Università degli Studi di Salerno

Dottorato di Ricerca in Management & Information Technology
Ciclo XXXII – a.a. 2019/2020

TESI DI DOTTORATO / PH.D. THESIS

Supporting the Intelligence Analysis stages with Approximate Reasoning: Methods and Tools based on Granular Computing

ANGELO GAETA

SUPERVISOR: **PROF. FRANCESCO ORCIUOLI**

PHD PROGRAM DIRECTOR: **PROF. VALERIO ANTONELLI**

Dipartimento di Scienze Aziendali – Management
& Information Systems

Abstract

Current threats, such as terrorism and cyber-terrorism, pose new challenges to security and defence communities, and the ability to reason with different perspectives and detecting connections between facts, relationships and events becomes crucial to address these challenges. To this purpose, a less procedural and standardized approach is useful, able to leverage current computational and artificial intelligence technologies to detect threats and protect physical and cyber-physical systems. This raises a strong interest in defining and adopting new methods and techniques that, to a certain extent, are such as to replicate, or at least to support, human cognitive processes. If we consider the "creativity" behind some recent attacks, such as that one of 09/11/2011, we can understand the need to rethink security in *situational* rather than *procedural* terms, and this has an important implication that helps to frame the problem and research objectives of this thesis. This implication is a shift from being aware of what we need to prevent (and the related rules and procedures to that end) to gaining greater awareness of what might happen. From this consideration, it emerges the need of methods and tools that support decision makers in their ability to carry out analyses that allow to hypothesize different threat scenarios, and to reason about their evolutions. This is, essentially, the main objective of the so-called *intelligence activities*.

The research problem investigated in the Ph.D period is how to improve the awareness of analysts and decision makers in the early stages of an intelligence analysis to prevent intentional attacks, and the specific objectives concern the definition and validation of

reasoning methods based on Granular Computing (GrC) for this purpose. Specifically, methods to:

- carry out analysis and assessment of hypotheses of intentional attacks, and to attribute these hypotheses to terrorist groups;
- Define security perimeters to protect a target of attack;
- Analyse evolutions of an attack, considering also the dependencies between components of a target, and estimate the resilience of a target.

The results share a common methodological basis consisting of the use of rough sets and their extensions, such as fuzzy probabilistic rough sets and dominance based rough sets, for data analysis and processing, and models of 3 way decisions to reduce the cognitive effort of decision makers in the decision-making phase.

The three methods defined are intended to support the intelligence cycle stages.

The first method combines probability theory, fuzzy and rough sets to analyse different attack scenarios, such as high probability - low risk and low probability - high risk, and attribute the assumptions of attack to known groups. It starts from a minimum set of information, vague and preliminary, to derive hypotheses concerning attack events and evaluate them with respect to a body of evidence collected from historical data on terrorism events. The body of evidence is defined in terms of similarity of behaviour of known groups. This is constructed with an algorithm that combines equivalence classes and fuzzy equivalence classes to derive similarity matrices of terrorist groups behaviours. After the phase of evidence collection, the proposed method uses two parameters that allow the derivation and assessment of a wide range of hypotheses, starting from intelligence information on possible attack strategies, weapon types and target types. This happens through the use of Ordered Weighted Averaging (OWA) operators with probability distribution to aggregate information coming from intelligence sources, and the use of a probabilistic three way decisions model based on Bayesian rough sets to carry out a tri-partition of terrorist groups into groups that can be: associated to the created hypotheses (POS), not associated (NEG) or for which no decision can be made (BND). The evaluation of results has been carried out on real data relating to five years (2012-2016) of terrorist activities extracted from the Global Terrorism Database (GTD). To consider only information that is assumed to be available in the initial phases of an intelligence analysis, we have reduced the descriptive features of the GTD from 135 to 3: attack strategy, type of target and type of weapon. The method has been experimented on three representative cases: 1) a rare pattern, 2) a distinctive pattern, 3) a combination of patterns. The results have been evaluated with respect to error metrics such as Sensitivity, Specificity and Balanced accuracy.

The second method aims at defining security perimeters to defend targets of attack. Based on the information previously derived, and including estimates of expected losses, Threat Scenarios are defined and analysed to increase the security level of the target. The method supports decision makers in the analysis and protection of targets (i.e., large-scale infrastructures or urban areas) by identifying an adequate partition of the infrastructure or area being analysed. The method works on a very limited set of information related to components vulnerabilities and probabilistic information on how vulnerabilities can impact on significant partitions. Based on this information, the method involves the definition of Threat Scenarios, triples that include: attacks, expected losses, and probability of having losses whose value is at most equal to the expected one. Threat Scenarios are compared based on the principle of stochastic dominance using an approach based on Dominance Rough Sets, specifically Dominance-based Rough Set Approach under uncertainty. The results of the case study, based on a hypothesis of a terrorist attack derived from GTD events, show that the method provides approximate solutions that allow reasoning at different levels of granularity (such as a single attack or groups of attacks). A measure to understand the goodness of resulting partitions, both overall and with respect to specific attacks, has been defined by contextualizing quality measures traditionally used in the 3 way partitions.

The third method is devoted to analyse the evolution of an attack, and evaluates the resilience of the target considering also the dependencies between components of the target. The method relies on a hierarchical granular modelling approach to define information granules of the attack. Dependencies, of various kinds (such as physical, cybernetic, logical or geographical), are modelled with granular structures. The attack informative granules are used to estimate the resilience of the target, based on an operational resilience model adapted for interval operations. The method has as its element of originality the systemic integration of the GrC for resilience analysis, and has been validated on a case study modelled on a smart grid. However, it requires further development in order to be better contextualized to the application sector of this thesis.

Acknowledgments

At the end of this pleasant and demanding journey, I thank God who gave me strength and support in difficult moments.

This thesis is the culmination of the hard work and dedication of many people.

First and foremost, I thank Prof. Vincenzo Loia: without his vision, experience and insights this thesis, simply, would not have reached this stage.

All my gratitude goes to my supervisor, Prof. Francesco Orciuoli, for his support, encouragement and belief in me. Working with him has always been pleasant and rewarding.

Special thanks go to the Ph.D coordinator, Prof. Valerio Antonelli, and all the DISA-MIS staff. They have always been present and available to answer all my requests and doubts. I must thank the thesis evaluators, Prof. Fabio Scotti and Prof. Angelo Genovese, for their useful comments and suggestions.

I am grateful to my mother, my wife and my sister, who have supported me along the way. I am also grateful to my daughters and grandchildren who have provided me through moral and emotional support in my life.

And last but absolutely not least, to my late father Osvaldo: because I owe it all to you. Many Thanks!

A chi mi vuole bene.

Contents

Chapter 1

Introduction

Mica Endsley defines Situation Awareness (SA) as [1] "*the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*". Being aware of a situation supports better decision making, and better decisions can save the life in so many contexts that it seems superfluous to mention them.

Achieving a good awareness of the situation is not, however, a result of the case or a purely accidental event, but comes from the combination of numerous factors. In [2], the authors report three perspectives of situation awareness and discuss "*whether situation awareness is a phenomenon best described by psychology, engineering or systems ergonomics*". The three perspectives associated to these disciplines are, respectively, refereed to as situation awareness "in-mind", "in-world" or "in-interaction" and, in [2], it is suggested to consider these perspectives as declaration of levels or boundaries for a correct analysis of the SA phenomenon.

These are, however, like fuzzy boundaries in the sense that, as Endsley and Jones argue [3] "*SA does not exist by creating information in some technical system. SA exists only when it is developed within the cognition of a person who assesses the information*" and, in our opinion, data and information processing methods have to be aligned to individual cognitive views and capabilities, and support human way of reasoning.

To this purpose, Granular Computing (GrC) [4] is gaining attention as a paradigm to represent, reason on, and process basic chunks of information, namely granules, where a a granule is defined as "*a clump of points (objects) drawn together by indistinguishability, similarity, proximity or functionality*". GrC allows to group objects in the same fashion humans observe elements of an environment, and perceive them by proximity, shape or similarity, making our cognitive process more effective. Besides this, GrC is useful to explore the multi-level granularity that exists in the physical world, helping us to arrive at accurate and natural descriptions, as well as in-depth understanding, of the inherent structures and complexity of the real world [5].

GrC seems to be a natural way to improve awareness and comprehension of situations but, so far, the adoption of GrC to enhance SA has not received much attention from researchers and practitioners, and these two research areas are still today considered as silos. What is missing is a systematic approach to study interactions and correlations between GrC and SA, and before my Ph.D period I have collaborated in a research activity devoted to analyse this gap and propose a direction for further investigations [6].

In [6] the integration between GrC and SA is envisioned via: *i)* the definition of an high-level view describing how concepts, principles and perspectives of GrC fit into the Endsley's SA model, *ii)* an overview of GrC methods and techniques that can be useful to address some issues of the three levels of the Endsleys model, and *iii)* a proposal showing the adoption of computational intelligence and Semantic Web techniques to support the development of a multi-agent based framework for SA aligned with the GrC principles. This last (i.e., *iii)*) point, however, has been covered with a discussion on some methodological and architectural aspects of a SA framework without any claim of completeness, and examples of concrete applications.

The research conducted in these three years and reported in this thesis starts from here and continues in the direction of the definition and validation of approximate

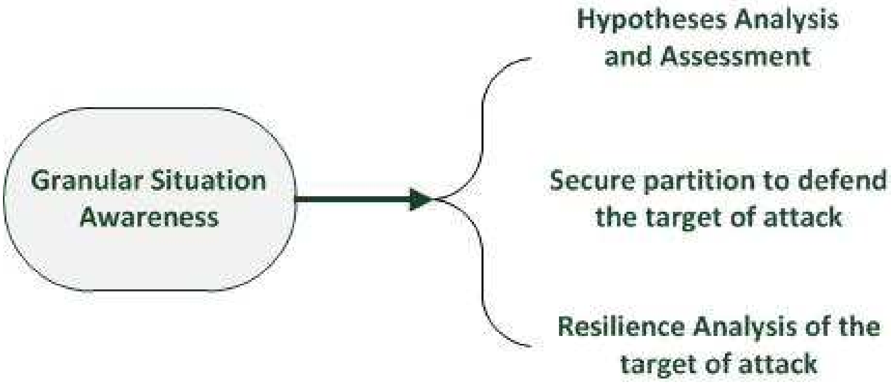

Granular Situation Awareness
Hypotheses Analysis and Assessment
Secure partition to defend the target of attack
Resilience Analysis of the target of attack

Figure 1.1: Research results of the thesis

reasoning methods based on GrC to improve awareness of decision makers operating in security and defence domains. An overview is presented in fig. 1.1 that shows the three methods reported in this thesis.

1.1 The Context: re-thinking security

To describe the context of the study, we answer three key questions: **why?**, **what?**, and **so what?**, with the last one referring to implications and limitations of the results for stakeholders.

1.1.1 Why? - Problem Statement and Research objectives

Current threats, such as terrorism and cyber-terrorism, pose new challenges to security and defence communities. It appears crucial to find a way of being able to reason with different perspectives and to detect connections between facts, relations and events. In other words, it is required a more creative approach, able to apply current Computational and Artificial Intelligence technologies patterned on human thought processes to detect threats and protect physical and cyber-physical systems. This raises a strong interest within the security and defence communities in the definition and adoption of new methods and techniques for solving challenging problems.

