3

Neural and Bayesian Networks to Fight Crime: the NBNC Meta-Model of Risk Analysis

Gaetano Bruno Ronsivalle
"Sapienza" University of Rome
Italy

1. Introduction

According to a recent study quoted by the Union National Observatory, in 2009 about 50% of European bank robberies took place in Italy. Beyond the reliability of this percentage value, such datum highlights one of the most complex problems security bank officers have to face in order to make all national branches more secure.
Since 2009 ABI (Italian Banking Association) has been trying to solve such problem by using a software to analyze the bank robbery risk. The software is based on a model involving the analysis, description, explanation and estimation of the phenomenon. The last version of the tool, released in May 2010, is the final result of a five-year activity of researches, experimentations and sharing with companies managers.
The latest update of the software supplies an online control panel to analyze the actual state of all Italian branches and scientifically support the robbery risk management in real time. The specific goal of this tool is to provide Italian bank security managers with an operative model able to:

a. "describe" the variables and define the "robbery" phenomenon;
b. "explain" the modalities to calculate (i) the "Exogenous", (ii) the "Endogenous" and (iii) the Global Risk Indexes for each single branch;
c. "predict", by a simulation module, the variations of the compound risk in relation with the different branches security systems.

Thanks to these data resulting from years of experience, I decided to generalize and extend the features of the model in other contexts such as the management of the Cash Risk, energy sources, e-learning courses and so on. Then I developed a meta-model exclusively focused on criminal phenomenology, NBNC (Neural and Bayesian Network to fight Crime). Such meta-model integrates ANN and Bayesian network in order to effectively analyze many kinds of operative risks related to the organized crime, such as anti-terrorism and criminal investigation techniques.
The present chapter includes:

- a premise about the concepts of "complexity" and "risk management" applied to crime phenomenology;
- an analytical presentation of the logic structure and the main features of the NBNC meta-model;
- a brief discussion about the method used in order to derivate a Bayesian network from a database through an ANN;

- a description of a concrete application of this meta-model, that is the ABI model applied to analyze the robbery risk in Italian Banking System.

2. Complex phenomena and risk management in criminality

The NBNC meta-model represents a theoretical framework to design and develop "intelligent models" in order to analyze the Risk in criminality.
This meta-model is based on three elements: a hybrid architecture integrating a database related to the phenomenology we need to analyze, a Bayesian network reproducing the probabilistic conditions between the variables involved, an ANN network system defining the rules that build the Bayesian simulator.
The structure of the NBNC model has been designed according to the complexity of the criminality and the risk analysis techniques: before describing its features, it would be useful to answer some questions:
what is "complex criminality"? Why it's so difficult to analyze and prevent "events" like bank robberies or terrorist attacks? Why is it almost impossible to build an "intelligent model" in order to effectively apply the most advanced criminal investigation techniques? Which are the Risk general features in criminality?

2.1 Definition of "complex phenomenon" in criminality

Let's start from a general definition: the complexity of a phenomenon essentially derives from the "impossibility" of representing its fundamental characteristics and dynamic evolutions through a linear quantitative frame. Such frame can correspond to any polynomial function, as:

$$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \quad (1)$$

where n is the function degree f, coefficients a_i are real numbers entirely independent of each others and a_0 is the constant term.
This "impossibility" depends on several interrelated factors:

- the coefficients of the hypothetical function meant to describe the phenomenon are interdependent;
- the variables composition effects can't be explained through the analysis of each single variable behavior;
- the phenomenon shows a very high number of inhomogeneous variables;
- the initial conditions affect the phenomenon dynamic evolution and show a "chaotic" behavior.

A phenomenon having these characteristics is defined as a "complex phenomenon". For instance, in most cases a "robbery" represents an "unpredictable" phenomenon related to different and interdependent factors (social, economic, psychological, geographical and environmental).
Similarly, a terrorist attack represents the effect of some variables interactions: International Relations, religious views, conflicting interests, social and economic conditions, links with the organized crime.
The same happens in case of many criminal events, in particular murders involving specific investigation techniques. As forensics experts could tell, the phenomenon shows a strong

fragmentation and stratification of several factors and initial conditions. That's why the model should take into account the following variables:

- the preliminary investigations results, that are the final outputs of public prosecutor, police, lawyers and defense experts activities;
- the crime scene reconstruction through planimetry, photos, collection of trace evidence, autopsies;
- the identity checks, through several kind of identification techniques (fingerprint, anthropological, vocal, genetic identification, graphology and so on);
- the forensic ballistics results.

2.2 The criminal "risk" analysis

The "criminal" phenomena analysis entails five different and complementary meanings of "risk". Then a risk can be:

1. the probability some conditions B can occur and cause the criminal event A: P(B);
2. the probability that, given some initial conditions B, the criminal event A: P(A|B) can occur;
3. the probability that, given some initial conditions B, the criminal event A can occur with some particular characteristics or specific magnitude $P(A_i|B)$;
4. the probability that, given some initial conditions B, the criminal event A can determine some (almost always harmful) effects C while P[C|(A *and* B)] is happening;
5. the probability that, given some initial conditions B, the criminal event A can determine some (almost always harmful) effects D after P{D|[C *and* (A *and* B)]} happened.

