Intellectual Capital for Communities In the Knowledge Economy

United Nations Educational, Scientific and Cultural Organization

Information for All Programme

Safe and Ethical Cyberspace, digital assets and risk :

How to assess the intangible impacts of A growing phenomenon?

The World Conference on Intellectual Capital for Communities

14th Edition

Organised by
The European Chair on Intellectual Capital, the University Paris-Sud
And UNESCO's Intergovernmental Information for All programme (IFAP)

June 14 & 15

With a Regional Focus :

France

Venue : UNESCO

7, Place de Fontenoy, 75007 Paris
Room IV

Registration: https://soco.jm.u-psud.fr/colloque/13

PRESENTATION

The central theme of the 14th Edition of the World Intellectual Capital (IC) Conference is **"Cybersecurity, digital assets and risk: *How to assess the intangible impacts of a major hidden phenomenon?*"** Many countries, firms and organisations are now concerned and challenged by cyberattacks , a phenomenon which is often hidden, but for which we are still lacking analytical tools as well as extensive data, even though several regulations have been put in place for these events reporting , especially in US. The first law on cyber-attacks, in the form of data breach notification law, *California S.B. 1386* bill, was passed in 2002. Since 2002, many other states adopted similar laws. A security breach notification law requires any organization which has been subject to a data breach to inform customers and other parties. Academic studies related to the impact of data breach on economy started almost at the same time. The first studies have been mainly analysing this effect through changes observed in stock exchange markets. Later works studied the impact of data breaches on firm reputation. With the advent of cyber-attack databases such as datalossdb.org, Privacy Rights Clearinghouse, etc. new studies using higher number of incidents have been published. Nearly all research has been carried out on the analysis of the changes in stock market prices in the timeframe of the cyber-attack incidents. Few have analysed this change through social media data. These analyses are carried out with the event study method. The convergent conclusion of such studies is that there is a negative return for a limited period of time for most of the firms which are subject to a cyber-attack.

The meso/macroeconomic effects of cyber-attacks

In recent years, the macroeconomic impact evaluation of disruptions of different types have been explored by academic researchers with a growing interest in the subject, for policy perspectives notably. These research papers include disaster risk management for terrorism risk management and for natural disasters impact, supply chains networks, energy disruptions), etc.
The growing importance of digital in the economic system (and the increasing dependence of other economic sectors on the IT one, make the IT sector one of the most important sectors nowadays. This led government officials to classify the latter as a *critical infrastructure sector*.
Given its relatively high importance, the IT sector is subject to a number of cyber-attacks of different types and with different aims and strategies. These include industrial spying, but also data breach, all of which aim to destroy or lower a firm's profit, or to make profit out of these data breaches, from the attackers' perspectives. This has led governments to include cybersecurity in their national defense strategies, hence reinforcing the cybersecurity level of public and private firms. This is usually done by imposing a number of security checks and constraints at the firm side. However, despite numerous legislations and rules imposed by countries and regions via their national agencies dedicated to fighting against cyber-attacks and vulnerabilities, there is an observed growing number of sophisticated cyber-attacks, which makes it important, in both the microeconomic and macroeconomic perspectives, to assess their impacts. The evaluation of the macroeconomic effects of cyber-attacks helps estimate the relative importance of cybersecurity on economic activity and manage risks accordingly, with the help of economic models on growth.

Due to the importance of cybersecurity in economic activity, literature on this subject is getting copious with the use of state-of-the-art (economic/econometric) modelling strategies. However, the nature and length of cyber-attacks often make it difficult to assess these meso/macroeconomic impacts. However, even with short lasting cyber-attacks, significant meso and/or macroeconomic effects may occur, due on the one hand to the interdependencies between firms, and on the other hand to interdependencies within and between economic sectors. Such interdependencies are usually modelled using a model that originates from Leontief (1986) *Input-Output Model (I-O)* in which it is argued that there are interdependencies between sectors in the economy such that some industry outputs constitute intermediary goods or inputs to other industries.
Santos et al. (2007) propose a framework aimed at linking cybersecurity metrics to macroeconomic interdependencies. They use a hierarchical modelling system and estimate the ripple effects of cyber risk scenarios using metrics from the *SCADA* (Supervisory Control and Data Acquisition) system components. They also use the *IIM (Inoperability Input-output Model)* in order to perform their analysis.