If we consider the "creativity" behind some recent attacks, we can understand the need of rethinking security in situational terms more than procedural ones, and this has an important implication that helps to frame our problem and research objectives.

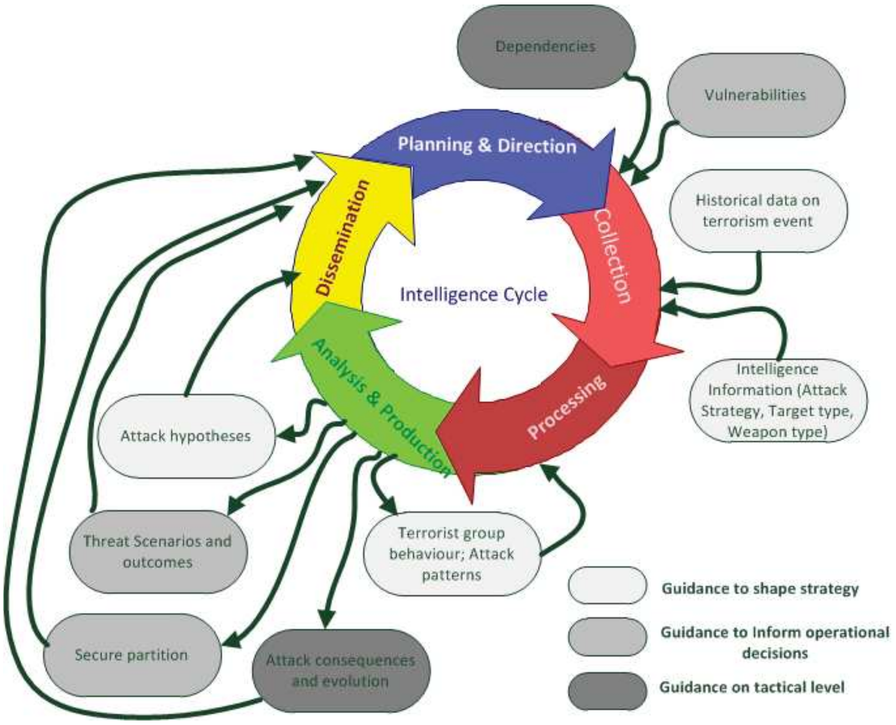
This implication is a shift from "*being aware of what we need to prevent*" to "*gaining awareness of what could happen*". In other words, as reported in [7] "*researching situational awareness reaches its fullest challenge when security personnel and ordinary people alike figure out live what is happening and what needs to be done, in the face of a kind of event that has not occurred yet, when the nature of the danger and the imminent dynamics must be speculated upon, by all sorts of non-orchestrated agencies*". Here the keyword is "speculation", and indicates the necessity of analysis and assessment of different hypotheses about "*the nature of the danger and the imminent dynamics*" and, indeed, this requires reasoning in the early stages of analysis on who can be the perpetrator of an attack, what can be the consequences of the attack and how is it possible to defend a target.

The problem afforded in this research study is **how to improve awareness of analysts and decision makers in the early stages of a security analysis on intentional attacks** and the research objectives relate to **the definition and validation of approximate reasoning methods supporting decision making** on perpetrators and consequences of an attack.

To be more concrete, we refer to "early stages" of a security analysis as those phases typical of an intelligence cycle that are devoted to produce rapid decisions and guidance based on the available (usually scarce and uncertain) information. As reported in [8], guidance can be provided at different levels such as:

- to shape a strategy, for instance decision makers must choose for which hypotheses and scenarios to develop response plans,

- to inform operational decisions, such as how to deploy re-



Dependencies
Vulnerabilities
Planning & Direction
Historical data on terrorism event
Dissemination
Collection
Intelligence Cycle
Intelligence Information (Attack Strategy, Target type, Weapon type)
Analysis & Production
Processing
Attack hypotheses
Threat Scenarios and outcomes
Terrorist group behaviour; Attack patterns
Secure partition
Attack consequences and evolution
Guidance to shape strategy
Guidance to Inform operational decisions
Guidance on tactical level

Figure 1.2: The enhanced intelligence cycle

sources and modify operations to enhance security,

- on a tactical level informing, for instance, critical infrastructure owners and operators when greater security is required.

Fig. 1.2 shows the intelligence cycle [9] and its connections to the methods proposed in this thesis.

The intelligence cycle [9] presents five phases: definition of the direction of intelligence activities, collection of information, its processing, analysis and production of new information, and its dissemination and adoption. As such, the goal of an intelligence cycle is to create new information and, as challenge, the new information is "*more valuable if the intelligence cycle operates faster than the opponent's*" [8]. Feeding the information cycle with methods of approximate reasoning and rapid decision making can support faster recognition of threats and adaptation to attackers changes.

In fig. 1.2 the grey ovals represent phases and artefacts supported or created by the methods presented in this thesis. The different shades refer to the guidance levels reported in the previous bullet points. Even if fig. 1.2 shows a clear distinction, some phases and artefacts are shared among the three methods.

Let us firstly consider the intelligence cycle devoted to offer strategic guidance. The planning and direction phase is, therefore, focused on planning intelligence analysis activities to generate and assess hypotheses and threat scenarios. This can start with the collection of information on past terrorism events, and information from intelligence sources on possible attack strategies, targets and weapon types. This information is processed and analysed to produce models of terrorist groups behaviour and attack patterns. These can be further processed and analysed to derive a set of attack hypotheses that can be assessed against available evidence to identify perpetrators. The steps described follow the operations of the method reported in section 3.1.1 of this thesis.

The hypotheses of intentional attacks can be used in a second intelligence cycle to inform decision makers on how to partition a target (e.g., an urban area or infrastructure) under attack in order to better deploy resources and/or modify security operations to fulfil requirements about expected losses. Besides the derived hypotheses, in this cycle it is necessary to collect, process and analyse information on vulnerabilities of the target area or infrastructure. This information is combined to formalize a threat scenario including also outcomes, in terms of looses and/or damages, and a probability distribution of these outcomes. Following the method reported in section 3.1.2 of this thesis, threat scenarios are analysed to identify a suitable partition of the target to defend, allowing to deploy resources and security operations to fulfil the initial requirements.

This partition is, lastly, analysed with regards to consequences and evolutions of some attacks. Additional information, such as nature and type of dependencies among the objects of an area, or components of an infrastructure, is required to perform evaluation of attacks evolutions. This cycle is such to inform decision makers on the level of resilience of the target area or infrastructure in order to implement additional security operations. The resilience analysis is the objective of the method reported in section 3.1.3.

Fig. 1.2 is a way to show how the results achieved during these three years can be correlated within intelligence cycles, in order to support the shift towards a situational-oriented security where decision makers can operate at different levels (strategic, tactic, operative). Another view, which gives a methodological perspective, is reported in fig. 3.1 of chapter 3.

1.1.2 What? - Overview of the results

The results achieved during this period consist of:

- a method to create, analyse and assess hypotheses of intentional attacks;

- A method for protecting target areas or infrastructures from intentional attacks by identifying a suitable partition of the target;

- A method to analyse the resilience of infrastructures in the case of intentional attacks.

After the description of the methods in section 3.1, section 3.2 presents an overall comparison with other methods and techniques for supporting intelligence cycles. However, it is useful to summarize here the distinctive aspects of each one of the methods with a brief comparison with the main competitors.

The first method is devoted to create, analyse and assess hypotheses of intentional attacks (i.e., terrorism events). It combines probability, fuzzy and rough set theories and supports decision makers and analysts of counter-terrorism in the analysis of intelligence information and its correlation to behaviours of terrorist groups. In comparison with other approaches based on structured analytic techniques for intelligence analysis (e.g., [10]), computational intelligence techniques (e.g., [11], [12], [13]), evidential reasoning (e.g., [14]) or combinations of structured analytic techniques with Bayesian probabilistic framework (e.g., [15]), we provide an interesting enhancement with the inclusion of a three way decisions model that allows decision makers to reason in a simplest and more immediate way [16]. Furthermore, the method is interactive and such to analyse and assess hypotheses on the basis of a very limited and coarse-grained set of information.

The second method works in continuity with the results of the first one. Once assessed attack hypotheses, this method has the objective of supporting decision makers in analysing and protecting targets of attack, such as large-scale infrastructures or urban areas, by identifying a secure partition of the target area. The method works on a limited set of information relating to the vulnerabilities of targets, and probability information regarding how vulnerabilities can impact meaningful partitions. This method is a heuristic for rapid decision making on how to defend targets by splitting these targets into parts. It can be compared with *i)* zone partition methods (e.g., [17], [18], [19]), and *ii)* game theory heuristics based on attacker-defender models ([20], [21], [22], [23], [24]). With respect to *i)*, the proposed method introduces concepts and ideas originating from resilience programmes, such as risk and vulnerability indexes, and uses the concept of stochastic dominance to analyse and compare different threat scenarios. Moreover, an important objective of our method is to maintain the human (i.e., the decision maker) in the loop by explicitly considering her/his perspective into the definition of parts, and supporting her/him in the analysis of results at different levels of granularity. With regards to *ii)*, the basic assumptions of the proposed method differ from these works, since there are no strict assumptions on the utility for an attacker, which may be reasonable in the early stages of analysis in most cases.

With the third method, concepts of resilience analysis are integrated in the Granular Situation Awareness (GSA) model. GSA [25] is a cognitive model based on the application of GrC in and across all the levels of a SA model. The objects of computation in GSA are granules and granular structures that can be constructed according to different criteria. We consider the definition of resilience of a system provided by the National Academy of Science, i.e. the ability *to plan and prepare for, absorb, respond to, and recover from disasters and adapt to new conditions* [26], and use the model defined in [27] that is aligned with the above reported definition. The main merit of this last result lies in the proposal of a general frame that clearly underpins the adoption of GrC for resilience analysis allowing to support the shift previously outlined concerning the rethinking of security in situational and resilience terms.

1.1.3 So what? - Implications and limitations for the stakeholders

The results reported in this thesis are intended for analysts and decision makers that want to have an improved awareness on what happens under an intentional attack, and take rapid decisions on possible perpetrators of an attack, on assets that have to be better protected and/or to preserve an adequate level of resilience. The improved awareness has to be gained at both the levels of *causes* (e.g., analysis and assessment of attacks hypotheses) and *effects* (e.g., consequences of the attacks). The rationale behind the proposed approaches is to maintain the human in the loop of this process by providing granular information allowing him to rapidly perceive, comprehend and project a situation of attack in terms of potential perpetrators, threat consequences, attack evolutions.

However, to improve awareness, information must be provided in a simple and effective way to take decisions. To this purpose, the methods proposed in this thesis share a common approach that models a particular class of human ways of problem solving and information processing: the theory of three-way decisions (3WD) [28]. As Yao precisely discusses in [28][1], 3WD are built on solid cognitive foundations and offer cognitive advantages and benefits.

[1] See section ”Cognitive Basis and Advantages of Three-Way Decisions” of

Instead of repeating the considerations already done in [28], we only evidence how 3WD are used in several real scenarios such as triage systems in emergency departments, medical decision making (i.e., treatment, further test, or non-treatment), hypothesis testing (i.e., accept, reject, or continue testing).

