EG 2061

Towards an Information Strategy for Combating Identity Fraud in the Public Domain: Cases from Healthcare and Criminal Justice

Marijn G.A. Plomp and Jan H.A.M. Grijpink
Utrecht University, The Netherlands
m.g.a.plomp@uu.nl
j.h.a.m.grijpink@uu.nl

Abstract: Two trends are present in both the private and public domain: increasing interorganisational co-operation and increasing digitisation. More and more processes within and between organisations take place electronically, on local, national and European scale. The technological and organisational issues related to this prove to be difficult on a local scale and barely manageable on national and European scales. We introduce the theoretical framework of Chain-computerisation, which explains large-scale chain co-operation as an answer to a dominant chain problem. Identity fraud proves to be the dominant chain problem in many chain co-operation situations. Therefore, our main research question is: how to arrive at a successful information strategy to combat identity fraud in the large-scale processes that constitute the public domain? We demonstrate the problem of identity fraud on the basis of two Dutch cases, from the criminal justice chain and the healthcare sector. These cases are taken from our chain research programme in which we test empirical findings against the theoretical framework of Chain-computerisation to derive a successful chain-specific information strategy. In both cases, the problem of identity fraud presents a threat to the chain co-operation. Identity fraud has to be tackled with an approach focused on large-scale processes and with specific person-oriented security procedures and instruments preventing identity fraud from happening undetected. This study forms an important contribution to information science and to the security realm that still pivots only on traditional authentication frameworks that cannot cope with 'wrong person' identity fraud. In large-scale situations, therefore, additional safeguards will be necessary. Taking into account that the problem of identity fraud rises in many other domains and countries as well, we conclude that it is a major threat to the European society. Finally, we argue that chain-specific information systems with random identity verification enable combating identity fraud.

Keywords: chain-computerisation, interorganisational information systems, chain co-operation, information strategies within the public sector, identity management, identity fraud

1. Introduction

Interorganisational co-operation is becoming increasingly important, as organisations are more and more interdependent. ICT can support the development of interorganisational relations through cost reduction and/or increasing possibilities for communication and coordination (Williams 1997). Since the internet has become mainstream, many organisations communicate with each other through this channel. This can be in the form of basic means like e-mail messaging, but nowadays also often takes place using advanced ICT applications like chain information systems. These developments are visible on local, national and European scales.

Research, strategy and policy often focus only on technological issues, like standards for interorganisational information exchange. Organisational issues however, like who co-operates with whom, shares which information and why, are complex and important as well. It can therefore be argued that attention should be given to both dimensions (Plomp and Batenburg 2010). Both technological and organisational issues prove to be difficult on a local scale and barely manageable on national and European scales, because the number of parties increases greatly and because of differences in culture, legislation and ICT infrastructure. These factors explain the difficulties and sensibilities that are encountered in large-scale interorganisational chain information infrastructures. Even when these large-scale communication initiatives are successfully deployed, there are many potential problems in their use that need to be taken into account. As interorganisational co-operation in the information age is becoming increasingly important, everyone working in (e-)government should be aware of its inherent risks. In this paper, we present those risks using two cases from the vital domains of criminal justice and healthcare.

We argue that one of the main threats in these domains is identity fraud, and show the potential danger if this problem is not properly handled.

In this paper, we introduce the theoretical framework of Chain-computerisation that explains large-scale chain co-operation as an answer to a dominant chain problem (see §2). Identity fraud proves to be the dominant chain problem in many chain co-operation situations. Many people think that through further securing the authentication process, the risk of identity fraud can be reduced (e.g. Drogkaris, Geneiatakis, Gritzalis, Lambrinoudakis and Mitrou 2008). This basic security is necessary, but we claim that this is only sufficient for small-scale situations. In large-scale chain co-operation situations, traditional authentication systems and procedures prove to be unable to cope with 'wrong person' identity fraud. Identity fraud proves to be hard to prevent in these situations. Therefore, our main research question is:

How to arrive at a successful information strategy to combat identity fraud in the large-scale processes that constitute the public domain?