The large February 2000 DoS attack that hit Yahoo, Amazon, Ebay and CNN, is a good example of a cyber-attack that lasted three days and had large economic impacts in the form of economic losses. Ali and Santos (2012) and Ali and Santos (2015) propose a model that estimates the economic loss associated with these DoS attacks. They use their so-called *extended* Dynamic Inoperability Input-Output Model (*DIIM*) in order to estimate such losses and the associated effects on each sector of activity that was impacted. Their study defines an IT sector which results from the aggregation (using the *S-aggregation* technique also used in Miller and Blair (2009)) of three different sectors: Information and Data, Computer systems design and related services, and Software Publishing. They further use the extended *DIIM* in order to assess the associated effects in terms of economic loss. They also propose a case study analysis of the 2000 DoS attacks in the US. Based on their model, they are able to rank the top ten critical sectors in terms of their cumulative economic loss and average inoperability over their simulated recovery horizon of the DoS attack. According to their study, the sector that ranks top, using the NAICS classification, is the Professional, Scientific and Technical Services sector, followed by the IT sector. The Federal Reserve Banks, Credit Intermediation, and Related Activities sector ranks 10th. The study also estimates an overall economic $18 billion loss, among which $1.6 billion of direct losses is attributed to the IT sector during the first 3 days of the attack. As argued in Ali and Santos (2012), the importance of this DoS attack prompted U.S. policymakers towards preparedness against future cyber-attacks.

Jonkeren et al. (2015) use a Systems Engineering approach coupled with a *DIIM* in order to create a modelling tool aiming at supporting European policies on Critical Infrastructure Protection. In their modelling strategy, they account both for resilience of infrastructure networks and economic sectors. The advantage of including a Systems Engineering approach is that they can account both for static *and* dynamic resilience. They also argue that an advantage of the *DIIM* that they propose is that it is able to explicitly model a failure and a recovery stage after a disruption has taken place instead of assuming that recovery starts immediately. One of the further advantages in using the *DIIM* is that it considers the recovery time of the attack in the affected sectors, allowing to estimate sector-overall impact while accounting for the diffusion aspects of the attack. Our own empirical strategy uses the *DIIM* in order to assess the economic impacts of cyber-attacks on intangibles assets.

The intangible impact on firms and organisations

As the knowledge economy has developed, the contribution of intellectual assets in the process of value creation is evident for holding companies / managers and strategists. Such importance is reflected by the large gap between firms' accounting book value (of tangible assets) and stock market value which captures all economic (material and knowledge) assets hold by a company. In order to evaluate intangible assets, many different methods and theories have been proposed in recent years.

Within the Hermeneut project, and taking a more practitioner-oriented our recent researches developed a holistic model for measuring the intangible impact of cyberattacks along a bench of complementary approaches.

Measuring impacts

The first approach is a simple Natural Language Processing (NLP) of the press coverage on the attacked firm. The second approach is the event study analysis on firms' stock prices. Finally, the third approach uses the noise generated on social media to determine the sentiment return found on social media websites. In Hermeneut project, we aggregate the intangibles categories into three distinct types of intangible assets:

1) Organizational capital (which comprises business activities, subsidiaries, value chain, organizational structure, organizational learning, etc.);
2) Key competences (which comprises brand equity, firm specific human capital, networks joining people, institutions, advertising and marketing);
3) Innovation and IP capabilities (which comprises scientific and non-scientific R&D, copyrights, designs and trademarks).

Business modelling of the attackers

The essence of a business model is how the enterprise delivers value to customers and their ecoystems. In general, the valuable item in a cyber-attack incident is the stolen data which are then delivered on the dark market and usually paid with cryptocurrency. Additionally, attributing cyber-attacks is difficult. At the same time, while most payments are generally made with cryptocurrency, most of them are not actually providing full anonymity. Specifically, the Bitcoin cryptocurrency, which is the most popular one with the highest market cap among all cryptocurrencies, only provides a pseudo-anonymity. This does not limit its use in the dark market. It is argued that cybercrime has evolved since the 1970s becoming a highly sophisticated big business, entering a new phase named *Crime as a Service* (CaaS). The main economic factors driving cybercrime are the attractiveness of the target and the economic conditions that the offender faces. Target attractiveness depends on how the offender perceives the target. Target attractiveness is also related to its accessibility, the attack surface and how easy it is to breach it. The lack of economic opportunities is also another factor which incites people to become cybercriminals
In the context of defining attackers' business plans, we aim to also evaluate cyber-attack risks in relation to attack types. To do so, we propose a model that characterizes the different types of attacks based on firms' personal characteristics. For this purpose, we propose the following ordered probit model.

Analysing systemic risks

Cyberrisks need to be assessed, measured and addressed reliably. There is then a need to develop frameworks for risk assessment as well as educational tools for dissemination among firms, government bodies and communities.