Clearly, these five meanings imply different analysis modalities and risk management typologies.

Focusing only on the first and second definition, we could analyze the risk by essentially monitoring the initial conditions in order to avoid the criminal event – robbery, terroristic attack, murder –. In terms of probabilistic conditions, it's necessary to control B so that P(A|B) = 0. In bank robberies this kind of approach could support the defense systems maintenance management or justify the introduction of a new armed security service. Or in the terroristic attack prevention, the initial conditions control could be focused on arms dealers travels in a particular risk area.

According to the third definition, the analysis model could be based on the assumption the criminal event is unavoidable: then, it would be necessary to focus on the initial conditions control in order to determine the criminal event characteristics. If A_i is the particular state describing the criminal event "expected" characteristics (the maximum threshold of magnitude), the goal is monitoring B so that $P(A_i|B) = 1$. Therefore, in case of a bank robbery, the risk analysis modality could be translated in a set of indications aimed at dealing some initial conditions (for example timed safes, instructions about cash management for all bank employees and so on) and reducing the robbery duration or the cash stolen amount.

The forth definition is an extension of the second one and suggests a more refined risk analysis model. According to the logical flow B→A→C, if we monitor B and, after that, A we can reduce C effects related to the criminal event. In the bank robbery example, the analysis results could induce the bank to provide all employees with some guidelines: learning

which are the most appropriate behaviors to keep in case of robbery can help avoiding things or people damages.
The fifth definition, a particular version of the third one, includes a risk analysis model aimed at monitoring the logical flow B →A → C → D (representing the criminal event A effects). In the case of a bank robbery, this analysis modality could be translated in some training activities to involve all the employees in the criminal event simulation in order to reduce the post-robbery psychological trauma. Another possibility could be the implementation of a communication plan to assure the customers the robbed bank branch is actually safe.

3. The NBNC meta-model

The NBNC meta-model includes the five "risk" meanings and summarizes them in a unique analysis modality: such approach includes the criminal event prevention, the analysis of possible practices to contain the event and the selection of specific activities to reduce its effects during and after.
In fact, given a **Ω** set of criminal phenomena, the meta-model application to the Ω analysis must guarantee:

1. a "description" of each Ω element state in a particular time interval t_n;
2. an "explanation" of every Ω event e_i in a specific moment t_n, according to the initial conditions set;
3. a definition of a "predictive system" to evaluate/simulate the Ω initial conditions and calculate the probability an event can occur in a specific time interval t_n;

The NBNC meta-model application shows a "descriptive" dimension based on the Ω modeling through the definition of an ontology in order to represent all the potentially occurring events (α_1, α_2, α_3, … , α_n) in Ω.
Hence the construction of a relational database describing the "story" of Ω consistently with the defined ontology.
The "explanatory" and "predictive" dimensions are based on a symbolic rules system and the construction of a Bayesian network. The ANN system recurrent training refers to an updated database describing the Ω phenomena story: this will help us building the Bayesian network.

3.1 The "descriptive" dimension

First, the meta-model must provide an exhaustive, quantitative and operative description of the α_i phenomenon in Ω. In other words it has to:

- identify all the different factors affecting and determining the criminal events α_1, α_2, α_3, … , α_n subject of the analysis;
- introduce a measurement system in order to translate the different factors in quantitative terms;
- clearly describe the identified factors characteristics in order to define the measurement different areas;
- adopt a "translator" handbook in order to map all the categories used by the field leading experts (who are the future users of the tool);
- develop a theoretical framework to "tell" the evolution of the phenomenon e_i over time;
- distinguish the dynamic variables defined in state description from the boundary structural variables;
- introduce new categories in order to circumscribe clusters of similar variables;

- define the observation conditions of each variable depending on the measurement system adopted;
- determine the specific factors frequency and the *a priori* probability through descriptive statistics tools;
- map the national and international legislation, in particular the different sanctions for criminal acts, affecting the categories definition;
- develop a relational database structure in order to include all the variables the model introduced.

In brief, it's about defining the system reference ontology and the specific vocabulary to highlight the more relevant aspects of the phenomenon α_i in Ω. The goal is determining a univocal "description" of the different criminal events involved. The identification of the "fundamentals" implies as final output a formalized language to represent every possible phenomenon α_i.

3.2 The transition from the "descriptive" to the "explanatory" dimension

After providing all the information and categories to describe every possible phenomenon, the tool must quantitatively define the involved variables rules and relations.

Therefore the explanatory dimension includes the preparation of a series of assumptions on the set functional rules meant to represent the variables relationships. These rules are essential in order to support the α_i criminal phenomenon "modeling" – which will be complete only when the phenomenon characteristics will be reproduced within a simulation -. A symbolic notation can synthesize the different elements without any loss of information.

