

# MODELLING THE COLLAPSE OF A CRIMINAL NETWORK

Martin Neumann

Ulf Lotzmann

Institute of Information Systems Research  
University of Koblenz-Landau  
Universitätsstraße 1, Koblenz 56070, Germany  
E-mail: {maneumann, ulf }@uni-koblenz.de

## KEYWORDS

Qualitative data analysis, conceptual modelling, agent-based simulation, normative agent architecture, criminal networks.

## ABSTRACT

Research activities aimed to understand the dynamics of criminal networks or organisations – like extortion racket systems – are of interest for criminologists and scientists in related fields, for practitioners from police and judiciary, as well as for political decision makers. This paper aims to contribute to this area by bringing together data analysis methods with conceptual modelling and simulation techniques employing normative agents. As an exemplary case the internal collapse of a criminal network is investigated. The outlined model development process involves qualitative data analysis of police files, specification of a conceptual model of the dynamics within the regarded criminal network, and the definition of intra-agent processes for the agents used in the simulation model.

## INTRODUCTION

The research outlined in the paper is part of the GLODERS research project (<http://www.gloders.eu/>), directed towards development of an ICT model for understanding the dynamics of Extortion Racket Systems (ERSs). These are criminal organisations of which the Mafia is but one example. Two scenarios have been selected to develop conceptual models in complementary ways which then can be transformed into formal simulation models:

- A Palermo scenario, describing the dynamics of the (at least formerly) culturally deep entrenched Sicilian Mafia within the society. This theory driven scenario can build on rich empirical research about the Sicilian Mafia, the Cosa Nostra.
- A contrasting scenario, describing the internal dynamics within a criminal organisation in a different European country. This data driven scenario applies a grounded theory approach, building on Police interrogations resulting from a number of investigations of a particular criminal group. This scenario is subject of this paper.

Internal dynamics of criminal organisations is of theoretical interest as subject of scientific research because criminal organisations face the specific problem of securing compliance with the norms of conduct in the absence of juridical norm enforcement. This generates a problem of conflict resolution: Theories of norms typically refer to the

notion of sanctions or punishment as a norm enforcement mechanism (Ullman-Margalit 1978, Hechter and Opp 2001, Bicchieri 2006, Horne 2007). In behavioural terms punishment can be described as some kind of aggression. If I get a fine for wrong parking, or if a mother scolds her child, this goes along with losses of utilitarian values (anyhow they are measured: in the case of a fine it is monetary value, in the case of scolding it might be the feeling of shame). However, obviously not every aggression is punishment. This is particular obvious in the case of criminals. Striking an old lady down to get her purse is aggression but certainly it is a norm deviation, not enforcement. Likewise extortion is a crime. However, without recourse to state monopoly of legitimate violence the motivation of aggression might remain ambiguous. For instance aggression can be self-interested. Robbery of a purse is one example. As another possibility it might simply be result of extensive drug consumption. In the case of criminal organisations this ambiguity is particular precarious. On the one hand, there is a need to enforce the norms of conduct in some way. On the other hand, the lack of the authority of juridical court provides an incentive to manipulate norm enforcement in its own interest. For instance Arlacchi (1992) describes the situation of the Cosa Nostra in the 2<sup>nd</sup> Mafia war in the 1980s (Arlacchi 1992, Dickie 2004) as a Hobbesian society of a war of everybody against everybody else. While formally aggression has been justified as sanction it became obvious that this justification was merely cheating. Thus aggression remains ambiguous. In the legal society recourse to the jurisdiction of the court provides an ultimate answer. This is absent in criminal organisations. For this reason criminal organisations provide a means to investigate mechanisms for conflict resolutions and how these might fail. In particular this involves reasoning about aggression (Andrighetto et al. 2013). This is a particular challenge for simulation of normative processes in which punishment is taken as a basic concept and thus the need to interpret aggression is not considered so far (Axelrod 1986; Conte and Castelfranchi 1995; Andrighetto et al 2007; Neumann 2008; Savarimuthu et al. 2013; Lotzmann et al. 2013).

This paper focuses on the scenario for which the data-driven modelling approach has been applied in order to find the relevant aspects of the dynamics that led to the breakdown on this particular criminal network. There are annotations from the real case used to show traceability of the conceptual model to the evidence base. However, the police files that constitute the evidence base for this scenario are not publicly available, thus the description had

to be rephrased in a neutral way in order to ensure protection of privacy.

## EVIDENCE BASE OF THE MODEL

The Scenario applies a grounded theory approach (Corbin and Strauss 2008) based on police interrogations in 2005 and 2006 that resulted from various police investigations of a criminal gang. Established in the early 1990s its business model consisted of drug trafficking and laundering the illegal money gained in the drug business. Drug trafficking was done by 'black collar criminals' with access to the production and distribution of drugs. 'White collar criminals' were ordinary businessmen responsible for the money laundering. They got roped into the business in the early 1990s. The psychological techniques applied to draw them in the illegal world beyond a point of no return will not be subject of this paper. Police files identified (at least) one white collar criminal working in the real estate business. It is important that the real estate trader had a good reputation in the legal society. This allowed him to invest illegal money in the legal market and give the return of investment back to the investor. Money laundering is essentially based on a norm of trust: the black collar criminals need to hand over the money to their partners and trust them that they will get the return of investment back from the trustee. In a covert organisation this cannot be secured by formal contracts. Therefore trust is essential. The network lasted for about 10 to 15 years until it collapsed. An initial divide went out of control, and the mistrust could not be encapsulated but spread rapidly through the whole network. Once trust was corrupted, a run on the bank was initiated. Black collar criminals attempted to get their invested money back before it was lost completely. Attempts to get the money back led to extortion. Thereby the white collar criminal became victim of his criminal business partners. A formerly symbiotic relationship between black and white collar criminals (a long term relation of a win-win situation for both) became parasitic (i.e. a lasting but no longer profitable situation). This generated a cascading effect through the network which destroyed the overall network in a violent blow-up. This characteristic of the case makes the data particularly interesting to identify essential elements in the mechanisms of conflict resolution in the absence of juridical law, i.e. the failure allows to identifying the elements which must not be missing.

Conflicts escalated to a degree of violence that has been described by witnesses as a 'rule of terror' in which 'old friends were killing each other'. In fact, many members of the network were killed. The 'rule of terror' could not be attributed to an individual member of the group but can be described as ruled by an invisible hand. Norms of conduct were only implicit, leading to many misperceptions which generated a cascading effect of spreading mistrust. This shall be illustrated here by one example: In the data it can be found the testimony of a member that "M. told the newspapers [about my role in the network] because he thought that I wanted to kill him to get the money." M. had survived an attack on his life, but he was wrong in the assumption that this particular member of the organisation was behind this attack. However, his counter-reaction caused further panic of other group member such as the one

who had been reported here and wrongly brought into trouble. This was the starting point of the cascading of mistrust in the group.

This example provides insights into processes of reasoning about aggression: first, M. interpreted the attack on his life not as a penalty (i.e. death-penalty) for deviant behaviour from his side such as being too greedy. Instead he concluded that the cause of the attack was based on self-interest (the other criminal 'wanted his money'). Thus he interpreted the attack as norm deviation rather than enforcement. Next, he attributed the aggression to an individual person and started a counter-reaction against this particular person by betraying 'his role in the network'. However, since his reasoning went wrong, this counter-reaction provoked further reasoning about the cause of and possible reactions to his aggression. This generated a cycle of revenge and counter-revenge.

In more abstract terms the cascading effect of spreading mistrust is due to the fact that the criminal group was based on personal acquaintanceship without a formal structure of positions. For this reason it remained precarious to differentiate between punishment and revenge, depending on subjective interpretation which factually initiated a lot of misunderstanding. Punishment entails a stop point for the aggression: Punishment is applied for a particular situation, e.g. a fine for wrong parking. Once the fine is paid, the punishment is over and the aggression terminates. As this example demonstrates, revenge might lead to counter revenge which again stimulates new aggression. However, interpretation of aggression as punishment requires at least minimal social structure: aggression applied by a higher hierarchy level is more likely to be interpreted as punishment (at least members may obey even if factually it might be wrong), whereas aggression between peers is more likely to be interpreted as revenge.