The *IC for Communities* conference series have discussed some of these issues in their earlier editions. However, they are the focus of IC 14, which looks at them from different angles: geographical (Asia, Europe, North and South America, and Africa), institutional (large companies, large international institutions, small firms) and professional (scholars, policy and private sector decision-makers).

We propose a set of themes that we consider to be highly relevant for decision-making:

- **Modeling and valuing data as digital assets.** How concretely to modelize value creation as a data driven process, beyond the general discourse on big data? Are there relevant practices to be shared? Is there a potential for developing a common language (and possibly standards) for data driven value creation? Are the approaches necessarily sectoral or organizational specific? What governance structure and rules to be considered and implemented?
- ***Data and Cloud computing business models.*** Cloud computing emerged as a new form of organizational design. What are its determining factors? What types of "organizational fits" (structure, culture, processes,) to be put forward? How data intervene in value creation processes and design for cloud computing?
- ***Analysing cyberrisks and measuring their impacts.*** How to analyse cyber risks? What programmes and actions taken by countries, firms and national and international institutions? What learning lessons to be taken for the next steps?
- ***Valuing cyber risks.*** What methodologies and what approaches to be deployed for cyberrisks measurement? What micro/meso and macro impacts? What programmes and actions to be deployed? What pricing policies for risk measurement?
- **Analyzing platforms and hybrid organizations.** The hybridation of resources is accelerated by the critical role of data. This is clear in the case of digital platforms (Gafa and alike) where this is a market power around which innovations are concentrated and organized. But this also the case for hybrid organizations with a mix of private and public resources or market and non market oriented organizations. Beyond establishing typologies of such organizing

forms, we need to document further their governance structure and processes, and the impact of innovation capabilities and sustainability of ecosystems and the society in general.

- **Intangibility and digitality.** The question here relates to the type of exchange instruments used by people, especially in a context where acceluction becomes a major production system. Due to the multiplicity of spaces for value creation and the ubiquity of digitality, we can expect exchange and social interaction to become organized along intangibles such as brands, data, and reputation. We can also expect traditional forms of knowledge to become digitized and therefore more easily disseminated worldwide (an example is the way the Massai café, as community product, has been branded). At the global level, we can expect to see the emergence of collective goods such as collective brands, or collective knowledge that is relevant to specific communities and is widely disseminated via digital artifacts.

This year, following the success of IC8 (South Korea), IC9 (the Mediterranean), IC10 (Brazil), IC11 (China), Africa (IC12), Japan (IC13), we focus on a country with several on-going projects on intangibles: France.

As at former IC conferences, these questions are addressed at various levels: countries, regions and territories, cities, firms and networks.

We will also address some of the recurrent topics of the IC conferences series, such as innovation policy, information sharing, knowledge transfer, measurement, valuation and reporting, as well as the next research and policy agenda for intangibles and intellectual capital.

Draft agenda – as of April 6 2018

Day 1 – Thursday June 14, 2018

8.15 – 8.45 am: Welcome Coffee, Registration

8.50-9.00 am Welcome address :, UNESCO & Etienne Augé, VP Research, Université Paris-Sud

Session 1

9.00-11.00

DIGITAL TRANSFORMATION, ETHICAL CYBERSPACE AND THE POLICY AGENDA :

Moderator: B. Radoykov

9.00 - 11.00

- "Safe and Ethical cyberspace", **Chafica Haddad,** Chair IFAP Council
- "Digital agenda and innovation policy**", Dominique Guellec**, OECD
- "Platformisation of government agencies: Lessons from Estonia", **Marten Kaevats,** Republic of Estonia Government Office
- "Digital agenda for cyber-risks", **Jakub Boratynski,** DG Connect (on-line)
- « How government addresses the issue of cyberrisks », **Guillaume Poupard,** Director General, ANSSI

Cafe Break – Networking: 11.00 – 11.30

Session 2

11.30-13.15

MODELLING AND VALUING THE INTANGIBLE IMPACTS OF CYBERRISKS

Moderator: tbd

- "Micro & macro impacts of cyberrisks: Interim results of H2020 HERMENEUT project" , **Ahmed Bounfour, Niaz Kammoun, Altay Ozaygen, and Rokhaya Dieye**, Paris-Sud University
- "The emerging insurance market for cyber risks" **Leigh Wolfrom**, OECD
- "How do large firms consider the intangible risk", **CIGREF (tbc)**
- "How to develop strategies for facing cyberrisks ? ", E&Y (tbc)

Lunch: 13.15 – 14.15

Session 3 – Key note speech

14.15-14.45

Title tbd: **ADG/CI, UNESCO (OR REPRESENTATIVE)**

Session 4

14.45-16.45

INTELLECTUAL CAPITAL OF FRANCE: RECENT DEVELOPMENTS

This session will present some of the recent works developed by large institutions in France.

Among the potential speakers :

- Measuring intangible investment in France, **France Stratégie**
- Investment in intangibles of territories**, CDC**
- Patents : Towards a suitable quantitative and qualitative measurement of an intangible ?, **Fréderic Caillaud** INPI
- Supporting investment in intangibles by SMEs, DGE/ **Christophe Descos**,Groupe BPCE
- IP assets and value creation, **André Gorius**, Solvay

.

Coffee break, Networking 16.45 – 17.00

Session 5

17.00-18.30

INSTITUTIONAL INNOVATIONS AND ECONOMIC GROWTH

- "The digitalization of SMEs in service industries: How can policy help?", **Maximilian Benner**, Vienna
- "Growing against conventional wisdom: economic development in Heilbronn-Franconia, Germany", **Johannes Glückler**, Heidelberg University
- **Sandra Hannig**, OECD: title to be confirmed by next Monday
- "Knowledge transfer and the impact issue: an institutional perspective", **Laura Kreiling, Ahmed Bounfour,** Paris-Sud University

Day 2 – Friday June 15, 2018

Session 5

INTANGIBLE CAPITAL OF NATIONS: AN UPDATE

Moderator: tbd

9.00-11.00

- "'Japan's strategic vision on IP and national branding.", **Takayuki Sumita,** Secretary General, Intellectual Property Strategy Headquarters, Cabinet Office
- "Intangible capital of Brazil : the need for impact evaluation", **Helena Tenório Veiga de Almeida**, BNDES
- "Intangible capital of Sweden: a navigation map", **Leif Edvinsson, Carol Lin** , National Chengchi University
- "The United Arab Emirates knowledge agenda", **Wael Osman,** Director of Strategy, Dubai (bc)

Cafe Break – Networking: 11.00- 11.15

Session 6

11.15 – 13.00

DIGITAL PLATFORMS , COMPETITION POLICY AND INNOVATION

Moderator: **tbc**

9.30-11.15

- "How do global firms deal with cyberrisks", Stephane Lenco, Chief Security Officer, AIRBUS
- "Digital platforms as evolving institutions: the case of China", **Xunhua Guo**, Tsinghua University
- "The internationalisation of Asian platforms: the case of Rakuten**", Motohiko Sato**, Rakuten
- "How do platforms use data for innovation" , **Christian Reimsbach-Kounatze**, OECD (tbc)
- "Global platforms and investment in intangible capital: a review", **Ahmed Bounfour**, Paris-Sud University

Lunch: 13.00– 14.15

Session 7

INTANGIBLE CAPITAL IN GLOBAL VALUE CHAINS

Moderator: tbd

14.15-16.45

This session will mainly discussion findings and arguments of the WIPO report on Global value chains.
by **Sacha Wunsch-Vincent**, WIPO

- The WIPR on intangibles and global value chains, **Sacha Wunsch-Vincent**, WIPO, "
- Measuring the income to intangibles in goods production: a global value chain approach**, Wen Chen,** University of Gorningen
- "Understanding the dynamics of global value chains for solar photovoltaic technologies", **Matthieu Glachant,** MINES ParisTech (tbc)

Panel discussion

Session 8

16.45-18.00

INTANGIBLES AND VALUE: THE MICRO/MACRO DIALOGUE, WHAT SHOULD BE NEXT STEPS

This final session will address the issue of the next agenda for intangibles, both from research and policy. Invited scholars, and policy makers will discuss some critical issues for the future of economies and societies, such as those related to measuring, impact, investment and ethics in a broader sense.
Introduction **: Feng Gu**, Chair, Associate Professor, School of Management, University at Buffalo on his book with Baruch Lev, NYU, " on The End of Accounting and the Path Forward for Investors and Managers"
Panel discussion : **Hannu Piekkola**, University of Vaasa (tbc), **Thomas J Housel**, NPS, **Yasuhito Hanado**, Waseda University, **Marianne Paasi,** DG Research (tbc)

Concluding remarks
18.00
End of the conference

Registration

https://soco.jm.u-psud.fr/colloque/13

Contacts

Scientific Direction: Ahmed Bounfour
Professor, European Chair on Intangibles, Paris-Sud-University
ahmed.bounfour@u-psud.fr

Organisation: Laura Kreiling
PhD candidate in management science, Paris-Sud-University
Laura.kreiling@u-psud.fr

Logistics: Marielle Rosine
Secrétariat RITM, Paris-Sud-University
Marielle.rosine@u-psud.fr