In order to provide an answer to this question, the remainder of this paper is structured as follows. First, we present the theory of Chain-computerisation and the three components of its chain perspective. This provides the background against which we formulate our approach for combating identity fraud. We describe our research method and pay specific attention to the process of conducting a chain analysis and deriving an information strategy from that. Next, we present our two cases in which identity fraud plays a central role, and indicate how this phenomenon can be countered. We conclude with our main findings and suggest some topics for future research.

2. Chain-computerisation and its specific chain perspective

Chain-computerisation (Grijpink 1999; 2010) is a theoretical framework which explicitly focuses on large-scale social chains, not on logistic chains (the process of handling goods), nor on information chains (closely linked information systems). Examples of social chains are social security, criminal law enforcement or drug addicts' healthcare: large-scale interorganisational processes that yield a social product such as income support, safety or survival.

Central to the theory of Chain-computerisation is a specific chain perspective to better understand large-scale chain co-operation processes and chain communication systems. This chain perspective consists of three components. The first component is the concept of a *dominant chain problem*; a problem that no party in the chain can solve on its own. The second component is the idea that a chain should be seen as a *multi-level phenomenon*, enabling a distinction between automation at the 'base level' and the 'chain level'. The third component is the *acknowledgement of irrational decision making at the collective chain level*. The rationale of this chain perspective is recognising *fallacies of the wrong level*. They lead to invalid assumptions and unjustifiable expectations causing large-scale communication systems to fail or sometimes even backfire. We will now discuss these four central elements.

2.1 The dominant chain problem as the trigger of chain communication

In a social chain, thousands of organisations and professionals work together without a clear relationship of authority, in ever-changing combinations depending upon the actual case. However, co-operating with other organisations and professionals takes a great deal of effort, time and money. There must be a cast-iron reason for doing so. Chain partners only co-operate if they are forced to do so by a dominant chain problem. A dominant chain problem is one that none of the partners can solve on its own. It is only by effectively co-operating that chain partners can prevent the systematic failure of their own organisation and the entire chain. Because common interests are less pronounced than people usually think – and are also often unclear – the badly needed cohesion can only be provided by a pressing dominant chain problem. Only such a barely-manageable problem can create an interplay of forces which triggers large-scale co-operation of so many organisations and individuals and promotes the development and maintenance of a large-scale chain communication system focused on the dominant chain problem. In a chain analysis, the dominant chain problem – if any – is uncovered, defined, examined and tested against the theoretical requirements that must be fulfilled to qualify as a trigger for large-scale chain co-operation. If in a specific chain a dominant chain problem cannot be found or – upon examination – does not seem to be vigorous or tenacious enough, a large-scale ICT-project for this chain will predictably fail or falter.

Thus, the dominant chain problem determines to a large extent the feasibility of a large-scale chain communication system.

2.2 The chain as a multi-level phenomenon

The theoretical framework of Chain-computerisation sees a chain as a multi-level concept (see Figure 1). It makes a distinction between interorganisational (or chain) information systems at 'chain level' on the one hand, and *intra*-organisational information systems (or source registers) at the 'base level' of the chain, that can be linked to a chain information system, on the other hand. A chain information system automatically detects in which intra-organisational system relevant information can be found or, for instance, which organisation should be informed depending on the actual dominant chain problem that the chain co-operation is focusing on. The dominant chain problem determines the content of the necessary chain communication. This chain communication is brought about even when chain partners themselves do not know which organisations are involved in the case at hand.

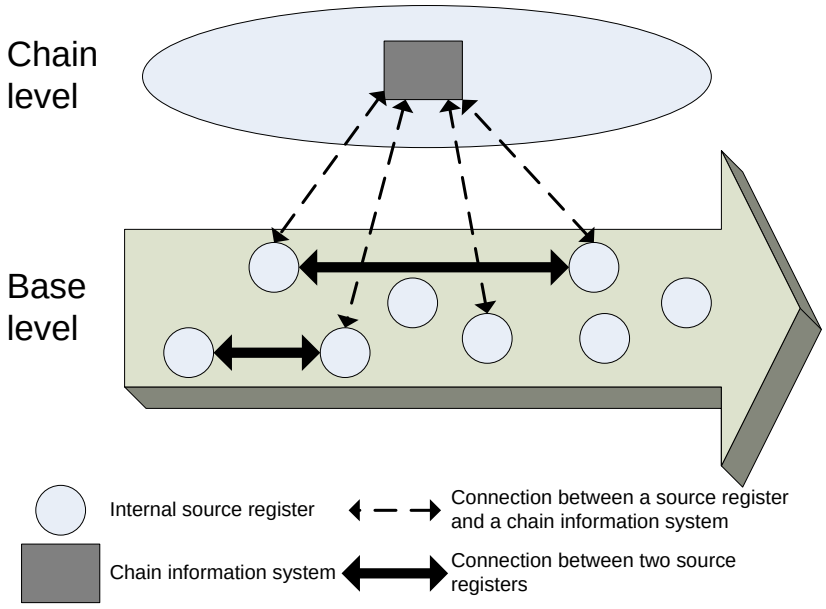

Figure 1: Two distinct levels of analysis, with different types of information systems

This distinction is meant to analytically enable separating information collection and storage in source registers from communicating essential details throughout the chain using chain information systems. It directs our attention to two notions:

- According to the theory of Chain-computerisation, only the critical details that are absolutely necessary for preventing the dominant chain problem should be available at the chain level.
- Irrational decision making takes place at the chain level, as will be explained next.

This way, large-scale chain communication systems have only minor influence on the chain partners' autonomy; projects meet less resistance, so the critical mass of participating organisations is reached as soon as possible.

This multi-level scheme – for a better understanding of the problems inherent in large-scale chain co-operation and communication – can be applied to any large-scale phenomenon.

2.3 Acknowledgement of irrational decision making at the collective chain level

Because overall leadership or authority is absent, the chain is a difficult administrative domain in which decision making and information exchange proceed differently than *within* organisations. Rationality and efficiency are often hard to find at the collective chain level and, as a consequence, unpredictability and lack of control are the order of the day. A model of irrational decision making that fits well with the

processes that take place at the chain level is the garbage can model of Cohen, March and Olsen (1972; March and Olsen 1976). This model states that the outcome of decision processes results from combining a random selection of problems, solutions and decision makers. Often this concept of irrationality at the chain level is hard to grasp. The crux is that – as there is no single party in command – group processes at the chain level are not rational, even if every individual professional and organisation acts rationally. The theoretical framework of Chain-computerisation takes this lack of an overall co-ordinating and enforcing authority as its starting point. Large databases containing substantive data to be used by many independent organisations call for more authority and willingness to co-operate and pool resources than are usually present in chains. Collective decision making is chaotic and unpredictable. Therefore, chain solutions should be basic and non-complex. A simple alert mechanism using a chain information system at the chain level is often the maximum result that can be attained.

The significance of a decision model as a component of our chain approach is that it creates awareness of the inherent complexities of any large-scale situation and warns against expecting clear objectives, ample support or well-articulated decisions. At the chain level, these ideal conditions will not be found. Instead, the model teaches us to expect setbacks and to develop chain communication systems only in a very gradual way.

2.4 Fallacies of the wrong level

In information science – as well as in management – we usually derive insights from small-scale situations such as a local information system, a small group experiment or a regional pilot. Thus, we have gained insights into the power of recording data and in management tools such as time schedules and budgets. If we transpose such insights to large-scale situations without checking the validity of underlying assumptions at that level, we often make a 'fallacy of the wrong level' (cf. Galtung 1969). This might partly explain why so many policy measures and large-scale systems unexpectedly produce poor results, fail or falter – and sometimes even backfire.

The concept elaborated upon in the previous subsection provides a good example of such a fallacy of the wrong level. Expecting that chain decision making takes place in a rational and well-articulated manner seems logical, as individual organisations use to behave rationally. At the collective chain level, however, this cannot be the case because essential preconditions for rational decision making are not fulfilled. Another example is providing a single sign-on e-government architecture, as discussed by Drogkaris et al. (2008) for the Greek situation. Although this may seem convenient from the perspective of an individual user, it also means that once a malevolent person obtains the possibility to fraudulently sign on, (s)he has access to all e-government services. The notion that a person who provides the right credentials (e.g. username and password) does not necessarily imply that this is also the right *person*, is important in this respect. In small-scale situations, the focus is often only on optimizing the authentication procedure. In large-scale situations, the focus should also be on preventing malicious use of these authentication means by someone other than the authorised person.

The theoretical framework of Chain-computerisation suggests several remedies against making fallacies of the wrong level, while taking into account the needs and preconditions of large-scale chain co-operation. One such remedy could be, for instance, taking a gradual approach to the development and implementation of large-scale systems. Most of all, we must stop treating large-scale communication systems as intra-organisational information systems with a somewhat larger group of users. This is a classic fallacy of the wrong level. Chain-computerisation features a chain approach with its three pillars (§2.1 - §2.3) which – taken together – provide professionals and researchers with a compass that is better suited for a working environment without a co-ordinating and enforcing authority, thus preventing from making fallacies of the wrong level that cause projects and systems to fail or falter.

3. Chain-computerisation and its method of chain analysis

Apart from the chain perspective, the theoretical framework of Chain-computerisation offers a specific method for chain analysis, to better assess the feasibility of large ICT-projects and information systems. The examples that we present in the following two sections are case studies taken from our chain research programme at Utrecht University based upon this method. This programme has an exploratory, empirical character and mainly consists of conducting chain analyses. A chain analysis tests empirical

findings against the theoretical framework of Chain-computerisation, to derive a suitable chain-specific information strategy to cope with the dominant chain problem.

By now, we have performed over 25 analyses of Dutch and international chains (Plomp 2011). For each chain analysis, desk and field research have been performed. Data collection took place from 2005 till 2010. By interviewing a number of stakeholders within a chain, we try to obtain an accurate picture of it, estimating the value of the variables used in the chain analysis. Each chain analysis consists of constructing the four assessment profiles provided by the theory of Chain-computerisation: the mission, coordination, information, and co-operation profile. Completing these profiles entails, among other things, determining what the dominant chain problem is and what critical details are necessary to prevent the dominant chain problem from spoiling the result of the chain co-operation effort, assessing the required coordination forms in this specific chain and gauging the current level of chain-wide co-operation. An example of constructed assessment profiles for the chain analysis of the manic-depressive disorder chain-of-care can be found in a recent article in the Journal of Chain-computerisation (Grijpink, Visser, Dijkman and Plomp 2010, pp. 5-6). The results of this chain analysis, together with other input from the interviews, make it possible to formulate a successful information strategy (Grijpink et al. 2010, p. 7).

Generic, recurring results of the more than 25 conducted chain analyses thus far have bearing on the dominant chain problem, fallacies of the wrong level and identity fraud (Plomp 2011). We have already seen the dominant chain problem and fallacies of the wrong level. In practice, identity fraud is poorly understood causing many social chains to dysfunction or be disrupted. Therefore, before turning to our two examples, we briefly explain the peculiar character of identity fraud. Identity fraud – using or stealing somebody else's identity with malicious intent – is becoming a major issue in our information society. The real problem is that if an identity fraud succeeds, all clues and traces lead to the victim instead of the culprit. Afterwards, the culprit cannot be found and the victim subsequently has much difficulty proving his/her innocence. Identity fraud is difficult to detect while it is taking place unless special preventive tools and procedures are installed. This is usually not the case. Thus, identity fraud goes by unnoticed. A major challenge, indeed.

The phenomenon of identity fraud leaves us with difficult puzzles. Identity checking as a process is greatly predictable and observable because it takes place in public spaces. Making identity checking less predictable is a major challenge, but rewarding because identity fraudsters do not want to be caught. Usually, we check identities with only one ID-instrument, which makes the process vulnerable because checks with one ID-instrument can easily be manipulated. But how can we check identities with two or three independent ID-instruments at the same time? That requires a careful situational design of the process, which has to be variable in order to diminish the predictability of the process. Another difficult characteristic of identity fraud is that its magnitude is very hard (if not impossible) to measure. Every statistic is useless, as it only indicates how often the fraud has been detected: successful identity fraud goes by unnoticed. With this realisation in mind, news items stating that "the incidence of fraud has gone down" suddenly become much less positive.

The chain perspective provides a better understanding of the problem of identity fraud by revealing that its real damage will ultimately be the disruption of important large-scale communication systems. Moreover, once a person has fraudulently changed his/her identity in one chain, the new 'identity' can affect other chains as well in which it is no longer possible to see through the preceding fraudulent identity change. Thus, our chain research programme has resulted in a more realistic view of our interorganisational world and will in turn lead to better information strategies for successful large-scale information infrastructures for national or international chain co-operation.

4. Case 1: Identity fraud in the Dutch criminal justice chain

4.1 The criminal justice chain at the national level

Because successful identity fraud cannot easily be detected and mostly goes unnoticed, only rarely can a successful fraudster be detected because (s)he is still there. One such situation where this *is* possible, is the prison cell. If a criminal finds someone willing to sit out his/her sentence in his/her place, we find his/her stand-in person in the cell. Alternatively, if the criminal has been successful in using the identity of someone else, we find the right person in the cell but with an identity that is not his/her own. If this identity fraud goes undetected, the criminal is untraceable after his/her release because the administrative details of the verdict – stored in the criminal registry for later use – point to someone else. This scenario could

explain how a criminal sometimes succeeds in pursuing his/her career with a clean slate without links to his/her previous aliases.

In 2004, more than 100,000 sets of criminal fingerprints linked to more than one administrative identity had been registered in the Dutch national forensic biometrics system HAVANK (Grijpink 2011). The cleverest criminals had succeeded in using more than 50 aliases, implying that they had managed to get their criminal verdicts spread to as many criminal records of other persons (who may not be aware of this). Note that this volume of identity fraud may be even bigger because a fingerprint set linked to a single name does not guarantee that this name actually belongs to the criminal. This volume of aliases was the result of only fifteen years of automatic biometric fingerprint checking in only a limited number of criminal cases, because until October 2010, the Criminal Procedure Law allowed the use of forensic biometrics only if necessary to prove someone's involvement in the criminal case at hand. An immediate confession thus prevented biometric identity checking. If the criminal retracted his confession in court, he could be pretty sure that fingerprint checking would not be done in this stage of the prosecution. Since January 2011 however, the Dutch Criminal Procedure Law provides for compulsory biometrical identity checking for every serious crime.

Apart from the HAVANK system, which is positioned at the base level of the chain, the criminal justice chain also has a chain information system at the chain level, a reference index for persons called VIP. This chain information system contains for every registered criminal a personal criminal number (the VIP-number) and a set of references pointing to criminal law enforcement agencies actually involved in this person's criminal justice procedures. The VIP-number is issued to a criminal when (s)he is registered in the information system of one of the chain partners for the first time; it will never be re-issued to another person and will be used at every new contact with one of the chain partners during the rest of his/her life. By 2004 however, the VIP system had already administered more than 1.2 million VIP-numbers since the introduction of the system in 1993. In 2004, this huge amount of VIP-numbers issued to first offenders suggested a large volume of identity fraud, because the Dutch population could not possibly account for so many criminals.

The above two systems, HAVANK and VIP, illustrate the apparent pollution that is present in the information systems of the Dutch criminal justice chain, as a consequence of successful identity fraud. In the future, this can be prevented or at least reduced by improving identity checking of criminals (i) by the police and (ii) in prisons:
(i) The police perform identity checking at the beginning of the chain. They used to do this by asking for an identity document or for name and address which are then checked against the residents' register of the relevant municipality. However, if name and address go together but belong to another person, this checking causes a wrong name mentioned in the official report as well as in the subsequent summons and criminal verdict. This way the criminal will leave the chain with a clean slate when using his real identity. In the new procedure since January 2011, the police have to perform a biometric identity check first together with high resolution photographs, both taken simultaneously at the start of the procedure. If more than one trustworthy identity comes up, a thorough identity investigation is required by law with the possibility of special detention.
(ii) Until recently, the detention process was only supported by an administrative information system. Nowadays, prison management also uses biometric details in order to check at every internal movement or leave whether there is a biometric match.

If the above is done properly by the police and the prison, the value of trying to use another name or sending somebody else to serve a sentence is greatly diminished. Still, we are left with the challenge of verifying that older verdicts have been booked under the right name.

4.2 Fading borders: The criminal justice chain at EU-level

As criminals more frequently operate internationally, criminal justice will also need to operate across national borders more often. Let us now see how extending this national scale to an international scale complicates our national approach. The difficulties that make national chain processes barely manageable hold even more for the European situation.

An example of this increased complexity is the case of Michel Fourniret. This Frenchman was sentenced in France to long-term imprisonment having raped and murdered several young women. By moving to Belgium, he was able to start with a clean slate and even work at a school there. Apparently, the Belgian

police never questioned the French criminal registry. The Belgian education chain might have questioned the Belgian criminal registry because, in many EU member states, Fourniret's job was considered sensitive enough to ask a job candidate for a so-called declaration of good conduct. However, consulting the Belgium criminal registry would wrongly have produced a clean slate, as his criminal past was only registered in France. To avoid this from happening in the future, criminal record information must be exchanged between EU-member states at the moment of a sensitive appointment of a person with another nationality. This communication will only be correct if two conditions are met:

- The national criminal law enforcement chain in every member state prevents identity fraud in its own criminal procedures.
- Each member state sends every criminal verdict to the convict's member state of nationality while preventing identity fraud during this transfer.

This implies a close co-operation among police forces within the EU, focused on the identity of their nationals in other EU-countries using the forensic biometrics procedures of the home country (i.e. the country of origin, not the country were the crime was committed). Chain-computerisation theory tells us that a physically centralised EU registry for criminal justice cannot be expected to work adequately at this enormous scale. Fortunately, at the moment, the efforts are being aimed at a bilateral exchange of criminal verdicts regarding member states' nationals based on a central access system and the use of the national biometric identities. In line with the theory of Chain-computerisation, this will eventually lead to a distributed EU criminal registry based on biometric identities that might be able to prevent criminal cases such as Fourniret's from happening again. At the moment, we are very far from this ideal situation, but much will already be gained if every criminal verdict that is to be exchanged between EU-member states is accompanied by fingerprints and photographs, similar to the Dutch national solution.

5. Case 2: The importance of identity in Dutch medical chains

We now shift our attention to another vital domain of our society where identity plays an important role: the healthcare sector. In the Netherlands, the government aims at introducing a national system of medical information exchange based on the national personal number as the sole identifier for recognition of persons and linking of data. Recently, there has been much debate about the implementation of this Electronic Personal Record (Schäfer et al. 2010). With the chain perspective of Chain-computerisation in mind, it is clear that the usual small-scale concept of the doctor-patient relationship does not adequately reflect the large-scale field of forces in healthcare between more than half a billion EU-patients and the EU's hundreds of thousands of medical service providers. A simple risk assessment might reveal, for instance, that some patients have a clear interest in using somebody else's personal number to be treated in cases (s)he is not insured for healthcare, to hide his/her illness from other persons or from his/her life insurance company. This identity fraud can take many forms but inevitably contaminates the medical record of the patient and of his/her victim. Identity fraud will probably surface in many large-scale healthcare chains as the dominant chain problem to be countered. This problem proves to be barely manageable on a regional scale. On a national scale, many preventive measures are needed; on an international scale, even more. At the moment, adequate preventive measures are generally absent.