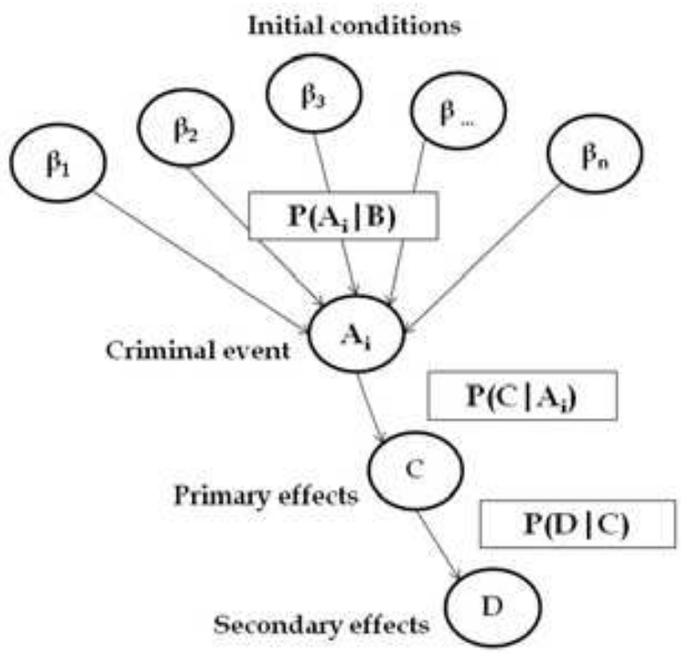


Fig. 1. Representation of simple conditional probabilities

As already mentioned, in case of complex phenomena such as bank robberies, terrorist attacks or murders, it may be useful to adopt the notation of the conditional probabilities calculation. A Bayesian framework can define the possible causal or interdependence

relations between initial conditions B = { β_1, β_2, β_3, … , β_n}, the criminal event A, the primary effects C and the secondary effects D (Fig.1).
Then on a descriptive level, it might be useful to identify a number of intermediate levels in order to define any clusters of variables and possible interactions within each level, as exemplified in the following Bayesian network (Fig. 2):

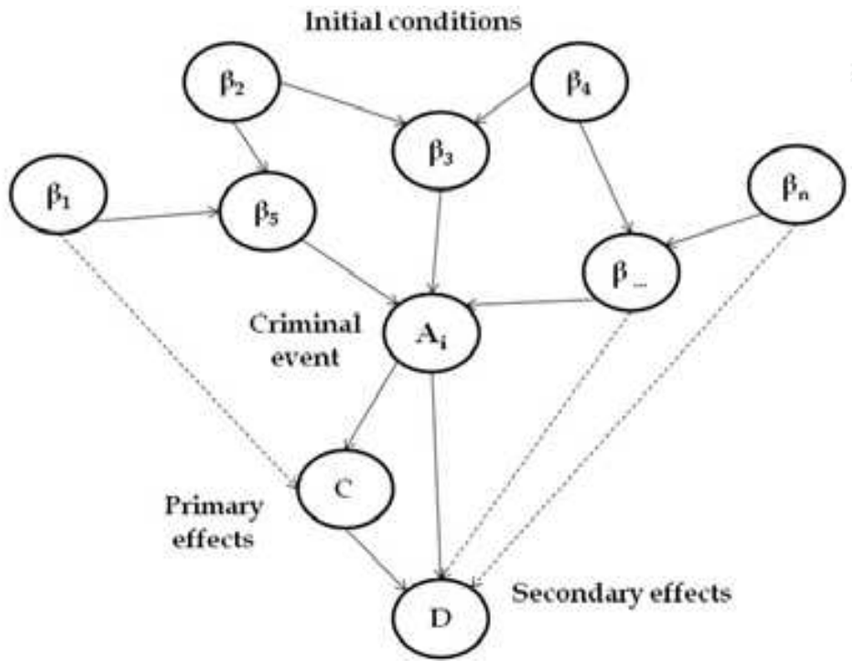


Fig. 2. Representation of complex conditional probabilities

3.3 The "explanatory" and "predictive" dimensions: Bayesian network learning system based on neural networks

The logical structure represented by the Bayesian network is still a hypothesis about general rules managing the phenomenology under observation. In fact, it shows the relationships but doesn't provide any information about the variables weight and the probability distributions values. At this point it is necessary to test the hypothesis derived from historical data and information necessary to effectively build the Bayesian network and turn the model into a powerful tool for risk analysis.
This can be possible by referring to the Motomura and Hara application of the method (Motomura & Hara, 2000). According to the authors we have to create one ANN for each conditional probability, that is each child node.
Let's start, for instance, from an elementary conditional probability: B → A.
According to Motomura and Hara method, we can build the ANN for the conditional probability P(A|B). This ANN has input neurons to represent the parent node B, hidden and output neurons to represent the child node A.
In our case, A and B are discrete variables and the number of ANN neurons input and output depends on the number of states A and B can assume.
In particular, if the child node A can assume a number of discrete values k, then:

$$A = (\alpha_1; \alpha_2; \alpha_3; \ldots ; \alpha_k). \quad (2)$$

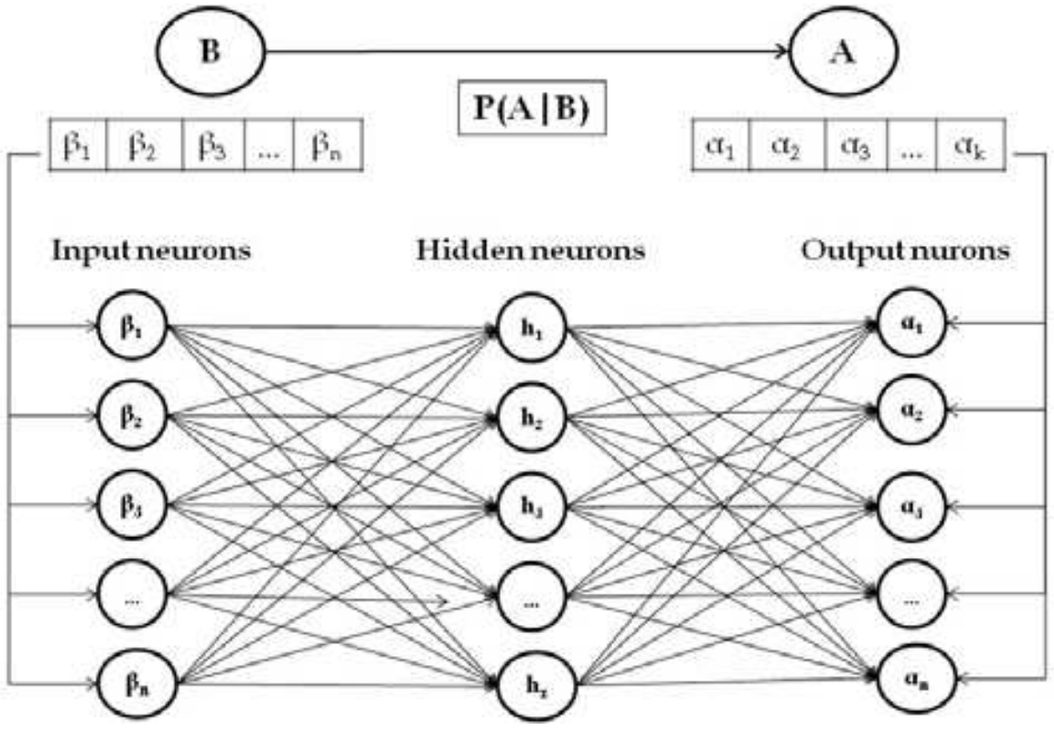


Fig. 3. The ANN representing P(A | B)

k is the neurons output number P(α_1); P(α_2) ; P(α_3); … ; P(α_k), that is the probability vector of the child node A (Fig. 3).

Then, how can we "neuronally" represent each conditional probability P(A | B = β) in order to build a Bayesian network?

First, we must analyze all α_k and β possible combinations:

	α_k	***not*** α_k
β	α_k *and* β	*not* α_k *and* β
not **β**	α_k *and not* β	*not* α_k *and not* β

Table 1. Possible combinations of α and β

Secondly, we have to determine the probability of each combination:

	α_k	***not*** α_k	***Sum***
β	P(α_k *and* β)	P(*not* α_k *and* β)	**P(β)**
not **β**	P(α_k *and not* β)	P(*not* α_k *and not* β)	**P(*not* β)**
Sum	**P(α_k)**	**P(*not* α_k)**	1

Table 2. Probabilities of α and β combinations

in the strength of these premises and according to Bayes Theorem,

$$P(\alpha_k \mid \beta) = \frac{P(\alpha_k \text{ and } \beta)}{P(\beta)}. \tag{3}$$

From a neuronal point of view,

- if v, w and b are ANN connection weights,
- and the logistic activation function is

$$g(\beta) = \frac{1}{1+\exp^{-\beta}} \tag{4}$$

- the Motomura and Hara (Motomura & Hara, 2000) solution will be:

$$f_k(\beta) = g\left(\sum_j v_{jk} g\left(\sum_i w_{ij}\beta_i + b_j\right) + b_k\right) \tag{5}$$

$$P(\alpha_k \mid \beta) = \frac{P(\alpha_k \text{ and } \beta)}{P(\beta)} = \frac{f_k(\beta)}{\sum_k f_k(\beta)}. \tag{6}$$

Similarly, in the case of a more complex network that describes the criminal phenomenon A and the related effects, this method allows us assigning step by step all the conditional probabilities values and exactly defining the functional architecture of the Bayesian network (Fig. 4).

In addition, through the ANN training we can indirectly verify the conditional dependency between each child node and its corresponding parent in the network. Indeed, the learning failure shows there isn't a conditional dependency between nodes and the network structure must be updated.