## METHODOLOGICAL APPROACH

Methodologically the data was loaded into MaxQDA as a tool for qualitative text analysis (see Corbin and Strauss 2008) and text passages were annotated which then were summarised into codes deriving concepts from data. Concepts stand for classes of object, events or actions which have some major properties in common. This enables concept identification supported by CAQDAS technology. The coding derived with MaxQDA served as the basis for concept relation identification with the CCD tool (a software for creating Consistent Conceptual Descriptions; Scherer et al. 2013). The CCD tool provides an environment for developing a conceptual model by a controlled identification of condition-action sequences (denoted as action diagram) which represent the micro-mechanisms at work in the processes described in the data. Whereas the data describes individual instantiations, the condition-action sequences represent mechanisms insofar as they describe generalisable event classes. However, empirical traceability is ensured by tracing the individual elements of the action diagram resulting from the identification of condition-action sequences in the CCD tool back to text annotation in the data. These annotations are extracted from the coding derived with MaxQDA. This approach is particular appropriate for dissecting cognitive elements in the data. Police interrogations are a situation of

dialogical conversation, not biased by categories in the mind of the researcher. This allows to bringing the empirical analysis very close to the subjective perception of the actors. An in-depth analysis of subjective meaning attributed to certain situations enables to establish an empirical evidence base for modelling intra-agent processes such as reasoning about aggression.

The agent architecture constituted by these intra-agent processes is the starting point for creating several types of software agents, which are able to interact within a simulation environment by different means, as described in the evidence base and specified in the conceptual model.

## CONCEPTUAL MODEL OF THE COLLAPSE OF THE GROUP

In the following the action diagram resulting from the data analysis will be exemplified. In the process of the collapse of the group four phases can be distinguished: the ordinary business of money laundering, a crystallising kernel of mistrust, a stage of conflict escalation and finally the 'corrupt chaos', including a run on the bank. The first two processes will be illustrated in detail, the others will only briefly be sketched.

### The ordinary business: money laundering

The ordinary process of money laundering (Figure 1) starts with illegal money available and ends when legal money is available for the black collar criminals. In the following this process is shown in detail.



Figure 1: Ordinary business of money laundering

In this diagram the conditions of, for instance, 'level of trust above threshold' and 'illegal money available' trigger the action 'give money to trustee'. Traceability of the empirical evidence is provided by annotations of the condition-action sequences. In the following, passages of the police interrogations will be documented which provide

the empirical evidence for all phases of the process. Names and dates have been hidden for reasons of protecting privacy.

*Annotation (illegal money available):* "In the period between 1990 and XX 1992 police investigations had been undertaken. These revealed a criminal organisation concerned with drug trafficking. The report from XX 1992 estimated the income and the costs. It is estimated a transaction volume of nearly 300 million."

If illegal money is available a second condition of trust need to be fulfilled for starting the process.

*Annotation (level of trust above threshold):* "O1 and V01 seem to be friends for me."

These annotations secure traceability of the starting conditions for the process. Money laundering is triggered when illegal money is given to a trustee with a legal business who invests the money in the legal market. The trustee is the link between the illegal and the legal world. The next step in the process is the investment of the money in the legal market as demonstrated in the following annotation:

*Annotation (return of investment available):* "On the basis of witnesses and financial investigations it is suspected that O1 and all persons directly or indirectly associated with him received considerable boni for transactions in which V01 and his companies had been involved."

The return of investment is redistributed to the investors. However not directly but via straw men who receive the money from the trustee and hands it over to the original investor.

*Annotation (straw man received money):* "The funding went from V1 to B3 and then to the father of M.O."

This annotation shows the process of money flow via so-called straw men. Finally legal money is available for black collar criminals.

*Annotation (legal money available):* "At the moment I have paid 800 000 in the firm which are now several millions worth through legal trade."

### Crystallising kernel of mistrust

The action diagram in Figure 2 shows the details of the initialisation of mistrust, followed by annotations, demonstrating the empirical traceability of the condition-action sequences.

Starting point is the event that for some reasons (out of the scope of the investigation) some member of the organisation becomes distrusted, as illustrated by the following annotation.

*Annotation (member X becomes disreputable):* "Since O8 is released from prison there were tensions observable between O6, O1 and V01 on the one hand and O8 on the other hand."

This triggers an aggressive action against this member, who needs to interpret the aggression once he recognises it. First an example for aggression will be provided.

*Annotation (perform aggressive action against member X):* "An attack to the life of M."

Aggression may be interpreted either as norm enforcement, i.e. a form of punishment for deviant behaviour (Norm of trust demanded), or as an arbitrary aggression (Norm of trust violated). In the former case the victim of aggression may obey, which restores the trust in the organisation, or

cheat. In the latter case the victim of the aggression decides about the reaction by either betraying the organisation or performing an act of counter-aggression. This is demonstrated by the examples of empirical evidence below. *Annotation (member X decides to betray criminal organisation):* Statement of V01: "M. told the newspapers 'about my role in the network' because he thought that I wanted to kill him to get the money."

As already indicated M.'s interpretation of the aggression was misleading. However, it is an example that he interpreted the aggression as a violation of his trust in V01 and reacted by betraying him. An example of counter-aggression is the following:

*Annotation (member X performs counter-aggression):* "Presumably V01 asked the Hells Angels to make an operation against O1 in return for a huge amount of money."

A different example is the following sequence, showing the pathway to obedience is the following sequence of aggression and the corresponding reaction.

*Annotation (aggression recognised by member X):* "At May XX, YY, O5 came to my house in order to say that at 8 in the evening I should come to the forest. This is standard: intimidate and request for money."

*Annotation (member X obeys):* "I paid, but I'm alive."

However, the victim of aggression may also decide to cheat:

*Annotation (member X decides to cheat):* "Following O1 C. betrayed to him even the people who they wanted to liquidate."

### Conflict escalation

The next sequences will only briefly be sketched. Selected annotations indicate the empirical evidence. The process of conflict escalation is an expansion of the initial mistrust. In particular a feedback is included from 'becoming victim of aggression' to 'interpret aggression'. In the case of counter-aggression performed by the original victim of an aggressive act, a new member of the group becomes victim of aggression, who in turn needs to interpret this aggression. This enfolds a positive feedback loop which may become unstable.

Betrayal can appear in various forms: whereas internal betrayal means that the person does something incorrect against a suspected aggressor, external betrayal consist of whistle-blowing to the police or even the wider public (such as e.g. a newspaper). Internal betrayal leads to the event that this member of the organisation becomes disreputable only if this becomes known.

*Annotation:* "V01, killed at May XXX had spoken several times with criminal investigation officers." The text example above provides also an example for the escalation of violence up to murder. In fact several members of the group were killed.

If the organisation becomes public (by external betrayal or because of visible violence such as murder), it becomes possible to fight against the criminal organisation from outside with police investigations. These might lead to juridical decisions. Both events might trigger a counter reaction which will be explained in the next section.

### 'A corrupt chaos'

Finally the escalation of the conflict may reach a stage at which trust is no longer recoverable. In particular this includes the cognitive element of 'fear for life' and the modelling perspective on this subjective cognition of 'evaluating the level of trust'.

The process of the collapse of the organisation can be described as a cascading effect in which a norm of trust in the organisation breaks down. A subjective perception of the overall situation is given below:

*Annotation:* "There is a rule of terror in the town."

This overall situation consists of several micro-elements. However, these were not visible for all members of the group, leading to the nebulous assumption of a rule of terror which could not be attributed to a single person. Subjectively the terror seemed to be ruled by an invisible hand.

*Annotation:* "There is a corrupt chaos behind it."

In modelling terms, this can be described as result of an evaluation of the trust. If the trust in the organisation still remains above a threshold, the usual business continues. If this is not the case it might trigger a panic reaction. Moreover, group members may also become victim of

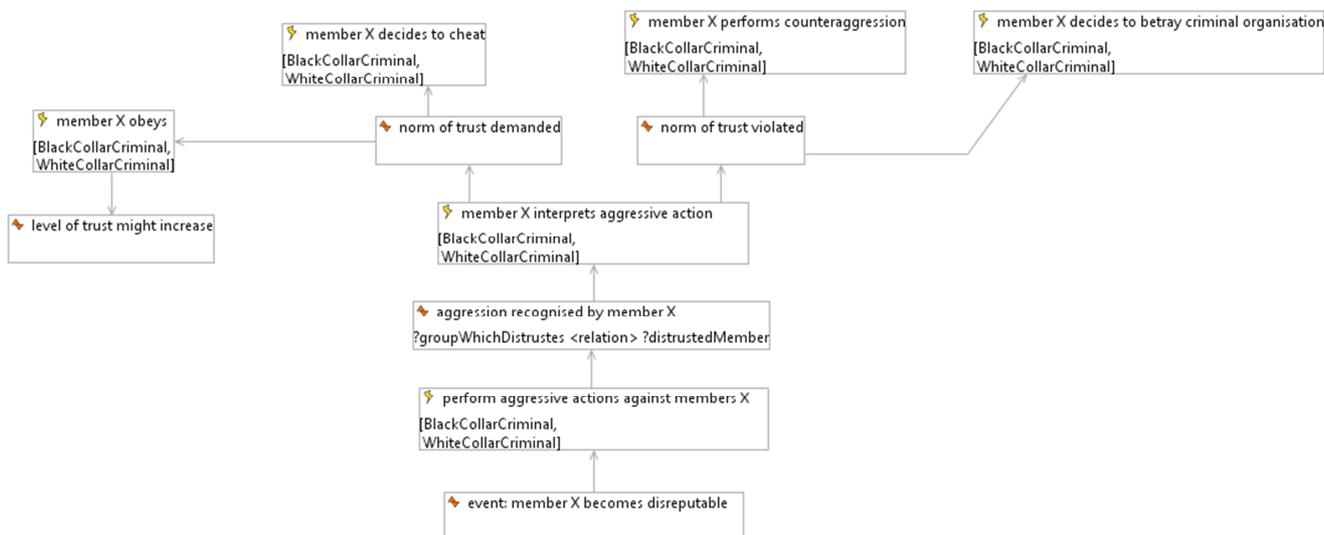


Figure 2: Crystallising kernel of mistrust

murder. The observation of the murder might again trigger the afore-mentioned panic reaction. A panic reaction is characterised by immediate and often irrational actions guided by fear. However, the object of a panic can be twofold: fear for life or fear for money. It remains unclear in the data if both are inherently intertwined or if they – at least possibly – might be distinct instances of panic. It will be a key objective of simulation experiments to investigate scenarios which clarify the causal relations between both kinds of panic. First, fear for life shall be considered. Fear for life triggers various possible reactions such as attempts of pre-emptive murder. This is illustrated in the following testimony:

*Annotation:* “He was at a point in which he was in a totally despaired situation. HLJ had several times tried to counteract. He had a plan to approach O1 with a weapon. However, in the last moment he didn't dare. At a different time he had two pistols with him. He planned to shoot O1 to death and to pass the other weapon in his hand in order that it appeared as if he had shot in self-defence.”

### Run on the bank

The ‘corrupt chaos’ sketched above triggers a ‘run on the bank’. Fear for money stimulates a request to get the invested money back before it is lost completely. An attempt to get the money back nevertheless might trigger intimidation of the trustee (the white collar criminal) who now becomes victim of aggression which he needs to interpret; i.e. this enfolds a positive feedback cycle.

*Annotation:* “In the last year he was strongly under pressure because he had been extorted. That's what he said to me.”

However, if the intimidation of the trustee becomes public in the organisation, this might trigger a run on the bank by stimulating a panic reaction among other group members. This is illustrated by the example below.

*Annotation:* “Soon after his death the widow of K had an affair with O1. She extorted 7 million from V01. Contrary to the claim of M. his entitlements had not been captured by this deal.”

This provided an incentive for M. to try to get his money back on his own.

### INTRA-AGENT PROCESSES

This section describes the first steps of the process of developing a simulation model from the conceptual description presented above. The two pilot scenarios which are developed are meant to integrate the normative approach based on EMIL-IA (the normative agent architecture developed in the EMIL project, extended by norm internalisation capabilities; Andrighetto et al. 2010) with properties of several stylised facts models.

The following subsections firstly give an overview on some important simulation model properties in order to exemplarily describe the formalisation approach for distinct behavioural aspects of individual agent types (as derived from the action diagram, which in contrast covers the behaviour of the entire system). The intra-agent processes are defined as modules and specified by flow charts, focussing on processing of data, in this context mainly events for triggering processes, and different kinds of parameters determining the control flow. The most

important kind of parameters is related to norms ruling the agents' behaviour.

### Simulation model properties

The conceptual model as derived from the qualitative data analysis comprises four major types of actors, which will become agent types in the simulation model. Three of the actor types constitute the criminal network:

- The black collar criminal, who is involved in drug trafficking, applies violent actions in various situations and for several reasons and needs the service of white collar criminals for money laundering.
- The white collar criminal, who is key person for money laundering and usually is less involved in violent actions. However, in the scenario of breakdown of the criminal network, his involvement in violence (i.e. the adoption of behaviour of black collar criminals) seems essential for the process.
- The (so called) straw men are supporting the other types of criminals in the money laundering process in different fashions.

The only actor outside the criminal organisation regarded in this scenario is the police. The actions of the police actor are currently limited to a general criminal investigation (eventually leading to a juridical decision) and the possibility of information leakage to actors of the criminal network.

All these actors are ruled by norms. As a result of the detailed examination of the empirical data, a restricted number of norms have been identified which implicitly govern the behaviour of the actors. As an example, for all types of criminals a ‘top-level’ moral norm exists:

NORM(1) “moral norm”: NOT VIOLATE TRUST  $c$   $o$

where  $c$  is a criminal and  $o$  is the criminal organisation or network. This norm describes the commitment to the norm of trust within the organisation which holds in the case of unexpected events and is entangled with interpretation of aggressive actions, self-reflexion and the consideration of own past actions.

Related to this norm, a number of concrete obligations are defined. An example is

NORM(1.3) “obligation”: PUNISH  $c_1$   $c_3$  IF  $c_3$  VIOLATE NORM(1)

where  $c_1$  is a criminal who punishes the deviant criminal  $c_3$  for a norm violation.

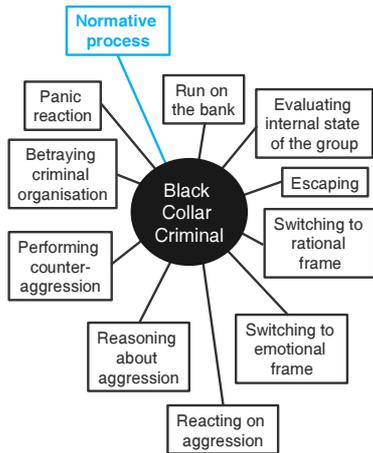
Such a punishment triggers a ‘reasoning on aggression’ process within the punished agent, where the agent must decide whether the experienced aggression was such a punishment, or rather a self-interested act of aggression. This process is detailed to some extent in the following description of the architecture of one of the agent types, the black collar criminal.

### Agent architecture of the black collar criminal

The architecture of the black collar criminal agent is defined by a number of processes which it partly shares with the other types of criminal agents (Figure 3). One of

these processes – the normative process – is of particular importance, as this encapsulates the core of normative reasoning and provides the link – even on software engineering level – between the simulation models for the two scenarios.

The other scenario-dependent intra-agent processes follow in large part the conceptual model, i.e. the behaviour described in the CCD action diagram is reflected in these processes. Exemplarily, two of these processes should be outlined in some more depth: ‘Reasoning about aggression’ together with ‘Reacting on aggression’. Subsequently, the functional interactions between these two processes and the ‘Normative process’ are shown.



**Figure 3: Intra-agent processes of the black collar criminal agent**

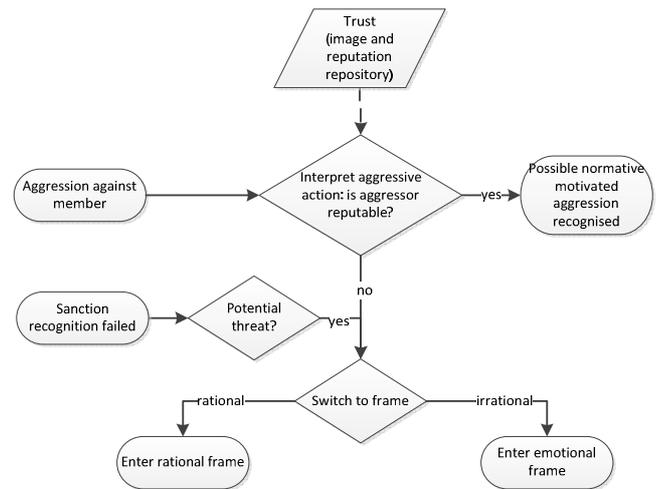
### Reasoning about aggression

The ‘Reasoning about aggression’ process (Figure 4) is triggered when the agent recognises an aggression against itself. It comprises the first of three stages of a decision process, eventually leading to possible reactions on the aggression.

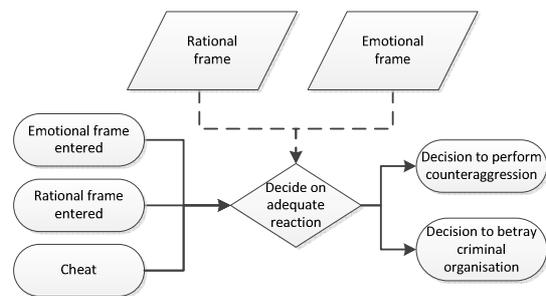
In the first stage it is decided whether the aggressor is reputable and the motivation for the aggression is not gratuitous. Information on trustworthiness of the aggressor from an ‘image and reputation repository’ (a data structure which stores the agent’s belief on image and reputation of other fellow agents) is regarded here. If the aggressor is reputable, a possibly normatively motivated aggression is anticipated and the normative process is triggered at the second stage. A possible result of the normative process might be that the inherent sanction recognition failed (see subsequent section), but the aggression poses a potential threat to the agent. In this case, and in the case that the aggressor is recognised as not reputable, reactions will be triggered by entering the third stage of the process in which the operational mode of the agent is either set to a rational or an emotional frame, amongst others depending on the strength of the initial aggression.

The actual switching to one of the two frames is done in two separate processes not shown here, followed by triggering the ‘Reacting on aggression process’ (Figure 5), in which the agent decides how to retaliate the aggression (either by counter-aggression or by betrayal of the criminal network, depending on the mental frame which the agent has adopted before). This process can also come into play if the agent decides to cheat, i.e. a sanction is recognised

within the ‘Normative process’ but the agent decides not to obey the norm behind the sanction but rather to follow some other (individual) drives.



**Figure 4: Intra-agent process for reasoning about aggression (rounded boxes are start and end events for the process, rhombi are decisions, parallelograms stand for parameters influencing decisions)**



**Figure 5: Intra-agent process for reacting on aggression**

### Normative process

The ‘Normative process’ is one of the major contributions of the GLODERS project and has been designed and is currently implemented with respect to support normative behaviour of agents in different kinds of simulation models. The architecture of this process is an extension and generalisation of EMIL-IA, which itself has been built upon EMIL-A, the normative architecture developed in the EMIL (Emergence in the Loop) project (Conte et al. 2014). The quite complex software design of this process contains six main components:

- An event classifier, pre-processing the incoming data (events like actions, sanctions etc., observation of such events, explicit norm invocations) and determining which of the following sub-processes to trigger.
- A ‘Norm Recognition’ sub-process, which tries to find a norm related to an action or sanction in the internal normative board (a database of norms, sanctions, relations between these two entities and salience values of particular norms).
- A ‘Norm Enforcement’ sub-process, which selects appropriate sanctions as reaction on perceived norm violations.
- A ‘Norm Salience’ sub-process which updates information on the salience of norms.

- A ‘Norm Adoption’ sub-process for normative learning.
- A ‘Norm Compliance’ function which calculates a normative drive, reflecting the strengths and salience of a norm. This value is used by several concrete decision processes of agents.

For the model presented in this paper, the normative process is triggered on two different events. Firstly, it is triggered by the observation that a member of the criminal network has become disreputable. This can be an external event, or due to (re-)actions in relation with the break-down of trust as specified by the conceptual model. This event is classified as observation of an (aggressive) action for which is checked whether a norm violation might be associated with the action. If this is the case, an appropriate sanction is issued.

The other triggering event of the normative process is associated with the ‘Reasoning about aggression’ process described in the previous section. If a possible normatively motivated aggression is recognised, the normative process then checks whether this aggression is a sanction or an aggression not related to any norm. In the former case, the agent can either obey to the norm, or intentionally cheat by not complying with the sanction related to a (potentially salient) norm and rather follow (even more salient) individual drives. For the latter case, a reaction on the aggression will be the consequence, expressed by the event ‘Sanction recognition failed’, signalled by the normative process.

The implementation of the sanction recognition sub-process is based on a search mechanism, trying to match the identifier of an experienced aggression (e.g. PUNISHMENT FOR TRUST VIOLATION) with an existing norm (in this artificial example the NORM(1) “moral norm”: NOT VIOLATE TRUST c o). These concepts have to be expressed in a formal language, which at the same time constitutes the interface to the ‘Normative process’ software component, i.e. which is used for defining the data stored within and processed by this component.

## CONCLUSIONS AND FUTURE WORK

This paper shows the results of the conceptual modelling of the collapse of a criminal network. The qualitative data analysis informing the conceptual model as well as the first formalisation activities towards a simulation model are outlined with emphasis on important design details, e.g. the realisation of normative behaviour. The conceptual modelling enables dissecting the micro-mechanisms of a complex empirical process. These enable a certain degree of generalisation beyond a narrative story of a certain case to shed light on the wheels of social processes. Nevertheless, the evidence based modelling approach retains traceability of the abstract mechanisms to the empirical social world.

The model implementation phase has just started. In the current state of development, the most important behavioural aspects of the organisational breakdown have been regarded in a level of abstraction which makes the development of a sophisticated simulation model reasonable. However, some details and aspects (mainly regarding the ‘everyday business’ of the criminal network –

drug trafficking and money laundering) have not been treated in detail so far, as the data analysis of this part has not been completed yet. The most important short-term future task is to continue the incremental implementation of the concepts and processes described above. The simulation model will then contribute to computational normative agents by implementing reasoning about aggression whether or not to interpret it as sanction.

## ACKNOWLEDGEMENTS

The research has been undertaken as part of the GLODERS project, co-funded by the European Commission under the 7<sup>th</sup> Framework Programme. This publication reflects the view only of the authors and the project consortium, and the Commission cannot be held responsible for any use, which may be made of the information contained therein.

## REFERENCES

- Andrighetto, G.; R. Conte; P. Turrini; and M. Paolucci. 2007. *Emergence In the Loop: Simulating the two way dynamics of norm innovation*. Schloss Dagstuhl, Germany, G. Boella, L. v. d. Torre and H. Verhagen (Eds.).
- Andrighetto, G.; D. Villatoro; and R. Conte. 2010. “Norm internalization in artificial societies”. In *AI Communications*, Volume 23 Issue 4, 325-339.
- Andrighetto G.; J. Brandts; R. Conte; J. Sabater; H. Solaz; and D. Villatoro. 2013. “Punish and Voice: Punishment Enhances Cooperation when Combined with Norm-Signalling”. In *PLoS One*, vol. 8 (6), 1-8.
- Arlacchi, P. 1992. *Mafia von Innen: Das Leben des Don Antonio Calderone*. Fischer, Frankfurt am Main.
- Axelrod, R. 1986. “An evolutionary approach to norms”. In *American Political Science Review* 80 (4), 1095-1111.
- Bicchieri, C. 2006. *The grammar of society: the nature and dynamics of social norms*. Cambridge University Press, New York.
- Conte, R. and C. Castelfranchi. 1995. “Understanding the effects of norms in social groups through simulation”. In *Artificial societies: the computer simulation of social life*, G.N. Gilbert and R. Conte (Eds.). UCL Press, London.
- Conte, R.; G. Andrighetto; and M. Campenni. 2014. *Minding norms: mechanisms and dynamics of social order in agent societies*. Oxford university press, Oxford.
- Corbin, J. and A. Strauss. 2008. *Basics of qualitative research, 3rd ed.* Sage, London.
- Dickie, J. 2004. *Cosanostra: A history of the sicilian mafia*. Palgrave Macmillan.
- Hechter, M. and K. D. Opp. 2001. *Social Norms*. Russell Sage Foundation, New York.
- Horne, C. 2007. “Explaining norm enforcement”. In *Rationality and Society* 19(2), 139-170.
- Lotzmann, U.; M. Möhring; and K. G. Troitzsch. 2013. “Simulating the emergence of norms in different scenarios”. In *Artificial Intelligence and Law* 21(1), 109-138.
- Neumann, M. 2008. “Homo socionicus. A case study of simulation models of norms”. In *Journal of Artificial Societies and Social Simulation* 11(4), <http://jasss.soc.surrey.ac.uk/11/4/6.html>
- Savarimuthu, B.; S. Cranefield; M. A. Purvis; and M. K. Purvis. 2013. “Identifying prohibition norms in artificial societies”. In *Artificial intelligence and law* 21(1), 1-46.
- Scherer, S.; M. Wimmer; and S. Markisic. 2013. „Bridging narrative scenario texts and formal policy modelling through conceptual policy modelling”. In *Artificial intelligence and law* 21(4), 455-484.
- Ullman-Margalit, E. 1978. *The emergence of norms*. Oxford university press, Oxford.