Consider the large-scale nation-wide electronic patient record on the one hand, and the small-scale doctor-patient situation on the other. In the Netherlands, even national policy makers usually think about healthcare with the small-scale situation in mind. It is the situation they are most familiar with. When someone ('patient X') receives treatment in a hospital and enrols with the health identification number of someone else ('patient Y'), the victim (Y) usually will not suffer much from this as long as the geographical distance between the treatment locations of X and Y is large enough. Both doctors – trapped in their small-scale thinking – believe they know their own patient Y very well. But if all medical data would be combined in a nation-wide information infrastructure – now we are in the realm of large-scale information systems – the data of patient X would also be part of the virtual medical file of patient Y. None of both physicians would notice, as both name and number of their patient are correct. So, in most cases identity fraud goes by unnoticed, as the data point to their own patient for both doctors. It should be clear that these situations can easily lead to medical errors.

We are very far from an ideal situation, but much will already be gained if any national linking of medical records would not be based on the patient's personal number alone and – additionally – would also automatically present a high resolution photograph of the patient on the doctor's computer screen. In the

near future, research should also establish which infrastructural elements and which additional safeguards are needed for the safe exchange of medical information on a European scale.

One such infrastructural element – that is also relevant for computerisation on national level – is the consideration that not all medical chains are similar, and thus may benefit from different information infrastructures. In our chain research we have found differences between for example the diabetes control chain and the manic-depressive disorder chain-of-care (Grijpink et al. 2010). These two diseases require fundamentally different medical data in order to provide adequate treatment. Furthermore, for diabetes it is usually sufficient to share patient data regionally, whereas manic-depressive people tend to be less 'sedentary', so it may be wise to share their data on a larger scale. And there are more relevant variables that vary across medical chains: differences in speed required, differences in the role of the patient (active/passive) and differences in the nature of the process (e.g. monitoring an illness, discovering an illness). For instance, the aforementioned illnesses are both chronic, but it is not hard to see that the acute medical care chain has other requirements.

Similar to the criminal justice example, we again see that a central – be it national or European – database for healthcare records is undesirable, as this facilitates identity fraud, makes it harder to keep all information up to date, and is more difficult from a privacy perspective.

6. Conclusion and discussion

Identity fraud/theft is easy and very profitable. In both cases discussed above, the dominant chain problem of identity fraud presents a threat to the relevant chain co-operation that has to be tackled with a large-scale approach and with person-oriented security procedures and instruments that are indeed able to prevent identity fraud from happening undetected. Taking into account that this problem exists in many other domains as well, we conclude that identity fraud is a major threat to our society. The main reason is that our social systems are not designed to prevent or detect identity fraud. Because committing identity fraud is not a seriously sanctioned criminal offence, the culprit can effectively evade such unpleasant consequences as long-term imprisonment. Often, the cost-benefit relationship is in his/her favour. Moreover, the interests and motivations of the target persons in a chain process vary greatly, depending on the dominant chain problem. We have seen that only preventive measures can protect against identity fraud.

Our examples illustrate that the chain concept is a powerful tool in understanding how large-scale public information infrastructures can effectively tackle identity fraud, even on an enormous scale. The chain perspective and chain analysis have proven useful to uncover hidden aspects of large-scale social systems and to develop and deploy successful chain information systems geared to the dominant chain problem at hand. Therefore, we argue that basic, but chain-specific information systems, combined with random identity verification procedures enable combating identity fraud.

An important contribution of this paper is that we have shown how the chain analysis method (Grijpink 2010) is tuned towards the peculiarities of large-scale chain co-operation and the corresponding chain information infrastructures. The impact of a dominant chain problem and of irrational decision making at the collective chain level bring about that simply scaling up the usual authentication procedures and traditional defence measures is not good enough. They do not take into account identity fraud of the 'wrong person'-type that cannot easily be detected within large-scale systems and surreptitiously spreads from chain to chain.

