Advances in Soft Computing 53

Editor-in-Chief: J. Kacprzyk

Advances in Soft Computing

Editor-in-Chief

Further volumes of this series can be found on our homepage: springer.com

Bernd Reusch, (Ed.)
Computational Intelligence, Theory and Applications, 2006
ISBN 978-3-540-34780-4

Jonathan Lawry, Enrique Miranda,
Alberto Bugarín Shoumei Li,
María Á. Gil, Przemysław Grzegorzewski,
Olgierd Hryniewicz,
Soft Methods for Integrated Uncertainty Modelling, 2006
ISBN 978-3-540-34776-7

Ashraf Saad, Erel Avineri, Keshav Dahal,
Muhammad Sarfraz, Rajkumar Roy (Eds.)
Soft Computing in Industrial Applications, 2007
ISBN 978-3-540-70704-2

Bing-Yuan Cao (Ed.)
Fuzzy Information and Engineering, 2007
ISBN 978-3-540-71440-8

Patricia Melin, Oscar Castillo,
Eduardo Gómez Ramírez, Janusz Kacprzyk,
Witold Pedrycz (Eds.)
Analysis and Design of Intelligent Systems Using Soft Computing Techniques, 2007
ISBN 978-3-540-72431-5

Oscar Castillo, Patricia Melin,
Oscar Montiel Ross, Roberto Sepúlveda Cruz,
Witold Pedrycz, Janusz Kacprzyk (Eds.)
Theoretical Advances and Applications of Fuzzy Logic and Soft Computing, 2007
ISBN 978-3-540-72433-9

Katarzyna M. Węgrzyn-Wolska,
Piotr S. Szczepaniak (Eds.)
Advances in Intelligent Web Mastering, 2007
ISBN 978-3-540-72574-9

Emilio Corchado, Juan M. Corchado,
Ajith Abraham (Eds.)
Innovations in Hybrid Intelligent Systems, 2007
ISBN 978-3-540-74971-4

Marek Kurzynski, Edward Puchala,
Michal Wozniak, Andrzej Zolnierek (Eds.)
Computer Recognition Systems 2, 2007
ISBN 978-3-540-75174-8

Van-Nam Huynh, Yoshiteru Nakamori,
Hiroakira Ono, Jonathan Lawry,
Vladik Kreinovich, Hung T. Nguyen (Eds.)
Interval / Probabilistic Uncertainty and Non-classical Logics, 2008
ISBN 978-3-540-77663-5

Ewa Pietka, Jacek Kawa (Eds.)
Information Technologies in Biomedicine, 2008
ISBN 978-3-540-68167-0

Didier Dubois, M. Asunción Lubiano,
Henri Prade, María Ángeles Gil,
Przemysław Grzegorzewski,
Olgierd Hryniewicz (Eds.)
Soft Methods for Handling Variability and Imprecision, 2008
ISBN 978-3-540-85026-7

Juan M. Corchado, Francisco de Paz,
Miguel P. Rocha,
Florentino Fernández Riverola (Eds.)
2nd International Workshop on Practical Applications of Computational Biology and Bioinformatics (IWPACBB 2008), 2009
ISBN 978-3-540-85860-7

Juan M. Corchado, Sara Rodriguez,
James Llinas, Jose M. Molina (Eds.)
International Symposium on Distributed Computing and Artificial Intelligence 2008 (DCAI 2008), 2009
ISBN 978-3-540-85862-1

Juan M. Corchado, Dante I. Tapia,
José Bravo (Eds.)
3rd Symposium of Ubiquitous Computing and Ambient Intelligence 2008, 2009
ISBN 978-3-540-85866-9

Erel Avineri, Mario Köppen, Keshav Dahal,
Yos Sunitiyoso, Rajkumar Roy (Eds.)
Applications of Soft Computing, 2009
ISBN 978-3-540-88078-3

Emilio Corchado, Rodolfo Zunino,
Paolo Gastaldo, Álvaro Herrero (Eds.)
Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS 2008, 2009
ISBN 978-3-540-88180-3

Emilio Corchado, Rodolfo Zunino,
Paolo Gastaldo, Álvaro Herrero (Eds.)

Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems CISIS 2008

Springer

Editors

Prof. Dr. Emilio S. Corchado
Área de Lenguajes y Sistemas
Informáticos
Departamento de Ingeniería Civil
Escuela Politécnica Superior
Universidad de Bugos
Campus Vena C/ Francisco de Vitoria s/n
E-09006 Burgos
Spain
E-mail: escorchado@ubu.es

Prof. Rodolfo Zunino
DIBE–Department of Biophysical and
Electronic Engineering
University of Genova
Via Opera Pia 11A
16145 Genova
Italy
E-mail: rodolfo.zunino@unige.it

Paolo Gastaldo
DIBE–Department of Biophysical and
Electronic Engineering
University of Genova
Via Opera Pia 11A
16145 Genova
Italy
E-mail: paolo.gastaldo@unige.it

Álvaro Herrero
Área de Lenguajes y Sistemas
Informáticos
Departamento de Ingeniería Civil
Escuela Politécnica Superior
Universidad de Bugos
Campus Vena C/ Francisco de Vitoria s/n
E-09006 Burgos
Spain
E-mail: ahcosio@ubu.es

ISBN 978-3-540-88180-3 e-ISBN 978-3-540-88181-0

DOI 10.1007/978-3-540-88181-0

Advances in Soft Computing ISSN 1615-3871

Library of Congress Control Number: 2008935893

Typeset & Cover Design: Scientific Publishing Services Pvt. Ltd., Chennai, India.

Printed in acid-free paper

5 4 3 2 1 0

springer.com

Preface

The research scenario in advanced systems for protecting critical infrastructures and for deeply networked information tools highlights a growing link between security issues and the need for intelligent processing abilities in the area of information systems. To face the ever-evolving nature of cyber-threats, monitoring systems must have adaptive capabilities for continuous adjustment and timely, effective response to modifications in the environment. Moreover, the risks of improper access pose the need for advanced identification methods, including protocols to enforce computer-security policies and biometry-related technologies for physical authentication. Computational Intelligence methods offer a wide variety of approaches that can be fruitful in those areas, and can play a crucial role in the adaptive process by their ability to learn empirically and adapt a system's behaviour accordingly.

The International Workshop on Computational Intelligence for Security in Information Systems (CISIS) proposes a meeting ground to the various communities involved in building intelligent systems for security, namely: information security, data mining, adaptive learning methods and soft computing among others. The main goal is to allow experts and researchers to assess the benefits of learning methods in the data-mining area for information-security applications. The Workshop offers the opportunity to interact with the leading industries actively involved in the critical area of security, and have a picture of the current solutions adopted in practical domains.