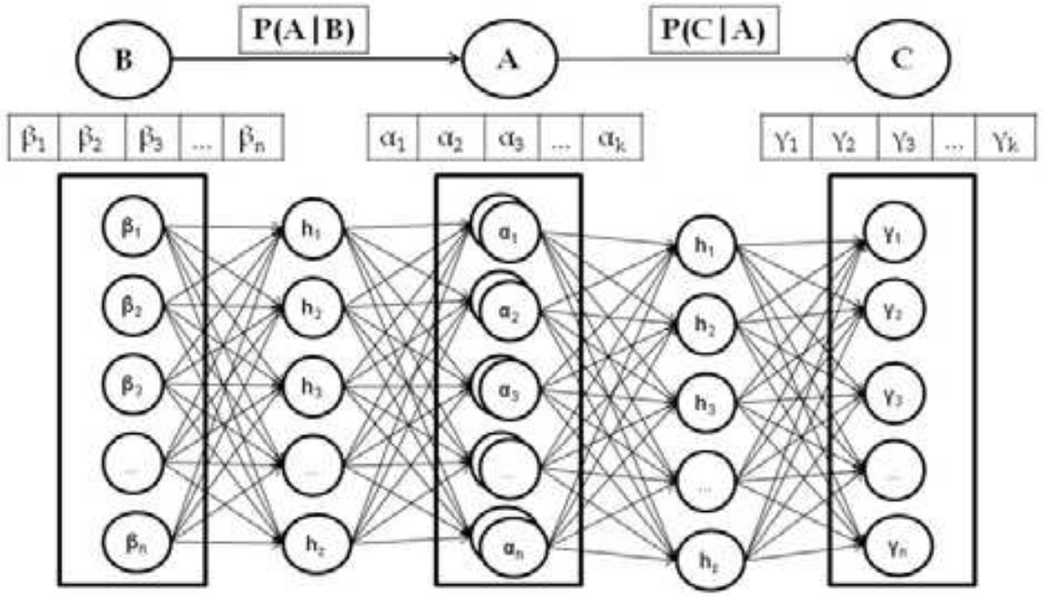


Fig. 4. ANN representing a complex Bayesian network

The final output is a Bayesian probabilistic model: describing, explaining and simulating a certain class of events allows supporting the security officers in the operational management of the different crime risk levels. In order to simulate different scenarios and the corresponding risk levels it will be sufficient to observe the states of the network independent variables and calculate the output values. Instead, in a preventing perspective, it will be necessary to go back to the initial functional values by associating the output to the expected values.

4. A real application of the NBNC meta-model: the ABI model of robbery risk analysis

The ABI robbery risk analysis model is a NBNC meta-model application in the world of crime.
First, the "descriptive" dimension of the model ensues from a compared analysis of different banks institutional data and involves the direct confrontation with the major Italian banking groups security representatives. Secondly, the "explanatory" dimension derives from the generalization of the robbery risk variables relations through the network recurrent training including other artificial neural networks (ANN). At last, the "predictive" dimension is based on the attribution of "weights" to the single internal variables and on the definition of a Bayesian network representing the probabilistic conditions and the variables dependence relations.

4.1 The "descriptive" dimension: the three robbery risk indexes

The first fundamental achievement of ABI research team was to create a univocal vocabulary of variables in order to describe all the basic features, plants and services of a bank branch. From this vocabulary the team elaborated the criteria to define the robbery risk different meanings and identify three Indexes:

1. the Exogenous Risk index,
2. the Endogenous Risk index,
3. the Global Risk Index.

Currently, security officers of the Italian banking system are using the three risk indexes in their analysis and robbery risk management. The integration of Exogenous, Endogenous and Global risk also supports an effective risk management procedure in order to prevent the robberies and mitigate the damages.

4.1.1 The Exogenous Risk index and the "environmental" variables of a bank branch

The Exogenous Risk index is annually calculated for every single Italian municipality and shows the concentration degree of criminal events in a specific area. The analyzed variables include:

- the geographical position,
- the population density,
- the annual crime rate in the area, calculated in relation with:
  - the ratio of robberies number per municipality's inhabitants (N),
  - the ratio of bank robberies number per N,
  - the ratio of thefts number per N,
  - the ratio of murders number per N,
  - the ratio of suicides number per N,

- the ratio of rapes number per N,
- the ratio of extortions number per N,
- the ratio of usury crimes number per N,
- the ratio of substance abuses number per N.

The latest version indicator shows a trend index calculated by the minimum square method and expressed by a geo-referenced probabilistic value. Its aim is defining the specific criminal exposure risk in the branch geographic area.

4.1.2 The Endogenous Risk index and the characteristics of a bank branch

The Endogenous Risk index expresses the single branch exposure degree to robberies apart from the geographic situation and the local crime rate. It consequently derives by the combination of the banking branch characteristics:

- the "basic characteristics": the number of employees, the location, the cash risk and so on.
- the "services": for example, the bank security guards;
- the "plants"': for example, the bandit barriers.

The index is calculated with a complex function of robberies in a single branch, during a unit of time in which every "event" has modified the branch internal order.

For example after a robbery, a bank can decide to put in a video camera directly connected to the police.

4.1.3 The Global Risk Index of a bank robbery

The Global Risk Index defines the actual robbery exposure degree of a specific bank branch, including its intrinsic features and geographic situation. It is calculated by considering the evolution of the suffered robberies in relation with the units of time and expresses a trend value.

