2008

A Symmetric Analysis of the Border Control Information Systems for People and Trade

E. A. Whitley
London School of Economics and Political Science, e.a.whitley@lse.ac.uk

Boriana Rukanova
1Vrije Universiteit Amsterdam, brukanova@feweb.vu.nl

Follow this and additional works at: http://aisel.aisnet.org/ecis2008

A SYMMETRIC ANALYSIS OF THE BORDER CONTROL INFORMATION SYSTEMS FOR PEOPLE AND TRADE

Whitley, Edgar A., Department of Management, London School of Economics and Political Science, Houghton Street, London WC2A 2AE United Kingdom, e.a.whitley@lse.ac.uk

Rukanova, Boriana, Department of Economics and Business Administration, Vrije University Amsterdam, De Boelelaan 1105, 1081 HV Amsterdam, The Netherlands, brukanova@feweb.vu.nl

Abstract

Innovative egovernment systems are increasingly being used to manage border controls for both people and goods. While cross–border passage of travelers and cargo are usually treated separately in research and in practice we bring these together in order to identify similarities and differences. We use the concept of "symmetry" from Actor–Network Theory as our conceptual lens. We apply two types of symmetric analyses. In the first type, we treat both technological and social aspects as equally important. In the second type we analyze border crossing for both people and goods. Our analysis illustrates that in the context of crossing borders these two types of symmetric analysis are meaningful and appropriate. Whilst ANT has been advocated as a means of studying egovernment, few studies have explicitly drawn on the symmetry for such work and our paper contributes to this corpus of research. We illustrate that a number of problems are very similar for both people and good, so practitioners and researchers can benefit from exchanging ideas and practices and by doing so can accelerate egovernment innovation. We suggest that a strict symmetry concerning people/goods does not apply, so the boundaries of these similarities and differences require careful consideration.

Keywords: egovernment, border control; symmetric analysis; ANT; control of people and goods

1 INTRODUCTION

According to Dunleavy et al. (2006) "the ability to control entry to and exit from a territory is one of the critical defining features of a state" (p. 189). Thus governments seek to develop borders and border controls for a variety of reasons including economic, political and military concerns. The ways in which they do this varies over time as differing pressures and concerns come to the fore. For example, the introduction of the Schengen aquis has led to a much looser sense of borders within Europe to facilitate travel and trade, whilst simultaneously strengthening the borders to Europe (Andreas, 2003). In North America, the opening up of borders through NAFTA has been countered by security concerns and the creation of the Department of Homeland Security with explicit border control responsibilities following the terrorist attacks of 11 September 2001 (Salter, 2004).

Controls exist in relation to the passage of both people and goods across borders, with information technology playing an increasingly important innovative role in these border controls. As such, whilst border control is not a typical egovernment process as found in the extant literature, it is a key activity of modern government that is worthy of study.

This paper applies a symmetric analysis inspired by Actor–Network Theory (ANT) to egovernment in the form of border controls as they are found within Europe. The analysis is

inspired by two projects, in which the authors are involved, namely UK's proposed Identity Cards Scheme[1], which includes a focus on border crossing for people, and the ITAIDE[2] project, which focuses on cross–border trade. The symmetric analysis is undertaken at two distinct levels. First, in common with many ANT studies, the paper starts with the assumption that the process of border control is implemented by a heterogeneous network of humans and non–humans: border control police, border control technologies, identification cards, RFID tags, excise documents, EU policies etc.

A second level of symmetry is obtained by focussing on both the networks associated with border controls for non–humans (in particular the movement of goods) and humans (travellers moving between countries in Europe).

The contributions of the paper can be seen against these two levels of symmetry. At a practical level, the paper demonstrates the ways in which the different networks of border control are developed and sustained in the two cases and highlights the various ways in which information systems are embroiled in these networks. The paper also demonstrates the utility of symmetrical analysis of these two forms of border control by identifying common approaches to border control for humans and non–humans as well as areas where their implementation differs. The techniques and technologies of border control are traditionally treated distinctly and the analysis presented in this paper seeks to overcome this silo mentality in policy and practice. Finally the paper adds to the body of evidence that proposes the use of ANT as a suitable methodology for studying egovernment information systems (e.g. Bonner & Chiasson, 2005; Heeks & Stanforth, 2007; Stanforth, 2006). Although the ANT symmetry principle has been applied to the study of information systems more generally (Pouloudi & Whitley, 2000; Sarker et al., 2006) it has not been applied in the area of egovernment.

