globalization. The role and behaviour of transnational agencies such as Cybercomm are scrutinized. One of the originalities of our paper lies also in its epistemology and methodology. After a phase of interpretation of case data through the translation theory (Callon, 1986; Latour, 1989; Czarniawska, 1996; Sahlin-Andersson, 1996), we undertake a step of “framework” construction (Porter, 1991; Claveau, Martinet and Tannery, 1998; Folger and Turillo, 1999; Tsoukas, 1996), in order to
offer managers an “ex ante” strategic decision tool. The translation school seems to offer a sensitivity for hybrid methodology (content and process), very useful for the analysis of transnational firms. The introduction of the notion of “actant non humain”, the technical objects which build socio-technical networks, has enormous potential in management science. This concept includes all the stakeholders of transnational networks of standardization.

We have then started with the interpretation of case data with translation theory concepts. We present detailed case studies in the area of transnational bankcard networks. For example a coalition between banks to create a de facto standard for transnational electronic payment security on the Internet. The case study is eye-opening. After a step of protecting its political interests and well-known technological solutions, the coalition understands that its mission becomes a matter of life and death for its members: brand new currency has been invented on the Web and one could develop business and monetary transactions without the banks!

This interpretative stage, while broadening our horizon and the relevance of our observations, has taught us much on the transnational mechanisms of regulation and standardization (participation in ISO meetings; creation of proprietary bodies; lobbying,…). But also on the “translation” steps regarding these transnational organizations. However, an additional step has to be added to this interpretative step. A step of “framework construction” (Porter, 1991, 95). The aim is to help managers of the transnational firms involved in regulations and standardization to anticipate the evolutions and make relevant decisions. The “framework” has three distinctive characteristics: the ability to help conception, the ability to help conceive problems “ex ante”, and the ability to facilitate collective conception of strategic manoeuvres (Claveau, Martinet et Tannery, 1998, 70; David, 1998, 44).

This paper brings twofold a contribution. On one hand, it enriches the interpretation of a very important, peculiar and potentially generic research object, through the lenses of the translation theory. On the other hand, it has key managerial implications regarding “political” strategies with regard to positioning as a regulatory institution. Discussion follows on the consequences of these agencies’ activities for business enterprises.

1- Presentation and Genesis of Internet payments (cyberpayments)

1.1- Presentation of cyberpayments

1.1.1- Definition and challenges of cyberpayments

In this article we will deal with the concerns around cyberpayments and their impact on the emergence of transnational regulation. What are the challenges of cyberpayments? Cyberpayments are an emerging new class of instruments and payment systems that support the electronic transfer of value. These transfers may take place via networks, such as the Internet, or through the use of stored-value type smart cards. Because of the efficiency and ease with which they transfer value, these systems may also present new challenges to law enforcement. Technology exists which could permit these systems to combine the speed of the present bank-based wire transfer systems with the anonymity of currency. As a result, there are issues that must be addressed as these systems are being developed to ensure the prevention and detection of money laundering and other illegal financial transactions.
Internationally, cyberpayment systems have also received extensive attention. Multilateral discussions and studies have been undertaken by both the G-7’s Financial Action Task Force (FATF) and the G-10’s Working Party on Electronic Money. For example, in June 1996, recommendation #13 was added to the FATF’s 40 Recommendations. It states that “countries should pay special attention to money laundering threats inherent in new or developing technologies that may favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes”.

1.1.2- Recent history of Internet payment systems

The market potential seemed tremendous, and payment systems started to advertise their ability to react to this new challenge. We propose to move back to 1994-1995 to reconstruct the Genesis of Internet payment systems, with the help of one of the gurus in the field at the time:

“New emerging network payment and Smart Card Purse schemes will make buying and selling quicker, easier and more convenient for merchants and consumers, while reducing cash handling costs for banks and retailers. “

(Vandenengel, 1995).

In a time of Genesis, it proves useful to define the words used by the stakeholders of the situation: “The electronic commerce that is being widely discussed deals with the consumer or “retail” commerce of main street, as opposed to the “wholesale” electronic commerce of Wall Street. Wholesale electronic commerce has been prevalent for at least ten years, and relates to the trillions in electronic funds transfer between banks, international currency trading, and other institutional transactions. The “retail” electronic commerce field can be roughly categorized into two general types: network cash or payment schemes, and Smart Card electronic purse systems, although many programs cross these boundaries.

The Actor-Network (Callon, 1986) ‘cannot wait’. He has to build a structure (a consortium, for example), so as to take advantage of an anticipated “gold rush”. “The Commerce Net consortium was started to allow companies to conduct almost all their business through the Internet, from browsing multimedia catalogues to submitting bids and placing purchase orders.” Some actors prove faster than, more pragmatic and more visionary than others: “Digicash envisions its electronic cash being used to pay for anything sold on the Internet, from software to pizza. Based on the RSA public-key cryptosystem, the user’s equipment (a PC or a Smart Card) generates a random number or “note”. The equipment then “blinds” the number and transmits it to the user. The user’s equipment can then “unblind” the note and transmit it electronically for payment in cyberspace.

The pursuit of a de facto standard accessible to the entire profession operates as a signal that the major players are eager to create a Common Good for the industry. However, It is noticeable in our example that they use this opportunity to act as partners with their competitors to impose a point de passage oblige (Callon, 1986), namely the use of the smart card technology they have been pioneering without success for many years. Hence this “translation process” (Callon, 1986; Czarniawska, 1996) could be analysed as a mean of “recycling” existing technologies in techno-political projects with high visibility and potential marketing gains for each of the Networked organizations. Subsequently, opportunistic pilot projects help “discipline” the stakeholders (suppliers, customers, national public
authorities, while actual physical deployment (including ATMs\(^1\) and EFTPOS\(^2\) materials) provide the basis for durable networking and standardization.

### 1.2- The concerns over cyberpayments

#### 1.2.1- The trend toward deterritorialization: cyberpayments in the Cyberspace

The first dimension of the cyberpayment concern relates to geopolitics and globalization. We are told that we face an era of radical changes. One of them is the “deterritorialization” (Toal, 1999). Quoting Paul Virilio (1983), we could say that, beyond some words like globalization, translocality, glocalization, transnational, cyberspace, what is being described is the re-arranging and re-structuring of spatial relations as a consequence of the technological, material and geopolitical transformations of the late 20\(^{th}\) century.

To speak of deterritorialization in contemporary discourse, according to Toal (1999) is to speak of a generalized dismantling of the complex of geography, power and identity that supposedly defined and delimited everyday life in the developed world for most of the 20th century. It is to speak of a new condition of speed and ‘informalization’, of the transgression of inherited borders, the transcendence of assumed divides, and the advent of a more global world. Though regimes of territoriality are constantly in flux and under negotiation, discourses of deterritorialization tend to ascribe a unique transcendency to the contemporary condition, defining it as a moment of overwhelming newness.

#### 1.2.2- Deterritorialization and financial markets

One of traditional markers of state sovereignty and territorial power is the ability of a government to print its own money and control its own financial destiny. But since the break-down of Bretton Woods, the state territorial character of financial markets has been thrown into question. Transnational corporations were forced to develop their own foreign exchange departments. Financial services companies became increasingly important to the conduct of international business and trade. The Bank of England allowed British banks to take deposits and make loans in dollars in 1958. The London subsidiaries of American banks were also allowed to do this. The eurodollar market began to grow, because they were not subject to the same reserve requirements and interest-rate restrictions as national markets and financial institutions. Another important development was the deregulation of financial markets in the late 1970s and 1980s. A third development was the introduction of information technology into finance. On-line transaction processing, electronic wire transfers, automatic transaction machines and electronic data interchange radically altered the space-time relationships governing the financial sector, integrating regional financial markets, encouraging global 24 hour trading horizons, and enabling faster transactional and response times.

#### 1.2.3- Disintegration of sovereignty

With the Global Information Infrastructure initiative (GII), for example, territorial borders disintegrate as key paradigms for regulatory governance (Reidenberg, 2000). Transnational information flows on the GII undermine the foundational borders and erode state sovereignty over regulatory policy and enforcement. Physical borders become transparent and foreign legal systems have local relevance. With electronic cash and new means of electronic stored

\(^1\) ATM : Automated Teller Machine

\(^2\) EFTPOS: Electronic Funds Transfer Point of Sale
value, such as those developed by Cybercash and Mondex, Internet transactions may take place entirely on the network without the physical delivery of goods and services and without resort to any national payment system. Yet the GII creates simultaneous ‘global’ rightholders. A given activity may be subject to differing rights at the same time, such as trademark or antitrust protections, because the activity transcends the borders of any single nation. In addition, the temptations to apply national laws and standards extraterritorially further compound the legal uncertainty.

Network borders have a strong tendency to replace national borders. The visible network borders are contractual ones. For example, the demarcation lines among network service providers such as America OnLine, CompuServe, EUNet, or Prodigy create important boundaries. Network architecture also creates a significant type of border. Gateways between different systems establish fundamental rules of conduct. In effect, technical standards exert substantial control over information flows. Technical standards set default boundary rules in the network that tend to empower selected participants. These visible network borders arise from complex rule-making processes. Technical standardization may be the result of a purely market-driven process or alternatively may be adopted through a standards body.

In this context we are faced with the incongruity of traditional regulatory policymaking. In the USA, for example, national regulators compete with each other for jurisdictional power. In Europe, though, ‘data protection’ agencies have played a significant role in the formulation of information policy. The European Union, too, has established an Information Society Project Office to coordinate a number of wide-ranging European Commission activities.

The development of a new model for governing networks is crucial for effective policy leadership. The new paradigm must recognize all dimensions of network regulatory power. For global networks, governance could be seen as a complex mix of state, business, technical, and citizen forces. Rules for network behaviour will come from each of these interest centres. Within this framework, the private sector could become a driving force in the development of the information society and governments could be involved in protecting public interests.

Should we recognize network systems as semi-sovereign entities? Networks have key attributes of sovereignty: participant/citizens via service provider membership agreements, ‘constitutional’ rights through contractual terms of service, and police powers through taxation (fees) and system operator sanctions. In effect, network users become stakeholders in transnational political and economic communities. Nevertheless, where networks develop parallel to physical society, traditional governments retain crucial public responsibilities and significant interests. The European principle of subsidiarity could fit a new model of governance, where state governments would not attempt to expropriate all regulatory power from network communities. States can even provoke the creation of network standards, but without interfering with each detailed item. The role of the state could shift toward the creation of an incentive structure for network self-regulation.

### 1.3- Cyberpayments’ specific concerns

A particular law enforcement concern regarding the enhanced ability to move funds, is the peer-to-peer payment facility being offered by some schemes. At least one card vendor, and several e-cash schemes, plan to offer consumers the ability to anonymously transfer purchasing power from one electronic purse to another; such payment transactions

---

2 EFTPOS : Electronic Fund Transfer at The Point of Sale
would eliminate the need for clearing procedures and may provide no audit trail, providing opportunities for criminal abuse.

Another concern relates to the ability of financial transactions and monetary value transfers to ‘escape’ from the regulated banking industry where regulators have some level of visibility. The issue of non-bank involvement in the provision of electronic purse services was explored by European Economic Community policymakers. A 1994 report from the working group on European payment systems proposed that only banks be allowed to issue electronic purses. At the November 1994 Financial Action Task Force (FATF) meeting in Paris, it was noted that laundering operations were spreading outwards from the banking to non-banking sector as launderers become more aware of the various directives, legislation and conventions requiring banks and financial institutions to follow the standard requirements of identification and reporting. These non-bank institutions, ranging from large to small less-traditional financial intermediaries, are subject to fewer regulatory requirements and examinations, making them potentially more vulnerable to money laundering.

2- Cyberpayments’ regulatory initiatives

2.1- Multiple initiatives

We can cite the G-7 Financial Action Task Force (FATF). It is an intergovernmental body which began in 1989. The main purpose of FATF is the development and promotion of policies to combat money laundering and specifically to prevent proceeds of crime from being utilized in future criminal activities and from affecting legitimate economic activities.

Another initiative is the one by the OECD. It considers that “as a matter of urgency, public and private sector institutions should re-evaluate many of the economic, legal and political frameworks that currently govern commercial activities and the technological and social environments in which they take place”. They recommend regulation of the information infrastructure:

“Electronic services infrastructures must be permitted and encouraged to converge in order to reflect the rapid convergence of networking technologies employed in Electronic Commerce applications.” They recommend also standardization:

“The Group urges governments to adopt a pragmatic approach that does not discourage the development of widely accepted proprietary solutions becoming adopted as if they were standards for Electronic Commerce, but which nevertheless monitors standardization developments closely to ensure that proprietary standards do not become barriers to market entry or impediments to further innovation (oecd.org/fatf/1998).”

Let us listen to what K. Sahlin-Andersson writes about the OECD and its role as producer of prototypes. “The OECD has been described as an information system (Sjostedt, 1973), a harmonising agent (Harrison and Mungal, 1990), an active disseminator of ideas and ideals (Egeberg, 1978; Olsen and Peters, 1996), and a driving force and creator of national ideas and ideals (Finnemore, 1992; Morth, 1996). International organizations such as the OECD play an important role in directing attention to specific countries, specific phenomena and specific aspects of
developments; they codify, compare and categorize reforms and changes. In other words, they are important editors of reform ideas and experiences” (Sahlin-Andersson, 1996).

We will at this stage present one example of translation regulation in the area of cyberpayments, more precisely in the effort to secure payments on the Internet. One of the initiatives is the construction of the SET specifications (Secured Electronic Transaction over the Internet).

3- The SET Initiative

3.1- Presentation

We present now an interpretation of cyberpayments’ issues and solutions in terms of the Translation Theory (Callon, 1986; Latour, 1989; Sahlin-Andersson, 1996).

What is SET? “The SET Specification is an open technical standard for the commerce industry developed by Visa and MasterCard as a way to facilitate secure payment card transactions over the Internet. Digital Certificates create a trust chain throughout the transaction, verifying cardholder and merchant validity, a process unparalleled by other Internet security solutions. Software vendors whose products pass SET Compliance Testing are eligible to display the SET Mark on their products. SET participants are merchants, financial institutions, and promotional sites that utilize or advertise licensed software. “ (Visa EU Region, Informations Presse, October 24th, 2000).

The concepts of Systems’ openness and of trust chain act as vehicles and metaphors of the necessary cooperation within the network. They pave the way for actors (human and non human) (Latour, 1989) to negotiate commonly accessible solutions. The stakeholders reside in differentiated settings: the merchant on a Pacific Island, the cardholder bank in a large European city, the network in the USA, for example. Service providers can be traced along this ‘trust chain’, ensuring quality and reliability of data transfer.

Let us present the introduction of a new service, the electronic wallet. As a major step forward in helping its issuing banks to provide secure authentication services to their cardholders, Visa EU today announced availability of the electronic wallet. The service will allow Visa card Issuers to provide authentication quickly and with minimal up-front investment, therefore helping to build consumer confidence in electronic commerce and reduce fraud. Bankgesellschaft Berlin will be the first to utilise the new service. “For Bankgesellschaft Berlin, the choice was very straightforward. We are committed to providing our cardholders a high level of internet security.” (managing director card service from Bankgesellschaft Berlin, Germany, in Visa Informations Presse (24 October 2000). Bankgesellschaft Berlin is one actor of the Regulation process, in a way. It comes once the SET Specifications have been developed, but participates in what Latour (1989) has called ‘le rallongement du réseau’, a kind of structural ‘cristallisation’ of the network, in order to make it sustainable.

What is the Genesis of the SET network? On February 1, 1996, Visa International and MasterCard International announced, with others in the industry, the development of a single technical standard for safeguarding payment card purchases made over open networks. On December 19, 1997 SET Secure Electronic Transaction LLC (SETCo) was formed to implement the SET Specification. The company is supported by borrowed resources from MasterCard and
Visa. SETCo manages the Specification and coordinates efforts related to the adoption of SET as the global payment standard.

### 3.2- Interpretation of the SET case through the Translation Theory

Czarniawska and Sevon (1996) have shown that the term of translation (Callon, 1986) calls attention to a richness of meanings associated: transference, linguistic translation, but also transformation, alteration and change. The term of translation is also associated with a constructionist view of power. For Callon and Latour (1981), ‘power’ stands for range of associations: actors associate with other actors (including non-humans) and the more numerous and important their associations are, the greater is the power of the whole network thus created. In this sense, power is a result and not a cause, and it does not ‘belong’ to anybody in particular (Czarniawska and Sevon, 1996).

The construction of the SET norm can be analysed as an illustration of the management of a controversy to help move toward a network reinforcement process. The controversy deals with security. The evolution of fraud on the Internet has caused a breakdown of the trust chain. Therefore, translators (bankcard networks, in this instance) endorse the role of putting together Business requirements and ‘selling’ them to the community. Not as a package, but as a process. A process of negotiation, the confrontation of actors’ interests materialized by a Business Requirements ‘edited’ document (Sahlin-Andersson, 1996) and a physical prototype: a smart card reader connected to a PC. Multiple ‘intermediaries’ (Callon, 1986) intervene in the process (documents, actors, data). They are being used as factors, and impediments, of consensus building.

#### 3.2.1- The phase of testing

The standardization process goes through a phase of testing. Although often strictly technical, this phase can help build legitimacy for the tested solution. For example, in Australia, four major banks have chosen to participate in the testing of a secured e-commerce solution. Why have they chosen one partner instead of another? They have invested time, energy and money with the organization with a capability and competencies to supply with the tools to implement the SET program. Implementation is a key element. It is as if Translation’s teleology was to facilitate implementation by the actors beyond the borders of the experimentation.

Translation means that there is freedom to conceive the solution (and its appropriate regulation package embedded into it). It is not given or imposed. Translation means also that the process of manipulating requirements and solutions goes through a step of ‘mise en équivalence’ (search for equivalence) between texts, statements in different contexts (Callon, 1986): a market demand in Sweden, to be translated by the London office of a bankcard network into a software functionality by the computer scientists at the World headquarters in the USA.

#### 3.2.2- Legitimacy
Legitimacy is an attribute of the organization, related to its ability to build trust between partners. A bankcard network, composed of thousands of banks in more than 100 countries, brings legitimacy every time it undertakes an experiment. It starts the virtuous circle of Translation. Organizational legitimacy encourages banks to become participants in pilot projects. Their participation improves the likeliness of success of such a project, which can pave the way to the development of a de facto standard.

The trust chain of human actors is a risk-reducing factor in the construction of regulation policy. In our example, the international network of bankcard members encourages the participation of Australian banks, provides them with a forum of discussion. These events act in favour of the SET 1.0 protocol. A good way of aligning actors is to expand the frontiers of a pilot to an entire industry, giving the experiment a real life dimension, thus improving the credibility and the readability of the results.

3.3- Summary of the interpretation through the Translation Theory

Let us look now at the steps of the translation process in our example.

✓ First step: Contextualization (actants, challenges, move toward convergence): Professionals and customers demand Internet payment securization to facilitate electronic commerce development. Actants are banks, Internet merchants; one of challenges is the development of secured online transactions; the convergence is in the common interest in developing a secured solution.

✓ Second step: problematization and emergence of a translator: What unites the actants is the need for security at a reasonable cost (SET seems too costly to some experts); what separates public and private actants is the secret around encryption, and the entry of trust intermediaries (possibly non-banks).

✓ Third step: Compulsory Crossing Point (CCP) and convergence (it can be a location or a piece of text): the major bankcard networks act as CCPs in the collective search for convergence.

✓ Fourth step: Selection of spokespersons of each organization: CyberCOMM, networks, banks, governments, consumerist associations select spokespersons.

✓ Fifth step: Formal investments: external (consortia, economic groups such as GEIE, …) and internal (regional committees; products’ groups; coordination bodies; participation in Normalization boards,…).

✓ Sixth step: management of intermediaries: data; technical objects; money; know-how, …). In our example, the intermediaries can be reporting data, chip card and card readers with their software, budget for Cyberpayments’ R&D, or organizational learning capabilities in international risk management.

✓ Seventh step: Actors’ mobilization (enrolment): alignment through the conception of systems integration and interoperability projects.

✓ Eight step: the search of network irreversibility: the creation of a European consortium, for example.

In summary, translation is an open and constructionist social process, which crosses national borders, and which has significant impacts on law and public policies (law enforcement, money laundering, consumer protection, …). One of
the major trends of such a process is the search for common good’s construction. There is a conceptual proximity with global information issues (in the GII project for instance).

If we draw an analogy with Internet payment mechanisms, we can propose that regulation is needed in the interest of the consumer. But who will be the consumer’s spokesperson? Who will propose a translation of his/her interests? And how? We have attempted to show an illustration of how it could work. We don’t consider it as a best practice, but more as an example of one possibility of management practice to be articulated with transnational regulation policy.

4- Further discussion

4.1- Is regulation the answer?

One aim of regulation is to resolve an issue. But in this case it is very difficult to re-sort to pre-emptive regulation as a resolution of issues we have not as yet identified. It is still early to make any judgments about the extent to which any of these systems really differ in kind from our present day payment system. We are, therefore, uncertain how our extant regulatory, legal, economic and policy frameworks may be able to evolve to cope with these new products—remembering that these frameworks were designed to accommodate new developments and have done so successfully so far, for example credit/debit cards, EFTPOS, ATMs. Another issue relates to the ability of the regulators generally, and law enforcement specifically, to enforce any legislation relating to electronic cash. It is quite possible that electronic money will prove as hard to regulate as any other form of digital information, especially when it is used on computer networks or transferred over other communication devices. How will governments control stateless electronic money?

4.2- Preliminary answers to regulatory concerns

At the European level, it has been suggested to distinguish payment systems from the payment infrastructure. At the level of the payment infrastructure regulated interoperability is the main aim and co-operation the way to reach it. At the level of payment products and services, competition is desired. Another approach is the self-regulatory one (with the example of money-laundering). Industry would be charged with setting and enforcing its own anti-money laundering standards under this regime, with government authorized to oversee this activity to ensure effective compliance. International oversight of cyberpayment systems would take place on a government-to-government basis, but with industry enjoying key representation in governmental bodies charged with setting overall controls and oversight.

A taxonomy of international mechanisms has even been proposed (Perritt H. 1999). Several types of international legal frameworks could regulate-or back up private regulation of consumer transaction on the Internet. The most traditional would be a treaty framework, giving rise to state-based institutions resembling the World Trade Organization, or supporting private regulation as in the case of UNCITRAL’s model laws for electronic commerce and for international credit transfers. Another approach involves delegation of rule making to international administrative agencies within a relatively broad statutory framework. Private self-regulatory mechanisms could build upon the
experience with international banking networks. The interaction between privatisation and pressures for some governmental involvement might produce hybrid international institutions-combinations of contracts and treaties, and combination of contracts and regulatory agency approvals and enforcement (Perritt, 1999).

**Conclusion**

Transnational regulation in the field of cyberpayments cannot be considered as a panacea. However, it may provide, in some cases, the basis for a positive and even fruitful dialogue between public and private organizations. From a Management Research’s standpoint, we consider that it can be useful and relevant to analyze transnational regulators as translators (Callon, 1986; Sahlin-Andersson, in Czarniawska and Sevon, 1996). They operate a ‘mise en equivalence’ between business requirements and political ones. It is fair to say that public regulators have an interest in co-developing regulation policies with private organizations, instead of imposing unrealistic standards. Solutions should be results of translation ‘cascades’, co-piloted in a constructionist way. The value of such a posture resides in the mobilization of all actors toward a common good, a regulation policy embedded within a techno-political solution to macro and micro-threats posed by the spread of cybertechnologies in a borderless world with a network texture.

**References**

Etiemble, *Parlez-vous franqais ?*, Gallimard, Paris,
Dyson and al. (1994) *A Magna Carta for the Knowledge Age*, *New Perspectives Quarterly*, 11, 4:26-37
Knorr-Cetina K (1981), The manufacture of knowledge, Oxford: Pergamon
Latour B. (1997), Nous n'avons jamais été modernes, Editions La Découverte, Paris
Michalet CA. (1985) Le capitalisme mondial, PUF, 2ed, Paris