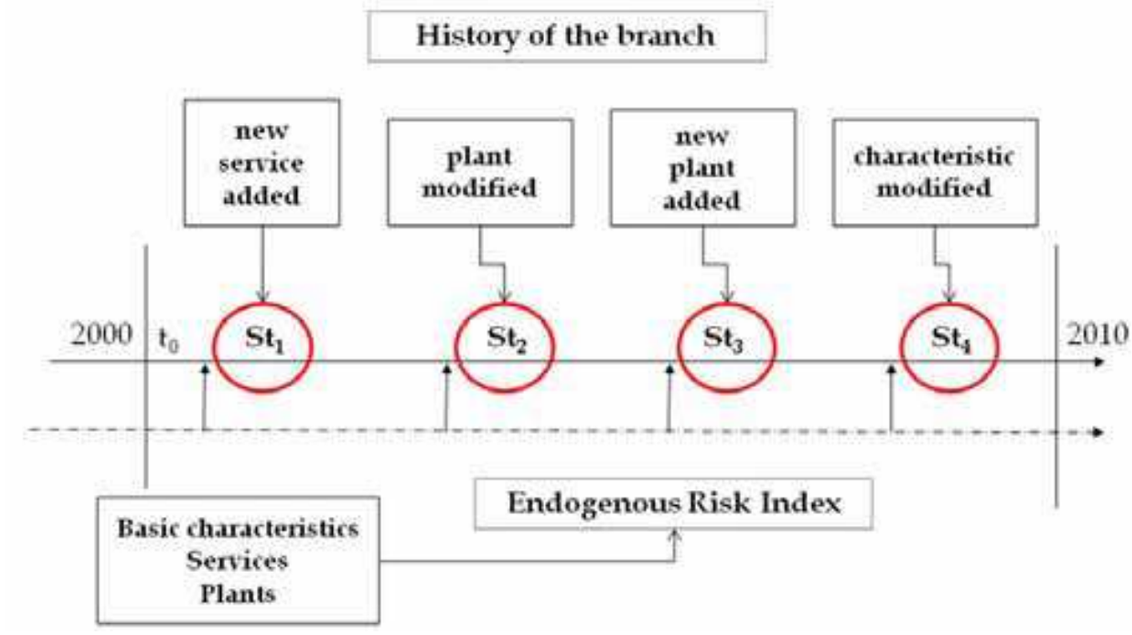


Fig. 5. Graphical representation of the branch states

Therefore the Global Risk Index derives by the non-linear combination of Exogenous and Endogenous Risk and corresponds to the synthesis of the robberies number per month and the number of days the branch is open.
Expressed by a value between 0 and 1, it can be calculated by the minimum square method and represents the trend in relation to the previous values.
But what Global Risk Index means and which is its relationship with the other risk indexes?
The model is based on the description of the branch history as a sequence of states (Fig. 5), taking into account every change of its structure (for example, the introduction of a new defending service). In this way we create a direct relation between the branch and the Robbery Global Risk evolutions (Fig. 6).

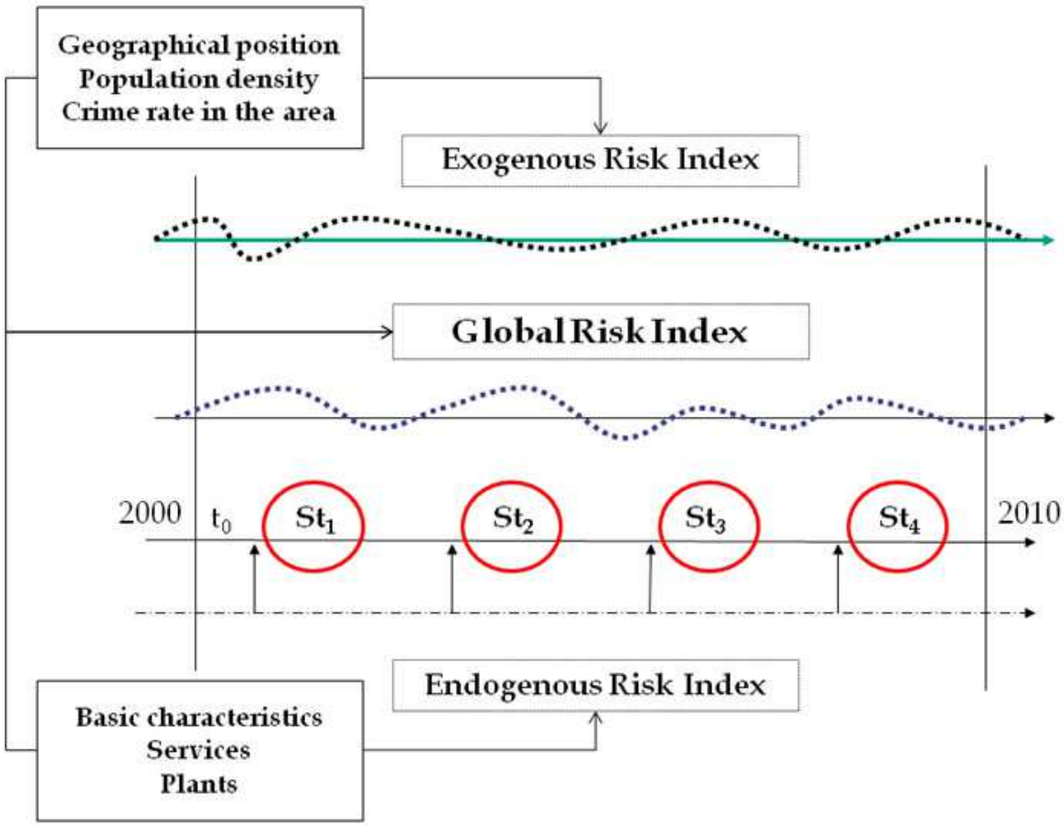


Fig. 6. Graphical representation of the evolution of Robbery Global Risk

To simplify the question, we can use a biological metaphor: the transformation of the branch over time is like a "mutation" of biological organisms populations.
This metaphor allows overcoming a wrong interpretation of the concept of "deterrent".
And the Robbery Global Risk suggests how the "robbery market" replies to the security managers activities.