The structure of the paper is as follows. In section two, we propose to use the notion of symmetry from ANT as a way to study border control for humans and non–humans. In section three, we build on insights from the two projects to review the need to secure borders for travel and trade, the possible technologies that can be used and the role that international developments play in that context. Section four presents the results of our analysis, pointing towards similarities and differences between border control issues for people and goods. We end the paper with reflections on the applicability of the symmetry analysis of ANT to reason about border controls in terms of theory and practice.

2 BACKGROUND

In common with many social sciences, the technological and the socio–political have often treated separately (Latour, 1992). However it is increasingly recognized that real world problems don't map neatly onto the boundaries formed by academic fields, or the division between government, industry and academia (Gibbons et al., 1994).

Traditionally, border controls for goods and passengers are treated separately in research and in practice. The discussions concerning cross–border trade are usually focussed on supply chains, where the businesses are the regulated entities and the transactions can be positioned in the

---

[1] The LSE Identity Project (http://identityproject.lse.ac.uk) provides ongoing, independent analysis of the UK Government's proposals to introduce biometric identity cards for all UK citizens and to use similar technology to provide biometric immigration documents for non–EEA foreign nationals applying to extend their leave to remain in the UK.

[2] The ITAIDE project (www.itaide.org) aims to illustrate how, by using innovative technologies and by redesigning current customs procedures, the administrative burden for cross–border trade can be reduced, while preserving the control and security requirements.

context of Government–to–Business (G2B) interactions. As a result there is specific legislation that deals with regulating the cross–border flow of goods and specific (customs) departments are responsible for implementing the law. On the other hand, cross–border passenger traffic is usually concerned with individual people, rather than supply chains and can be seen in a Government–to–Citizen (G2C) context with very different legislative demands (e.g. privacy issues are of major concern).

Despite these apparent differences, some issues are common to both forms of border control. One example is security, which is an overarching concern for both, another is the use of information sharing technologies to identify and give faster passage to low risk cases. It therefore seems appropriate to use a research approach that can deal with humans and non–humans and Actor–Network Theory is proposed as a suitable approach for this area although other techniques (such as process models, stakeholder analyses or context diagrams) could also have been used.

2.1 ANT's symmetry principle

This paper uses the symmetry principle from Actor–Network Theory. ANT began as a theoretical approach for the study of scientists and engineers in society (Callon & Latour, 1981; Latour, 1987). Since then, it has been extensively applied and developed in areas as diverse as healthcare, FLOSS, gender and even university strategy development. Through this empirical work, its conceptual base has been refined and developed so that the 'core' of the theory can no longer be considered as a stable artefact. This has caused one of the theory's leading proponents to despair that readers "would complain a lot less about [the theory] … if they could download version ANT 6.5, instead of sticking with the beta" (Latour, 2005 n. 273 p. 207). Recent years have even seen "post ANT" studies (McLean & Hassard, 2004; de Laet & Mol, 2000; Darking & Whitley, 2007) that present considerably more sophisticated applications of the concepts developed from ANT than earlier, more 'programmatic' works.

Variously described as a new ontology, a methodological approach, a mindset of doing research or a set of guidelines for what counts as a good explanation of phenomena (Latour, 2005; Walsham, 1997), one of the key features of the theory has been the advocacy of methodological symmetry when considering human and non–human actants (Latour, 1992). That is, ANT questions the need to apply different theoretical apparatus for considering the actions, agency and activities of humans and those of non–humans.

In actor–network theory, human and non–human actors (or actants) attempt to build and maintain ('perform') stable linkages or networks that can achieve particular goals. One common illustration is the way in which a hotel manager enrols humans and non–humans to remind guests to leave their keys at reception when leaving the hotel (Latour, 1991) whereby a combination ('network') of the doorman and a large weight attached to the key attempt to regulate the behaviour of hotel guests.

In this paper we apply two types of symmetric analyses. Type 1 symmetric analysis focuses on giving equal consideration to both technological and social issues when discussing the complexities related to the management of border–crossing processes. That is, we argue that border–crossing processes are performed by heterogeneous networks of humans and non–humans. We apply a second form symmetric analysis (Type 2) by explicitly looking at both goods and people as 'Border–Crossing Actants' (BCAs) in order to identify similarities and differences between the two.

2.2   Data collection and analysis

The next section presents basic information about border–crossing processes drawn from the two research projects described above. Although some of the data collection for this section was inspired by ANT, much of the data collection followed traditional qualitative approaches: document analysis, interviews, industry presentations, meetings with stakeholders etc. Further details about the data collected can be found in the appropriate project references. The data was collected about both current and future developments related to border control issues for people and goods.

The symmetric analysis, however, was explicitly undertaken for this paper and used the two forms of symmetry described above to examine the data collected for the two projects. By presenting the two cases, the authors were able to develop insights into the similarities and differences between border crossing systems for goods and humans that form the basis for the presentation of the different systems and the subsequent analysis.

3   IS AND BORDER CONTROL FOR HUMANS AND NON– HUMANS

3.1   Why we need to secure borders?

Modern borders face many tensions. They define insiders and outsiders (Delanty, 2006), often drawing as much on historical memories and identities to do this as on physical characteristics. Governments have a number of obligations towards border controls for goods. These range from fiscal obligations (i.e. collecting duties to finance budgets) and security concerns (e.g. that bombs are not transported in containers) to protection of public health (e.g. quality checks on food products and pharmaceuticals). Similarly, there is a need to facilitate cross–border movement of workers (Ackleson, 2005), whilst governments are also expected to provide rigorous controls so that only legitimate individuals enter the country seeking work, employment and welfare benefits (Broeders, 2007)

3.1.1   The need to secure borders for goods

- Security

The 2001 attacks on the USA had direct consequences for the movement of goods. As Sheffi (2001) writes, "On the morning of September 11th, 2001, the United States and the Western world entered into a new era—one in which large scale terrorist acts are to be expected. The impacts of the new era will challenge supply chain managers to adjust relations with suppliers and customers, contend with transportation difficulties and amend inventory management strategies" (p. 1). In response to these events, the US government launched several security initiatives to tighten border security for imports and exports (Sheu et al., 2006). Security also became important in the EU (as can be seen from various EU policy documents (DG/TAXUD, 2006a; DG/TAXUD, 2006b) and the developments of concepts like Authorized Economic Operator Security (DG/TAXUD, 2006a)) and worldwide (as seen in documents of the World Customs Organization in concepts such as AEO and secure supply chains (World Customs Organization, 2005)).

- Fiscal fraud

Another reason for EU governments to secure borders is to be able to collect necessary taxes and duties and to prevent fiscal fraud. Fraud has flourished in several major areas, including fraud with goods that are in transit, VAT and excise fraud. For example, it has been estimated that in

1998 fraud related to the transportation of alcohol amounted to 1.5 billion per annum, approximately 8% of the total excise duties receipts on alcoholic beverages (European Commission, 2006). The market share of illegal cigarettes is equivalent to approximately 9% of the total excise duty receipts on tobacco products (European Commission, 2006).   VAT losses are also estimated to be approximately 10% of nett VAT receipts (European Union, 2006).

3.1.2   *The need to secure borders for humans*

- Security

Issues of border control of humans also took on a particularly high profile following the terrorist attacks on the USA on 11 September, 2001 when none of the nineteen terrorists had been identified as 'suspicious' by immigration authorities (Dunleavy et al., 2006 p. 193). As a result, border control was expected to shift its focus from, for example, the large numbers of individuals who might be seeking illegal employment in a country to small numbers of terrorists seeking to enter the country as unremarkable individuals (Andreas, 2003) bringing together the work of both policing and security services (Bigo, 2005).

- Benefit fraud

During Parliamentary scrutiny of the UK Identity Cards Scheme, government ministers emphasised how the collection of biometrics for visa purposes was "proving useful for ensuring the integrity of the border and of the immigration services" [Andy Burnham, 14 July 2005 Hansard Column 279]. As such, identity cards and other forms of border control would prevent foreign nationals from being able to live and work in the UK illegally and would help ensure that public services are not abused by people not entitled to receive them, thus reducing the incidence of benefit fraud.

3.2   Technologies for border control

As a result of these twin pressures to filter and enable cross–border transactions, there has been much talk of 'smartening' up borders, so that those individuals and goods identified as low risk (e.g. goods being transported with appropriate documentation, frequent travellers, those coming from countries perceived to be low risk etc.,) are allowed easy passage across borders, whilst those that might be more problematic (however defined) are subject to more rigorous controls (Salter, 2004). Various technologies have been proposed for managing this and these are now discussed.

3.2.1   *Technologies for controlling cross–border trade*

- Information systems

In terms of the transportation of goods, it was realized that coordinated action at the EU level was needed (European Commission, 2006). A number of EU–wide information systems were introduced to support information exchange between member states including the VAT Information Exchange System (VIES), the New Computerised Transit System (NCTS) and the Export Control System (ECS).   Furthermore, other systems are currently in various stages of development (e.g. the Excise Movement Control System (EMCS) for the excise procedure, (see also (DG/TAXUD, 2006a)). Many of these systems are intended to provide guarantees to the appropriate governments that the goods have left that country and that they have either arrived in the intended destination or have left the EU.

At present, for these systems to work, companies need to develop multiple data–sharing interfaces with government systems. The Beer Living Lab (see Baida et al., 2008; Rukanova et

al., 2007), part of the ITAIDE project, is one of a number of pilot projects that are seeking to link existing supply chain systems with these various government systems. These can allow authorized authorities to have direct access to their commercial supply chain information, an approach that relies on open standards and service–oriented architectures.

- Other technologies (tracking and tracing, scanning, reading)

A number of other technologies are used to secure the cargo, as well as to capture or to read information about the goods or the movement of goods. One example of such technology is the TREC (2007) device developed by IBM, which is a smart container seal. It has the capability to register predefined events like unauthorized opening of the container, or unexpected temperature changes. It also has tracking and tracing capabilities and can signal the deviation of a container from its predefined route. This information can be made available to the authorities for audit purposes. If the goods are en route, handheld devices can be used to extract information from the TREC.

3.2.2   Technologies for controlling cross–border travel

- Information systems

Information about passengers travelling between borders is being exchanged via computerised systems. Data from passenger name records (PNR) is increasingly exchanged automatically between immigration systems in countries to help the smart borders process (Hosein, 2005; Lyon, 2006). It is not clear, however, exactly what data should reasonably be exchanged, to whom and for what purposes (BBC News, 2007) as it could include identification data such as name, date of birth, telephone number; transactional data including the dates of reservations, the travel agent where appropriate, the information displayed on the ticket, the itinerary; financial data including credit card number, expiration date, invoicing address, etc.; flight information including flight number, seat number, etc.; and links to earlier PNR data (Hosein, 2005 p. 600) alongside passport and visa details.

- Other technologies

For passport controls, there has been extensive investment by EU countries in eBorders and biometric passports, a development described by the then British Prime Minister Tony Blair as part of "a visa and passport revolution across the EU and the developed world" (Anonymous, 2005). Biometric passports have a chip that contains details of a person's biometric (e.g. facial image and possibly fingerprint and iris) that can be used to compare the passport holder against the biometric data held on the passport. Biometric passports increasingly use RFID technologies to allow the biometrics to be read at border control points.

3.3   Policies and international dimensions

3.3.1   Goods

In the efforts to secure borders for goods, governments are faced with contradicting goals. On the one hand they have an obligation to control cross–border trade activities in order to ensure security and to prevent fraud. On the other hand, increasing such controls can lead to delays in supply chains, which can hamper the competitiveness of an economic zone. When we look at the EU as an economic zone, for example, we see policy documents like the Draft eCustoms vision statement and multi–annual strategic plan (DG/TAXUD, 2006b), which define the future developments in eCustoms in the EU and IT is seen as an important driver that can help to address the EU government dilemma. However, supply chain operations are normally not limited to one economic zone but operate world–wide. Thus, especially when it comes to issues like

security and trade facilitation, forces outside of the EU also play a role. These include developments in other economic zones (like the security programs in the US), as well as worldwide (like the developments in WCO (World Customs Organization, 2005)). If we look at security in the EU and the US, we can find that in both cases we have certification programs (AEO in the EU and C–TPAT in the US) which allow companies to be granted a low–risk status and hence faster clearance at the borders if they fulfil certain requirement. These may seem to be similar developments but they are all issued by different authorities and in different economic zones and the mutual recognition of certificates has not yet been established.

3.3.2   *People*

Regulations regarding travel documents for humans can be found at various levels, including national policies associated with the issuing of passports etc., regional policies such as the Schengen aquis that allows for the abolition of systematic border controls between the participating countries, and supra–national legislation that determines the form of machine readable travel documents proposed by the International Civil Aviation Organisation (ICAO). In addition, the requirements of particular countries, such as the US, for visa free travel affect questions of border control

This idea of using supra–national legislation as a means of driving national policy has been described as "policy laundering" (Hosein, 2004). For example, in the UK a key argument for the introduction of identity cards was that changing requirements for travel documents made biometric identity cards a technology whose time had come.

4   ANALYSIS

This section analyses the two cases of information systems for border control. The cases are summarised in Table 1.

	Goods	**Passengers**
Need to secure borders	* Physical security * Fiscal fraud prevention	* Security * Benefit fraud prevention
Technologies used	* Information systems (e.g. VIES, NCTS, ECS) * Track and trace (e.g. TREC)	* Information systems (e.g. PNR) *Technologically advanced travel documents (e.g. RFID enabled biometric passports)
Policies	* Zones (EU, EEA, WCO) * Certification Standards (AEO, C-TPAT)	* Zones (e.g. Schengen) * Standards (e.g. ICAO)

Table 1   Summary of cases

We proposed two forms of symmetry as the basis of our analysis. The first, Type 1, highlights the heterogeneous range of factors that affects the border crossing information systems. The second, Type 2 symmetry, arises from our analysis of two kinds of border crossing actants: passengers and goods.

4.1   Symmetry Type 1: The heterogeneous networks of border control

Latour (2005) requests that we maintain the thread connecting the different kinds of elements we find in our analysis. In the cases of border control considered in this paper, there are a number of different elements that contribute to current and future border control practices.

The BeerLL project illustrates the network of actants (both human and non–human) involved in cross–border trade controls (Baida et al., 2008; Rukanova et al., 2007). We have systems of companies and governments that exchange information about a shipment; containers that can be armed with smart seals and if needed, handheld devices that can be used to obtain information from the smart seal. The containers can be scanned using scanners at the harbour. Furthermore, the authorities can decide to open a container and perform a physical inspection.

In the case of border controls for humans, the border control actants include international specifications of machine readable travel documents (based on policies produced by the ICAO) and the use of technologically advanced passports that incorporate biometric and RFID chips. These documents are examined by border control / immigration staff who may simply perform a visual inspection of travel documents, or may check the documents by using specialist readers potentially connected to databases of migrants and the passenger record data provided by the carrier.

Thus, we see that in both cross–border travel and trade, heterogeneous networks of actors are involved in controlling the processes. There are even links between the networks for border control for humans and those for border controls on goods. According to a recent report in The Observer newspaper the new Unified Border Force in the UK, formed by merging thousands of staff from Revenue and Customs, the Immigration and Nationality Directorate, and UK Visas, the passport agency is having to perform a range of border control functions, often with limited training or preparation. Thus, immigration staff (dealing with travellers) are being expected to undertake the duties of customs staff (who deal with goods) and vice versa (Doward, 2007).

It is important to note, however, that these networks may not necessarily be as strong or as stable as policy makers intend. For example, there is growing evidence that the chips being used in British biometric passports may only have technical warranties for two years, and can take an undue amount of time to 'read' at the border control point (National Audit Office, 2007). Similarly, whilst for cross–border trade there is a strong political will to have scanning of all containers it is not clear whether all ports are able to scan such large numbers of containers and interpret the data that will be accumulated. Thus, even if the networks of actants can be created, their long term stability cannot be guaranteed.

4.2 Symmetry type 2: Border–Crossing Actants (human and non–human)

With a number of apparent similarities between the border controls for humans and non–humans, it is instructive to explore some of the similarities and differences between these two in more detail.

4.2.1 The need to secure borders

As described above, in both cases the need for border controls for security purposes is significant: the checks are there to enable potentially problematic crossings to be identified and addressed. Similarly, both cases provide opportunities for pre–screening of border–crossing actants to allow those who have been checked and awarded low–risk status to have preferential passage with limited further checks required.

In terms of border controls to address fraud, whilst controls on humans can have an impact on fraudulent employment or benefit claims, addressing fraud is typically a relatively low priority. In contrast, fraud prevention is a major issue when it comes to cross–border trade. Fraud with excise, VAT, as well as transit goods can amount to billions of Euros and failure to identify such fraud can have direct effects in terms of lost revenue for national and EU budgets. Thus there is convergence between the two in the need to control borders for security reasons but there is less convergence for fraud control.

4.2.2   Technologies for border control

- Information systems

Both systems place a significant emphasis on the proper exchange and use of information in operating border controls. Companies need to send pre–departure information to the authorities in advance, which allows authorities to undertake risk analysis and decide whether they want to make a physical inspection of the cargo. For passengers, preferential passage is contingent on information about the traveller being made available in advance of the border crossing and in some cases (e.g. flying to the US) is a requirement before departure can be authorised.

In both cases, there are procedures in place that allow fast border passage for low risk individuals and companies. For companies, obtaining a low–risk status can be done via different certification procedures. Governments extensively study the company's internal IT systems and procedures to see whether the necessary control mechanisms are in place. Based on that analysis they can grant the company low risk status that allows them to ship their goods with the minimum of intervention allowing more emphasis on companies that represent a higher risk.   The identification of low–risk individuals typically involves a detailed security check as part of the enrolment into the scheme plus the collection of appropriate biometrics (e.g. iris biometrics). At present, however, these systems and procedures for low–risk border–crossing actants are not universal. For citizens, they are limited to particular locations (e.g. airports) or industry player (e.g. particular airlines). For companies, they are limited to a specific country or economic zone (e.g. the AEO certificate in the EU and the C–TPAT certificate in the US).

- Other technologies

Reading, tracking and tracing: In both cases, we see that technologies to read the electronic information play an important role. For example, it is becoming increasingly the norm that goods are tracked throughout their entire passage, not just when they cross the border itself: a container equipped with a TREC device can provide continuous location information and signal any deviation from a predefined route. For human travellers, the information collection / use is limited to information presented when booking the travel ticket and details of the travel document presented at the border control point. Although modern travel documents contain RFID chips, the RFID transmission is often not enabled until the document is 'scanned' at the control point.

Scanning and detecting: Scanners are used both for passengers, as well as for cargo. In the case of passenger travel by plane, 100 percent scanning is done; passengers need to pass through security gates and their luggage is scanned. For cargo, scanning is currently done on a limited number of containers, however for some economic zones like the US, it is expected that checks of all containers will soon become mandatory.

Smart container seals (e.g. TREC) aim to guarantee that the goods that were sent with the container were exactly the same as those that were received or notify the authorities that the container has been opened. Similarly, travel documents are intended to be tamper proof and the chip may not be read unless certain conditions have been met, such as the passport being fed through a suitable reader.

4.2.3   Policies and international dimensions

With respect to both travel and trade, we see different levels of borders and border control. However, a noticeable difference arises in terms of the geographical boundaries that apply to the different kinds of border controls. Thus, in terms of taxes and duties like VAT and excise, the important boundaries are the national borders or the EU as whole, whereas for human travel, the Schengen aquis (which covers most of mainland Europe) does not apply to the UK and Ireland

(which instead have a common travel area agreement). Thus within Schengen there are no border controls for humans, but a traveller coming from Schengen to the UK (e.g. coming from the NL to the UK) will have to pass through a border control. This illustrates that although in both cases we have certain defined border controls, the geographical boundaries of these borders are not necessarily the same for people and goods.

In both travel and trade, we see that policies and regulations are often not limited to a single country. Often these are driven by developments in other countries, economic zones, or events. As we already identified, although some of these drivers and events may be of similar nature for both trade and travel (e.g. security), other may be specific to only one or the other (e.g. fraud for trade).

5   CONCLUSIONS

This paper has proposed the use of ANT symmetry to study innovative egovernment practices regarding border control. Our analysis leads us to the observation that there are different levels at which symmetry between cross–border travel and trade may be identified. An implication for research and practice is that at the level where symmetry exists, learning about the two domains (people and goods) can be meaningful and insightful and can accelerate egovernment innovation. If we take traceability as an example, there is a lot of knowledge about how to do tracking and tracing of goods, which can be helpful if, in the future, a need for such a process is required for people. At the same time, the identification of differences can be a useful source of insights as well. It can help to reveal the unique features of border–control for people and goods. For example, the people domain is much more concerned with issues of privacy protection and this knowledge can bring valuable insights in the context of cross–border trade.

In terms of Type 1 symmetry, the paper has demonstrated that border control practices for goods and travellers involve a heterogeneous network of humans and non–humans, including intelligent devices, border control staff and international policies.

In terms of Type 2 symmetry, the paper explored the similarities and differences between the different types of border crossing actants. This strategy has proved particularly informative as it has highlighted a number of symmetries and synergies between the current practices of border control for both. For example, the cases illustrate that on a high level, the types of technologies that are needed for border control for goods and people are quite similar (readers, scanners, information carriers, identification technologies etc.). At a more detailed level, however, we can identify differences, as some technologies and processes are more appropriate for people but not for goods and vice versa.

In terms of contribution to theory, our paper is one of the first to apply ANT's symmetry principle to egovernment applications and we have demonstrated the utility of this approach and advocate it as a useful method for further research in egovernment and information systems more generally.

Acknowledgments

References

Ackleson, J. (2005) Border Security Technologies: Local and Regional Implications. Review of policy research 22 (2), 137-155.

Andreas, P. (2003) Redrawing the line: Borders and security in the twenty-first century. International security 28 (2), 78-111.

Anonymous (2005) Time has come for ID cards, says Blair The Daily Telegraph 28 June Archived at http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/06/27/uid.xml&sSheet=/portal/2005/06/27/ixportaltop.html

Baida, Z., Rukanova, B., Liu, J. and Tan, Y.-H. (2008) Preserving Control in Trade Procedure Redesign - The Beer Living Lab. Electronic Markets, The International Journal 18 (1), 53-64.

BBC News (2007) Q&A: EU passenger data row 31 January Archived at http://news.bbc.co.uk/1/hi/world/europe/5029258.stm

Bigo, D. (2005) Globalized (in)security: the Field and the Ban-opticon. Traces: a multilingual series of cultural theory 4,

Bonner, W. and Chiasson, M. (2005) If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. Information and Organization 15 (4), 267-293.

Broeders, D. (2007) Irregular Migrants: The New Digital Borders of Europe: EU Databases and the Surveillance of. International sociology 22 (1), 71-92.

Callon, M. and Latour, B. (1981) Unscrewing the big leviathan:. In Advances in social theory and methodology (Knorr-Cetina, K. and Cicoure, A., Eds), Routledge & Kegan Paul, Boston.

Darking, M. L. and Whitley, E. A. (2007) Towards an Understanding of FLOSS: Infrastructures, Materiality and the Digital Business Ecosystem. Science Studies 20 (2), 13-33.

de Laet, M. and Mol, A. (2000) The Zimbabwe bush pump: Mechanics of a fluid technology. Social studies of science 30 (2), 225-63.

Delanty, G. (2006) Borders in a changing Europe: Dynamics of openness and closure. Comparative European Politics 4 (2/3), 183-202.

DG/TAXUD (2006a) Authorized Economic Operators Guidelines 24 May 2006 Archived at http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_security/AEO_guidelines_en.pdf

DG/TAXUD (2006b) Electronic Customs Multi-Annual Strategic Plan (MASP Rev 7), Working document TAXUD/477/2004 - Rev. 7 - EN, 24 May 2006. European Commission, Taxation and Customs Union 24 May 2006 Archived at http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/e-customs_initiative/MASP_rev7.pdf

Doward, J. (2007) Flagship border force 'puts security at risk' The Observer 28 October Archived at http://www.guardian.co.uk/politics/2007/oct/28/immigration.immigrationpolicy

Dunleavy, P., Margetts, H., Bastow, S. and Tinkler, J. (2006) Digital era governance: IT corporations, the state and e-government. Oxford University Press, Oxford.

European Commission (2006) EU coherent strategy against fiscal fraud - frequently asked questions, MEMO/06/221 31 May 2006 Archived at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/06/221

European Union (2006) Taxation and customs Archived at http://ec.europa.eu/taxation_customs/taxation/tax_cooperation/reports/index_en.htm

Gibbons, M., Limoges, G., Nowotny, H., Schwartzman, S., Scott, P. and Trow, M. (1994) The new production of knowledge: The dynamics of science and research in contemporary societies. Sage, London.

Heeks, R. and Stanforth, C. (2007) Understanding egovernment project trajectories from an actor-network perspective. European Journal of Information Systems 16 (2), 165-177.

Hosein, I. R. (2004) The Sources of Laws: Policy Dynamics in a Digital and Terrorized World. The information society 20 (3), 187-199.

Hosein, I. R. (2005) Transforming travel and border controls: Checkpoints in the Open Society. Government Information Quarterly 22 (4), 594-625.

Latour, B. (1987) Science in action: How to follow scientists and engineers through society. Harvard University Press, Cambridge, MA.

Latour, B. (1991) Technology is society made durable. In A sociology of monsters: Essays on power, technology and domination (Law, J., Ed), pp 103-131, Routledge, London.

Latour, B. (1992) Where are the missing masses? The sociology of a few mundane artifacts. In Shaping technology / Building society: Studies in sociotechnical change (Bijker, W. E. and Law, J., Eds), pp 225-258, The MIT Press, Cambridge, MA.

Latour, B. (2005) Reassembling the social: An introduction to Actor-Network-Theory. Oxford University Press, Oxford.

Lyon, D. (2006) Airport Screening, Surveillance, and Social Sorting:Canadian Responses to 9/11 in Context. Canadian Journal of Criminology and Criminal Justice 48 (3), 397-411.

McLean, C. and Hassard, J. (2004) Symmetrical absence / symmetrical absurdity: Critical notes on the production of actor-network accounts. Journal of Management Studies 41 (3), 493-519.

National Audit Office (2007) Identity and Passport Service: Introduction of ePassports 5 February Archived at http://www.nao.org.uk/publications/nao_reports/06-07/0607152.pdf

Pouloudi, A. and Whitley, E. A. (2000) Representing human and non-human stakeholders: On speaking with authority. In Organizational and social perspectives on information technology (Baskerville, R. and Stage, J. and Gross, J. I. D., Eds), pp 339-354, Kluwer, Aalborg, Denmark.

Rukanova, B., Henriksen, H. Z., von Raesfeld, A., van Stijn, E. and Tan, Y.-H. (2007) A Collective Action Perspective on Technological Innovation in Business/Government Networks. In Proceedings of the Fifteenth European Conference on Information Systems (Österle, H. and Schelp, J. and Winter, R., Eds), pp 2135-2146, St. Gallen.

Salter, M. B. (2004) Passports, Mobility, and Security: How smart can the border be? International studies perspectives 5 (1), 71-91.

Sarker, S., Sarker, S. and Sidorova, A. (2006) Understanding business process change failure: An actor-network perspective. Journal of Management Information Systems 23 (1), 51-86.

Sheffi, Y. (2001) Supply chain management under the threat of international terrorism. International Journal of Logistics Management 12 (1), 1-11.

Sheu, C., Lee, L. and Niehoff, B. (2006) A voluntary logistics security program and international supply chain partnership. Supply chain management: An international journal 11 (4), 363-374.

Stanforth, C. (2006) Using actor-network theory to analyze egovernment implementation in developing countries. Information technologies and international development 3 (3), 35-60.

TREC (2007) TREC Archived at http://www.zurich.ibm.com/csc/process/securetradelane.html

Walsham, G. (1997) Actor network theory and IS research: Current status and future prospects. In Information systems and qualitative research (Lee, A. S. and Liebenau, J. and Degross, J. I., Eds), Chapman and Hall, Philadelphia.

World Customs Organization (2005) Framework of standards to secure and facilitate global trade Archived at http://www.Wcoomd.Org/ie/en/press/wco%20-%20framework%20of%20standards%20june%2021%20final.Pdf