This volume of Advances in Soft Computing contains accepted papers presented at CISIS'08, which was held in Genova, Italy, on October 23rd–24th, 2008. The selection process to set up the Workshop program yielded a collection of about 40 papers. This allowed the Scientific Committee to verify the vital and crucial nature of the topics involved in the event, and resulted in an acceptance rate of about 60% of the originally submitted manuscripts.

CISIS'08 has teamed up with the Journal of Information Assurance and Security (JIAS) and the International Journal of Computational Intelligence Research (IJCIR) for a suite of special issues including selected papers from CISIS'08. The extended papers, together with contributed articles received in response to subsequent open calls, will go through further rounds of peer refereeing in the remits of these two journals.

We would like to thank the work of the Programme Committee Members who performed admirably under tight deadline pressures. Our warmest and special thanks go to the Keynote Speakers: Dr. Piero P. Bonissone (Coolidge Fellow, General Electric Global Research) and Prof. Marios M. Polycarpou (University of Cyprus). Prof. Vincenzo Piuri, former President of the IEEE Computational Intelligence Society, provided invaluable assistance and guidance in enhancing the scientific level of the event.

Particular thanks go to the Organising Committee, chaired by Dr. Clotilde Canepa Fertini (IIC) and composed by Dr. Sergio Decherchi, Dr. Davide Leoncini, Dr. Francesco Picasso and Dr. Judith Redi, for their precious work and for their suggestions about organisation and promotion of CISIS'08. Particular thanks go as well to the Workshop main Sponsors, Ansaldo Segnalamento Ferroviario Spa and Elsag Datamat Spa, who jointly contributed in an active and constructive manner to the success of this initiative.

We wish to thank Prof. Dr. Janusz Kacprzyk (Editor-in-chief), Dr. Thomas Ditzinger (Senior Editor, Engineering/Applied Sciences) and Mrs. Heather King at Springer-Verlag for their help and collaboration in this demanding scientific publication project.

We thank as well all the authors and participants for their great contributions that made this conference possible and all the hard work worthwhile.

October 2008

Emilio Corchado
Rodolfo Zunino
Paolo Gastaldo
Álvaro Herrero

Organization

Honorary Chairs

Gaetano Bignardi – Rector, University of Genova (Italy)
Giovanni Bocchetti – Ansaldo STS (Italy)
Michele Fracchiolla – Elsag Datamat (Italy)
Vincenzo Piuri – President, IEEE Computational Intelligence Society
Gianni Vernazza – Dean, Faculty of Engineering, University of Genova (Italy)

General Chairs

Emilio Corchado – University of Burgos (Spain)
Rodolfo Zunino – University of Genova (Italy)

Program Committee

Cesare Alippi – Politecnico di Milano (Italy)
Davide Anguita – University of Genoa (Italy)
Enrico Appiani – Elsag Datamat (Italy)
Alessandro Armando – University of Genova (Italy)
Piero Bonissone – GE Global Research (USA)
Juan Manuel Corchado – University of Salamanca (Spain)
Rafael Corchuelo – University of Sevilla (Spain)
Andre CPLF de Carvalho – University of São Paulo (Brazil)
Keshav Dehal – University of Bradford (UK)
José Dorronsoro – Autonomous University of Madrid (Spain)
Bianca Falcidieno – CNR (Italy)
Dario Forte – University of Milano Crema (Italy)
Bogdan Gabrys – Bournemouth University (UK)
Manuel Graña – University of Pais Vasco (Spain)
Petro Gopych – V.N. Karazin Kharkiv National University (Ukraine)
Francisco Herrera – University of Granada (Spain)
R.J. Howlett – University of Brighton (UK)
Giacomo Indiveri – ETH Zurich (Switzerland)
Lakhmi Jain – University of South Australia (Australia)
Janusz Kacprzyk – Polish Academy of Sciences (Poland)

Juha Karhunen – Helsinki University of Technology (Finland)
Antonio Lioy – Politecnico di Torino (Italy)
Wenjian Luo – University of Science and Technology of China (China)
Nadia Mazzino – Ansaldo STS (Italy)
José Francisco Martínez – INAOE (Mexico)
Ermete Meda – Ansaldo STS (Italy)
Evangelia Tzanakou – Rutgers University (USA)
José Mira – UNED (Spain)
José Manuel Molina – University Carlos III of Madrid (Spain)
Witold Pedrycz – University of Alberta (Canada)
Dennis K Nilsson – Chalmers University of Technology (Sweden)
Tomas Olovsson – Chalmers University of Technology (Sweden)
Carlos Pereira – Universidade de Coimbra (Portugal)
Kostas Plataniotis – University of Toronto (Canada)
Fernando Podio – NIST (USA)
Marios Polycarpou – University of Cyprus (Cyprus)
Jorge Posada – VICOMTech (Spain)
Perfecto Reguera – University of Leon (Spain)
Bernardete Ribeiro – University of Coimbra (Portugal)
Sandro Ridella – University of Genova (Italy)
Ramón Rizo – University of Alicante (Spain)
Dymirt Ruta – British Telecom (UK)
Fabio Scotti – University of Milan (Italy)
Kate Smith-Miles – Deakin University (Australia)
Sorin Stratulat – University Paul Verlaine – Metz (France)
Carmela Troncoso – Katholieke Univ. Leuven (Belgium)
Tzai-Der Wang – Cheng Shiu University (Taiwan)
Lei Xu – Chinese University of Hong Kong (Hong Kong)
Xin Yao – University of Birmingham (UK)
Hujun Yin – University of Manchester (UK)
Alessandro Zanasi – TEMIS (France)
David Zhang – Hong Kong Polytechnic University (Hong Kong)

Local Arrangements

Bruno Baruque – University of Burgos
Andrés Bustillo – University of Burgos
Clotilde Canepa Fertini – International Institute of Communications, Genova
Leticia Curiel – University of Burgos
Sergio Decherchi – University of Genova
Paolo Gastaldo – University of Genova
Álvaro Herrero – University of Burgos
Francesco Picasso – University of Genova
Judith Redi – University of Genova

Contents

Computational Intelligence Methods for Fighting Crime

Text Mining and Intelligence

Critical Infrastructure Protection

Network Security

Biometry

Information Protection

Industrial Perspectives

An Artificial Neural Network for Bank Robbery Risk Management: The OS.SI.F Web On-Line Tool of the ABI Anti-crime Department

Carlo Guazzoni and Gaetano Bruno Ronsivalle*

OS.SI.F - Centro di Ricerca dell'ABI per la sicurezza Anticrimine
Piazza del Gesù 49 – 00186 Roma, Italy
spsricercasviluppo@abiformazione.it, gabrons@gabrons.com

Abstract. The ABI (Associazione Bancaria Italiana) Anti-crime Department, OS.SI.F (Centro di Ricerca dell'ABI per la sicurezza Anticrimine) and the banking working group created an artificial neural network (ANN) for the Robbery Risk Management in Italian banking sector. The logic analysis model is based on the global Robbery Risk index of the single banking branch. The global index is composed by: the Exogenous Risk, related to the geographic area of the branch, and the Endogenous risk, connected to its specific variables. The implementation of a neural network for Robbery Risk management provides 5 advantages: (a) it represents, in a coherent way, the complexity of the "robbery" event; (b) the database that supports the AN is an exhaustive historical representation of Italian Robbery phenomenology; (c) the model represents the state of art of Risk Management; (d) the ANN guarantees the maximum level of flexibility, dynamism and adaptability; (e) it allows an effective integration between a solid calculation model and the common sense of the safety/security manager of the bank.

Keywords: Risk Management, Robbery Risk, Artificial Neural Network, Quickprop, Logistic Activation Function, Banking Application, ABI, OS.SI.F., Anti-crime.

1 Toward an Integrated Vision of the "Risk Robbery"

In the first pages of The Risk Management Standard[1] - published by IRM[2], AIRMIC[3] and ALARM[4] - the "risk" is defined as «the combination of the probability of an event and its consequences». Although simple and linear, this definition has many implications from a theoretical and pragmatic point of view. Any type of risk analysis shouldn't be limited to an evaluation of a specific event's probability without considering the effects, presumably negative, of the event. The correlation of these two concepts is not banal but, unfortunately, most Risk Management Models currently in use

[*] Thanks to Marco Iaconis, Francesco Protani, Fabrizio Capobianco, Giorgio Corito, Riccardo Campisi, Luigi Rossi and Diego Ronsivalle for the scientific and operating support in the development of the theoretical model, and to Antonella De Luca for the translation of the paper.

[1] http://www.theirm.org/publications/PUstandard.html

[2] The Institute of Risk Management.

[3] The Association of Insurance and Risk Managers.

[4] The National Forum for Risk Management in the Public Sector.

E. Corchado et al. (Eds.): CISIS 2008, ASC 53, pp. 1–10, 2009.
springerlink.com

for banking security are characterized by low attention to these factors. In fact, they are often focused on the definition of methods and tools to foresee the “harmful event”' in probabilistic terms, without pay attention to the importance of a composed index considering the intensity levels of events that causally derive from this “harmful event”'. But then the little book of the above mentioned English Institutes, embraces an integrated vision of the Risk Management. It is related to a systemic and strategic meaning, giving a coherent description of data and defining the properties of the examined phenomenon. This wide vision provides explanatory hypothesis and, given a series of historical conditions, may foresee the probable evolutions of the system. Thanks to the joint effort of the inter-banking working group - coordinated by ABI and OS.SI.F -, the new support tool for the Robbery Risk Management takes into account this integrated idea of “risk”. In fact it represents the Risk Management process considering the strategic and organizational factors that characterize the phenomenon of robbery. Hence, it defines the role of the safety/security manager in the banking sector. The online software tool, indeed, integrates a general plan with a series of resources to attend the manager during the various phases of the decisional process scheduled by the standard IRM:

1. from the Robbery Risk mapping - articulated in analysis, various activities of identification, description and appraisal - to the risk evaluation;
2. from the Risk Reporting to the definition of threats and opportunities connected to the robbery;
3. from the decisional moment, supported by the simulation module (where we can virtually test the Risk Management and analyze the Residual Risk) to the phase of virtual and real monitoring[5].

The various functions are included in a multi-layers software architecture, composed by a database and a series of modules that elaborate the information to support the analysis of the risk and its components. In this way, the user can always retrace the various steps that gradually determine the Robbery Risk Global Index and its single relative importance, starting from the primary components of the risk, he/she can focus the attention on the minimum element of the organizational dimension. Thus, the analysis is focused on the complex relationship between the single banking branch - that represents the system cell and unity of measurement - and the structure of relationships, connections, relevant factors from a local and national point of view. In this theoretical frame, the Robbery Risk is not completely identified with the mere probability that the event occurs. According with IRM standard, instead, it is also taken into account the possibility that the robbery may cause harms, as well as the combined probability that the event occurs and the possible negative consequences for the system may have a different intensity.

2 Exogenous Risk and Endogenous Risk

According to the inter-banking working group, coordinated by OS.SI.F, which are the factors or the variables that compose and influence the robbery and its harmful effects?

[5] ``The Risk Management Standard", pp. 6-13.

2.1 The Exogenous Risk

The “Exogenous”' components include environment variables (from regional data to local detailed data), tied to the particular geographic position, population density, crime rate, number of general criminal actions in the area, as well as the “history”' and/or evolution of the relationship between the number of banking branches, the defense implementations and the Robbery Risk. So the mathematical function, that integrates these factors, must take into account the time variable. In fact it's essential to consider the influence of each variable according to the changes that occur at any time in a certain geographic zone.

The analysis made up by the working group of ABI has shown that the composition of environment conditions is represented by a specific index of “Exogenous risk”. Its dynamic nature makes possible to define a probabilistic frame for in order to calculate the Robbery Risk. Such index of “Exogenous” risk allows considering the possibility of a dynamic computation regarding the variation rate of criminal actions density. This variation depends on the direct or indirect intervention of police or central/local administrations in a geographic area. The Exogenous risk could provide some relevant empirical bases in order to allow banks to share common strategies for the management/mitigation of the Robbery Risk. The aim is to avoid possible negative effects tied to activities connected to only one banking branch.

2.2 The Endogenous Risk

A second class of components corresponds, instead, to material, organizational, logistic, instrumental, and technological factors. They characterize the single banking branch and determine its specific architecture in relation to the robbery. Such factors are the following:

1. the “basic characteristics”'[6]
2. the “services”'[7]
3. the “plants”'[8]

The interaction of these factors contributes to determine a significant part of the so-called “Endogenous” risk. It is calculated through a complex function of the number of robberies on a single branch, calculated during a unit of time in which any “event” has modified, in meaningful terms, the internal order of the branch. In other terms, a dynamic connection between the risk index and the various interventions planned by the safety/security managers has been created, both for the single cell and for whole system. The aim was to control the causal sequence between the possible variation of an Endogenous characteristic and its relative importance (%) to calculate the specific impact on the number of robberies.

2.3 The Global Risk

Complying with the objectives of an exhaustive Robbery Risk management, the composition of the two risk indexes (Exogenous and Endogenous) defines the perimeter

[6] E.g. the number of employees, the location, the cash risk, the target-hardening strategies, etc.

[7] E.g. the bank security guards, the bank surveillance cameras, etc.

[8] E.g. the access control vestibules (man-catcher or mantraps), the bandit barriers, broad-band internet video feeds directly to police, the alarms, etc.

of a hypothetical “global” risk referred to the single branch. A sort of integrated index that includes both environment and “internal” factors. Thus the calculation of the Global Risk index derives from the normalization of the bi-dimensional vector obtained from the above mentioned functions.

Let us propose a calculation model in order to support the definition of the various indexes.

3 Methodological Considerations about the Definition of “Robbery Risk”

Before dealing with the computation techniques, however, it is necessary to clarify some issue.

3.1 Possible Extend of “Robbery Risk”

First of all, the demarcation between the “Exogenous” and “Endogenous” dimensions cannot be considered absolute. In fact, in some specific case of “Endogenous” characteristics, an analysis that considers only factors that describe the branch isn't enough representative of the variables combination. In fact, the ponderation of each single element makes possible to assign a “weight” related to the Endogenous risk index. But it must be absolutely taken into account the variability rate of influence according to the geographic area. This produces an inevitable contamination, even though circumscribed, between the two dimensions of the Robbery Risk. Then, it must be taken into account that these particular elements of the single cell are the result of the permanent activity of comparison made by the inter-banking working group members coordinated by ABI and OS.SI.F.

Given the extremely delicate nature of the theme, the architecture of the “Endogenous” characteristics of the branch must be considered temporary and in continuous evolution. The “not final” nature of the scheme that we propose, depends therefore, by the progressive transformation of the technological tools supporting security, as well as by the slow change - both in terms of national legislation, and in terms of reorganization of the safety/security manager role - regarding the ways in which the contents of Robbery Risk are interpreted.

Finally it's not excluded, in the future, the possibility to open the theoretical scheme to criminological models tied to the description of the criminal behaviour and to the definition of indexes of risk perception. But, in both cases the problem is to find a shared theoretical basis, and to translate the intangible factors in quantitative variables that can be elaborated through the calculation model[9].

3.2 The Robbery Risk from an Evolutionistic Point of View

Most bank models consider the Robbery Risk index of a branch, as a linear index depending on the number of attempted and/or consumed robbery in a certain time interval.

[9] On this topic, some researches are going on with the aim to define a possible evolution of this particular type of ``socio-psychological" index of perceived risk. But it's not yet clear if and how this index can be considered as a category of risk distinguished both from the ``exogenous" and ``endogenous" risk.

This index is usually translated into a value, with reference to a risk scale, and it is the criterion according to which for the Security Manager decide.

These models may receive a series of criticisms:

1. they extremely simplify the relation between variables, not considering the reciprocal influences between Exogenous and Endogenous risk;
2. they represent the history of a branch inaccurately, with reference to very wide temporal criteria;
3. they don't foresee a monitoring system of historical evolution related to the link between changes of the branch and number of robberies.

To avoid these criticisms, the OS.SI.F team has developed a theoretical framework based on the following methodological principles:

1. the Robbery Global Risk is a probability index (it varies from 0 to 1) and it depends on the non-linear combination of Exogenous and Endogenous risk;
2. the Robbery Global Risk of a branch corresponds to the trend calculated by applying the Least Squares formula to the numerical set of Risk Robbery values (monthly) from January 2000 to March 2008 in the branch;
3. the monthly value of the Robbery Global Risk corresponds to the relation between the number of robberies per month and the number of days in which the branch is open to people. It is expressed in a value from 0 to 1.

An consequence follows these principles: it is necessary to describe the history of the branch as a sequence of states of the branch itself, in relation to changes occurred in its internal structure (for example, the introduction of a new defending service or a new plant). Thus it is possible to create a direct relation between the evolution of branch and the evolution of Robbery Global Risk. In particular, we interpret the various transformations of the branch over time as "mutations" in a population of biological organisms (represented by isomorphic branches).

The Robbery Global Risk, thus, becomes a kind of value suggesting how the "robbery market" rewards the activities of the security managers, even though without awareness about the intentional nature of certain choices[10].

This logical ploy foresees the possibility to analyze indirect strategies of the various banking groups in the management and distribution of risk into different regions of the country[11]. This methodological framework constitutes the logical basis for the construction of the Robbery Risk management simulator. It is a direct answer to criticisms of the 2nd and 3rd points (see above). It allows the calculation of the fluctuations referred to the Exogenous risk in relation to the increase - over certain thresholds - of the Robbery Global Risk (criticism of the 1st point).

[10] This "biological metaphor", inspired by Darwin's theory, is the methodological basis to overcome a wrong conception of the term "deterrent" inside the security managers' vocabulary. In many cases, the introduction of new safety services constitutes only an indirect deterrent, since the potential robber cannot know the change. The analysis per populations of branches allows, instead, to extend the concept of "deterrent" per large numbers.

[11] While analyzing data, we discovered a number of "perverse effects" in the Robbery Risk management, including the transfer of risk to branches of other competing groups as a result of corrective actions conceived for a branch and then extended to all branches in the same location.

4 The Calculation Model for the Simulator

The choice of a good calculation model as a support tool for the risk management is essentially conditioned from the following elements:

1. the nature of the phenomenon;
2. the availability of information and historical data on the phenomenon;
3. the quality of the available information;
4. the presence of a scientific literature and/or of possible applications on
5. the theme;
6. the type of tool and the output required;
7. the perception and the general consent level related to the specific model
8. adopted;
9. the degree of obsolescence of the results;
10. the impact of the results in social, economic, and political, terms.

In the specific case of the Robbery Risk,

1. the extreme complexity of the "robbery" phenomenon suggests the adoption of analysis tools that take into account the various components, according to a non linear logic;
2. there is a big database on the phenomenon: it can represent the pillar for a historical analysis and a research of regularity, correlations and possible nomic and/or probabilistic connections among the factors that determine the "robbery" risk;
3. the actual database has recently been "normalized", with the aim to guarantee the maximum degree of coherence between the information included in the archive and the real state of the system;
4. the scientific literature on the risk analysis models related to criminal events is limited to a mere qualitative analysis of the phenomenon, without consider quantitative models;
5. the inter-banking group has expressed the need of a tool to support the decisional processes in order to manage the Robbery Risk, through a decomposition of the fundamental elements that influence the event at an Exogenous and Endogenous level;
6. the banking world aims to have innovative tools founds and sophisticated calculation models in order to guarantee objective and scientifically founded results within the Risk Management domain;
7. given the nature of the phenomenon, the calculation model of the Robbery Risk must guarantee the maximum of flexibility and dynamism according to the time variable and the possible transformations at a local and national level;
8. the object of the analysis is matched with a series of ethics, politics, social, and economic topics, and requires, indeed, an integrated systemic approach.

These considerations have brought the team to pursue an innovative way for the creation of the calculation model related to the Robbery Risk indexes: the artificial neural networks (ANN).

5 Phases of ANN Design and Development for the Management of the Robbery Risk

How did we come to the creation of the neural network for the management of the robbery Global Risk? The creation of the calculation model is based on the logical scheme above exposed. It is articulated in five fundamental phases:

1. Re-design OS.SI.F database and data analysis;
2. Data normalization;
3. OS.SI.F Network Design;
4. OS.SI.F Network Training;
5. Network testing and delivery.

5.1 First Phase: Re-design OS.SI.F Database and Data Analysis

Once defined the demarcation between Exogenous and Endogenous risks, as well as the structure of variables concerning each single component of the Global Risk, some characteristic elements of OS.SI.F historical archive have been revised. The revision of the database allowed us to remove possible macroscopic redundancies and occasional critical factors, before starting the data analysis. Through a neural network based on genetic algorithms all possible incoherence and contradictions have been underlined. The aim was to isolate patterns that would have been potentially “dangerous” for the network and to produce a “clean” database, deprived of logical “impurities” (in limits of human reason).

At this point, the team has defined the number of entry variables (ANN inputs) - related to the characteristics above mentioned - and the exit variables (ANN output) representing the criteria for design the network. The structure of the dataset is determined, as well as the single field types (categorical or numerical) and the distinction among (a) information for the training of the ANN, (b) data to validate the neuronal architecture, and (c) dataset dedicated to testing the ANN after training.

5.2 Second Phase: Data Normalization

The database cleaning allowed the translation of data in a new archive of information for the elaboration of an ANN. In other words, all the variables connected to the Exogenous risk (environment and geographic variables) and the Endogenous risk (basic characteristics, services and plants of each single branch) have been “re-write” and normalized. All this has produced the historical sequence of examples provided to the ANN with the aim to let it “discover” the general rules that govern the “robbery” phenomenon. The real formal “vocabulary” for the calculation of the Global Risk.

5.3 Third Phase: OS.SI.F Network Design

This phase has been dedicated to determine the general architecture of the ANN and its mathematical properties. Concerning topology, in particular, after a series of unlucky attempts with a single hidden layer, we opted for a two hidden layers network:

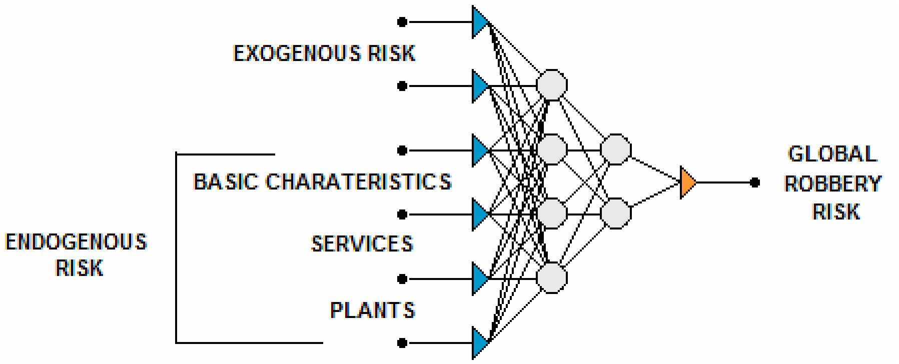

Fig. 1. A schematic representation of the Architecture of OS.SI.F ANN

This architecture was, in fact, more appropriate to solve a series of problems connected to the particular nature of the "robbery" phenomenon. This allowed us, therefore, to optimize the choice of the single neurons activation function and the error function.

In fact, after a first disastrous implementation of the linear option, a logistic activation function with a sigmoid curve has been adopted. It was characterized by a size domain included between 0 and 1 and calculated through the following formula:

$$F(x) = \frac{1}{1+e^{-x}} \tag{1}$$

Since it was useful for the evaluation of the ANN quality, an error function has been associated to logistic function. It was based on the analysis of differences among the output of the historical archive and the output produced by the neural network. In this way we reached to the definition of the logical calculation model. Even though it still doesn't have the knowledge necessary to describe, explain, and foresee the probability of the "robbery" event. This knowledge, in fact, derives only from an intense training activity.

5.4 Fourth Phase: OS.SI.F Network Training

The ANN training constitutes the most delicate moment of the whole process of creation of the network. In particular with a Supervised Learning. In our case, in fact, the training consists in provide the network of a big series of examples of robberies associated to particular geographic areas and specific characteristics of the branches. From this data, the network has to infer the rule through an abstraction process. For the Robbery Risk ANN, we decided to implement a variation of the Back propagation. The Back propagation is the most common learning algorithm within the multi-layer networks. It is based on the error propagation and on the transformation of weights (originally random assigned) from the output layer in direction to the intermediate layers, up to the input neurons. In our special version, the "OS.SI.F Quick-propagation", the variation of each weight of the synaptic connections changes according to the following formula:

$$\Delta w(t) = \left(\frac{s(t)}{s(t-1) - s(t)} \Delta w(t-1) \right) + k \tag{2}$$

where **k** is a hidden variable to solve the numerical instability of this formula[12].

We can state that the fitness of the ANN-Robbery Risk has been subordinated to a substantial correspondence between the values of Endogenous and Exogenous risk (included in the historical archive), and the results of the network's elaboration after each learning iteration.

5.5 Fifth Phase: Network Testing and Delivery

In the final phase of the process lot of time has been dedicated to verify the neural network architecture defined in the previous phases. Moreover a series of dataset previously not included in the training, have been considered with the aim to remove the last calculation errors and put some adjustments to the general system of weights. In this phase, some critical knots have been modified: they were related to the variations of the Exogenous risk according to the population density and to the relationship between Endogenous risk and some new plants (biometrical devices). Only after this last testing activity, the ANN has been integrated and implemented in the OS.SI.FWeb module, to allow users (banking security/safety managers), to verify the coherence of the tool through a module of simulation of new sceneries.

6 Advantages of the Application of the Neural Networks to the Robbery Risk Management

The implementation of an ANN to support the Robbery Risk management has at least 5 fundamental advantages:

1. Unlike any linear system based on proportions and simple systems of equations, an ANN allows to face, in coherent way, the high complexity degree of the "robbery" phenomenon. The banal logic of the sum of variables and causal connections of many common models, is replaced by a more articulated design, that contemplates in dynamic and flexible terms, the innumerable connections among the Exogenous and Endogenous variables.
2. The OS.SI.F ANN database is based on a historical archive continually fed by the whole Italian banking system. This allows to overcome each limited local vision, according to the absolute need of a systemic approach for the Robbery Risk analysis. In fact, it's not possible to continue to face such a delicate topic through visions circumscribed to one's business dimension.
3. The integration of neural algorithms constitutes the state of the art within the Risk Management domain. In fact it guarantees the definition of a net of variables opportunely measured according to a probabilistic - and not banally linear - logic.

[12] Moreover, during the training, a quantity of "noise" has been introduced (injected) into the calculation process. The value of the "noise" has been calculated in relation to the error function and has allowed to avoid the permanence of the net in critical situations of local minims.

The Robbery Risk ANN foresees a real Bayes network that dynamically determines the weight of each variable (Exogenous and Endogenous) in the probability of the robbery. This provides a higher degree of accuracy and scientific reliability to the definition of "risk" and to the whole calculation model.

4. A tool based on neural networks guarantees the maximum level of flexibility, dynamism and adaptability to contexts and conditions that are in rapid evolution. These are assured by (a) a direct connection of the database to the synaptic weights of the ANN, (b) the possible reconfiguration of the network architecture in cases of introduction of new types of plants and/or services, and/or basic characteristics of branches.
5. The ANN allows an effective integration between a solid calculation model (the historical archive of information related to the robberies of last years), and the professional and human experience of security/safety managers. The general plan of the database (and of the composition of the two risk indexes), takes into account the considerations, observations and indications of the greater representatives of the national banking safety/security sectors. The general plan of the database is based on the synthesis done by the inter-banking team, on the normalization of the robbery event descriptions, and on the sharing of some guidelines in relation to a common vocabulary for the description of the robbery event. The final result of this integration is a tool that guarantees the maximum level of decisional liberty, through the scientific validation of virtuous practices and, thanks to the simulator of new branches, an a priori evaluation of the possible effects deriving from future interventions.

References

1. Corradini, I., Iaconis, M.: Antirapina. Guida alla sicurezza per gli operatori di sportello. Bancaria Editrice, Roma (2007)
2. Fahlman, S.E.: Fast-Learning Variations on Back-Propagation: An Empirical Study. In: Proceedings of the 1988 Connessionist Models Summer School, pp. 38–51. Morgan Kaufmann, San Francisco (1989)
3. Floreano, D.: Manuale sulle reti neurali. Il Mulino, Bologna (1996)
4. McClelland, J.L., Rumelhart, D.E.: PDP: Parallel Distributed Processing: Explorations in the Microstructure of Cognition: Psychological and Biological Models, vol. II. MIT Press-Bradford Books, Cambridge (1986)
5. Pessa, E.: Statistica con le reti neurali. Un'introduzione. Di Renzo Editore, Roma (2004)
6. Sietsma, J., Dow, R.J.F.: Neural Net Pruning – Why and how. In: Proceedings of the IEEE International Conference on Neural Networks, pp. 325–333. IEEE Press, New York (1988)
7. von Lehman, A., Paek, G.E., Liao, P.F., Marrakchi, A., Patel, J.S.: Factors Influencing Learning by Back-propagation. In: Proceedings of the IEEE International Conference on Neural Networks, vol. I, pp. 335–341. IEEE Press, New York (1988)
8. Weisel, D.L.: Bank Robbery. In: COPS, Community Oriented Policing Services, U.S. Department of Justice, No.48, Washington (2007), http://www.cops.usdoj.gov

Secure Judicial Communication Exchange Using Soft-computing Methods and Biometric Authentication

Mauro Cislaghi[1], George Eleftherakis[2], Roberto Mazzilli[1], Francois Mohier[3], Sara Ferri[4], Valerio Giuffrida[5], and Elisa Negroni[6]

[1] Project Automation , Viale Elvezia, Monza, Italy
{mauro.cislaghi,roberto.mazzilli}@p-a.it
[2] SEERC, 17 Mitropoleos Str, Thessaloniki, Greece
eleftherakis@city.academic.gr
[3] Airial Conseil, RueBellini 3, Paris, France
francois.mohier@airial.com
[4] AMTEC S.p.A., Loc. San Martino, Piancastagnaio, Italy
sara.ferri@elsagdatamat.com
[5] Italdata, Via Eroi di Cefalonia 153, Roma, Italy
valerio.giuffrida@italdata-roma.com
[6] Gov3 Ltd, UK
j-web.project@gov3innovation.eu

Abstract. This paper describes how "Computer supported cooperative work", coped with security technologies and advanced knowledge management techniques, can support the penal judicial activities, in particular national and trans-national investigations phases when different judicial system have to cooperate together. Increase of illegal immigration, trafficking of drugs, weapons and human beings, and the advent of terrorism, made necessary a stronger judicial collaboration between States. J-WeB project (http://www.jweb-net.com/), financially supported by the European Union under the FP6 – Information Society Technologies Programme, is designing and developing an innovative judicial cooperation environment capable to enable an effective judicial cooperation during cross-border criminal investigations carried out between EU and Countries of enlarging Europe, having the Italian and Montenegrin Ministries of Justice as partners. In order to reach a higher security level, an additional biometric identification system is integrated in the security environment.

Keywords: Critical Infrastructure Protection, Security, Collaboration, Cross border investigations, Cross Border Interoperability, Biometrics, Identity and Access Management.

1 Introduction

Justice is a key success factors in regional development, in particular in areas whose development is lagging back the average development of the European Union. In the last years particular attention has been paid on judicial collaboration between Western Balkans and the rest of EU, and CARDS Program [1] is a suitable evidence of this cooperation. According to this program, funds were provided for the development of closer relations and regional cooperation among SAp (Stabilisation and Association

E. Corchado et al. (Eds.): CISIS 2008, ASC 53, pp. 11–18, 2009.
springerlink.com

process) countries and between them and all the EU member states to promote direct cooperation in tackling the common threats of organised crime, illegal migration and other forms of trafficking. The Mutual assistance [2] is subject to different agreements and different judicial procedures.

JWeB project [3], [9], based on the experiences of e-Court [4] and SecurE-Justice [5] projects, funded by the European Commission in IST program, is developing an innovative judicial cooperation environment capable to enable an effective judicial cooperation during cross-border criminal investigations, having the Italian and Montenegrin Ministries of Justice as partners.

JWeB (started in 2007 and ending in 2009) will experiment a cross-border secure cooperative judicial workspace (SCJW), distributed on different ICT platforms called Judicial Collaboration Platforms (JCP) [6], based on Web-based groupware tools supporting collaboration and knowledge sharing among geographically distributed workforces, within and between judicial organizations.

2 Investigation Phase and Cross-Border Judicial Cooperation

The investigation phase includes all the activities carried out from crime notification to the trial. Cross-border judicial cooperation is one of them. It may vary from simple to complex judicial actions; but it has complex procedure and requirements, such as information security and non repudiation. A single investigation may include multiple cross-border judicial cooperation requests; this is quite usual when investigating on financial flows. Judicial cooperation develops as follows:

1) In the requesting country, the magistrate starts preliminary checks to understand if her/his requests to another country are likely to produce the expected results. Liaison magistrate support and contacts with magistrates in the other country are typical actions.
2) The “requesting” magistrate prepares and sends the judicial cooperation request (often referred to as “letter of rogatory”) containing the list of specific requests to the other country. Often the flow in the requesting country is named “active rogatory”, while the flow in the requested country is named “passive rogatory”.
3) The judicial cooperation request coming from the other country is evaluated, usually by a court of appeal that, in case of positive evaluation, appoints the prosecutors’ office in charge of the requested activities. This prosecutors’ office appoints a magistrate. The requesting magistrate, directly or via the office delegated to international judicial cooperation, receives back these information and judicial cooperation starts.
4) Judicial cooperation actions are performed. They may cover request for documents, request for evidences, request for interrogations, request for specific actions (for example interceptions, sequestration or an arrest), requests for joint investigation.

Most of the activities are still paper based. The listed activities may imply complex actions in the requested country, involving people (magistrates, police, etc.) in different departments. The requesting country is interested on the results of the activities, not on the procedures followed by the judicial organisation fulfils the requests. The liaison magistrate can support the magistrate, helping her/him to understand how to address the judicial counterpart and, once judicial cooperation has been granted, in understanding and overcoming possible obstacles. Each national judicial system is independent from the other, both in legal and infrastructural terms. Judicial cooperation, on the ICT point of view, implies cooperation between two different infrastructures, the "requesting" one ("active") and the "requested" ("passive"), and activities such as judicial cooperation setup, joint activities of the workgroups, secure exchange of not repudiable information between the two countries. These activities can be effectively supported by a secure collaborative workspace, as described in the next paragraph.

3 The Judicial Collaboration Platform (JCP)

A workspace for judicial cooperation involves legal, organisational and technical issues, and requires a wide consensus in judicial organisations. It has to allow straightforward user interface, easy data retrieval, seamless integration with procedures and systems already in place.

All that implemented providing top-level security standards. Accordingly, the main issues for judicial collaboration are:

- A **Judicial Case** is a **secure private virtual workspace** accessed by law enforcement and judicial authorities, that need to collaborate in order to achieve common objectives and tasks;
- **JCP services** are on-line services, supplying various collaborative functionalities to the judicial authorities in a secure and **non repudiable** communication environment;
- **User profile** is a set of access rights assigned to a user. The access to a judicial case and to JCP services are based on predefined, as well as, customised role based user profiles;
- **Mutual assistance** during investigations creates a shared part of investigation folder.
- **Each country will have its own infrastructure.**

The core system supporting judicial cooperation is the secure JCP [6]. It is part of a national ICT judicial infrastructure, within the national judicial space. Different JCPs in different countries may cooperate during judicial cooperation. The platform, organised on three layer (presentation, business, persistence) and supporting availability and data security, provides the following main services:

- **Profiling:** user details, user preferences
- **Web Services**
  - **Collaboration:** collaborative tools so that users can participate and discuss on the judicial cooperation cases.
  - **Data Mining:** customization of user interfaces based on users' profile.
  - **Workflow Management:** design and execution of judicial cooperation processes

  - **Audio/Video Management:** real time audio/video streaming of a multimedia file, videoconference support.
  - **Knowledge Management:** documents uploading, indexing, search.
- **Security and non repudiation:** Biometric access, digital certificates, digital signature, secure communication, cryptography, Role based access control.

Services may be configured according to the different needs of the Judicial systems. The modelling of Workflow Processes is based on the Workflow Management Coalition specifications (WfMC), while software developments are based on Open-Source and the J2EE framework. Communications are based on HTTPS and SSL, SOAP, RMI, LDAP and XML. Videoconference is based on H323.

4 The Cross-Border Judicial Cooperation Via Secure JCPs

4.1 The Judicial Collaborative Workspace and Judicial Cooperation Activities

A secure collaborative judicial workspace (SCJW) is a secure inter-connected environment related to a judicial case, in which all entitled judicial participants in dispersed locations can access and interact with each other just as inside a single entity. The environment is supported by electronic communications and groupware which enable participants to overcome space and time differentials. On the physical point of view, the workspace is supported by the JCP.

The SCJW allows the actors to use communication and scheduling instruments (agenda, shared data, videoconference, digital signature, document exchange) in a secured environment.

A judicial cooperation activity (JCA) is the implementation of a specific judicial cooperation request. It is a self contained activity, opened inside the SCJWs in the requesting and requested countries, supported by specific judicial workflows and by the collaboration tools, having as the objective to fulfil a number of judicial actions issued by the requesting magistrate.

The SCJW is connected one-to-one to a judicial case and may contain multiple JCAs running in parallel. A single JCA ends when rejected or when all requests contained in the letter of rogatory have been fulfilled and the information collected have been inserted into the target investigation folder, external to the JCP. In this moment the JCA may be archived. The SCJW does not end when a JCA terminates, but when the investigation phase is concluded. Each JCA may have dedicated working teams, in particular in case of major investigations. The "owner" of the SCJW is the investigating magistrate in charge of the judicial case.

SCJW is implemented in a single JCP, while the single JCA is distributed on two JCP connected via secure communication channels (crypto-routers, with certificate exchange), implementing a secured Web Service Interface via a collaboration gateway.

Each SCJW has a global repository and a dedicated repository for each JCA. This is due to the following constraints:

1) the security, confidentiality and non repudiation constraints
2) each JCA is an independent entity, accessible only by the authorised members of the judicial workgroup and with a limited time duration.

The repository associated to the single JCA contains:

- **JCA persistence data**
  1) "**JCA metadata**" containing data such as: information coming from the national registry (judicial case protocol numbers, etc.), the users profiles and the related the access rights, the contact information, the information related to the workflows (state, transitions), etc.
  2) "**JCP semantic repository**"**.** It will be the persistence tier for the JCP semantic engine, containing: ontology, entity identifiers, Knowledge Base (KB)
- **JCA judicial information**
  The documentation produced during the judicial cooperation will be stored in a configurable tree folder structure. Typical contents are:
  1) "**JCA judicial cooperation request**"**.** It contains information related to the judicial cooperation request, including further documents exchanged during the set-up activities.
  2) "**JCA decisions**"**.** It contains the outcomes of the formal process of judicial cooperation and any internal decision relevant to the specific JCA (for example letter of appointment of the magistrate(s), judicial acts authorising interceptions or domicile violation, etc.)
  3) "**JCA investigation evidences**"**.** It contains the documents to be sent/ received (Audio/video recordings, from audio/video conferences and phone interceptions, Images, Objects and documents, Supporting documentation, not necessarily to be inserted in the investigation folder)

4.2 The Collaboration Gateway

Every country has it own ICT judicial infrastructure, interfaced but not shared with other countries.

Accordingly a SCJW in a JCP must support a 1:n relationships between judicial systems, including data communication, in particular when the judicial case implies more than one JCA. A single JCA has a 1:1 relationship between the JCA in the requesting country and the corresponding "requested" JCA. For example, a single judicial case in Montenegro may require cross-border judicial cooperation to Italy, Serbia, Switzerland, France and United Kingdom, and the JCP in Montenegro will support n cross border judicial cooperations.

Since JCP platforms are hosted on different locations and countries, the architecture of the collaboration module is based on the mechanism of secured gateway. It is be based on a set of Web Services allowing one JWeB site, based on a JCP, to exchange the needed data with another JWeB site and vice and versa.

The gateway architecture, under development in JWeB project, is composed by:

- **Users and Profiling module**
- **Judicial CASES and Profiling Module**
- **Calendar/Meeting Module**

Workflow engines exchange information about the workflows states through the collaboration gateway.

4.3 Communication Security, User Authentication and RBAC in JCP

Security [7] is managed through the Security Module, designed to properly manage Connectivity Domains, to assure access rights to different entities, protecting information and segmenting IP network in secured domains. Any communication is hidden to third parties, protecting privacy, preventing unauthorised usage and assuring data integrity.

The JCP environment is protected by the VPN system allowing the access only from authenticated and pre-registered user; no access is allowed without the credentials given by the PKI.

User is authenticated in her/his access to any resource by means of his X.509v3 digital certificate issued by the Certification Authority, stored in his smart card and protected by biometry [7], [8].

The Network Security System is designed in order to grant the access to the networks and the resources only to authenticated users; it is composed by the following components:

- Security Access Systems (Crypto-router). Crypto-routers prevent unauthorized intrusions, offers protection against external attacks and offer tunneling capabilities and data encryption.
- Security Network Manager. This is the core of security managing system that allows managing, monitoring and modifying configurations of the system, including accounting of new users.
- S-VPN clients (Secure Virtual Private Network Client). Software through which the users can entry in the IP VPN and so can be authenticated by the Security Access System.

The Crypto-router supports routing and encryption functions with the RSA public key algorithm on standard TCP/IP networks in end to end mode. Inside JCP security architecture Crypto-router main task is to institute the secure tunnel to access JCP VPN (Virtual Private Network) and to provide both Network and Resources Authentication.

In order to reach a higher security level, an additional biometric identification system is integrated in the security environment. The device integrates a smart card reader with a capacitive ST Microelectronics fingerprint scanner and an "Anti Hacking Module" that will made the device unusable in case of any kind of physical intrusion attempt.

The biometric authentication device will entirely manage the biometric verification process. There is no biometric data exchange within the device and the workstation or any other device. Biometric personal data will remain in the user's smart card and the comparison between the live and the smart card stored fingerprint will be performed inside the device.

After biometric authentication, access control of judicial actors to JCP is role-based. In Role Based Access Control [11] (RBAC), permissions are associated with roles, and users are made members of appropriate roles. This model simplifies access administration, management, and audit procedures. The role-permissions relationship changes much less frequently than the role-user relationship, in particular in the judicial field. RBAC allows these two relationships to be managed separately and gives much clearer guidance to system administrators on how to properly add new users and their associated permissions. RBAC is particularly appropriate in justice information sharing systems where there are typically several organizationally diverse user groups that need access, in varying degrees, to enterprise-wide data. Each JCP system will maintain its own Access Control List (ACL). Example of roles related to judicial cooperation are:

- SCJW magistrate supervisor: Basically he/she has the capability to manage all JCAs.
- JCA magistrate: he/she has the capability to handle the cases that are assigned to him
- Liaison Magistrate: a magistrate located in a foreign country that supports the magistrate(s) in case of difficulties.
- Judicial Clerk: supporting the magistrate for secretarial and administrative tasks (limited access to judicial information).
- System Administrator: He is the technical administrator of the JCP platform (no access to judicial information)

5 Conclusions

Council Decision of 12 February 2007 establishes for the period 2007-2013 the Programme ‘Criminal Justice’ (2007/126/JHA), with the objective to foster judicial cooperation in criminal matter. CARDS project [1] and IPA funds represent today a relevant financial support to regional development in Western Balkans, including justice as one of the key factors. This creates a strong EU support to JCP deployment, while case studies such as the ongoing JWeB and SIDIP [10] projects, demonstrated that electronic case management is now ready for deployment on the technological point of view.

Judicial secure collaboration environment will be the basis for the future judicial trans-national cooperation, and systems such as the JCP may lead to a considerable enhancement of cross-border judicial cooperation. The experience in progress in JWeB project is demonstrating that features such as security, non repudiation, strong authentication can be obtained through integration of state of the art technologies and can be coped with collaboration tools, in order to support a more effective and straightforward cooperation between investigating magistrates in full compliance with national judicial procedures and practices. The JCP platform represents a possible bridge between national judicial spaces, allowing through secure web services the usage of the Web as a cost effective and the same time secured interconnection between judicial systems.

While technologies are mature and ready to be used, their impact on the judicial organisations in cross-border cooperation is still under analysis. It is one of the main non technological challenges for deployment of solutions such as the one under development in JWeB project. The analysis conducted so far in the JWeB project gives a reasonable confidence that needed organisational changes will become evident through the pilot usage of the developed ICT solutions, so giving further contributions to the Ministries of Justice about the activities needed for a future deployment of ICT solutions in a delicate area such as the one of the international judicial cooperation.