4.2 A Bayesian simulator for the robbery risk analysis

The recent implementation of a Bayesian network in the simulation module is a significant evolutionary factor in the ABI robbery risk analysis model. Compared to the 2009 release the new version:

i. contributes to make the compound risk predictive system more effective,
ii. allows an exhaustive check and an indirect validation of the ANN training results,
iii. introduces an algorithm that can be easily integrated in many computer system supports,
iv. facilitates the final users (bank security managers) to understand the model functionalities, solving all the skepticisms outcropped in the previous versions.

The analysis of the variables and of the three risk indexes allows defining the logical structure of the probabilistic conditions governing the "bank robbery" phenomenon:

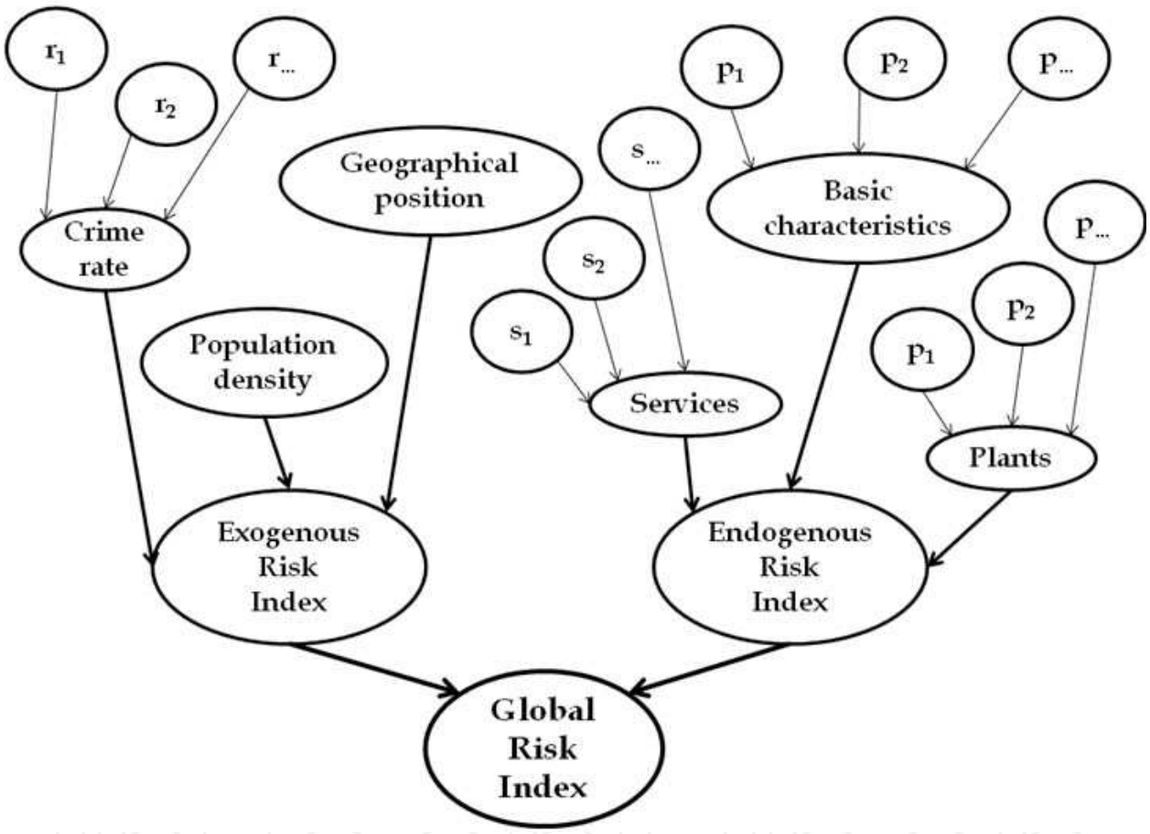


Fig. 7. Bayesian Network of the ABI robbery risk analysis model

The Bayesian Network in Fig. 7 graphically represents the output of the design process: the probabilistic model to analyze the robbery risk. The input values of the simulation software are the elements composing the external and internal risks, whereas the output is defined by the *a priori* calculation of the global risk. The reference database consists of a branches and criminal acts historical archive concerning the time interval 2000-2010.

The creation of the Bayesian Network was articulated in five phases.

