Chain Communication Systems

J.H.A.M. (Jan) Grijpink
Emeritus Professor
Utrecht University, The Netherlands
j.h.a.m.grijpink@uu.nl

Abstract: This paper[1] elaborates on large-scale chain communication between autonomous organisations and professionals focused on solving social problems. We introduce a dynamic chain concept combined with a special chain information strategy that may help us to better understand and anticipate the complexities of large-scale information exchange - with or without ICT – in a chain context lacking sufficient overall co-coordinating and enforcing authority. Many chain projects fail and large-scale systems produce unexpected negative side-effects or even backfire. We use the criminal law enforcement chain to explain how these adversities and negative side effects may disrupt a large-scale social system. This example stands as a model for other vital, large-scale systems such as identity management and health care management. At the core of such chains we have a chain communication system enabling the chain partners to co-operate effectively. Chain research at Utrecht University – now covering more than twenty three social chains in the Netherlands – has led to seven valuable insights and breaking views on the theory, practice and the content of chain analysis. We indicate ten challenges for information science and its practitioners as suggestions for future research and development.

Keywords: Chain-computerisation, chain co-operation, dominant chain problem, chain level, chain communication, interorganisational information system.

1 Preface

Chain-computerisation as a sub-discipline of information science offers new concepts, strategies, theories and tools that are better suited to successfully bring about large-scale information solutions for wicked[2] social problems. Within information science, it challenges the bias of 'small-scale thinking' characterising our traditional perspective on large information infrastructures. Information science urgently needs a theoretical framework based on 'large-scale thinking' to better understand why we are so often confronted with failing large ICT projects and systems.

Mainstream information science is no exception in struggling with bringing together small-scale and large-scale perspectives, as many sciences are in the process of trying to balance different perspectives, sometimes indicated with prefixes such as 'micro' and 'macro'. This process is taking place within information science only since the mid-nineties as a result of the Internet revolution. While economists have a long tradition of

---

[1] This paper has also been published in the e-Journal of Chain-computerisation, vol 5, #3, pp.1-23

[2] Rittel and Webber (Rittel & Webber, 1973) coined the term in the context of problems of social policy, an arena in which a purely scientific-rational approach cannot be applied because of the lack of a clear problem definition and differing perspectives of stakeholders. Wicked problems can be characterised by
a. the solution depends on how the problem is framed and vice-versa;
b. stakeholders have radically different world views and different frames for understanding the problem;
c. the constraints that the problem is subject to and the resources needed to solve it change over time;
d. the problem is never solved definitively.
Although Rittel and Webber framed the concept in terms of social policy and planning, wicked problems occur in any domain involving stakeholders with differing perspectives. (From: Wikipedia, November 22, 2014)

antagonist opinions since Keynes published his General Theory in 1936, information scientists and professionals are not yet fully aware of the challenge wicked social problems pose to their traditional small-scale thinking as reflected in tools and methods.For example, a successful local medical file system for a general practitioner is not automatically suited to successfully provide a similar functionality on a regional or national scale. The main reason is that the local system's implicit axiom -that a GP knows his patients- doesn't hold at that much larger level. Usually, this so-called 'fallacy of the wrong level' is not diagnosed as the root cause of ICT-disasters. Due to the traditional small-scale thinking of ICT-professionals and -scientists disasters are wrongfully blamed to poor project management or individual incompetence.

To get an idea of how to handle antagonist opinions based on small-scale and large-scale thinking in information science, we may look at how the antagonisms between micro-economists and macro-economists are handled in the process of tackling the actual economic depression in the Euro zone. Micro-economists favor reduction of government debt and budget deficits; macro-economists plead for stimulating the economy by government investments in infrastructures to offset low consumer spending. While the consequences of bad policy are felt by many people and public pressure on politicians and experts is very high, balancing micro- and macro-economic thinking proves to be nearly impossible. At the moment, budget cuts still prevent stimulating the economy.

It is interesting to point to a similar antagonism in the field of data protection. The concepts and definitions of the European Union's Data Protection Directive (1995), such as data collecting, data processor, data processing, inspection rights and correction rights reflect small-scale thinking only. However, deleting incorrect data from the Internet or in 'big data' solutions in the Cloud proves nearly impossible within current regulations. Data Protection, too, needs new concepts and definitions which take the barely manageable large-scale digital environment into account. Unfortunately in the draft (2012) of the forthcoming European General Data Protection Regulation the data protection authorities stick to their small-scale thinking[3]. And information specialists promoting Cloud solutions stick to their small-scale thinking to convince their clients, too. So, we have to wait until chain-wide co-operation focusing on wicked social problems using Cloud solutions is confronted with the same privacy problems we know from the traditional large ICT solutions.

The problem with competing perspectives and explanations within one scientific discipline is that each of them is right within its own theoretical framework. This type of antagonism is difficult to handle without an explicit balancing mechanism. Balancing different perspectives or explanations is not about deciding which one is right, but which one should be given priority in the light of a particular situation or during a certain period of time. If such a balancing mechanism is not available and accepted, social debates can go on indefinitely without scientific or practical progress being made.

Chain-computerisation contributes to mainstream information science by providing an explicit balancing mechanism by encompassing both small-scale and large-scale thinking within a multi-level chain concept making a distinction between two separate levels of analysis: at the 'base-level' of a chain small-scale thinking dominates, chain partners follow their own interests and efficiency is the standard; at the 'chain-level' large-scale thinking gets priority and effective chain-wide communication fighting the dominant chain problem is the standard. This unique feature of Chain-computerisation is explained in more detail in this paper.

---

[3] E.g., look at the following proposed change to the data protection regulation that will be directly applicable in all member states of the European Union: New privacy rights, including data subject's "right of portability" and the "right to be forgotten", will be established in the EU. The "right of portability" will allow a transfer of all data from one provider to another upon request, for example transfer of a social media profile or email, whereas the "right to be forgotten" will allow people to wipe the history clean.

In information science, the antagonism between micro and macro perspectives still remains hidden in the background of social debates. Failing big ICT-projects, however, are getting more and more attention and come across more and more public indignation, but the prevailing micro perspectives stress inadequate management control, greediness and incompetence as the main root causes of ICT disasters. In The Netherlands, the temporary Second Chamber Commission on big ICT projects recently (October 2014) reported this way. Inadequate management control, greediness and incompetence may be problematic, but without acknowledging that our strategies and system designs do not suit large-scale and barely-manageable environments, only marginal improvement will be attainable. It is about time that Chain-computerisation comes to the fore stimulating professionals and scientists in the field of information science to address the challenge of big information solutions for wicked social problems.

2 Introduction

Ten years ago the concept of a 'chain' was still a vogue word without the practical significance that we know from logistic chains. These days, we are more aware that each organisation must participate effectively in a large number of different social chains. The quality of life in an information age will largely depend on it. The construction of national and international chain information infrastructures turns out to be a major challenge. Successful large-scale chain communication systems are still rare. We know precious little about how to bring about information exchange on a large scale, especially when we have to ensure the data being used lawfully. The gap between what we are actually doing in the area of large-scale information exchange and what we need to do is getting larger rather than smaller. Hence we need an approach to organise interorganisational communication that is suited to the adversities of large-scale chain environments with more suitable concepts, models and theories and with more effective methods. These are offered by Chain-computerisation, an information science subdiscipline in its own right. I developed this theoretical framework in my doctoral thesis (Grijpink, 1997) in order to be able to cope with the peculiarities of large-scale information exchange in the Dutch criminal law enforcement chain. It was subsequently introduced in *Information Infrastructures & Policy* (Grijpink, 2000a; Grijpink, 2000b), in *Computer Law and Security* Report (Grijpink, 2005) and in the *European Journal of Crime, Criminal Law and Criminal Justice* (Grijpink, 2006). From 2010 it has been firmly established by the open access *Journal of Chain-computerisation* (https://jcc.library.uu.nl) with its founding articles Chain Analysis for Large-scale Communication Systems (Grijpink, 2010a) and A Chain Perspective on Large-scale Number Systems (Grijpink, 2012a).
Chain analysis and number systems now being covered, this third founding article presents the remaining parts of the theoretical framework of Chain-computerisation. By way of example, this framework is applied to the Dutch criminal law enforcement chain and to the criminal justice chain co-operation between EU member states. Finally, we briefly discuss seven breaking views resulting from the chain research programme at Utrecht University (Grijpink & Plomp eds., 2009a). Ten challenges for future research and development in the field of large-scale chain communication are indicated.

Barely a day goes by without chain issues making the news. Today's headlines are about terrorists' attacks and football hooliganism, tomorrow's about juvenile delinquency and medical errors as a result of faulty data transfer. Over and over again we are confronted with many large-scale chain issues that are difficult to resolve. Usually, these issues can be related to the need for information exchange between large numbers of autonomous chain partners, no single one having the power to coerce other chain partners to cooperate effectively. Moreover, chain partners are often confronted with sloppy compliance or sometimes direct opposition or sabotage by the persons for whom the chain activities are meant: e.g. a forgetful patient, a defiant or angry citizen or a dissimulating criminal. If the communication in a chain fails, wrong decisions are likely to be taken. If this happens on a regular basis, the chain becomes disrupted and discredited, thus reducing the quality of life in our information society.

3 The chain concept

Defining Chain-computerisation's special chain concept
Chain-computerisation's chain concept does not refer to a logistic chain (the process of handling goods) that we so often come across in the business community, nor to a chain of closely linked information systems nor to a chain of transactions nor to a chain of data. The chain concept of Chain-computerisation explicitly refers to a 'social' chain: large-scale interorganisational processes that yield a social product such as health, safety or prosperity. Logistics, linked transactions, linked information systems and data chains are of course components of a social chain, but in our studies we focus explicitly on the level of chain-wide co-operation of organisations and professionals. That level we refer to with 'social chain'. In a social chain, thousands of organisations and professionals work together without a clear relationship of authority, in ever-changing combinations depending on an actual case. But co-operating with other organisations and professionals without adequate co-ordinating or enforcing authority takes a lot of effort, time and money. There must, therefore, be a cast-iron reason for doing so. Therefore, an important element of our chain concept is that chain partners co-operate only when they are forced to do so by a 'dominant chain problem', being a recurring problem that can disrupt activities of every chain partner and that none of the partners can solve by its own. In an environment without an overall co-ordinating and enforcing authority it is only such a problem that creates the interplay of forces that triggers large-scale co-operation. Only effective chain co-operation can prevent the entire chain from being disrupted and discredited.

> *Example: the Identity chain*
> At the moment, the Identity chain cannot prevent your identity from being misused by someone else. If only a single chain partner inadvertently accepts a false identity, the identity fraudster can use it anywhere else without arousing suspicion. So, in the identity chain the dominant chain problem 'identity fraud' forces organisations and professionals to co-operate. This dominant chain problem determines the essential chain-communication required to effectively prevent identity fraud from succeeding.

The irrational character of chain decision making
In a social chain thousands of organisations and professionals work together without a clear relationship of authority, in ever-changing combinations depending on the actual case. On this huge scale, collective decision-making takes place in a context within which the four basic assumptions of the rational model are not valid (Grijpink, 1997, 135). These assumptions are:
(a) there is a choice between alternative solutions;
(b) the consequences of every alternative are completely and clearly known;
(c) the goals of a decision maker are known, and thus alternative solutions can be ranked;
(d) there is a decision rule to make a best choice.
As these assumptions are invalid in social chains, rational decision making is not to be expected. Fortunately, since 1972 our management literature is providing a model of decision-making in an irrational context, which is often referred to as the Cohen, March and Olsen *Garbage Can* model (Cohen, March & Olsen, 1972; March & Olsen, 1976; Padgett, 1980; Miller, Hickson & Wilson, 1996). This model warns us of surprising twists and catastrophes and of unexpected locks and rapids in the process of chain decision-making at the collective level. Even if every chain partner were a clever and rational chain player, the *Garbage Can* model predicts that collective decisions are mostly poor or, at best, mediocre. It suggests to chain players to take this unpredictability into account by having a Plan B and C ready and by simple and flexible chain communication systems.

The relation between a dominant chain problem and its pattern of chain co-operation
Chain-computerisation has been built on the hypothesis that every dominant chain problem gives rise to interplay of forces triggering its own chain co-operation. And conversely, at the core of our chain concept lays the idea that every chain has a single dominant chain problem. We know now from our chain research that this hypothesis is valid and that dominant chain problems turn out to be very different and chain-specific (Grijpink & Plomp, 2009a). Thus, a chain project aimed at bringing about a chain information infrastructure for a multi-chain environment or sector, e.g. youth care or healthcare, is prone to fail because for the sector as a whole the link with a specific dominant chain problem is too weak. Only if each of the chains of which the sector is made up, is being ruled by its own specific dominant chain problem requiring an identical information infrastructure with the same content and structure, a sector-wide information infrastructure is feasible. However, we haven't been able to identify such a sector yet.

The dominant chain problem as a useful guide
Within a social chain common interests are less pronounced than people usually think and also often unclear. Therefore, common goals or good intentions alone are not good enough as the basis for improving the quality of chain co-operation. The badly needed cohesion within the chain can only be enforced by a serious dominant chain problem. Only this generates sufficient official and professional support for large-scale information exchange. A chain communication system focused on tackling the dominant chain problem will have a good chance of being successfully developed and implemented benefiting from the underlying interplay of forces that provokes this chain co-operation. And conversely, if a project to bring about such a chain communication system in this chain fails, then other chain projects have no chance of success at all.

The dynamic character of this special chain concept
Most people regard a chain as a *fixed* - or at best *stationary* - pattern of co-operating autonomous organisations and professionals. In contrast with this prevailing chain concept, we introduce a *dynamic* chain concept (Grijpink, 2000c), because pattern and intensity of chain co-operation change over time, depending on the extent to which the dominant chain problem is combated effectively. The second reason for our chain concept being dynamic is that a ruling dominant chain problem can be overtaken by another, causing both co-operation patterns and the core content of the chain communication to adapt to the new dominant chain problem. New data become indispensable and chain partners gain or lose influence. This way, the dominant chain problem is the 'boss' in the chain, but only as long as it is having the chain in its grip.
The advantage of this dynamic chain concept is that it warns against big projects, because the time it takes to implement a system may be longer than the dominant chain problem's life. It also opens our eyes to the varying importance of chain partners' contributions towards effectively tackling the dominant chain problem.

The multi-level character of this special chain concept
Our dynamic chain concept is a multi-level one as well, implying a distinction between:
a. the 'chain-level'
b. the 'base-level' of the chain.

This distinction enables us to better understand and anticipate the problems inherent in large-scale chain co-operation and communication. A chain communication system is analytically positioned *at chain-level* meaning that this system is - or can be - used by every chain partner without any chain partner being in control of the system for his own purposes or interests. If we say that an information system is analytically positioned *at the base-level* of the chain*,* we mean that this system is only being used by its owner, predominantly in his own interest. Within our chain concept, case handling by an individual chain partner using its own information system - with or without small-scale or bilateral information exchange - is seen as positioned at the base-level of a chain, in contrast with a chain communication system.
There are two reasons for distinguishing these two levels.

First, a social chain inherently is a large-scale phenomenon. At that enormous scale, intentions, goals and methods are ambiguous or even contradictory. Moreover, it is often unclear which chain partners are actually involved. These factors cause decision-making and other chain processes to be unpredictable, irrational and barely manageable. That is why chain-wide communication focused on the dominant chain problem is to be positioned at chain-level. At that collective level traditional management instruments, such as time schedules, budgets and allocation of responsabilities, fail.

Second, in information processing we usually do not make a distinction between *communication* and *registration* of data. This is very efficient in a well-controlled environment with a clear line of command. But to bring about and maintain large-scale chain communication we have to cope with the large-scale chain environment. That is why Chain-computerisation takes as starting-point that this can only be done by separating chain-wide communication focusing on tackling the dominant chain problem from the chain partners' full content databases focused on the chain partners' own activities. This chain communication is then conceptually positioned at the chain-level, only very loosely coupled to the chain partners' full content working data at the base-level of the chain. Contrary to the chain partners' data, a chain communication system contains only the (meta-) data indispensable to tackling the dominant chain problem.

Unfortunately, quite often the chain partners' collaboration is not intense enough to make a chain communication system feasible at chain-level. This can be concluded from a *chain analysis* (Grijpink, 1997; Grijpink & Plomp, 2009a; Grijpink, 2010a) leaving no other option than improving information exchange at the base-level of the chain, between some major chain partners. Chain-wide ambitions must be kept away and scaling up of a small-scale communication solution should not be undertaken without prior testing the validity of its underlying assumptions at that larger scale.

Fallacy of the wrong level

Let us look at our chain concept from yet another point of view in order to assess its practical significance. Information science derives its core concepts and theories from several scientific (sub-) disciplines. So we are familiar with the need to combine concepts from different theoretical frameworks, keeping in mind that knowledge and insights are only valid within the boundaries of the theoretical framework from which they have been drawn. Even if we apply insights from one discipline to the real world, we are confronted with validity errors. But rarely do we realise that this is only part of our validity problem. The validity of insights and knowledge is also context dependent and limited to the level or scale for which they are formulated. In information science as in management science, we usually derive insights from small-scale situations such as an information system, a small group experiment or a local pilot. In this way we have gained insights into small-scale phenomena such as the power of recording data in databases and of management tools such as time schedules, responsibility structures and budgets. If we transpose such small-scale insights to large-scale situations without checking at that level the validity of the underlying assumptions, we often commit a so-called 'fallacy of the wrong level'. This risk of commiting a fallacy of the wrong level lurks everywhere and every time. We often are not aware that in 'small-scale thinking' - compared with 'large-scale thinking' – we focus on different aspects, risks, opportunities and problems, leading to different assumptions, theories and expectations. This might explain why – given our general propensity for small-scale thinking - so many national policy measures and large-scale systems unexpectedly produce adverse results - or even backfire.

> *Example: the European Union's biometric visa system, a risk of backfiring?*
> Biometrics (measurement of physical or behavioral features, such as fingerprints or a voice) is regarded as a very precise way of recognising people, because the biometric detail is directly taken from the person, whereas an administrative detail is not. This is a small-scale insight gained from pilots and laboratory experiments with biometrics. Testing its assumptions when applying biometrics at a national or international scale, we are confronted with several validity problems. First, in a large-scale environment

it is difficult to assess the uniqueness of a specific type of biometric detail (e.g. a fingerprint or an iris) and thus its inherent risk of mistaken identity. Second, in large-scale applications the controllability of enrollment and measurement conditions is weak, causing the system to be unpredictably vulnerable to mistakes, manipulation or fraud depending on many situational factors such as location or time of the day. Third, any measurement is inherently variable, because of its statistical nature: the person recognition thus depends on preset confidence levels in a biometric system reflecting which measurement variation is acceptable for a specific application. Apart from these technical and managerial aspects, there are implicit assumptions at the functional level as well. Will a biometric system serve its purpose better or differently than the system without biometrics? Is that expectation still valid at a larger scale?

A few years ago, biometric person recognition was added to the European Union's visa system - aimed at preventing unwanted foreigners from coming to the EU. Nowadays, the Dutch embassy in some foreign countries takes the traveller's fingerprints which are then sent to the Netherlands. If those fingerprints correspond to the fingerprints of an unwanted foreigner in the European Eurodact database, the visa is refused. Will biometrics applied at this global scale prove to be effective to prevent unwanted foreigners from coming to the EU? Even regardless inherent technical and managerial problems the answer is: probably not.

Consider, for instance, the following scenario: a criminal network wants to send someone to the Netherlands for a criminal job. Suppose that a visa is refused because his fingerprints are in the Eurodact database. By this refusal the network knows that it has to send someone else or choose a route where traffic control is weak. This causes the arrival of unwanted foreigners to go largely unnoticed instead of the intended greater control of incoming passenger traffic. The overall result of the biometric visa system is that we have placed an ineffective burden of biometric enrolment and fingerprint checking on good citizens and have lost sight of the arrival of unwanted visitors who were the prime target of the system! When we take into account that only good citizens will protest against unjustified visa refusal, this biased feedback will presumably cause the preset confidence levels in the biometric verification system to be lowered which, by consequence, will increase the chance of an unwanted criminal unjustifiedly getting a visa. In this scenario, biometrics applied in a global visa system risks being counter-productive aggravated by the fact that this will go unnoticed, because the negative effects cannot be detected within the visa system itself.

Starting from this risk analysis, having a large-scale perspective on the biometric visa system in mind, one should consider other system designs and different scenarios for risk assessment. Take for instance another system design with a clever mix of monitoring, observing or warning procedures for unwanted visitors instead of visa refusal. This way, the elements of surprise and control can again turn over to the government's side.

This example demonstrates how easily a fallacy of the wrong level is commited unless we take into account a certain number of plausible scenarios when designing and building large-scale systems. The larger the scale of a system, the more sophisticated and numerous the checks and balances within the system should be and the smaller the steps to be taken in the process of implementing it, thus offering more opportunities to amend the system as and if needed.

A final example of a fallacy of the wrong level: we must stop treating large-scale *inter*-organisational information systems as *intra*-organisational information systems with a somewhat larger group of users.

Example: a single chain database

Let us consider the common belief that chain co-operation will be effectively supported by a single chain-wide database, containing all the relevant information for every chain partner. At this huge scale, that yields little more than a concentration of

information management activities, not communication. And that information management must be carried out by people who have barely any affinity with the registered details and have no authority to enforce co-operation. In our chain concept, this chain database is positioned at chain-level. This tells us immediately that content, quality and data use cannot possibly be sufficiently managed because overall co-ordination and enforcing authority does not exist at that level. Therefore, it is much better if every chain partner collects and manages its own information. Analytically, this can be seen as occurring at the base-level of the chain where chain partners behave as rationally as they can and are supposed to support their work processes in their best interests. This is precisely an important precondition for high quality information management. At the same time, a chain needs a central communication system at chain-level, so that partners in the chain can gain immediate access to vital information, depending on the chain's dominant chain problem. The chain communication system derives this information directly from the chain partners' databases without human interference, thus benefiting directly from the quality assurance mechanisms at the base-level of the chain.

Summary
Although, at the base-level of the chain, individual organisations and professionals act as rationally as possible, we have to remove the assumption of rationality at the chain-level to gain a better understanding of the interplay of forces and of the peculiarities that prevail at that collective level. Chain-computerisation facilitates anticipating the adversities of the irrational large-scale chain context and preventing fallacies of the wrong level by:
(1) a special chain concept;
(2) a distinction between the base-level of a chain and its chain-level;
(3) a model of irrational decision making at chain-level;
(4) problem-oriented chain communication at chain-level to be separated from full content data collection and registration at the base-level of a chain;
(5) developing a lean chain communication system at the chain-level;
(6) focusing this chain communication system on the chain's dominant chain problem only.

Chain-computerisation adds to this arsenal (1)-(6) a *chain analysis methodology* (Grijpink, 1997; Grijpink, 2010a) – not treated here – and a *chain information strategy* suitable for large-scale chain communication systems. This chain information strategy is the subject of section 3.

3 Chain information strategy: 'chain laws'

The information strategy of Chain-computerisation can be summarised in – by way of metaphor – four 'chain laws' (Grijpink, 2002a: 23-31; Grijpink, 2010b: 27-29):

a. *Big solutions risk adequate support*
The grander a solution, the less adequate the actual support will be. Lacking support causes systematic shortcomings in the intended large-scale system and unexpected setbacks and failures in its making. In a large-scale environment without co-ordinating and enforcing authority only a step by step approach has any chance of success. In chains, major changes can only gradually take place spread over many years. Chain processes may easily stagnate or get blocked for a long period of time. Therefore, a gradual approach may often require a different design of the project, because even the first deliverables should be fit for immediate and longtime use.

b. *Interference with intra-organisational matters is counterproductive*
Policy measures at chain-level that exert a strong influence on the chain partners' internal state of affairs come up against a great deal of resistance blocking effec-

tive chain-wide solutions. We know this from the world of international diplomacy, but we rarely apply this insight to large-scale interorganisational co-operation. Applying this 'chain law' to large-scale information exchange, these rules of thumb stand out:

i. First computerise, then reorganise

Reallocating tasks and responsibilities is one of a manager's favourite approaches towards problems. In a chain - unlike within an organisation - this hurts the roots of chain partners' autonomy. Information exchange is less penetrating than reallocating responsibilities or integrating chain partners' information systems. Therefore, it follows from the rule of 'mind your own business' that exchanging essential data has a better chance of success than reallocating tasks or responsibilities between organisations. Nevertheless, managers and public administrators often prefer solutions that change interorganisational responsibility structures or division of work between autonomous chain partners above less pervasive instruments such as improving chain communication.

ii. Instead of full content, use meta-data in wafer-thin information infrastructures

It follows from this rule as well that, at chain-level, chain communication systems should only contain data that are indispensable for tackling the dominant chain problem, and even then only in the most minimalistic form: for instance, a personal number instead of a name; or a reference instead of full content data. This chain communication cannot result in more than triggering chain co-operation, but large-scale communication systems with full content data are unlikely to be successfully brought about at all, thus resulting in even less effect.

c. The Dominant Chain Problem Rules

Only a dominant chain problem creates an interplay of forces that is vigorous enough to trigger large-scale chain co-operation. A dominant chain problem is a problem that frustrates every chain partner, while none of them is able to solve it on his own. Only by effectively co-operating can chain partners prevent the entire chain from being disrupted and discredited. The theory of Chain-computerisation is based on the hypothesis that each dominant chain problem triggers its own chain co-operation. There is a wide variety of dominant chain problems, each provoking a different pattern and intensity of collaboration, thus requiring a different chain communication system. Such a chain-specific communication system can offer an adequate solution for a limited period of time only, because a dominant chain problem can be overtaken by some other dominant chain problem. In the sections 4 and 6 we will see this happen in the Criminal law enforcement chain.

d. Crisis opens up opportunities for change, but only for a short period of time

Large-scale social change based on the power of persuasion and good intentions alone is slow-moving and laborious. However, a crisis does make more fundamental chain-wide changes possible - be it during a short period of time only. Usually, we let that opportunity slip through our fingers, because crisis management demands our attention. It proves to be a major challenge to combine crisis management with change management, requiring different attitudes, personalities and processes. Because of the very short period of time during which chain patterns and conditions are more fluid, this chain information strategy suggests having always one or two plans B ready for immediate use for improving chain co-operation and chain communication.

Projects that violate these 'chain laws' have little chance of being successful. Put simply, chains form a bleak and discouraging working environment causing many large-scale ICT solutions and projects to fail. However, that is where the computerisation of society is -

to a significant extent - taking place, thus determining the quality of life in our future information society. We have no other choice but to meet this challenge.

4 The Dutch Criminal Law Enforcement Chain

In this section the Dutch criminal law enforcement chain serves as an example of a major chain to illustrate the relevance and the significance of Chain-computerisation's body of knowledge.

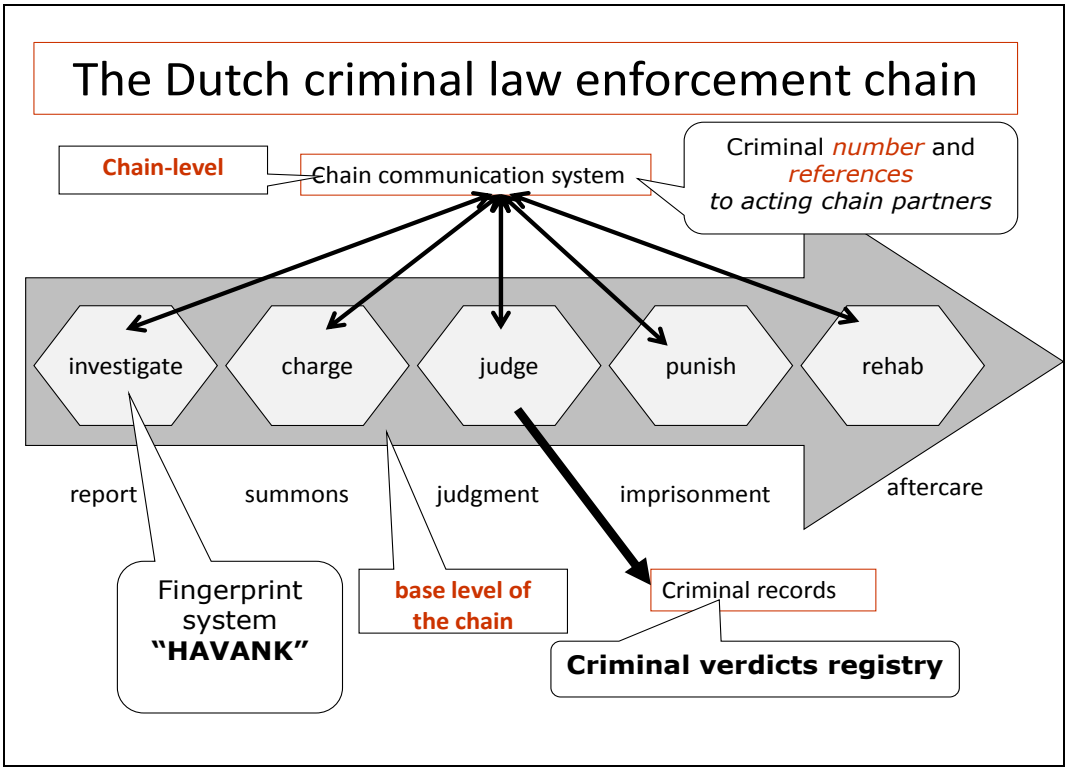

Figure 1 The Dutch criminal law enforcement chain

First, we present some figures to underline the need of large-scale thinking. Second, we explain the impact of the three successive dominant chain problems that have been ruling this chain and how the Dutch Ministry of Justice step by step paved the way to better solutions in this chain. In fact, the theory of Chain-computerisation was especially developed for this chain. Identity fraud as one of the three successive dominant chain problems is only mentioned in this section; the phenomenon of identity fraud itself is treated in more depth in section 5, before its international aspects are explained in section 6.

The Dutch criminal law enforcement chain

In the Dutch criminal law enforcement chain, more than a thousand independent organisations with more than 100,000 more or less autonomous professionals co-operate to handle more than 500,000 serious crimes every year. The chain process can be visualised by the consecutive steps that, by law, must be taken in every criminal case (see figure 1): investigating, charging, judging, punishing and rehabilitating. These steps are the links of this chain each resulting in an intermediate product as indicated, such as report, summons, judgement, imprisonment and aftercare. Moreover, figure 1 shows two major national registers which are being kept by two different chain partners: the forensic fingerprint system HAVANK being kept by the national police (named after the famous Dutch detective writer HAVANK) and the Dutch criminal verdicts registry being kept by the Public Prosecutors Department.

The three dominant chain problems in the Dutch criminal law enforcement chain
Criminal Law is about facts, the offenses. So, until the mid-nineties, the Dutch criminal law enforcement chain had been focusing on individual criminal cases. The dominant chain problem was how we can prove that the suspect is the culprit while the law protects him with the right to keep silent. From the mid-nineties onwards, criminal law enforcement agencies began to understand that multi-offenders should be treated as such with different sanctions and prison regimes to discourage recidivism and to get more results from the chain's efforts. This approach focused on the person of the offender. The dominant chain problem became: how we can distinguish between first-offenders and multi-offenders in a chain that processes every crime as a separate case. Unlike the old situation of processing every crime as a separate case and the ruling dominant chain problem 'how we can prove that the suspect is the culprit', this new dominant chain problem 'recidivism' for the first time required a chain-wide communication system to be able to present an *integral* picture of a criminal to each of the chain partners being involved with him. In this chain communication system every first-offender is attributed a lifetime criminal number that will never be re-issued to another person to be used at every contact with one of the chain partners during the rest of his life. Linked to this unique criminal number are references to chain partners' information systems actually processing details about his cases. This chain communication system offers a clear distinction between people with only one or two references, a first-offender, and people with screens full of references, a multi-offender. In the beginning of the 21st century, the Dutch criminal law enforcement chain seemed to succeed in combating the dominant chain problem 'recidivism' with this chain communication system.

But a chain is a dynamic phenomenon and criminals do not co-operate with the Dutch criminal justice authorities. They escape from being recognised as multi-offender by using aliases (names of other people, real or invented). For some years we had been monitoring the staggering amount of criminal numbers issued to newly arrested first-offenders. Because the *Garbage Can* model made us look for surprises and unexpected adversities, it made us uncover the clever misuse of other people's identities by criminals in still an early stage. Without the Garbage Can model we wouldn't have been on our guard. Situations, in which, after a successful identity fraud, the fraudster can be detected because he is still there, are exceptionally rare. One such rare situation is a prison cell. If a criminal finds someone willing to sit out his sentence in his place, we find a stand-in person in the cell who is not the prisoner we expect. If he is unmasked as a stand-in, he must be sent home because serving a sentence in a criminal's place is not a crime. In the meantime, the criminal has often been able to disappear. Alternatively, a criminal can also use the identity of someone else while sitting out his own criminal sentence. If the criminal has been successful in using an alias, we find the right person in the cell but with an identity that is not his own. This scenario could explain how delinquents, after being punished, sometimes succeed in pursuing their careers with a clean slate. Thus, in 2006, a full identity check of the people in a multi-prison site was carried out revealing a considerable amount of identity fraud in its various forms (Grijpink, 2006b). The ruling dominant chain problem 'recidivism' proved to have been overtaken by the third successive dominant chain problem 'identity fraud'. This is summarised in figure 2.

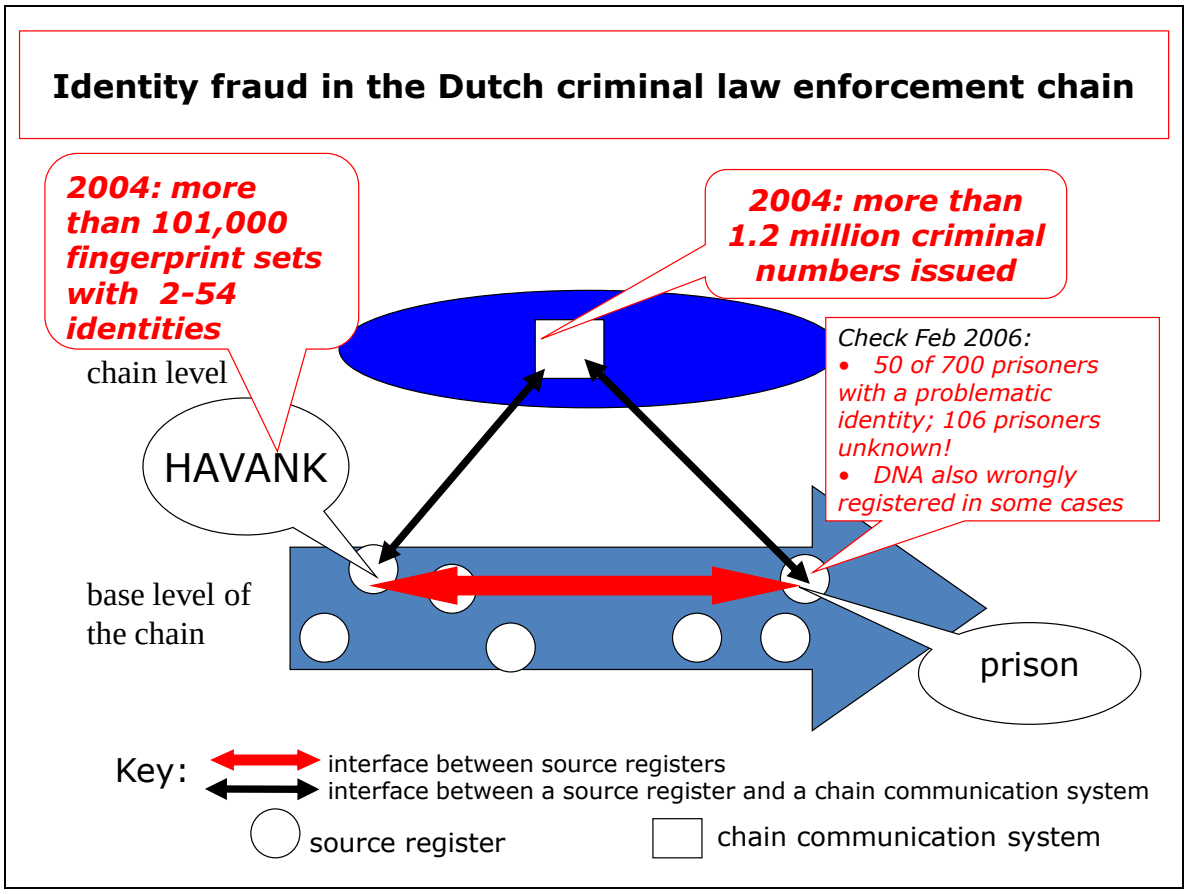

Figure 2 Identity fraud in the criminal law enforcement chain (2006)

Figure 2 shows that, by 2004, the chain communication system had already given out more than 1.2 million criminal numbers to first offerders since the system was introduced in 1993. This amount suggested serious problems because the Dutch population cannot plausibly comprise so many criminals. In February 2006, therefore, the identity of every prisoner in a big multi-prison site with 700 prisoners was thoroughly checked using the forensic biometrics available in the HAVANK system. This involved a huge logistical operation, which required four months lead time and could not possibly be kept secret. But, despite the long preparation time that offered many opportunities to evade the biometric checking, 7% of the prisoners were found not to use their own name or not to be the right person. In some cases, the DNA data were registered under a false name, too, which can lead to the arrest of the wrong person in a new criminal case. Some 106 persons were registered in no criminal justice information systems at all.

To understand how this can happen under the eye of the criminal law enforcement authorities, we consider some possible scenario's in the first link of the criminal law enforcement chain: checking the identity of criminals by the police. Until October 2010, the Dutch criminal procedure law provided for the use of forensic biometrics only in order to prove someone's involvement in the specific crime under investigation. An immediate confession prevents biometric identity checking because proving the suspect's involvement in the crime at hand is not necessary any more. The police will then simply ask for an ID document or, if the suspect cannot produce one, ask for name and address which are then checked against the residents' register of the relevant municipality. Note that if name and address go together but belong to another person, this checking causes a wrong name mentioned in the official report and the subsequent summons and criminal verdict. Even if the suspect produces an ID, it might be somebody else's. Many people look quite similar and very few people can accurately compare a tiny vague ID photo with a 3D face in front of them, even if they are trained to do so. If, in the next stage of the prosecution, the suspect withdraws his confession, the process of identity checking is

only rarely restarted from the beginning. Eventually this causes a criminal verdict to be wrongly filed in the criminal registry. This might be in the file of the criminal's henchman who then later reports to the prison to serve the criminal verdict on behalf of his sponsor. It might also be the file of an innocent or fictional person. Fortunately, from October 2010 the law has been changed on this point; biometrical ID checking *before* checking any administrative details is compulsory now for serious crimes regardless of spontaneous confessions.

Fortunately, in the Dutch forensic HAVANK system every name used by a criminal is recorded with its link to his fingerprint set with its unique HAVANK number. Figure 2 shows that, in 2004, more than 101,000 criminal fingerprint sets linked to more than one administrative identity had been registered in the Dutch national forensic biometrics system HAVANK. The cleverest criminals had succeeded in using more than 54 aliases, implying that they managed to get their criminal verdicts spread to as many criminal records of other persons (who may not be aware of it). The true volume of identity fraud in the criminal law enforcement chain might be even bigger, because a fingerprint set linked to a single name does not guarantee that this name actually is the criminal's true name.

In the next section we will see that identity fraud is a nasty problem, because traces do not lead to the fraudster but to the victim. Thus, this dominant chain problem can only be tackled by *preventing* identity fraud from happening. This is possible using a chain communication system combining the forensic fingerprint HAVANK-number and the criminal justice number thus providing every chain partner with an *integral and integer* (complete and correct) chain picture of every individual criminal. This could be done because since 1993 this chain's communication system had been based upon a simple and flexible design (a number system and a set of references). So, the criminal law enforcement authorities could quickly adapt the national criminal justice chain communication system towards being able to tackle *identity fraud*, as well. This enlarged chain communication system, combining the HAVANK number and the criminal justice number, will immediately warn any chain partner involved of a mistaken identity.

This example illustrates that a chain concept based on a temporary dominant chain problem is a powerful tool to understand how large-scale chain co-operating can be effectively supported with a lean and flexible chain communication system.

Small-scale thinking against large-scale thinking
To close with, let us consider the role large-scale thinking has been playing in this example. The forensic biometrics HAVANK system is used by the Police to prove someone's involvement in the crime under investigation. If the suspect does not use his true name, this does not influence the value of the fingerprint evidence in a particular case. Because of this evidence, the convicted person's name mentioned in the criminal verdict has been taken for granted by the criminal registry manager until recently.
Notice these two examples of *small-scale* thinking: (1) proving someone's involvement in a crime and (2) storing and producing criminal records. Until 2003, nobody bothered about the use of aliases, because both tasks could be performed. The negative effects of an alias in the subsequent links of the criminal law enforcement chain were not well understood.
Large-scale thinking - having in mind the criminal law enforcement chain as a whole – clearly reveales the negative effects of an alias: if a criminal succeeds in using an alias, he keeps his own slate clean. The verdict is stored in somebody else's criminal record. If this identity fraud goes undetected, the criminal is untraceable after his release, because the administrative details point to someone else. In case of recidivism, some-one else is arrested and the true culprit cannot be found. In addition, because an incorrect verdict does not provide a clue to its reliability, even the correct records cannot be trusted anymore, causing the criminal registry to become unreliable and undermining all national security systems based on so-called Declarations of good conduct.

Without large-scale thinking these devastating facts would not have surfaced easily as we discovered in international discussions with justice and police agencies of other EU-countries. This is explained more fully in section 6. First, we now turn to the subject identity fraud to make sure its character and implications are fully understood.

5 Identity Fraud

To better understand the new dominant chain problem 'identity fraud' in the national and EU criminal law enforcement chain, we need a closer look at the phenomenon of identity fraud. Identity fraud - deliberately & dishonestly passing oneself off under somebody else's identity - is not a new phenomenon, but our increasingly digitising mobile and anonymous society gives identity fraud new dimensions that boost its impact and frustrate fighting it. Many politicians and civil servants do not grasp its essence and impact. It is not about tampering with ID-documents, but with suggesting being someone else. People, who say that identity fraud is not happening in their working environment because they have never run into a case of identity fraud, haven't understood this phenomenon, because successful identity fraud goes unnoticed. Three dimensions of identity fraud stand out:

a. *Traces point to the victim, not to the culprit: more traces, no evidence!*
   In a digital world our transactions leave an increasing number of (digital) traces, but in case of identity fraud they always point to the victim instead of to the culprit. Therefore, if a case of identity fraud is reported to the police, the victim is seen as the prime suspect. He has to prove that he isn't the culprit. If one succeeds in registering a car in somebody else's name, duties, fines and collections are presented to the victim instead of the true car owner. Irrespective of the victim's protestations, government agencies keep considering traces as pointing to the culprit, even if they, in turn, are unable to prove their suspicions. If identity fraud keeps growing, police investigation will increasingly end in unsolvable cases or lead to convicting the wrong person. Only prevention can counter an increasing number of identity fraud cases. Unfortunately, the prevailing preventive measures are not up to detect clever manipulating and cannot protect against someone piggybacking on one's identity. In our digital world, even the very best security provisions very rarely safeguard against 'the wrong person'.

b. *Successful identity fraud goes unnoticed*
   Because successful identity fraud goes unnoticed, it is difficult to get a clear picture of the problem and its impact. Successful identity fraud committed in a weak spot of a chain easily spreads to other chains. If one succeeds in using somebody else's social security number, one can also get medical treatment without being entitled to it. Moreover, the culprit's medical data are stored in the file of the victim without his being aware of the contamination of his medical file. Long afterwards, this can lead to wrong medical decisions. This way, identity fraud and its risks for the person whose identity is misused spread unnoticed into the tiniest capillaries of social processes where they will be detected too late or not at all.

c. *Balance of power shift in a digital environment*
   A third new characteristic of identity fraud that one still rarely takes into account relates to a shift in the balance of power between the person or equipment that must check someone's identity and the person being checked. Traditionally, during the process of identity checking, the checker is the boss: he takes initiatives whereupon the person to be checked has to react. In digital procedures - or when digital equipment is being used - the person to be checked has the initiative. The average ID checker has to rely on the results of the electronic verification not fully understanding how the equipment works. He will not readily detect equipment or procedures being manipulated. Furthermore, the initiative shifts to the fraudster

who can easily initiate an exception procedure, for instance by deliberately using wrong data or damaging the token necessary for the electronic verification procedure or simply by reporting the loss of it. This way, the surprise is on the fraudster's side. The ID-checker has to rely upon unverified or unverifiable information presented to him by the person to be checked who is well prepared.

Identity fraud is difficult to detect while it is taking place unless special preventive tools and procedures are installed which are aimed at unmasking the fraud as it is happening. Unfortunately, this seldom is the case. This way identity fraud is gradually undermining many large-scale social systems (Grijpink, 2004a; Grijpink, 2004b; Grijpink, 2005; Grijpink, 2006a; Grijpink, 2006b).

6 Identity Fraud in the Criminal Law Enforcement Chain at the Level of the European Union

Let us now consider how our Dutch national solution is complicated by extending the scale of this chain co-operation from national to the European Union. European co-operation among *national police forces* has a long and fruitful tradition, but chain-wide co-operation goes further: many other chain partners from other links of the chain must join – from investigation to rehabilitation. Within the European Union, this broad collaboration is new and fragile, because it takes place within the realm of intergovernmental co-operation. All the difficulties that make national chain processes barely manageable a fortiori hold for the European situation.

Fourniret's case triggering an EU criminal registry
2003/2004 A Frenchman living in Belgium and working in a Belgian school failed to abduct a 13-year old girl. For lack of evidence he was about to be released after a short detention. He was then accused by his wife of having abducted, raped and murdered 8 girls and young women. During Fourniret's failed abduction investigation in 2003 the Belgian police apparently 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 as a handyman is considered sensitive enough to ask a job candidate for a so-called 'declaration of good conduct'. But consulting the Belgian criminal registry only would wrongly have shown a clean slate. This started a political debate about a European Criminal Registry in 2005. EU-decision: exchange of criminal verdicts between EU-member states. Exchange of criminal verdicts would have shown to the Belgian authorities that he was imprisoned several times in France, lately in 1987 (5 years for having raped 11 girls). After release he moved from France to Belgium and became a handyman at a Belgian village school with a clean slate. This would not have happened if his criminal record was checked in France. In 2006 Fourniret was extradited by the Belgian authorities to France to be tried and punished.

Fourniret's case provides a nice example to understand the disruptive forces surrounding the dominant chain problem *identity fraud* (Grijpink, 2005; Grijpink, 2006a), because it covers two EU member states and also involves communication between the criminal law enforcement chain and two other chains, education and residence. Exchange of criminal verdicts between EU-member states will only be correct if two conditions are met:

1. every national criminal law enforcement chain is preventing identity fraud ;
2. every member state sends every criminal verdict to the criminal's EU-country of nationality while preventing identity fraud during transfer, as well.

As Figure 3 shows, this implies a close co-operation between police forces and prison institutions within the EU, using forensic biometrics from the country of nationality.

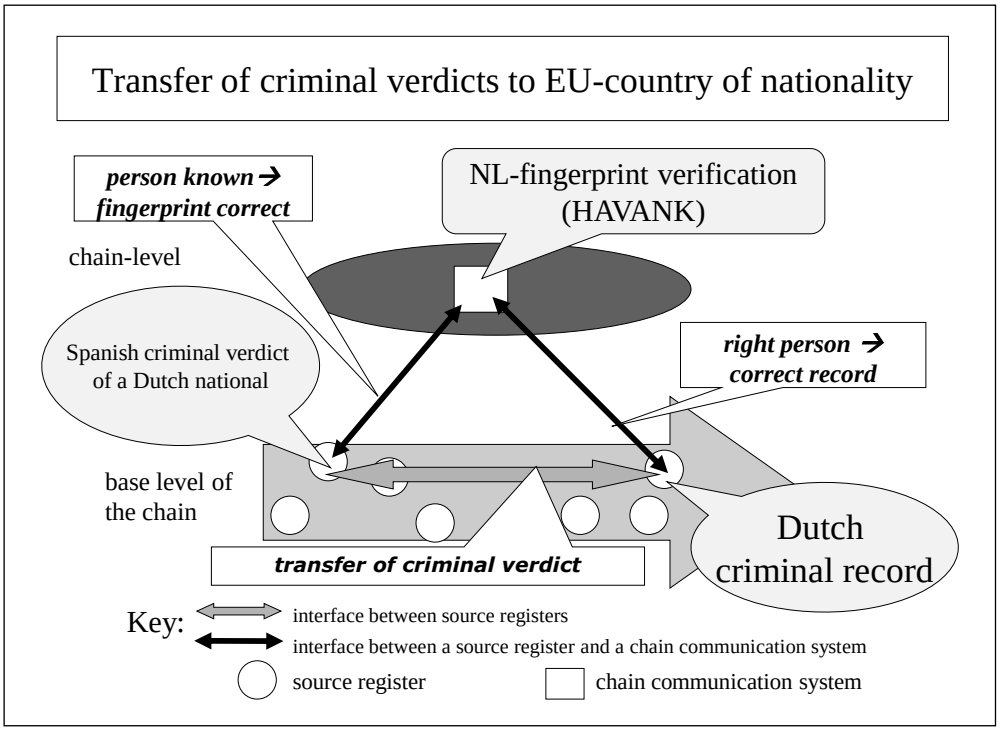

Figure 3 Transfer of criminal verdicts between EU member states.

The European Counsel first wished to bring about a single, central European criminal registry (Grijpink, 2006a). Chain-computerisation theory tells us that a physically centralised EU criminal registry cannot be expected to work adequately at this enormous scale. Fortunately, the efforts are now being aimed at bilateral exchange of criminal verdicts between member states, so that every member state has a complete criminal record of every criminal having its nationality. Eventually, this will establish a distributed EU criminal registry that might indeed be able to successfully prevent border crossing criminal cases - such as that of Fourniret - from happening again.

Eventually, the dominant chain problem identity fraud might generate the interplay of forces that could lead to a European chain communication system enabling forensic biometric identity verification in all criminal proceedings all over the European Union. A pilot was carried out in 2012 to check whether identity fraud by criminals can be considered to be the dominant chain problem triggering effective chain co-operation on the European scale. The UK police sent 9000 verdicts of EU-citizens convicted in the UK to the respective EU-coutries of nationality with the request to check the ID relevant details in the national justice information systems. We do not know whether this sample was a random sample or not. In any case, the results are alarming: 47% of the convicted persons were reported known, 16% of whom with different details (identity fraud); 53% of the convicted persons were reported unknown. Supposing that first-offenders do not commit their first offence in a foreign country, this high percentage 'unknown' might conceal many cases of successful identity fraud, probably at least as much as the 16% of the group of known persons. This brings the incidence of identity fraud by EU-citizens in the UK to somewhere between 16 and 69% in this sample of 9000 verdicts. The UK police asked the EU-member states to send back their verdicts of convicted British nationals: 63% of the convicted British were known, with 21.4 % proven identity fraud; 37% unknown. This brings the incidence of identity fraud by convicted British criminals somewhere between 21.4 and 58.4 percent. We have seen in section 4 how the Dutch criminal law enforcement chain has been successful in tackling the dominant chain problem identity fraud. The dominant chain problem identity fraud should induce other EU member states to adopt a similar chain communication infrasructure and prevent cross border

identity fraud. Much will already be gained if every transferred criminal verdict is accompanied by a document containing the convicted person's fingerprint set and two high resolution photographs (front and profile) taken right at the start of the criminal procedure, at the same time as the enrolment of the fingerprints. If this document is missing, the criminal verdict should not be filed in the criminal registry of the criminal's member state. If the convicted person is transferred to his country of nationality to serve his sentence, this forensic biometric ID-checking should be repeated to make sure that he is the right person with the correct administrative identity. The issue of getting an integer criminal registry will keep the criminal justice authorities within the EU busy for the next decades.

This example stands for many other big systems on EU scale. If, in future, we are not able to adequately counteract dominant chain problems of this type - also, for example, in large-scale EU co-operation in the fields of identity management and health care - government and information science will ultimately lose much of their legitimacy. Usually, politicians and managers like to simplify this type of complicated interdependence between and within large-scale systems, but our chain research has taught us that we had better deal with the world as it really is. This does not exclude simple solutions, as this example shows.

7 Breaking Views and Challenges from Chain Research

During the past ten years, twenty three large-scale Dutch chain co-operation cases were studied at the Institute of Information and Computer Sciences of Utrecht University (UU), using the guidelines and the chain analysis tools provided by the theoretical framework of Chain-computerisation. See Table 1 for the list of chain co-operation situations studied (Grijpink & Plomp, 2009a: 17). This research programme has led to seven valuable insights and breaking views.

1. *Large-scale systems cannot do without a suitable chain approach*
   Based on our twenty three chain analysis cases we conclude that large-scale systems cannot do without a suitable chain approach, because they must inevitably be implemented without adequate management support during development and exploitation. Moreover, many chains focus on chain subjects that do not (fully) collaborate. A chain approach that takes this rough and chaotic working environment into full account is indispensable, at least if we want better designed social systems and more successful implementation. Above all, that approach should warn of *fallacies of the wrong level*. In public administration and information practise, fallacies of the wrong level abound, causing many large-scale systems to carry more weaknesses and risks than people think and robust systems to be rare. More *risk analyses* should therefore be undertaken, preventing naïve solutions. Risks associated with the dominant chain problem are the most significant ones and should also be monitored during the development and exploitation phases of large-scale systems.

2. *Large-scale projects cannot do without chain analysis*
   Chain analysis has proven to be able to distinguish between potentially successful and failing chain projects and should be undertaken on a regular basis in every large-scale initiative. In the majority of the cases studied in our Utrecht University Chain Research programme our chain analysis resulted in the conclusion that – although a chain communication system was necessary – a large-scale chain communication system was not feasible due to lacking co-operation habits and mechanisms. Fortunally, in many of the cases studied, our chain analysis suggested alternative information strategies that seemed more feasible in the chain in question.

Social Product	**Chain**
Health	Emergency health care

	Stroke (CVA) care Diabetes care Medication monitoring Organ transplant care Veterans health care Manic Depressive health care Infectious diseases outbreak management
Safety &security	Excavation damage prevention Identity management Child abuse prevention Nuclear products & waste management Disaster prevention and management Criminal law enforcement Combating terrorism Combating football hooliganism
Prosperity	Social security Debt Relief Combating traffic jams
Welfare	Jobseekers service Combating juvenile prostitution Combating SPAM Drug addicts' health care

Table 1 Chain co-operation situations studied in the UU Research Programme.

3. *Large-scale chain information infrastructures need a multi-level architecture*
In the vast majority of the chain co-operation situations studied, our chain analysis resulted in the conclusion that a large-scale chain communication system was necessary to solve the dominant chain problem requiring a suitable chain information architecture. We know that single central databases - on that enormous scale - yield little more than a concentration of information management activities, not communication. Information must stay within reach of its source and be managed there, too. Therefore, chain communication (at chain-level) must be separated from data collection and storage (at the base-level of the chain). This implies that a chain has to be analysed as a multi-level phenomenon.

4. *The vigorous impact of a dominant chain problem*
Because a chain has no overall co-ordinating and enforcing authority, a chain communication system can only cope with inherent resistance and lack of support in a chain, if it is implemented in a lean and flexible chain information infrastructure containing a central access system including a method for signals and alerts. What is remarkable here is that the access mechanism differs between chains depending on the chain's dominant chain problem. Our chain research uncovered a wide variety of dominant chain problems, each provoking a different intensity of collaboration and requiring a different and customised chain communication system. For someone who has had a heart attack, it is important that a small number of details are immediately available to the consulting physician so that he can effectively intervene when necessary. The chain will therefore have to be able to supply those details as quickly as possible. This communication system is completely different from that for diabetics, for instance, which is focused on monitoring the patient's condition and depends upon his own lifestyle and self-discipline.
In some of our cases, the dynamic chain concept of the theoretical framework of Chain-computerisation enabled us to sharply highlight the new chain communication system and to formulate a concrete transition strategy. In section 4 and 6 we have seen this happen in the criminal law enforcement chain.

5. *Chain partners have only a limited view of chain issues and priorities*
Chain partners look at chains only from the viewpoint of their own organization, interests and priorities, thus overestimating chances and opportunities and underestimating risks and difficulties. This might be the principal reason why big projects and systems fail or disappoint. In our chain research, we were confronted with the problem that, as a result, dominant chain problems are usually hidden and cannot be found by interviewing chain partners and adding the responses. We had to perform disciplined analysis to discover a chain problem, if any, and to then assess its dominant character, if any. The good news is that, once it has been defined, chain partners generally recognise the dominant chain problem as the major common problem.

6. *Two major causes of failing large-scale projects and systems*
Two major causes of failing large-scale projects and systems have surfaced in our chain research. The first relates to the complexity of chain processes, the second to inadequate collaboration mechanisms required to benefit from large-scale information exchange.

   i. It is only complex chains - requiring feed-forward *and* feedback mechanisms for adequate case handling in the chain - that cannot do without a chain communication system for the mutual information exchange. In a simple, lineair chain with a dominant chain problem that can be tackled within sequential dependency of the chain partners, a chain communication system at chain-level is not necessary, because feed-forward mechanisms alone will suffice. If a chain communication system is not necessary due to a lineair chain structure, successfully developing and implementing a large-scale chain communication system will be very difficult. Particularly interesting here are chains that appear to be in a transition process from a linear chain to a complex chain due to a new dominant chain problem triggering the need of feedback overtaking the ruling dominant chain problem that could do without. In the long run, this opens the way to a large-scale communication system depending on the new dominant chain problem. The criminal law enforcement chain offered an example. Until *recidivism* triggered special chain co-operation with feedback mechanisms, the criminal law enforcement chain could be seen as a linear chain with feedforward mechanisms only. Later on, the dominant chain problem of *identity fraud* created an even rougher interplay of forces leading to a higher level of chain organisation and intensifying the need of chain communication, with feedback *and* feed-forward mechanisms.

   ii. The second major obstacle to the successful development and implementation of large-scale communication systems lies in a lack of chain organisation: the chain partners should be familiar with collaboration mechanisms that enable handling feedback and interdependency. Most of the complex chains studied so far in our chain research have an inadequate level of organisation, causing national projects to fail. However, sometimes a regional approach is promising, but politicians, public administration and information science have a strong preference for big, nationwide and ambitious projects. Fortunately, the methodology of Chain-computerisation is now available to be able to assess a large-scale project's or system's feasibility beforehand.

7. *Identity problems threaten the constitutional state*
Identity fraud/theft is easy and profitable and our systems are generally not designed to prevent or detect identity fraud or identity theft. Identity checking is considered to be an invasion of privacy, thus requiring regulation and transparency. This implies that procedures can be observed and predicted. So, identity fraudsters can be well prepared.

Most of the chains studied in our chain research are struggling with identity problems, but in different ways depending on the dominant chain problem. Identity management and checking must be chain-specific to be able to cope with the particular dominant chain problem. General ID-instruments are prone to attack in the weakest (part of the) chain depending upon the dominant chain problem facilitating false identities to surreptitiously spread to other chains. Unless we develop chain-specific ID solutions, identity fraud will increasingly threaten our constitutional state because victims have to prove their innocence more and more often. Preventive measures against identity fraud are rare and sloppy and methodologies to distinguish culprits from victims are mostly poor and erroneous. Procedures and instruments should be tested against the criterion: will it prevent or detect identity fraud; especially will it protect me against someone piggybacking on my identity? Identity checking should be smarter and imply at least 'three or four times knocking', e.g. a combination of a biometric detail, a token and one or two details that only the right person can be expected to know.

We conclude with a list of some major challenges for government and information science:

1. better methodologies to quickly discover a dominant chain problem and find out about its dynamics and impact on large-scale chain co-operation;
2. better risk analysis and risk monitoring methodologies for large-scale social systems (criminal records, patient files, identity records) before, during and after development;
3. better methodologies to develop suitable checks & balances within large-scale social systems that can effectively prevent or cope with threats and risks;
4. better methodologies to incrementally develop chain co-operation practise and large-scale communication systems;
5. a better balance between on the one hand the burden on complying citizens and on the other hand security mechanisms to withhold non-complying people from manipulating large-scale systems;
6. better ways to protect identities and underlying personal data;
7. better ways to detect manipulation and misuse;
8. new methods and models of identity fraud prevention in large-scale systems;
9. methodologies to separate culprits from victims in cases of successful identity fraud;
10. methods to clean contaminated files that contain data from more than one person as a consequence of identity fraud.

If at least a few of these challenges could be solved in the next decennium, our information society will be a better place to live.

Biographical notes: Jan Grijpink (1946) is since 2011 Emeritus Professor of Utrecht University. From 1984-1995 he was responsible for information system development and from 1995-2011 he was Principal Advisor at the Dutch Ministry of Justice, with a special focus on information strategy and identity issues in the context of large-scale public-private chain co-operation.
He is senior advisor of PBLQ, the IT consultants for government in The Hague.
He is editor-in-chief of the e-Journal of Chain-computerisation. http://jcc.library.uu.nl
He studied Economics (1969) and Law (1971) at Groningen University and earned a postgraduate degree in Organisation & Management Science (S.I.O.O., Utrecht) in 1976. In 1997 he obtained his doctorate at Eindhoven Technical University with a thesis about Chain-computerisation.
Jan Grijpink regularly publishes on chain and identity issues in a complex information society focusing on large-scale information systems and chain interdependencies.

References

Cohen, M.D., March J.G. & Olsen, J.P. (1972). A garbage can model of organizational choice. *Administrative Science Quarterly*, 17(1), 1-25.

Grijpink, J.H.A.M. (1997). *Keteninformatisering. Met toepassing op de justitiële bedrijfsketen. Een informatie-infrastructurele aanpak voor de communicatie tussen zelfstandige organisaties.* [*Chain-computerisation. Applied to the Criminal Law Enforcement Chain. An information-infrastructural approach to the communication between autonomous organisations.*] The Hague: Sdu Uitgevers.

Grijpink, J.H.A.M. (1999). *Werken met Keteninformatisering. Informatiestrategie voor de informatiesamenleving*. [*Chain-computerisation in practice. An information strategy for an information society*.] The Hague: Sdu Uitgevers.

Grijpink, J.H.A.M. (2000a). Chain-computerisation for interorganisational policy implementation. *Information Infrastructures & Policy, 6*, 81-93. Amsterdam: IOS Press.

Grijpink, J.H.A.M. (2000b). Chain-computerisation for better privacy protection. *Information Infrastructures & Policy, 6,* 95-107. Amsterdam: IOS Press.

Grijpink, J.H.A.M. (2000c). Een Dynamisch Ketenbegrip voor Informatisering van Externe Samenwerking [A Dynamic Chain Concept for the Computerisation of Inter-organisational Co-operation]. In van Duivenboden, van Twist, in 't Veld en Veldhuizen (eds), *Ketenmanagement in de publieke sector [Chain Management in the public sector]*. Utrecht, Lemma.

Grijpink, J.H.A.M. (2002a). *Informatiestrategie voor Ketensamenwerking: Keteninformatisering als visie, resultaat en methode.* [*Information Strategy for chain co-operation. Chain-computerisation as perspective, result and methodology.*] The Hague: Sdu Uitgevers.

Grijpink, J.H.A.M. (2004a), Identity fraud as a challenge to the constitutional state, in: *Computer Law and Security Report*, 20(1), 29-36.

Grijpink, J.H.A.M. (2004b), Two barriers to realizing the benefits of biometrics: A chain vision on biometrics, and identity fraud as biometrics' real challenge, in: *Optical Security and Counterfeit Deterrence Techniques V*, edited by Rudolf L. van Renesse, Proceedings of SPIE-IS&T Electronic Imaging, SPIE 5310, 90-102.

Grijpink, J.H.A.M. (2004c), ICT, Spelbederver of Dwarskijker? [ICT, spoiler or snoop?] *Valstar & van Genuchten (eds.), 50 Jaar informatiesystemen 1978-2028, Liber Amicorum Theo Bemelmans, p. 335-353, p. 352*

Grijpink, J.H.A.M. (2005). Our emerging information society: The challenge of large-scale information exchange in the constitutional state. *Computer Law and Security Report*, 21(4), 328-337.

Grijpink, J.H.A.M. (2006a). Criminal Records in the European Union: The challenge of large-scale information exchange. *European Journal of Crime, Criminal Law and Criminal Justice*, 14(1), 1-19.

Grijpink, J.H.A.M. (2006b). Identiteitsfraude en overheid [Identity fraud and government]. *Justitiële verkenningen*, 32(7), 37-57.

Grijpink, J.H.A.M. & Plomp, M.G.A. (Eds.). (2009a). *Kijk op ketens: Het ketenlandschap van Nederland* [*View on chains: The Chain Landscape of The Netherlands*]. Den Haag: Centrum voor Keteninformatisering.

Grijpink, J.H.A.M. (2009b). Ketenvisie [Chain Perspective]. In J.H.A.M. Grijpink & M.G.A. Plomp (Eds.), *Kijk op ketens: Het ketenlandschap van Nederland* [*View on chains: The Chain Landscape of The Netherlands*] (pp. 29-49). The Hague: Centrum voor Keteninformatisering.

Grijpink, J.H.A.M. (2009c). Ketenanalyse [Chain Analysis]. In J.H.A.M. Grijpink & M.G.A. Plomp (Eds.), *Kijk op ketens: Het ketenlandschap van Nederland* [*View on chains: The Chain Landscape of The Netherlands*] (pp. 51-68). The Hague: Centrum voor Keteninformatisering.

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

Grijpink, J.H.A.M. (2010b). *Keteninformatisering in kort bestek. Theorie en praktijk van grootschalige informatie-uitwisseling*. 2nd edition. [*Chain-computerisation in brief. Theory and Practice of large-scale information exchange*.] The Hague: Boom/Lemma Uitgevers

Grijpink, J.H.A.M. (2012a). A Chain Perspective on Large-scale Number systems. *Journal of Chain-computerisation,* 3, 1-26.

Grijpink, J.H.A.M. (2012b), Large-scale Information Exchange: breaking views and challenges, in Snellen, Thaens & van de Donk (eds.), *Public Administration in the Information Age: Revisited.* 182-204. Amsterdam: IOS Press

Grijpink, J.H.A.M. (2012b), Large-scale Information Exchange: breaking views and challenges, in Snellen, Thaens & van de Donk (eds.), *Public Administration in the Information Age: Revisited*, 182-204. Amsterdam: IOS Press

March, J.G. & Olsen, J.P. (1976). *Ambiguity and Choice in Organisations*. Bergen: Norway Universitetsforlaget.

Miller, S.J., Hickson, D.J. & Wilson, D.C. (1996). Decision-Making in Organizations. In S.R. Clegg, C. Hardy, & W.R. Nord (Eds.), *Handbook of Organization Studies* (pp. 293-312). London: Sage.

Padgett, J.F. (1980). Managing garbage can hierarchies. *Administrative Science Quarterly*, 25(4), 583-604.

Rittel, H.W.J. and M.M. Webber (1973). Dilemmas in a General Theory of Planning. *Policy Sciences*, 4, 155-169