Future research could focus on how identity fraud differs across social chains as for severity of the consequences, ease of detection and available prevention methods. We have already seen in this paper that there are similarities but also great differences between identity fraud in the context of serving a sentence in a prison cell and receiving medical treatment at a hospital. Another possible future stream of research could focus on the relationship between the identity fraud problems covered in this paper and the processes occurring in 'for-profit chains', e.g. online ordering in web shops.

Politicians and public managers like to simplify complicated interdependencies between and within large-scale systems and preferably produce simple measures. Our chain research has taught us that this is fruitless in the real world; we had better deal with the world as it really is. This does not exclude a simple solution, as these two examples show. The example of the criminal law enforcement chain also applies to many other large systems at EU scale. If it proves to be that easy to use other people's identity under the

watchful eyes of the criminal law enforcement officials, we must not delude ourselves about the future of identity fraud in less well-guarded public information infrastructures, such as employment, education or travel. If, in the future, we are not able to adequately counteract identity fraud – even, for example, in large-scale EU co-operation in the vital fields of identity management and healthcare – governments will ultimately lose much of their legitimacy.

References

Cohen, M.D., March, J.G. and Olsen, J.P. (1972) "A garbage can model of organizational choice", *Administrative Science Quarterly,* Vol. 17 No. 1, pp. 1-25.

Drogkaris, P., Geneiatakis, D., Gritzalis, S., Lambrinoudakis, C. and Mitrou, L. (2008) "Towards an Enhanced Authentication Framework for eGovernment Services: The Greek Case", in Ferro, E., Scholl, J. and Wimmer, M. (Eds.), *Proceedings of the 7th International Conference on Electronic Government*, pp. 189-196.

Galtung, J. (1969) *Theory and Methods of Social Research*, Columbia University Press, New York, USA.

Grijpink, J.H.A.M. (1999) "Chain-computerisation for interorganisational public policy implementation: A new approach to developing non-intrusive information infrastructures", *Information Infrastructure and Policy,* Vol. 6 No. 2, pp. 81-93.

Grijpink, J.H.A.M. (2010) "Chain Analysis for Large-scale Communication Systems: A Methodology for Information Exchange in Chains", *Journal of Chain-computerisation,* Vol. 1, pp. 1-32.

Grijpink, J.H.A.M. (2011) "Public information infrastructures and identity fraud", in Van der Hof, S. and Groothuis, M. (Eds.), *Innovating Government: Normative, policy and technological dimensions of modern government*, T.M.C. Asser Press/Springer, The Hague, The Netherlands.

Grijpink, J.H.A.M., Visser, T., Dijkman, J.J. and Plomp, M.G.A. (2010) "Towards an Information Strategy for the Manic-Depressive Disorder Chain-of-care", *Journal of Chain-computerisation,* Vol. 1, pp. 1-11.

March, J.G. and Olsen, J.P. (Eds.) (1976) *Ambiguity and choice in organisations,* Universitetsforlaget, Bergen, Norway.

Plomp, M.G.A. (2011) "Chain-computerisation as a research methodology: The fruits of six years of Chain Landscape Research at Utrecht University", *Journal of Chain-computerisation,* Vol. 2, pp. 1-7.

Plomp, M.G.A. and Batenburg, R.S. (2010) "Measuring chain digitisation maturity: An assessment of Dutch retail branches", *Supply Chain Management: An International Journal,* Vol. 15 No. 3, pp. 227-237.

Schäfer, W., Kroneman, M., Boerma, W., Van den Berg, M., Westert, G., Devillé, W. and Van Ginneken, E. (2010) "The Netherlands: Health system review", *Health Systems in Transition,* Vol. 12 No. 1, pp. 1-229.

Williams, T. (1997) "Interorganisational information systems: issues affecting interorganisational cooperation", *The Journal of Strategic Information Systems,* Vol. 6 No. 3, pp. 231-250.