1. In the first phase the team revised the database in order to remove possible critical factors.
2. In the second phase all variables connected to the Exogenous and Endogenous Risk were normalized.
3. The third phase was dedicated to design the general structure of the system of ANN and its mathematical properties in relation with the Bayesian network of reference;

4. In the fourth phase we decided to implement a variation of the Back propagation: the "OS.SI.F Quick-propagation" to solve numerical instability and avoid the net permanence in critical situations of local minima.
5. Finally, in the last phase of the process we verified the Bayesian network structure based on ANN. Also some critical nodes were modified in strength of the Exogenous Risk variations according to the population density and the relationship between Endogenous Risk and some new plants.

4.3 The advantages of applying the NBNC meta-model to the robbery risk analysis

The implementation of NBNC to support the Robbery Risk analysis has five fundamental advantages:

- it coherently faces the high complexity degree of the robbery phenomenon;
- it overcomes limited local vision in aid of the Robbery Risk analysis systemic approach;
- it provides a higher degree of accuracy and scientific reliability to define the "risk" and the whole calculation model;
- it ensures the maximum level of flexibility, dynamism and adaptability to contexts and conditions;
- it guarantees an effective integration between a solid calculation model and the security managers professional and human experience.

5. Conclusion

The NBNC meta-model was successfully applied in the creation of the ABI robbery risk analysis tool (currently used in the Italian banking system). Moreover it is a theoretical tool to design "intelligent" systems for the risk analysis in criminal investigations. In fact, it represents an operational framework for the models implementation and takes into account the criminal phenomenology complexity.

In the previous pages I tried to present the meta-model main features, primarily focusing on the importance of the descriptive dimension in the criminal risk analysis tool. In fact, the creation of a formalized language constitutes the foundation to identify some criteria and rigorously analyze the five risk levels. Experience taught me in most cases the community of experts in criminal risk management adopts different words to express the same variables or labels to describe unlike events. This causes ambiguities and misunderstandings that hamper the theoretical framework definition.

Secondly, I reflected on the power of a Bayesian model based on neural networks to adequately describe the complexity of the crime phenomenon. This method allows:

- identifying relevant variables in the mechanism governing the crime phenomenon;
- introducing new variables or redefining the previous ones;
- weighing each variable in relation to the overall structure;
- discarding irrelevant variables;
- falsifying or supporting the same consistency of the assumed logical structure;
- identifying the likely strong causal links between variables;
- defining the values of the Bayesian network probability distributions;
- limiting the reliability of the results expected.

By supporting the activities of prevention, monitoring, control and mitigation of the five risk typologies related to a wide range of phenomena, this method represents a useful contribution to the fight against crime.

6. Acknowledgment

Thanks to Marco Iaconis, Francesco Protani, Fabrizio Capobianco, Giorgio Corito, Giovanni Gioia, Riccardo Campisi, Luigi Rossi, Fausto Ligis and Diego Ronsivalle for the scientific support in the NBNC meta-model development, and to Marisa Orlando and Laura Ferraris for translating the chapter.

7. References

Donato, F. (2006). *Criminalistica e Tecniche investigative*, Editoriale Olimpia, ISBN 88-253-0116-2, Sesto Fiorentino (Firenze), Italy

Einstadter, W.J. & Henry, S. (2006). *Criminological Theory. An analysis of its underlying assumptions*, Rowman & Littlefield Publishers, Inc., ISBN 978-0-7425-4290-7, Lanham, Maryland

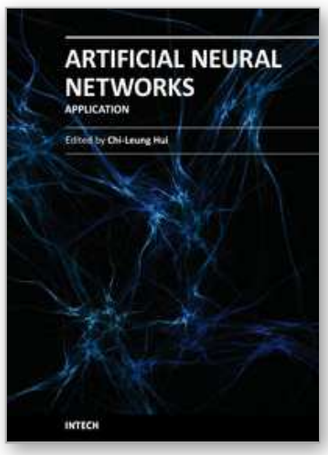
Floreano, D. (1996). *Manuale sulle reti neurali*, Il Mulino, ISBN 88323074-4, Bologna, Italy

Iaconis, M. & Corradini, I. (2010) *Guida alla sicurezza per gli operatori di sportello*, Bancaria Editrice, Roma, Italy

Motomura, Y. & Hara, I. (2000). Bayesian Network Learning System based on Neural Networks, *Proceedings of AFSS2000, International Symposium on Theory and Applications of Soft Computing*

Pessa, E. (2004). *Statistica con le reti neurali*, Di Renzo Editore, ISBN 88323074-4, Roma, Italy

Wilson, A.G. & Wilson, G.D. & Olwell, D.H. (2006). *Statistical Methods in Counterterrorism. Game Theory, Modeling Syndromic Surveillance and Biometric Authentication*, Springer Science+Business Media, LLC, ISBN 978-0387-32904-8, New York, USA



Artificial Neural Networks - Application

Edited by Dr. Chi Leung Patrick Hui

ISBN 978-953-307-188-6
Hard cover, 586 pages
Publisher InTech
Published online 11, April, 2011
Published in print edition April, 2011

This book covers 27 articles in the applications of artificial neural networks (ANN) in various disciplines which includes business, chemical technology, computing, engineering, environmental science, science and nanotechnology. They modeled the ANN with verification in different areas. They demonstrated that the ANN is very useful model and the ANN could be applied in problem solving and machine learning. This book is suitable for all professionals and scientists in understanding how ANN is applied in various areas.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen