T09P11 / The Governance of Innovative Technologies

Topic : T09 / Governance, Policy networks and Multi-level Governance
Chair : Araz Taeihagh (National University of Singapore)
Second Chair : Li Yanwei (Nanjing Normal University)

GENERAL OBJECTIVES, RESEARCH QUESTIONS AND SCIENTIFIC RELEVANCE

Innovative technologies, such as high-speed railways, wind turbines, solar, geothermal, and other types of renewable energy projects, etc. along with the recent developments in ICT such as the sharing economy, block chain technology, crowdsourcing, big data and open data initiatives are increasingly adopted around the world to increase efficiency and effectiveness and improve decision making (Taeihagh, 2015; Prpic, Taeihagh and Melton, 2015; Janssen and Helbig, 2016; Hilbert, 2016). However, these technologies become sources of new problems due to unintended consequences and by creating new, previously unimaginable risks, as a result of which the social acceptability of these innovative projects may be low (Gerrits, 2016; Li, 2016). For decision makers and practitioners, how to address these issues in order to govern risks and uncertainties in a satisfactory manner is a challenge (Brown and Osborne, 2013). This raises several interesting questions awaiting to be answered by public administration and governance scholars.

- What types of unanticipated outcomes can result from adoption of innovative technologies in different fields (such as ICT, energy, transport, climate change, water management etc.)?
- How to govern risks and uncertainties inherent in innovative and often disruptive technologies?
- How to reconcile the relationships between innovative technologies and incumbent industries?
- What are the limitations of the traditional top-down approaches in governing uncertainties in the adoption of innovative technologies?
- What are the implications of responsible (technological) innovation for public administration and how to achieve it?
- What are the best practices in governing risks and uncertainties in adopting innovative technologies?
- What can we learn from other disciplines in regards to the governance of unintended consequences and unintended challenges in adopting innovative technologies?

This panel will be dedicated to addressing this issue through enhancing our theoretical understanding of risk and uncertainty, and our empirical insights into their governance. Papers are welcome on the following topics:

- Theoretical and conceptual approaches to uncertainties and risks,
- Risk and innovation in public service delivery,
- Risk / uncertainty and its governance,
- Innovation and governance,
- Risk and complex socio-technical systems,
- Robustness and resilient thinking (including Antifragility pending the working definition used for resilience),
- High-reliability organizations (HRO),
- Risk and engagement of vulnerable stakeholders,
- Transfer of risk to vulnerable stakeholders (through Automation, Sharing economy etc.)

Reference:

Brown, L., & Osborne, S.P. (2013). Risk and innovation. Public Management Review, 15 (2), pp. 186-208.

Gerrits, L.M. (2016). For the love of complexity: Governing technological innovations. Inaugural lecture delivered in abridged form on the acceptance of the Chair of Political Science, especially Governance of Complex and Innovative Technological Systems. Bamberg: University of Bamberg Press.

Hilbert, M. (2016). Big data for development: a review of promises and challenges. Development Policy Review, 34(1), 135-174.

Justen, A., Schippl, J., Lenz, B., & Fleischer, T. (2014). Assessment of policies and detection of unintended effects: Guiding principles for the consideration of methods and tools in policy-packaging. Transportation Research Part A: Policy and Practice, 60, 19-30.

Li, Y.W. (2016). Governing environmental conflicts in China: Government responses to protests against

incinerators and PX plants. Rotterdam: Erasmus University Rotterdam.

Prpi? J., Taeihagh A., and Melton J. (2015). The fundamentals of policy crowdsourcing. Policy & Internet, 7(3), 340-361.

Taeihagh A. (2015). Policy and Planning on the Interface of Socio-Technical Systems. Instruments of Planning: Tensions and Challenges for More Equitable and Sustainable Cities, 193-207.

CALL FOR PAPERS

Innovative technologies, such as high-speed railways, wind turbines, solar, geothermal, and other types of renewable energy projects, etc. along with the recent developments in ICT such as the sharing economy, block chain technology, crowdsourcing, big data and open data initiatives are increasingly adopted around the world to increase efficiency and effectiveness and improve decision making (Taeihagh, 2015; Prpic, Taeihagh and Melton, 2015; Janssen and Helbig, 2016; Hilbert, 2016). However, these technologies become sources of new problems due to unintended consequences and by creating new, previously unimaginable risks, as a result of which the social acceptability of these innovative projects may be low (Gerrits, 2016; Li, 2016). For decision makers and practitioners, how to address these issues in order to govern risks and uncertainties in a satisfactory manner is a challenge (Brown and Osborne, 2013). This raises several interesting questions awaiting to be answered by public administration and governance scholars.

I What types of unanticipated outcomes can result from adoption of innovative technologies in different fields (such as ICT, energy, transport, climate change, water management etc.)?

I How to govern risks and uncertainties inherent in innovative and often disruptive technologies?

I How to reconcile the relationships between innovative technologies and incumbent industries?

I What is the limitations of the traditional top-down approaches in governing uncertainties in the adoption of innovative technologies?

I What is the implications of responsible (technological) innovation for public administration and how to achieve it?

I What are the best practices in governing risks and uncertainties in adopting innovative technologies?

I What can we learn from other disciplines in regards to the governance of unintended consequences and unintended challenges in adopting innovative technologies?

This panel will be dedicated to addressing this issue through enhancing our theoretical understanding of risk and uncertainty, and our empirical insights into their governance. Papers are welcome on the following topics:

· Theoretical and conceptual approaches to uncertainties and risks,

· Risk and innovation in public service delivery,

· Risk / uncertainty and its governance,

· Innovation and governance,

· Risk and complex socio-technical systems,

· Robustness and resilient thinking (including Antifragility pending the working definition used for resilience),

· High-reliability organizations (HRO),

· Risk and engagement of vulnerable stakeholders,

· Transfer of risk to vulnerable stakeholders (through Automation, Sharing economy etc.)

T09P11 / The Governance of Innovative Technologies

Chair : Araz Taeihagh (National University of Singapore)

Second Chair : Li Yanwei (Nanjing Normal University)

Session 1 Theoretical Discussions

Thursday, June 29th 10:30 to 12:30 (CJK 1 - 1)

Discussants

MIKOLAJ FIRLEJ (University of Oxford, Faculty of Law)

The Regulation of Cyber-Physical Systems (CPS): Facing the Rise of Sensor Networks, Artificial Intelligence, and Robotics

Alberto Asquer (SOAS, University of London)

Inna Krachkovskaya (SOAS University of London)

Contemporary advances in sensor networks, artificial intelligence (AI), and robotics have cast a shadow of apprehension over the implications of uncontrolled technological applications on individuals and societies. Notable figures like Stephen Hawking publicly voiced their concerns, for example, that AI could "spell the end of the human race" and others like Elon Musk warned that AI could be "potentially more dangerous than nukes". Occasional accidents, like the racist comments of a conversational bot on 24th March 2016 and the first death for a driverless car crash on 7th May 2016, spurred further uneasiness towards electronic automated systems. On the other hand, technological advances in so-called Cyber-Physical Systems (CPS) promise to boost productivity and stimulate innovations in many areas of the economy, from healthcare to transport, from energy to education. The apparent inevitability of research and technological progress stimulated early attempts to regulate CPS, such as, for example, the issue of guidelines to to the ethical design and application of robots and robotic systems by the British Standards Institution (BSI) and the formulation of recommendations in studies of the working group on robotics and artificial intelligence of the European Parliament's Committee on Legal Affairs (JURI).

Building on an analysis of the contemporary discourse on the regulation of CPS, this paper aims to develop a theoretical framework for the governance of risk and regulation of innovative technologies. A distinctive feature of innovative technologies is the continuous exploration of novel applications rather than the exploitation of installed technological systems. The novel applications that arise from CPS, in particular, include a role for electronic systems of detection and surveillance, analysis and formulation of (original) inferences, and intervention into the social domain in unanticipated ways. The framework, therefore, draws the distinctions between known and unknown sources of risk that arise from known or unknown forms of application of technologies. The distinctions provide the basis for the identification of alternative strategies for coping with risks, which include the options of ignoring the source of risk at will or attending to the actual or potential hazard that arise from unregulated use of CPS.

The implications of the theoretical framework take the form of recommendations for the design of institutions for the governance of risk and regulation of innovative technologies. The recommendations include attention to the kinds of harm that CPS can inflict to either individuals or to the public, such as, for example, in surgeries, automated transport, stock market trading, and existential threats. It is argued that two main regulatory processes will most probably drive the co-evolution of future CPS and social systems, namely a tendency to legitimise CPS application through investments in symbolic capital (such as, for example, the formulation of legal personality and ethical responsibility for electronic entities) and another one to relocate CPS development and applications to the most advantageous regulatory environment.

The Role of Transnational Expert Associations in Governing the Cybersecurity Risks of the Internet of Things

Irina Brass (University College London (Department of Science, Technology, Engineering and Public Policy))

Jesse Sowell (Stanford University)

Madeline Carr (Cardiff University)

Blackstock Jason (UCL STEaPP)

The benefits and challenges of the Internet of Things (IoT) are increasingly capturing the attention of policy-makers, the media and the wider public. On the one hand, IoT is perceived as enabling societal and economic progress by facilitating customised and efficient production processes (industrial IoT), enabling forward planning by uncovering structural weaknesses in critical infrastructure (transport, energy) or responding to the challenges of an ageing population through personalised medicine and increased mobility (health, autonomous vehicles). On the other hand, the long-term public acceptance of IoT will be challenged by the increasing number of cyberattacks originating from IoT endpoint devices and the challenges of monitoring and enforcing basic security policies on these devices. These security vulnerabilities expose fundamental concerns about the stability of the IoT ecosystem and raise questions about the appropriate security safeguards necessary to limit abuse.

Through an analysis of the Mirai distributed denial of service (DDoS) attacks on KrebsonSecurity, OVH and Dyn using compromised IoT endpoint devices (routers, CCTVs and TV sets connected to the Internet), this paper investigates the unique cybersecurity risks and uncertainties that are emerging from the growth of IoT. There are two distinguishing characteristics of IoT botnets. The first is the higher potential utilization rate of permanently switched on, "connected" things. The second is that infections are more durable given the lack of or limited capacity of these devices to incorporate security features in their hardware as well as control and lifetime vulnerability management in their software. The result is a malware infrastructure that is more reliable for abusive activities than conventional botnets.

A key problem here is that agreeing on a single standard for minimum security specifications for IoT endpoints has proven challenging at both domestic and international level. In order to move forward, this paper proposes a new conceptual framework for understanding and evaluating the role of transnational expert associations, such as the Message, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) and the Anti-Phishing Working Group (APWG) in developing transnational IoT security standards and monitoring regimes. In particular, we argue that participants in groups like M3AAWG and APWG form expert communities effectively positioned to develop unique decision-making frameworks and to document information security processes for monitoring and mitigating the cybersecurity risks associated with the growth of IoT. The paper draws upon the literature on "transnational private regulation" (Cafaggi 2012, Scott et al 2011) and "global private governance" (Mattli and Büthe 2011, Mattli and Woods 2009) to highlight the growing role of expert communities of ICT manufacturers and network operators in providing best practice, information sharing and monitoring capacity in order to respond to the unique cybersecurity challenges of IoT in the absence of top-down regulatory regimes.

The governance of risks in ridesharing: Lessons learned from Singapore

Li Yanwei (Nanjing Normal University)

Araz Taeihagh (National University of Singapore)

In the past few years, we have witnessed that many different types of innovative technologies, such as crowdsourcing, ridesharing, open and big data, have been adopted around the world with the aim of delivering public services in a more efficient and effective manner. Among them, ridesharing has received substantial attention from decision makers around the world. Because of the multitude of currently understood or potentially unknown risks associated with ridesharing (unemployment, information privacy, environmental risk due to increased emissions, liability and insurance), governments in different countries adopted diverse strategies in coping with risks associated with ridesharing. In some countries or municipalities, ridesharing is prohibited. In other countries, ridesharing, has received strong support from governments. In this paper we address the question how are risks involved in ridesharing governed over time. To answer this question, we present an in-depth single case on Singapore and examine how the Singaporean government has addressed risks in ridesharing over time. Singaporean has a strong ambition to become a leading hub in innovation, and many innovative technologies have been adopted and promoted. At the same time, decision makers in Singapore are reputable for their proactive approach in social governance. In this study, we will explore how Singaporean government copes with risks in adopting ridesharing. This case study about Singapore can be regarded as a revelatory case study, helping us to further explore the governance practices in other countries.

T09P11 / The Governance of Innovative Technologies

Chair : Araz Taeihagh (National University of Singapore)
Second Chair : Li Yanwei (Nanjing Normal University)

Session 2 Applied research

Thursday, June 29th 13:30 to 15:30 (CJK 1 - 1)

Discussants

Irina Brass (University College London (Department of Science, Technology, Engineering and Public Policy))

The Effect of Deployment Policy Design on the Lock-In of Innovative Technologies – A Model of Alternative Policy Design Scenarios and the Case of the Solar PV Feed-In Tariff in Germany

Leonore Haelg (ETH Zurich)

Tobias Schmidt (ETH Zurich)

An ample and rapid energy transition is necessary to address societal challenges such as climate change. Globally, a trend towards deployment policies to trigger this transition can be observed. At the same time, technological change is highly path-dependent, and policymakers face an important dilemma, similar to the "Collingridge dilemma": On the one hand, they need to foster the diffusion of novel technologies to overcome the existing carbon lock-in. On the other hand, the extensive deployment of new technologies may result in yet another (undesired) technological lock-in. In recent literature, the design of deployment policies has been shown to be important for technology selection, fostering or avoiding unintentional lock-ins. While *technology specificity* (i.e., how much a policy differentiates between technologies on different hierarchy levels) is a widely discussed design dimension of deployment policies, the concept of *application specificity* (i.e., how much a policy differentiates between applications) has only recently been introduced. Yet, how exactly different levels of these two design dimensions act on technology diffusion is not well understood.

Here, we try to address this literature gap by investigating the effect of the two design dimensions *technology specificity* and *application specificity* on technology selection. The aim is to provide insights on how deployment policies should be designed in the presence of big technological uncertainties (e.g., related to innovation and cost-reduction potentials) to support decisions concerning technology diversity, competition and avoidance of (premature) lock-in on the level of technology or sub-technology. To do so, we use a dynamic and historically calibrated agent-based investment decision model which allows for policy design modifications. The empirical case is the solar photovoltaics feed-in tariff in Germany.

The modelling results suggest a high path dependency with tendency for locking into one technology for all policy designs. The competition between technologies within applications and the respective market volumes, which allow for spillovers between the applications, thereby play a crucial role in technology diffusion. We find that feed-in tariffs which are unspecific in terms of technology and application exhibit a high potential for technological lock-in. Technology-specific tariffs may also lead to technological lock-in, yet not necessarily to the more extensively supported technology. Contrarily, application-specific tariffs allow for competition between the technologies for longer periods and may hence prevent premature lock-ins by increasing the financial attractiveness and the market volume of otherwise unattractive technologies.

The findings allow for several implications for policymakers. First, competition between technologies within and across applications need to be well understood when designing deployment policies in order to avoid unintended picking of winners. Second, application-specific policy design can help opening up niches for immature technologies to become competitive with more mature technologies. Third, the changes in competitiveness between technologies happen gradually allowing for policymakers to react tend adapt the policies accordingly. Finally, from a methodological perspective our study contributes to the ex-post policy evaluation of technology diffusion by proposing the first historically calibrated model allowing for dynamic analysis of path dependency created by deployment policies.

Regulatory Adaptation in the Face of Technological Adaptation: Conceptual Framework and Hypotheses

Eric Montpetit (Université de Montréal)

It is overwhelmingly accepted that government regulation needs adaptation when technology evolves. As rational as regulatory adaptation might seem, it is unlikely to occur straightforwardly. When aligning regulations with technology, regulators must rely on expert information, seemingly independent from political influence. In reality, finding and selecting this expert information is intermingled with political considerations. How does politics influence regulatory adaptation? The question is pressing, as technology and scientific knowledge are changing quickly. With the arrival of self-driving cars, car safety regulations no longer suffice; regulations that protect private information need revising to keep up with the progress of big data and machine learning; and GMO regulations can easily be bypassed by biotechnology developers using new gene-editing technologies. Drawing from policy process theories, this paper will put forward a conceptual framework to better approach this issue of regulatory adaptation and will offer testable hypotheses about the effect of political factors. The theoretical framework and hypotheses will notably rest on Baumgartner and Jone's Politics of Information.

How to govern risks and uncertainties inherent in lethal autonomous weapon systems? Key legal challenges.

MIKOLAJ FIRLEJ (University of Oxford, Faculty of Law)

The lethal autonomous weapon systems (LAWS) are weapons designed to select and attack targets without direct human control. A further development of these weapons will open for the first time the possibility of removing the human operator from the battlefield. At present, around 40 nations are developing military robotics. Although LAWS do not yet exist, it is clear that technology is moving in the direction of their development. Some deployed weapons have already been coined as almost fully "autonomous" since they, "once activated, can select and engage targets without further intervention by a human operator."

At present there are no explicit legal rules on both international and domestic level aimed at establishing legal regime of research, development and deployment of LAWS. Recently, some countries (US, Israel) have developed initial policies towards LAWS but these policies can be changed anytime and have no-binding power.

On international level, there is a growing campaign in favour of universal prohibition of LAWS, primarily run by Human Rights Watch ('Losing Humanity' 2012). It is claimed that LAWS will violate principles of humanitarian law, i.e. the principle of distinction, the principle of proportionality, the military necessity and the Martens Clause. It is also suggested that there are significant problems in attributing responsibility for LAWS' wrongdoings. The possibility of attributing responsibility is argued to be a precondition for the application of the in bello laws of war.

In my paper, I explore how to govern risks and uncertainties related to LAWS.

First, I present what are the key characteristics of LAWS and how LAWS are different to currently existing weapons with a particular emphasize on the concept of meaningful human control. Then, I explore what are the key legal principles currently applicable to LAWS, in particular in the context of legal and moral significance of human judgment and attribution of responsibility.

The UN Convention on Certain Conventional Weapons (CCW) and article 36 of Protocol I to the Geneva Conventions typically address legal issues related to emerging technologies but according to some, existing legal rules do not fully capture the qualitatively different weapons such as LAWS.

I analyse whether LAWS comply with key principles of international law, particularly with Article 36 of Protocol I. Further questions include: are these principles sufficient in governing LAWS? Are there any additional conditions upon which LAWS could comply with international law? If not, why LAWS challenge the principles behind existing regulatory regimes? What legal responsibilities do or should states bear when developing and deploying autonomous weapons? What types of frameworks for accountability and management of the risks entailed in such weaponry are appropriate at the inter-state level?

I conclude that existing legal principles are not sufficient in governing LAWS. Detailed answers provide argumentation why there is a need for additional regulation rather than prohibition.

Beyond normative methods of analysing text, I will use case-based reasoning, particularly with the Amended Protocol for Landmines, which -according to some- provides a suitable framework for regulating LAWS.

Emergent Challenges in International Investment Law: Investing in ICT

Ivory Mills (Northwestern University)

Information and communication technologies (ICTs) represent a comprehensive sector of communication devices, applications, and services. As this sector has rapidly developed, its transformative impact on nearly every component of modern life has made sustainable development a priority, as detailed in many national economic agendas, as well as the 2030 Agenda for Sustainable Development. Countries around the world invest in and/or receive investments in ICTs to support their growth and development goals. International investment laws, namely bilateral investment treaties govern these investments and attempt to balance the interests of the host states with those of foreign investors. These competing interests and laws raise questions and create unique challenges for the respective parties - challenges that emerge within the context of the international investment laws governing foreign investment in ICTs. This article explores three particularly tenacious categories: strategic, structural, and substantive. Strategic challenges threaten macro-level interests and major policy aims that influence the survival and inherent functions of a nation state when considering and allowing actors from other locales to own and/or control technologies that have far reaching public policy implications including economic progress, national security, and human development. In contrast, structural challenges in this context relate to the compositional and definitional makeup of the investment agreements, demonstrating the incompatibility of terms and coverage detailed in investment agreements and treaties for investments in the ICT sector's intellectual property and digital assets. Finally, substantive challenges relate to the rights and duties included in investment agreement provisions and are key to determining what investors and host states can/cannot do post-investment.