In all these settings, the adoption of 3WD offers advantages in terms of reduction of cognitive load, simplicity and flexibility that can enable rapid decision making, allowing decision makers make quick and right decisions for some cases and focus more efforts on some other cases. However, 3WD are based on human heuristics and, as such, suffer from cognitive biases and errors.

In intelligence analysis, cognitive biases and errors are well analysed by Heuer in [29]. Even if biases and errors can not be eliminated, they can be reduced adopting structured analytic techniques [10] involving a step-by-step process that "externalizes" the analysts thinking. In other words, the idea behind the adoption of these techniques is to make explicit some implicit assumptions of the analysts. This makes easier to identify biases and errors.

The methods presented in this thesis share the rationale behind the structured analytic techniques, i.e., to generate a wide set of hypotheses and scenarios that can challenge the analysts thinking. Furthermore, the methods defined use probability theory allowing to "*include mechanisms to ensure analysts reason probabilistically*" and to "*be less likely to over-estimate the likelihood of rare outcomes and more likely to make calibrated assessments that properly identify the relative strengths of the arrayed hypotheses*" [30].

1.2 Structure of the thesis and Publications

The structure of this thesis is as follows:

- Chapter 2 provides background information on GrC. Since 3WD, Rough Sets and their extensions are the principal for-

[28]

mal setting of GrC employed in this thesis, the chapter also reports information on these models.

- Chapter 3 presents the three methods contextualised in an unifying scenario. It positions also the presented results with respect to competitors. Specifically:
    - section 3.1.1 presents the method to derive, analyse and assess hypotheses of intentional attacks,
    - section 3.1.2 presents the method for secure partition of targets of intentional attacks,
    - section 3.1.3 presents the method to analyse the resilience of infrastructures or urban areas in the case of intentional attacks.
- Chapter 4 presents experimental results and an evaluation based on a case study for, respectively, the first and second methods above mentioned.
- Chapter 5 presents conclusions and draws future works.
- Appendices A and B report tables related to experimentation of the method to create, analyse and assess intentional attacks hypotheses.

The results presented in this thesis have been accepted for publication or published in international journals. Specifically:

- The method described in section 3.1.1 and evaluated in 4.1 has been accepted for publication in IEEE Transactions on Fuzzy Systems journal with the title "Hypotheses Analysis and Assessment in counter-terrorism activities: a method based on OWA and Fuzzy Probabilistic Rough Sets" (Authors: H. Fujita, A. Gaeta, V. Loia, and F. Orciuoli) [31].
- The method described in section 3.1.2 has been published in the paper "Improving awareness in early stages of security analysis: A zone partition method based on GrC." in

Applied Intelligence, 2019, 49.3: 1063-1077 [32]. The evaluation of this method in section 4.2 has been contextualised, starting from [32], to terrorism events from GTD.

- The method described in section 3.1.3 has been published in the paper ”Resilience Analysis of Critical Infrastructures: A Cognitive Approach Based on Granular Computing” in IEEE Transactions on Cybernetics, vol. 49, no. 5, pp. 1835-1848, May 2019 [33].

In addition, the Granular Situation Awareness model, at the core of the resilience analysis, has been published in the chapter ”Ambient Intelligence: A Perspective of Granular Computing.” In Wiley Encyclopedia of Electrical and Electronics Engineering, J. G. Webster (Ed.) [25].

Chapter 2

Background on Granular Computing

GrC is a computational paradigm devoted to represent, reason on and process basic information, namely granules. Zadeh [4] defines a granule as a clump of points (objects) drawn together by indistinguishability, similarity, proximity or functionality.

GrC can be defined according to different perspectives. Yao [5] defines a triarchic theory of granular computing combining three perspectives: philosophy of structured thinking, methodology of structured problem solving, and mechanism of structured information processing. As structured thinking, GrC allows discovering and reasoning on multi-level abstractions that exist in the real world, and supports analysts in achieving both an accurate and natural description, as well as in-depth understanding, of the inherent structures and complexity of the real world. As a structured problem solving method, GrC is based on a divide and conquer strategy, which promotes the creation and adoption of hierarchical organizations and structures. With this strategy, a problem described with larger granules can be decomposed into a family of sub-problems (top-down) described with smaller granules, and the solution of the problem is obtained by combining the solutions of sub-problems (bottom-up). With respect to the perspective of information processing, GrC offers a way to create and process information granules. The creation of granules is usually refereed to as granulation. The created granules can be considered as basic elements of knowledge. Granules may be built at different levels of abstraction and, by changing the size of the granules, it is possible to hide or reveal a certain amount of details.

Different formal settings, such as set theory, interval calculus, fuzzy sets, rough sets, shadowed sets, can be used for granulation. In each one of these environments, granules and granulation are defined in different ways but, in all cases, granules can be organized in more complex Granular Structures. A wide set of relationships has been developed [34] [28] to organize granules in hierarchies, trees, networks, and so on.

A challenge in GrC is how to design granules in an appropriate way, where the term "appropriate" refers to the creation of information suitable and representative of experiential evidence, a specific context or application domain. Pedrycz et al. [35] [36] have proposed the principle of justifiable granularity as a way to evaluate the performance of informative granules. This principle is based on a trade-off between two measures that do not strictly depend on the specific application: coverage and specificity. In general, coverage is related to the ability of covering data and specificity deals with the level of abstraction of the granule by considering its size. Another criterion to design granules is the principle of uncertainty level preservation [37] [38] that is mainly focused on evaluating the quality of the granulation itself. By considering information granulation as a mapping between input and output, this principle considers the quantification of the uncertainty as an invariant property to be preserved during the process of granulation. The difference between the input and output entropy is considered as an error to be reduced for a proper granulation of information.

As mentioned, for the results presented in this thesis, we have adopted mainly rough sets and some of their extensions (namely, dominance based rough sets and fuzzy probabilistic rough sets) as principal formal setting for granulation, and Ordered Weighted Averaging (OWA) operators to perform aggregations on fuzzy values. Background information on these approaches is given in the following sections.

2.1 Rough Sets and three way decisions

The Rough Set Theory (RST) of Pawlak is a well-known mathematical tool that is useful to deal with imprecise, inconsistent, incomplete information and knowledge [39]. RST can be used to form concepts and infer rules through an equivalence relation [40].

The basic concepts and definitions of RST are reported in the following.

First of all, being S an information system defined as the 4-tuple: $S =< U, R, V, f >$, $R = C \cup D$, where U is a finite non empty set of objects, R is a finite non empty set of attributes, the subsets C and D are called condition and decision attribute sets, respectively. $V = \bigcup_{a \in R} V_a$, where V_a is the set of values of attribute a, and $f : R \to V$ is an information or a description function. Given any subset of attribute set $B \subseteq R$, an indiscernible relation $IND(B)$ on the universe U can be defined as follows,

$$IND\left(B\right) = \left\{ (x, y) \,|\, (x, y) \in U^2, \forall_{b \in B} \left(b(x) = b(y)\right) \right\} \tag{2.1}$$

The equivalence relation is an indiscernible relation, the equivalence class of an object x is denoted by $[x]_{IND(B)}$ and the pair $\left(U, [x]_{IND(B)}\right)$ is an *approximation space*.

Given an information system $S =< U, R, V, f >$, for a subset $X \subseteq U$, its lower approximation set is defined as:

$$\underline{apr}\left(X\right) = \left\{x \in U | \left[x\right] \subseteq X\right\} \tag{2.2}$$

and its upper approximation set by:

$$\overline{apr}\left(X\right) = \left\{x \in U | \left[x\right] \cap X \neq \emptyset\right\}, \tag{2.3}$$

where $[x]$ is the equivalence class of x.

The rough membership for the element $x \in U$ can be defined as:

$$\mu_X(x) = \frac{|X \cap [x]|}{|[x]|} \tag{2.4}$$

and can be used to describe inaccuracy for $x \in X$.

The Three-way Decisions Theory (3WDT) [41] has been introduced to divide the universe U into three disjoint regions: positive (POS), negative (NEG) and boundary (BND). These three regions are viewed, respectively, as the regions of acceptance, rejection, and non-commitment in a ternary classification [42]. More formally, it is possible to define:

$$\begin{gathered} POS(X) = \underline{apr}(X), \\ BND(X) = \overline{apr}(X) - \underline{apr}(X), \\ NEG = U - \overline{apr}(X). \end{gathered} \tag{2.5}$$

If $x \in POS(X)$, then it belongs to target set X certainly. If $x \in NEG(X)$, then it doesn't belong to target set X certainly. As third option, there is the non-commitment region: if $x \in BND(X)$, then it cannot be determined whether the object x belongs to target set X or not.

A variant of traditional rough sets is represented by probabilistic rough sets [43]. In particular, suppose U the universe and let $E \subseteq X \times X$ be an equivalence relation on U. For an element $x \in U$, the equivalence class containing x is $[x]_E = \{y \in U | xEy\}$ and the quotient set of U is denoted by $U/E = \{[x]_E | x \in U\}$. For a particular $X \subseteq U$ containing instances of a concept, $Pr(X|[x]_E)$ denotes the conditional probability of an object in X given that the object is in $[x]_E$. The lower and upper approximations of a concept X are defined by using a threshold pair (α, β) (with $0 \leq \beta < \alpha \leq 1$) as follows:

$$\underline{apr}_{(\alpha,\, \beta)}(X) = \bigcup \{[x]_E \in U/E | Pr(X|[x]_E) \geq \alpha\}, \tag{2.6}$$

$$\overline{apr}_{(\alpha,\, \beta)}(X) = \bigcup \{[x]_E \in U/E | Pr(X|[x]_E) > \beta\}. \tag{2.7}$$

Similarly to eq. (2.5), the (α, β)-probabilistic positive, negative and boundary regions can be defined based on (α, β)-lower and upper approximations, which are also named as probabilistic three-way decision model [44]:

$$POS_{(\alpha,\beta)}\left(X\right) = \underline{apr}_{(\alpha,\beta)}\left(X\right), \tag{2.8}$$

$$NEG_{(\alpha,\beta)}\left(X\right) = \left\{[x]_E \in U/E | Pr\left(X|[x]_E\right) \leq \beta\right\}, \tag{2.9}$$

$$BND_{(\alpha,\beta)}\left(X\right) \ = \ \left\{[x]_E \in U/E |\ \beta < Pr\left(X|[x]_E\right) < \alpha\right\}. \tag{2.10}$$

The conditional probability may be defined as a degree of confidence that an object having the same description as x belongs to X. We accept it to be in X if the confidence level is greater than or equal to level α. The same object may be rejected to be in X if the confidence level is less than or equal to level β. The decision about object may be deferred if the confidence is between the two levels.

In 3WD models [45], it is of fundamental importance the determination of the thresholds, α and β. Several approaches have been proposed based on Shannon entropy [46], chi-square statistic [47], game theory [48].

In [49], authors present a Bayesian Rough Set (BRS) model, where the three regions are defined by using the prior probability as a reference. The two thresholds value is settled to $Pr(X)$. As a consequence, in the BRS model, an object X is classified in the positive region if the posterior probability $Pr(X|E)$ is grater than the prior probability $Pr(X)$. In [49], the local gain $g(X|E) = \dfrac{Pr(X|E)}{Pr(X)} - 1$ is associated with every elementary set E, and can be used as quality measure to evaluate the increase of the degree of certainty of decision making. In [50], the BRS model is further elaborated, and the inverse probabilities ($Pr(E|X)$ and $Pr(E|X^c)$) are compared to define the thresholds. The rule for positive region $Pr(X|E) > Pr(X)$ is equivalent to the inequalities $Pr(E|X) > Pr(E|X^c)$ meaning that the observed evidence is more probable assuming hypothesis X instead of its complement X^c. A pair of thresholds values can be defined on the basis of the likelihood ratio $\dfrac{Pr(E|X)}{Pr(E|X^c)}$ that is called *Bayes Factor*. A formulation of α and β proposed in [50] is:

$$\alpha = \frac{Pr(X)}{Pr(X) + \varepsilon_1^0(1 - Pr(X))} \tag{2.11}$$

$$\beta = \frac{\varepsilon_0^1 Pr(X)}{\varepsilon_0^1 Pr(X) + (1 - Pr(X))} \tag{2.12}$$

where α and β are function of prior probabilities $Pr(X)$ and $Pr(X^c)$, and of two parameters ε_1^0 and ε_0^1 correlated to the Bayes factor.

It is admissible to set $\varepsilon_1^0 = \varepsilon_0^1 = \varepsilon \in [0, 1)$, and we can see that if $\varepsilon \approx 0$ then $\alpha \approx 1$ and $\beta \approx 0$, leading to the traditional rough set regions. If $\varepsilon \approx 1$ it leads to the BRS model with $\alpha \approx Pr(X)$ and $\beta \approx Pr(X)$. Significance scale values for Bayes factor and ε are reported in [50]. Those values are also used in the method presented in section 3.1.1.

2.1.1 Fuzzy Probabilistic Rough Sets

Fuzzy Rough Sets are fuzzy generalization of rough sets introduced in [51]. The idea was the following. Let be X a non-empty universe, R a similarity relation on X, and $F \in$ *F(X)* a fuzzy set. A fuzzy rough set is a pair $(R_*(F), R^*(F))$ s.t. for every $x \in X$:

$$R_*(F)(x) = inf_{y \in X} max\{1 - R(x, y), F(y)\} \tag{2.13}$$

$$R^*(F)(x) = sup_{y \in X} min\{R(x, y), F(y)\} \tag{2.14}$$

Dubois and Prade fuzzy rough sets have been generalized from max, min to border implicators and T-norm. For an overview readers can refer to [52].

Traditional models of fuzzy rough sets do not account for probability distribution. Among the works that integrate probability into fuzzy rough sets, we consider [53] and [54].

Hu et al. [53] introduce the concept of fuzzy probabilistic approximation space as a three-tuple $< U, P, R >$ where U is a non empty universe, P is a probability distribution over U and R is a fuzzy equivalence relation. On a fuzzy probabilistic approximation space, Hu et al. define a measure that can be of interest for us. First, they define the expected cardinality of a fuzzy equivalence class $[x_i]_R$ as:

$$\tau_i = \sum_{j=1}^{n} p(x_j) r_{ij} \tag{2.15}$$

where $p(x_j)$ is the probability of x_j and r_{ij} is the degree of equivalence between x_i and x_j. On the basis of this measure of cardinality they also define the information quantity of a fuzzy relation R_A as:

$$H(R_A, P) = -\sum_{i=1}^{n} p(x_i)\, log\, \tau_i \tag{2.16}$$

The information quantity measures the discernibly power of the subset A.

In [54], fuzzy probabilistic approximation spaces are investigated in relation to 3WD. Authors of [54] recall that the concept of fuzzy event can be useful in situations in which an ”event” is fuzzy rather than crisp, such as a group is *mostly* characterized by the attack strategy bombing/explosion. If $U = \{x_1, ..., x_n\}$ is a finite set and $p_i = Pr(x_i)$ for $i = (1, 2, ..., n)$, the probability of a fuzzy event Ω is [55]:

$$Pr(\Omega) = \sum_{i=1}^{n} \Omega(x_i) p_i \tag{2.17}$$

Given a fuzzy approximation space, a fuzzy event Ω, and a pair of thresholds α and β s.t. $0 \leqslant \beta < Pr(\Omega) < \alpha \leqslant 1$, Zhao and Hu define the α-lower and β-upper approximation spaces of Ω as

[54]: $\underline{R^\alpha(\Omega)} = \{x \in U : Pr(\Omega|[x]_R) \geqslant \alpha\}$, and $\overline{R^\beta(\Omega)} = \{x \in U : Pr(\Omega|[x]_R) > \beta\}$ that in terms of regions is equivalent to:

$$\begin{gathered} POS(\Omega) = \underline{R^\alpha(\Omega)} = \{x \in U : Pr(\Omega|[x]_R) \geqslant \alpha\} \\ NEG(\Omega) = (\overline{R^\beta(\Omega)})^c = \{x \in U : Pr(\Omega|[x]_R) \leqslant \beta\} \\ BND(\Omega) = \overline{R^\beta(\Omega)} - \underline{R^\alpha(\Omega)} = \{x \in U : \beta < Pr(\Omega|[x]_R) < \alpha\} \end{gathered} \tag{2.18}$$

The computation of the conditional probability is defined as follows:

$$Pr(\Omega|[x_t]_R) = \frac{\sum_{i=1}^{n} p(x_i) r_{ti} \Omega(x_i)}{\sum_{i=1}^{n} p(x_i) r_{ti}} \qquad \forall x_t \in U \tag{2.19}$$

that can be written also in terms of the expected cardinality of eq. (2.15).

2.1.2 Dominance Based Rough Sets

Another extension of the rough set model is the dominance-based rough set approach (DRSA) [56] that uses the dominance relation $\succeq$ instead of the equivalence one. This approach defines a preference relation $\succeq_a$ s.t. $x \succeq_a y$ means that x is preferable to y with respect to the attribute $a \in A$. If $x \succeq_a y$ for every $a \in A$, we say that x dominates y, i.e., xD_Ay. For every object x, we can define a set of objects that dominates x and a set of objects that are dominated by x, and these are called cones of dominance and are formalized, respectively, as $D_A^+(x) = \{y \mid yD_Ax\}$ and $D_A^-(x) = \{y \mid xD_Ay\}$.

In our results, we use traditional DRSA for the third method devoted to analyse resilience of targets of attacks in section 3.1.3, and a variant of the DRSA that is based on the concept of stochastic dominance [57], for the secure partition method in section 3.1.2. We report in the following, when possible directly from [57], basic notations and definitions of this DRSA variant, called dominance rough set approach under uncertainty:

- $U = \{u_1, ..., u_m\}$ is a set of objects.

- $Q = D \cup V$ is a set of attributes that describe the objects. In the context of our applications, let be $D \subseteq Q$ a set of domain and/or performance attributes, and $V \subseteq Q$ a set of attributes related to attacks.

- Let $P = \{p_1, ..., p_n\}$ be a set of states of the universe that are mutually exclusive and collectively exhaustive. Let $\lambda = \{\lambda_1, ..., \lambda_n\}$ be an a priori probability distribution over the states, s.t. $\Sigma_{i=1}^{n} \lambda_i = 1$.

- Let $A = \{a_1, ..., a_j\}$ be a set of acts.

- $L = \{L_1, ..., L_r\}$ is a set of outcomes, $l : P \times A \to L$ is a function that associates with a pair (p_n, a_j) a value of L. In our context, the outcomes can be considered losses.

- $\Pi = \{\pi \in [0, 1] \; s.t. \; \pi = P(W), W \subseteq P\}$ is a set of probabilities, where $P(W) = \Sigma_{i:p_i \in W} \lambda_i$ is the probability that one of the states of $W \subseteq P$ is verified.

- $z : A \times P \to \Pi$ and $z^{'} : A \times P \to \Pi$ are two functions assigning to each couple (a_j, p_n) a probability of Π as follows:

  $$z(a_j, p_n) = \Sigma_{y:l(a_j,p_y) \geq l(a_j,p_n)} \lambda_y \tag{2.20}$$

  $$z^{'}(a_j, p_n) = \Sigma_{y:l(a_j,p_y) \leq l(a_j,p_n)} \lambda_y \tag{2.21}$$

  Therefore, $z(a_j, p_n)$ represents the probability of obtaining an outcome whose value is at least $l(a_j, p_n)$ by act a_j. Analogously, $z^{'}$ represents the probability of obtaining an outcome whose value is at most $l(a_j, p_n)$ by act a_j.

- $\rho : A \times \Pi \to L$ and $\rho^{'} : A \times \Pi \to L$ are two functions defined as follows:

  $$\rho(a_j, \pi) = max_{i:z(a_j,p_i) \geq \pi} \{l(a_j, p_i)\} \tag{2.22}$$

  $$\rho^{'}(a_j, \pi) = min_{i:z'(a_j,p_i) \geq \pi} \{l(a_j, p_i)\} \tag{2.23}$$

  These functions report information on outcomes with probabilities. Specifically, $\rho(a_j, \pi) = x$ means that by the act a_j, the outcome is at least (i.e., greater than or equal to) x with a probability of at least π. For $\rho^{'} = x$, by the act a_j, the outcome is at most (i.e., smaller than or equal to) x with a probability of at least π.

As reported in [57], if we order the probabilities of Π, e.g., $0 = \pi_0, \pi_1, \pi_2..., \pi_n = 1$ where $n = |\Pi|$, we have $\rho(a_j, \pi_i) = \rho^{'}(a_j, \pi_{1-i})$; therefore, we can reason in terms of ρ or $\rho^{'}$ independently.

Before concluding this section, we report a definition of stochastic dominance as follows [58] [57]: given two acts a and b, a dominates b iff, for each outcome x, a gives an outcome at least as good as x with a probability at least as great as the probability that b gives the same outcome.

2.2 Ordered Weighted Averaging operators

The Ordered Weighted Averaging (OWA) operator has been defined by Yager [59] and provides a general class of mean like aggregation operation. It has been extensively used and has the possibility of implementing different types of aggregation by simply changing parameters associated to OWA. Another interesting aspect of OWA is that in some situations the weights generation function can be expressed in natural language with linguistic labels (such as Relaxed, Moderated, and so on).

In this section we report only basic information on OWA and, in particular on OWA with probability distribution over the arguments, that is the method we are going to use for derivation of attack scenarios in section 3.1.1. Interested readers can refer to [60] for details.

An OWA operator is a mapping $F : R^n \to R$. Given a set of n weights $w_j \in [0, 1]$ s.t. $\sum_{j=1}^{n} w_j = 1$ and a set of n values to aggregate $(a_1, a_2, ..., a_n)$, OWA is evaluated as:

$$F(a_1, a_2, ..., a_n) = \sum_{j=1}^{n} w_j a_{\rho(j)} \qquad (2.24)$$

where ρ is an index function s.t. $\rho(j)$ is the index of the $j-th$ largest a_i. Special cases of OWA are max (when $w_1 = 1$ and the others weights are 0), min (when $w_n = 1$ and the others weights are 0), and mean (when $w_j = 1/n \, \forall j$).

In [61], OWA aggregations are considered in the case we have a probability distribution over the arguments. So, in addition to the set of n values to aggregate, we have a set of n probabilities p_i s.t. $\sum_{i=1}^{n} p_i = 1$ and:

$$F((a_1, p_1), (a_2, p_2), ..., (a_n, p_n)) = \sum_{j=1}^{n} (f(T_j) - f(T_{j-1})) a_{\rho(j)} \quad (2.25)$$

where $T_j = \sum_{k=1}^{n} p_{\rho(k)}$. Readers can refer to [60] for details and a discussion on properties of T_j and $f(T_j)$. We conclude mentioning that, for derivation of attack scenarios in section 3.1.1, as weights generation function we use $f(x) = x^{\gamma}$ that is interesting because the γ parameter allows to generate values ranging from the min (when $\gamma = \infty$, since $x < 1 \longrightarrow f(x) = 0$ and $f(1) = 1$) to the max (when $\gamma = 0$, since $x > 0 \longrightarrow f(x) = 1$ and $f(0) = 0$), and this flexibility is useful for derivation of attack scenarios ranging from low probability - high risk to high probability - low risk scenarios.

Chapter 3

The approximate reasoning methods to support Intelligence Cycle Stages

This chapter presents the three methods defined in this research study that, with the support of fig. 3.1, we are going to outline here before describing them in detail. As we mentioned in the Introduction chapter, the Intelligence Cycle [9] is the glue among the presented results. In fig. 3.1, each method is enclosed in a dashed square. Curved arrows represent the information that is required. This information can be collected, analysed, processed and disseminated within an intelligence cycle. Furthermore, to reinforce the link with the different forms of guidance expected by an intelligence cycle, left-hand side of fig. 3.1 reports questions at strategic, tactical and operational levels that are answered by the methods.

The first method is devoted to create, analyse and assess hypotheses of attacks from terrorist groups. It uses historical information on terrorism events to model the behaviour of terrorist groups, information on possible attacks and probabilities that groups are active in the time period and geographical context under analysis. The output of this method is twofold. First, it produces a wide spectrum of hypotheses of attack aggregating, in

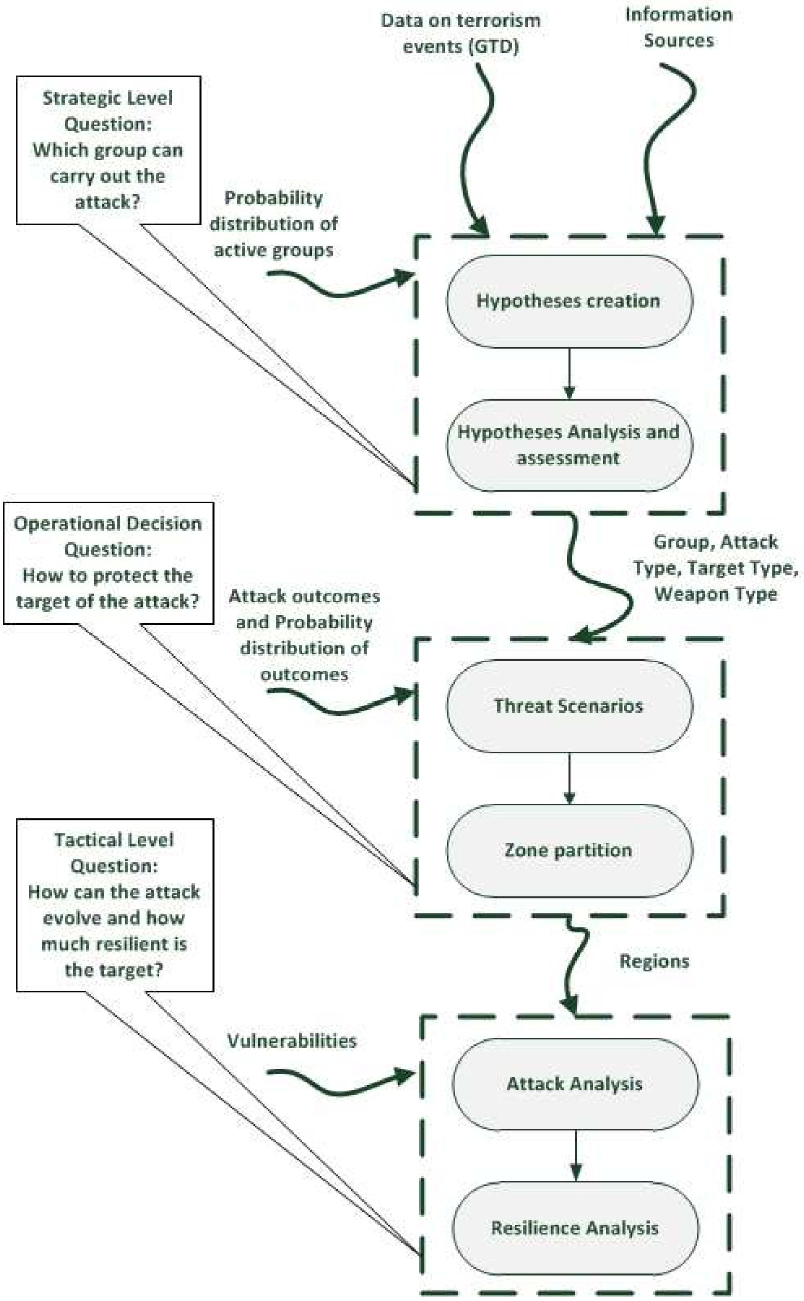

Data on terrorism events (GTD)
Information Sources
Strategic Level Question: Which group can carry out the attack?
Probability distribution of active groups
Hypotheses creation
Hypotheses Analysis and assessment
Operational Decision Question: How to protect the target of the attack?
Group, Attack Type, Target Type, Weapon Type
Attack outcomes and Probability distribution of outcomes
Threat Scenarios
Zone partition
Tactical Level Question: How can the attack evolve and how much resilient is the target?
Regions
Vulnerabilities
Attack Analysis
Resilience Analysis

Figure 3.1: Overview of the three methods

different ways, information on possible attacks. The range of hypotheses spans from *optimistic* scenarios (i.e., Low Impact - High Probability scenarios) to *pessimistic* (i.e., High Impact - Low Probability scenarios) and, as second output, these hypotheses can be analysed and assessed with regards to possible perpetrators of attacks, on the basis of available evidence.

The second method starts from this information, characterized by uncertainty, about a possible threat, and has the objective of creating a secure partition of the area or the infrastructure that is under attack. This initial information is refined to derive and analyse a set of threat scenarios. A threat scenario is defined as a combination of an *act*, its *outcomes* and the *probability distribution* of these outcomes. An act is an attack targeting some objects and has outcomes in terms of losses/damages. The values of outcomes depend on how the target areas are defended (e.g., a red zone should be better defended than a green one), and the probability distribution of the outcomes depends on how the zones are created (e.g., if an act can impact on objects in one or more zones). The modification of the partition, therefore, involves a change of the outcomes and of how they are distributed. The method finds the optimum partition by respecting a requirement of maximum acceptable losses/damages.

The output of the second method can be formalised in a decision table that partitions the area or the infrastructure under analysis in three regions, namely red, yellow and green, with different security requirements. Starting from these regions, and considering the dependencies among objects of these regions, the third method performs a resilience analysis to evaluate how the attack can evolve and its consequences.

3.1 An unifying scenario

The methods are described with the support of an unifying scenario shown in fig. 3.2, which gives indication on the correspondence between a phase of the scenario and the section of this thesis reporting the specific method to execute the phase.

3.1.1 Analysis and Assessment of attack hypotheses[1]

Let us suppose that from a set of intelligence sources (such as informants, social media monitoring services, confidential reports) information comes up about possible attacks. This information can refer to attack strategies, types of weapons to be adopted, types of targets. The decision maker, at this point, starts an activity of analysis of the possible scenarios compatible with such information. A number of them can be hypothesized to identify situations of high probability - low impact, let us call *optimistic*, and vice versa, let us call *pessimist* (see fig. 3.3)

One of the objectives of the analysis is to establish, with a certain degree of certainty, the possible perpetrator(s) of the attack. This also serves to better understand the degree of danger of the threat. To do this, the decision maker collects evidence and evaluates the scenarios created based on the body of available evidence. The evaluation is done following a three way approach and, therefore, the set of possible perpetrators is divided in three regions: a positive (POS) region including the groups that can perpetrate the attack, a negative (NEG) region including the groups that can not perpetrate the attack, and a boundary (BND) region including the groups for which the analyst can not take decisions (see fig. 3.4). This kind of analysis can be done for different scenarios, such as optimistic and pessimistic (see the abscissa axis in fig. 3.4), and the results can be more or less supported by the body of evidence (see the ordinate axis in fig. 3.4). The analysis is interactive and the decision maker can use two parameters, γ and ε.

From a formal point of view, the proposed method combines fuzzy and rough sets with probability theory, and is shown in fig. 3.5.

[1] The method presented in this section has been proposed and accepted for publication in [31]

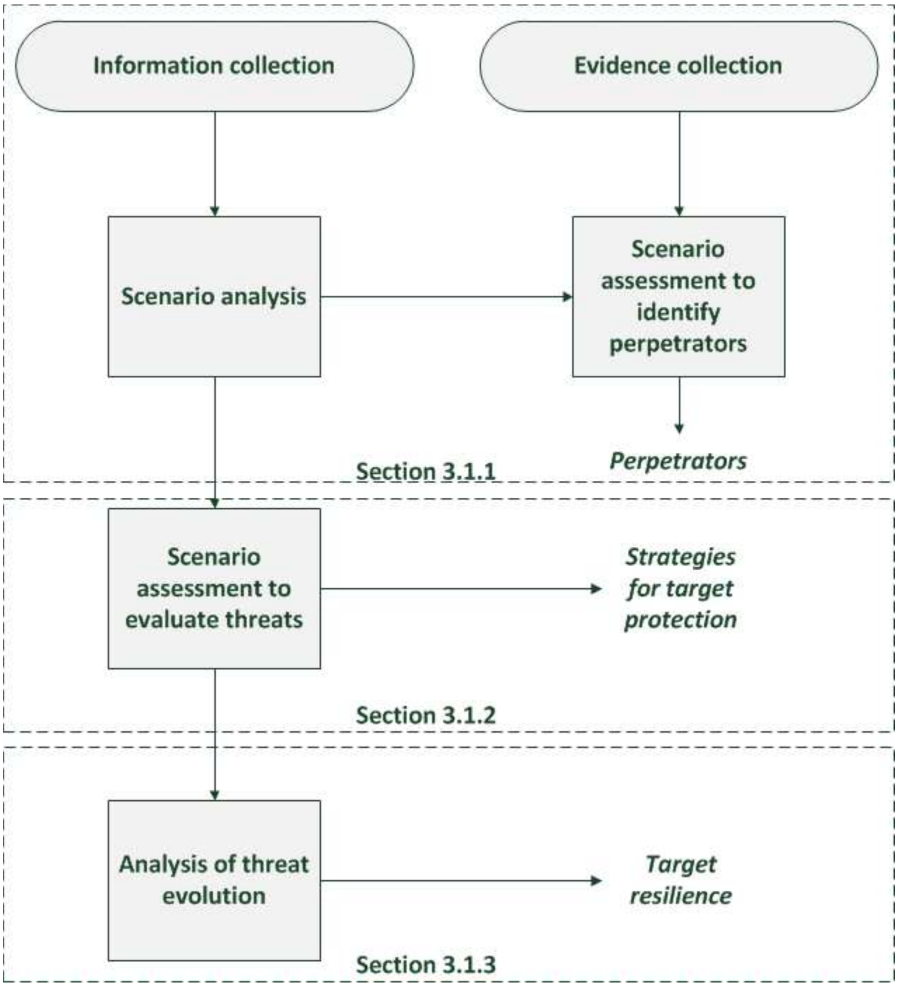
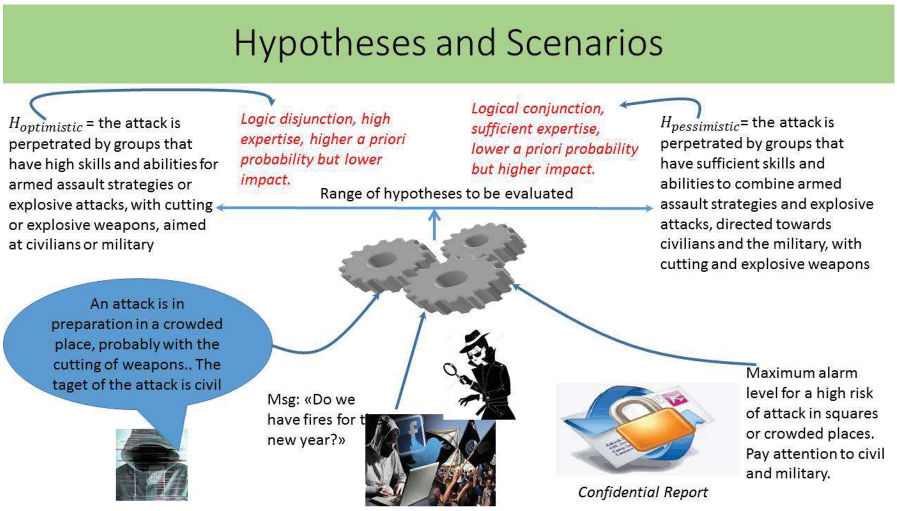

Information collection
Evidence collection
Scenario analysis
Scenario assessment to identify perpetrators
Perpetrators
Section 3.1.1
Scenario assessment to evaluate threats
Strategies for target protection
Section 3.1.2
Analysis of threat evolution
Target resilience
Section 3.1.3

Figure 3.2: Unifying scenario



Hypotheses and Scenarios

$H_{optimistic}$ = the attack is perpetrated by groups that have high skills and abilities for armed assault strategies or explosive attacks, with cutting or explosive weapons, aimed at civilians or military

Logic disjunction, high expertise, higher a priori probability but lower impact.

Logical conjunction, sufficient expertise, lower a priori probability but higher impact.

$H_{pessimistic}$= the attack is perpetrated by groups that have sufficient skills and abilities to combine armed assault strategies and explosive attacks, directed towards civilians and the military, with cutting and explosive weapons

Range of hypotheses to be evaluated

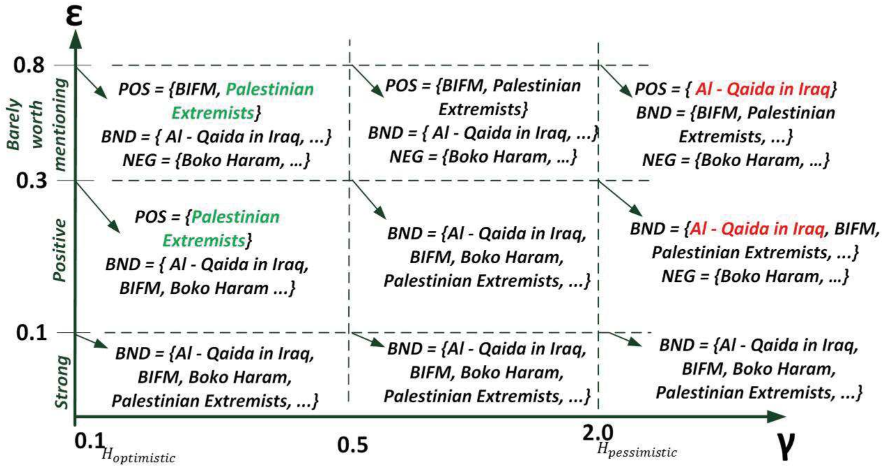
An attack is in preparation in a crowded place, probably with the cutting of weapons.. The taget of the attack is civil

Msg: «Do we have fires for t new year?»

Confidential Report

Maximum alarm level for a high risk of attack in squares or crowded places. Pay attention to civil and military.

Figure 3.3: Hypotheses and Scenarios



	0.1	0.5	2.0

0.8	POS = {BIFM, Palestinian Extremists}
	BND = { Al - Qaida in Iraq, ...}
	NEG = {Boko Haram, ...}
		POS = {BIFM, Palestinian Extremists}
		BND = { Al - Qaida in Iraq, ...}
		NEG = {Boko Haram, ...}
			POS = { Al - Qaida in Iraq}
			BND = {BIFM, Palestinian Extremists, ...}
			NEG = {Boko Haram, ...}

0.3	POS = {Palestinian Extremists}
	BND = { Al - Qaida in Iraq, BIFM, Boko Haram ...}
		BND = {Al - Qaida in Iraq, BIFM, Boko Haram, Palestinian Extremists, ...}	BND = {Al - Qaida in Iraq, BIFM, Palestinian Extremists, ...}
			NEG = {Boko Haram, ...}

0.1	BND = {Al - Qaida in Iraq, BIFM, Boko Haram, Palestinian Extremists, ...}	BND = {Al - Qaida in Iraq, BIFM, Boko Haram, Palestinian Extremists, ...}	BND = {Al - Qaida in Iraq, BIFM, Boko Haram, Palestinian Extremists, ...}

Figure 3.4: Tri-partition of the groups

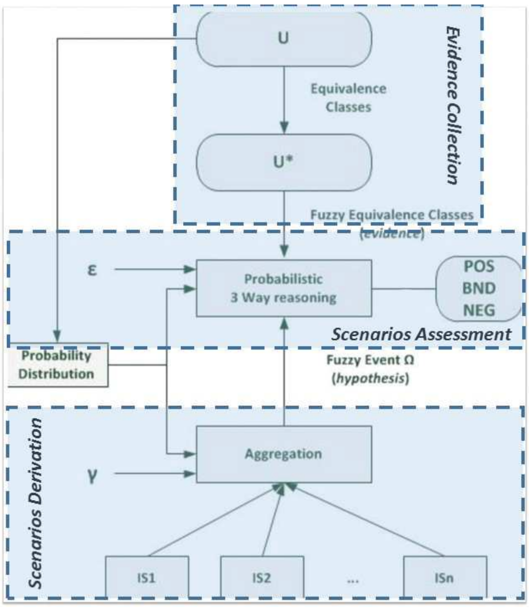


Figure 3.5: Overview of the method (elaborated from [31])

It consists of three parts devoted, respectively, to: *i)* create a body of evidence from historical data on terrorism events, *ii)* derive a set of scenarios from the information of Intelligence Sources (IS), and *iii)* make an assessment of these scenarios to identify possible perpetrators of the attack.

i): Evidence collection. The first part relates to the collection of evidence. The starting point is a data set of terrorism events, U, correctly classified with respect to perpetrators[2]. An object of U has to be described with an attack strategy, a target type, and a weapon type used to perpetrate the attack. A triple $< attack\ strategy, target\ type, weapon\ type >$ is what we refer to as attack pattern. An example of U is reported in table 3.1, where AT is attack type, TT target type, WT weapon type and D is the group perpetrating the attack. AT, TT, and WT are categorical attributes that describe an attack pattern. Let us suppose that

[2] Here and in the following, perpetrator refers to the group that has perpetrated the terrorist attack

AT can take 3 values, TT can take 4 values and WT can take 3 values.

Table 3.1: Attack Event Dataset (from [31])

	AT	TT	WT	D
e1	3	2	2	g1
e2	2	4	3	g1
e3	3	2	2	g1
e4	3	4	3	g2
e5	3	2	1	g2
e6	2	1	3	g2
e7	3	3	2	g3
e8	3	4	3	g3
e9	3	3	2	g3
e10	1	4	3	g3

From U, we derive a new data set, U^*, reporting information on groups behaviour. For each group we create an object of U^* and describe this object in terms of relative frequencies of attack strategies, target types and weapon types. We can regard a relative frequency of specific attack strategy (e.g., bombing/explosion) as a degree of membership of this strategy to a group. In a similar way, we consider the relative frequencies of a target type and a weapon type. Objects of U^* can be considered as fuzzy models of groups behaviour. U^* can be easily created using elementary granules of knowledge (i.e., equivalence classes) from U.

More formally: let be (U, A, V) a decision table with U an universe of objects, $A = C \cup D$ a set of attributes, and V a set of attributes values. Let be C the set of conditional attributes, D the set of decisional attributes, and $C \cap D = \phi$.

Let be U^* the partition of U induced by D, $U^* = \{U/D\} = \{[d_1], ..., [d_n]\}$ with $n = |D|$, where $| \cdot |$ is a measure of cardinality. Let be C^*_{ip} the partition of U induced by the $i-th$ conditional attribute and $p-th$ decisional attribute $C_{ip} = \{c_i, d_p\}$, $C^*_{ip} = \{U/C_{ip}\} = \{[c_{ip}]_1, ..., [c_{ip}]_m\}$ with $m = |V_{C_i}|$ where $V_{C_i} \subseteq V$ is the subset of all the values admissible for c_i.

Let us define $f : C_i \times V_{C_i} \to A_i^*$. f generates a new attributes set A_i^* derived from the conditional attribute c_i. This set has the same cardinality m of V_{C_i}. Let us define an information function $s : U^* \times A_i^* \to V(A_i^*)$ s.t. for any $u^* \in U^*$ and $a* \in A_i^*$ we have: $s(u^*, a^*) = v(a_l^*) = \dfrac{|[c_{ip}]_l|}{|[d_p]|}$ for $l = 1, ..., m$.

Now let be $A^* = \cup_i \{A_i^*\}$ and $V^* = \cup_i \{V(A_i^*)\}$, and we can define an information system (U^*, A^*, V^*)

An example is reported in table 3.2. In this case, U^* derives from the table 3.1. We can observe that there are 3 conditional attributes ($i = 1, 2, 3 = AT, TT, WT$) and 3 classes ($p = 1, 2, 3 = g1, g2, g3$). $U^* = \{U/D\}$ consists of the following equivalence classes: $\{[g]_1, [g]_2, [g]_3\} = \{\{e1, e2, e3\}, \{e4, e5, e6\}, \{e7, e8, e9, e10\}\}$. For $i = 1$ and $p = 1$, we evaluate the partition of U induced by the first conditional attribute AT and the first group $g1$: $C^*_{AT1} = \{[AT_1]_1, [AT_1]_2, [AT_1]_3\} = \{\{\phi\}, \{e2\}, \{e1, e3\}\}$. From f we have $A^*_{AT} = \{AT1, AT2, AT3\}$ and from s, in the case of group 1 (i.e., $u^* = [g]_1$), we have $V(A^*_{AT}) = \{0, 1/3, 2/3\}$.

We repeat these steps for the other conditional attributes: $C^*_{TT1} = \{[TT_1]_1, [TT_1]_2, [TT_1]_3, [TT_1]_4\} = \{\{\phi\}, \{e1, e3\}, \{\phi\}, \{e2\}\}$; $C^*_{WT1} = \{[WT_1]_1, [WT_1]_2, [WT_1]_3\} = \{\{\phi\}, \{e1, e3\}, \{e2\}\}$. From f and s: $A^*_{TT} = \{TT1, TT2, TT3, TT4\}$, $A^*_{WT} = \{WT1, WT2, WT3\}$, and $V(A^*_{TT}) = \{0, 2/3, 0, 1/3\}$, $V(A^*_{WT}) = \{0, 2/3, 1/3\}$.

A similar procedure is applied for $u* = [g]_2$ and $u* = [g]_3$, and we have the results reported in table 3.2.

A row of U^* represents a fuzzy model of the behaviour of a group with respect to its attacks strategies, targets and weapons adoption.

Table 3.2: Fuzzy models of group behaviour (from [31])

	AT1	AT2	AT3	TT1	TT2	TT3	TT4	WT1	WT2	WT3
g1	0	0,333333	0,666667	0	0,666667	0	0,333333	0	0,666667	0,333333
g2	0	0,333333	0,666667	0,333333	0,333333	0	0,333333	0,333333	0	0,666667
g3	0,25	0	0,75	0	0	0,5	0,5	0	0,5	0,5

From U^* we use a fuzzy equivalence relation, R, to derive a body of evidence in the form of fuzzy equivalence classes. When derived from U^*, in fact, a fuzzy equivalence class is a sort of *evidence* that a group behaves more or less similarly to others. With the addition of a probability distribution, P, we construct a fuzzy probabilistic approximation space, $< U^*, P, R >$, as defined in [53] (see section 2.1.1). A $p_i \in P$ is the probability that a group g_i is active in the time period and geographical context under analysis. P is derived from U referring the number of events of g_i to the total number of events in U.

Specifically, as fuzzy relation, we adopt the Gaussian kernel:

$$k(a,b) = exp(-\frac{|a-b|}{2\sigma^2}) \tag{3.1}$$

that, as described in [62], induces a fuzzy relation satisfying the properties of reflexivity and symmetry, and as shown in [63] [64] is $T_{cos} - transitive$, where $T_{cos}(a,b) = max(ab - \sqrt{1-a^2}\sqrt{1-b^2}, 0)$ is a t-norm. Thus any fuzzy relation computed with Gaussian kernel is a T_{cos} equivalence relation [62]. An interesting property of Gaussian kernel is that the kernel induced by the individual fuzzy relations [62] comes in the form:

$$R^n_{GK}(x_i, x_j) = \prod_{s=1}^{n} R^s_{GK}(x_i, x_j) \tag{3.2}$$

Let us give an example of evidence collection. Let be $\{A^*_{AT}\} \subset \{A^*_{AT} \cup A^*_{TT}\} \subset A^*$ a nested sequence of attributes. Using eq. (3.1) we have the three similarity matrices reported in tables 3.3, 3.4 and 3.5. Since $A^* = AT^* \cup TT^* \cup WT^*$ we can derive from tables 3.5 and 3.4 a similarity matrix for WT^* using eq. (3.2): $SIM_{WT^*} = \dfrac{SIM_{A^*}}{SIM_{A^*_{AT} \cup A^*_{TT}}}$ shown in table 3.6.

These tables can be analysed to reason on similarity of behaviour of groups with respect to different attributes. For instance, table 3.3 reflects the fact that $g1$ and $g2$ adopt the same attack strategies, and table 3.6 informs that $g1$ and $g3$ are similar with respect to the selection of weapon types. Besides this, they describe the fuzzy partition of the universe in terms of fuzzy equivalence classes of groups. These are basic elements of knowledge

Table 3.3: $SIM_{A^*_{AT}}$

	g1	g2	g3
g1	1	1	0.6447183
g2	1	1	0.6447183
g3	0.6447183	0.6447183	1

Table 3.4: $SIM_{A^*_{AT} \cup A^*_{TT}}$

	g1	g2	g3
g1	1	0,582611	0,111391
g2	0,582611	1	0,191193
g3	0,111391	0,191193	1

Table 3.5: SIM_{A^*}

	g1	g2	g3
g1	1	0,115216	0,097318
g2	0,115216	1	0,074282
g3	0,097318	0,074282	1

Table 3.6: SIM_{WT^*}

	g1	g2	g3
g1	1	0,197759	0,873664
g2	0,197759	1	0,388519
g3	0,873664	0,388519	1

for 3 way reasoning and, thus, we may understand that the discernibility power of a relation can play a key role in classification. Here the measures introduced by Hu et al. in [53] and reported in section 2.1.1 are of interest for our cases since include probabilities of objects.

Let us better explain the importance of probabilities in our context with an example similar to the one reported in [53]. Let us suppose two relations, $R1$ and $R2$, an look at tables 3.7 and 3.8. They seem to have a similar discernibility power, allowing to differentiate one group in both the cases. This is confirmed if we evaluate the information quantity using eq. (2.16) of section 2.1.1 in the case of objects uniformly distributed, i.e. $p(g_i) = \frac{1}{3}$. In this case: $H(R1) = H(R2) = 0.041$.

Table 3.7: SIM_{R1}

	g1	g2	g3
g1	1	1	0.8
g2	1	1	0.8
g3	0.8	0.8	1

Table 3.8: SIM_{R2}

	g1	g2	g3
g1	1	0.8	1
g2	0.8	1	0.8
g3	1	0.8	1

However the if we consider the probability distribution of our example, $Pr = (3/10, 3/10, 4/10)$, it results that: $H(R1) = 0.044$, $H(R2) = 0.038$ with $H(R1) > H(R2)$. This is the effect of probabilities: since $p(g3)$ is greater than $p(g1)$ and $p(g2)$, and $g3$ is separable with $R1$, the discernibility power of $R1$ is higher than the one of $R2$.

For terrorism groups analysis this has an important consequence: relations with high discernibility power induce partitions that tend to better separate more active groups (e.g., with high probability values) to less active ones.

ii): Scenarios derivation. The second part of the method is focused on the derivation of scenarios, such as the pessimistic and optimistic ones already mentioned, starting from the information of the IS. These scenarios are based on hypotheses related to terrorism attack events, which are modelled as fuzzy events such as: a group with a certain degree of expertise (e.g., low, medium, high) can perpetrate the attack. More formally, they are modelled as:

$$\Omega = \frac{\lambda_1}{g_1} + \frac{\lambda_2}{g_2} + ... + \frac{\lambda_n}{g_n} \tag{3.3}$$

where n is the number of known groups, $+$ is the union operator and λ_i is a degree of similarity between the group g_i and the Target Group (TG). TG refers to the group that could perpetrate the hypothetical event, and if we define a way to create a behavioural profile of this TG we can use a similarity measure, such as the one proposed in [65], to evaluate the extent to which the behaviour of a known group is similar to the target one. Values of λ_i in eq. (3.3) can be obtained with:

$$\lambda_i = Sim(G_i, TG) = \frac{|G_i \cap TG|}{|G_i|} \tag{3.4}$$

Eq. (3.4) gives information on how much the profile of a know group, G_i, is similar to the profile of the target one, TG, by comparing the common elements between these two profiles and referring this number to the elements of G_i. Let us note that in general $Sim(G_i, TG) \neq Sim(TG, G_i)$.

The challenge is how to profile TG. The approach we follow is to start from information of intelligence sources, $IS_1, ..., IS_n$, about patterns of attacks, derive some values referring to these patterns from the active groups, and aggregate these values. Here OWA operators are interesting since allow different kinds of aggregation, supporting derivation of different cases: from *pessimistic* one referring, generally, to situations where also groups with a relative low experience on the patterns assumed by the IS can carry out the attack combining all the patterns, to *optimistic* one referring, generally, to situations where groups with a relative high experience on the patterns assumed by the IS can carry out one of the pattern. The two situations mentioned refer respectively to *low probability - high impact* and *high probability - low impact* scenario analysis.

To create a profile of TG, we use a concept similar to the user signature defined in [65]. First, we create profiles of the known groups with respect to the types of information of our interest. For the triples $< AT, TT, WT >$ we derive a fuzzy set starting from the data set of events in table 3.1: $G_i = \hat{AT} \times \hat{TT} \times \hat{WT}$ where $\hat{AT}$, $\hat{TT}$ and $\hat{WT}$ are the fuzzy sets derived following the approach of user signature in [65] [66] and we use min as a tNorm. G_i is a fuzzy set of the co-occurrences of $< AT, TT, WT >$ for the group g_i, and can be written as: $G_i = \{\frac{\mu_{AT_aTT_bWT_c}}{ATaTT_bWT_c}\}$ where

$$\mu_{AT_aTT_bWT_c} = \begin{cases} min(\mu_{AT_a}, \mu_{TT_b}, \mu_{WT_c}), & \text{If a co-occurrence} \\ & \text{exists.} \\ 0, & \text{Otherwise.} \end{cases}$$

We assume: *i)* IS are trusted, *ii)* information on patterns of attack refers to elements (e.g., attack strategies, weapon types) available in the data set, and *iii)* we have not a probability distribution that can be associated to IS (e.g., if two out of three IS report the same information, this does not represent information with greater probability).

Let us suppose $IS1$ gives the following information: the hypothesis of attack follows the pattern $< AT2, TT1, WT3 >$. We can derive n values associated to this pattern, if n is the number of active group. We use OWA with probability distribution over the arguments to aggregate the n values and obtain one value for this pattern that will be associated to TG. The probability distribution we use is the probability distribution of activity of the groups. We repeat the procedure for all the IS and we create a profile of TG. Then we can use a tNorm, such as min, to evaluate the cardinality of $G_i \cap TG$ in eq. (3.4).

The parameter γ of OWA has influence on the aggregation procedure. Variations of γ from ∞ to 0 lead to results that can vary between the minimum and maximum of the values to be aggregated, and therefore the construction of TG profiles with different behaviours (e.g., more or less similar to groups with low or high degrees of experience in the execution of a pattern). This allows the derivation of different scenarios to be investigated based on different fuzzy events Ω that can move in the range $\Omega_{\gamma\to\infty}$ (e.g., a group with very low experience can carry out the attack) to $\Omega_{\gamma\to 0}$ (e.g., a group with very high experience can carry out the attack).

Let us give an example of derivation of Ω for 3 scenarios.

Let us suppose two IS agree on an attack towards military units ($TT4$) with a weapon whose components are produced from radioactive material ($WT3$). They diverge on the attack strategy supposing, respectively,a bombing/explosion ($AT3$) and an armed assault ($AT2$). From table 3.1 we construct the fuzzy profiles of the groups (only the elements for which the membership is $\neq 0$ are reported):

$G_1 = \{\frac{0.667}{AT_3TT_2WT_2}, \frac{0.333}{AT_2TT_4WT_3}\}$;

$G_2 = \{\frac{0.333}{AT_3TT_2WT_1}, \frac{0.333}{AT_2TT_1WT_3}, \frac{0.333}{AT_3TT_4WT_3}\}$;

$G_3 = \{\frac{0.5}{AT_3TT_3WT_2}, \frac{0.25}{AT_1TT_4WT_3}, \frac{0.5}{AT_3TT_4WT_3}\}$.

The values to aggregate for the first IS are $IS1 = (0, 0.333, 0.5)$ and the probability distribution is $Pr = (3/10, 3/10, 4/10)$. Since $IS1_3 > IS1_2 > IS1_1$ the order of indexes is $\rho_1 = 3$, $\rho_2 = 2$ and $\rho_3 = 1$. The values of T are: $T_1 = 0.4$, $T_2 = 0.7$, and $T_3 = 1$ and we can use these values to generate the weights for the OWA using the generation function parametrized on γ: $f(T) = T^\gamma$. Let use consider three cases: $\gamma = \infty$, $\gamma = 0.5$ and $\gamma = 0$ and associate to these cases three labels: *pessimistic*, *moderated*, and *optimistic*. These labels refer to the creation of fuzzy events modelling different hypotheses.

The OWA values are: $IS1_{pessimistic} = 0$, $IS1_{moderated} = 0.384$, and $IS1_{optimistic} = 0.5$. The first and the third correspond to the minimum and maximum values of $< AT_3, TT_4, WT_3 >$ of the three groups. We can repeat the same operations for $IS2 =<$

$AT_2, TT_4, WT_3 >$ and obtain: $IS2_{pessimistic} = 0$, $IS2_{moderated} = 0.183$, and $IS2_{optimistic} = 0.333$

The fuzzy profile of the TG group in the *moderated* case is: $TG = \{\frac{0.384}{AT_3TT_4WT_3}, \frac{0.183}{AT_2TT_4WT_3}\}$. In the other two cases, *pessimistic* and *optimistic*, the membership values for the two elements are the respective OWA values. Using eq. (3.4) and (3.3) we have: $\Omega_{pessimistic} = \frac{0}{g_1} + \frac{0}{g_2} + \frac{0}{g_3}$, $\Omega_{moderated} = \frac{0.183}{g_1} + \frac{0.333}{g_2} + \frac{0.307}{g_3}$, and $\Omega_{optimistic} = \frac{0.333}{g_1} + \frac{0.333}{g_2} + \frac{0.400}{g_3}$.

We note that $\gamma = \infty$ and $\gamma = 0$ are theoretical values and, in the experimentation reported in section 4.1, we use different values to model pessimistic and optimistic scenarios.

iii): Assessment of scenarios to identify perpetrators. The derived hypotheses must be assessed with the support of evidence, and the last phase evaluates Ω using probabilistic three way reasoning methods such as the ones reported in the section 2.1.1. The computation of conditional probabilities is done with eq. (2.19) of section 2.1.1. Using the BRS model summarized in section 2.1, the evaluation of α and β is parametrized on ε according to eq. (2.11) and (2.12) of section 2.1. ε gives information on the evidence supporting Ω. From [50] we know that:

Ω *is* $\varepsilon -$ *positively verified, if and only if* $Pr([g]|\Omega^c) \leqslant \varepsilon Pr([g]|\Omega)$

and that for lower values of $\varepsilon \in [0, 1)$, the positive hypothesis verification under the evidence $[g] \in \frac{U}{R_B}$ requires more significant advantage of $Pr([g]|\Omega)$ over $Pr([g]|\Omega^c)$.

So, the second parameter of the method, ε, has an influence on setting the three way decision thresholds in the BRS model. In particular, variations of ε from 1 to 0 lead to enlargements of the boundary region. This fact implies that more evidence is required in support of the hypothesis Ω.

The decision procedure of the method is shown in fig. 3.6, where the boxes related to collection of information and derivation of hypotheses refer to part *ii)* of the method, the box related to

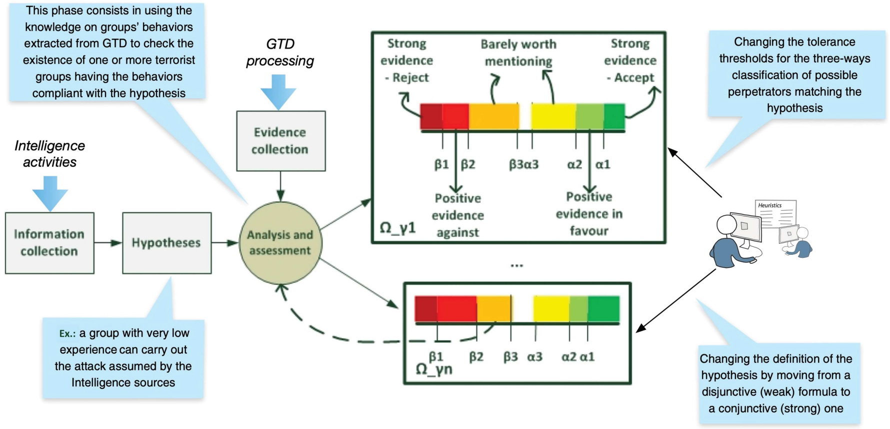

This phase consists in using the knowledge on groups' behaviors extracted from GTD to check the existence of one or more terrorist groups having the behaviors compliant with the hypothesis
GTD processing
Evidence collection
Intelligence activities
Information collection
Hypotheses
Analysis and assessment
Ex.: a group with very low experience can carry out the attack assumed by the Intelligence sources
Strong evidence - Reject
Barely worth mentioning
Strong evidence - Accept
β1 β2 β3α3 α2 α1
Positive evidence against
Positive evidence in favour
Ω_γ1
...
β1 β2 β3 α3 α2 α1
Ω_γn
Changing the tolerance thresholds for the three-ways classification of possible perpetrators matching the hypothesis
Heuristics
Changing the definition of the hypothesis by moving from a disjunctive (weak) formula to a conjunctive (strong) one

Figure 3.6: Decision Making Process (from [31])

collection of evidence refers to part *i)*.

As mentioned, different values of γ allow to derive hypotheses that model different scenarios.

Let us discuss the analysis and assessment of $\Omega_{\gamma 1}$ derived with a specific value of γ. With 3WD, the decision maker can classify the groups under analysis in three regions: a positive region (POS) where s/he can accept the hypothesis that the groups falling in this region may perpetrate the attack, a negative one (NEG) where s/he can reject the hypothesis that the groups falling in this region may perpetrate the attack, and a non commitment one (BND) where s/he needs additional information to take decision. Let us suppose $\Omega_{\gamma 1}$ refers to a low value of ε. As already discussed, low values of ε bring to large boundary regions, and to decision results that are more supported by evidence. Let be $\alpha 1$ and $\beta 1$ the two thresholds obtained with this value of ε for $\Omega_{\gamma 1}$. The decision maker can accept the hypothesis that groups in the POS region (shown with a dark green colour in fig. 3.6) can perpetrate the attack, and can reject groups in the NEG region (with dark red colour in fig. 3.6) as perpetrators. The decisions taken with low values of ε are strongly supported by evidence. However, between $\beta 1$ and $\alpha 1$, the decision maker can not take decisions with the same level of support. S/he should defer the decision awaiting new information on the target sub-type, a specific weapon, or other details that can not be available in the early stages of analysis. So, the decision maker can decide to reassess the hypothesis with a reduced support of evidence, using a higher value of ε. This means the creation of new regions (shown with light green and light red colours in fig. 3.6), with a reduction of the non commitment one and, thus, new information can emerge. The trade off is, however, that this information is less supported by the evidence.

The decision maker can also start the assessment with a high value of ε to obtain preliminary information (barely noteworthy, the orange and yellow regions in fig. 3.6) and proceed with a reassessment reducing the values of ε to verify if these indications are better supported by evidence. This way of working is illustrated with the dashed line in fig. 3.6.

Using the two parameters, γ and ε, the decision maker can therefore derive and assess several scenarios against the body of evidence, obtaining results that can be more or less supported by evidence. The scenarios, as stated previously, can consider *pessimistic* and *optimistic* cases. The decision maker can also understand how groups behave when moving among these types of scenarios.

First, we clarify why the term *experience* used as a predicate that can vary its degree (e.g., between very low and very high) is realistic in the phenomenon of terrorism. Terrorism is a human phenomenon, not deterministic, but the success of a terrorist attack, as well as the mere possibility of executing it, are not the result of chance. Behind the execution of a particular attack pattern, there are several factors including training, skills, availability of information and weapons, which make the difference in the possibility that a group has or does not have to carry out an attack. We decided to group all these elements together into the term *experience* and measure it based on the historical information of a group.

Now, we believe that a method of analysis that has the ability to reveal the degree of a group's experience with respect to a pat-

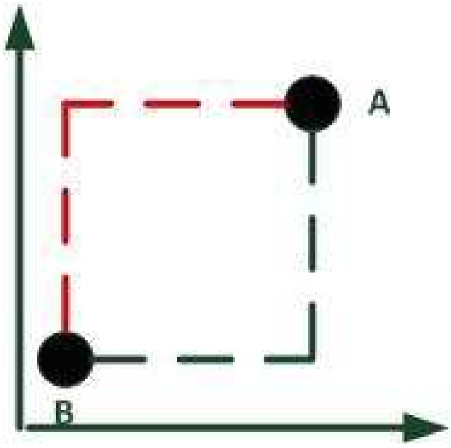


Figure 3.7: Horizontal and Vertical movements

tern, or a combination of attack patterns, offers a higher and more useful knowledge than a simple classification or prediction result. To better clarify the usefulness of the method, we can make an analogy with the difference between trajectory and position. The first represents the movement an object makes to get to a position. It is clear that his knowledge is superior, also due to the mere fact of being able to identify intermediate points with respect to the final position. In deriving and analysing different hypotheses, from $\Omega_{\gamma\to\infty}$ to $\Omega_{\gamma\to 0}$, we reflect this analogy between trajectory and position, and we provide the analyst with information on the movement that detects the degree of groups' experience. But, precisely, in this way we make movement in a single direction, that of degree of experience, which we define as horizontal.

Still with reference to our analogy, and looking at fig. 3.7, we know that a trajectory (e.g., from A to B) combines horizontal movements with vertical ones. The vertical movement in our method is equivalent to requiring more or less evidence to assess the hypotheses we are investigating. With reference to fig. 3.7 a vertical movement from A to B is executed with a variation from $\varepsilon \to 1$ to $\varepsilon \to 0$.

An analyst can decide to follow the red dotted line of fig. 3.7

and s/he looks at how groups reveal their degree of experience and, at a certain point of this trajectory, looks for more evidence supporting the hypotheses, or s/he can decide the opposite way following the black dotted line, or also use other trajectories.

We have to answer now the question of why an analyst should spent time and effort in analysing hypotheses that fall around point A, i.e., low degree of experience and low support of evidence. The answer, in our opinion, can be found in [67] and, specifically, in reference to the danger of inherited assumptions. Even if stated in a somewhat different context, this problem can be formulated also in our case. The fact that a group has a high experience on a pattern builds a sort of preference for this hypothesis and, on the other hand, a low experience on a pattern becomes (or better, is treated as) evidence against an hypothesis. Inherited assumptions are like stones or fixed points in a plane and, to avoid the risk of over-reliance on these assumptions, they have to be sufficiently questioned in reference to concrete evidence and examined also in reference to their possibility of gradually change. This motivates the need for our vertical and horizontal movements.

The method has been evaluated and validated on real data extracted from the GTD. Results are reported in section 4.1.

3.1.2 Secure partition for target protection[3]

Attributing scenarios to possible perpetrators improves the awareness of the decision maker with regards to threats. S/he is now aware of who can carry out the attack, of his experience and potential danger, and can make an assessment of the scenario regarding expected losses. This is aimed at establishing strategies and actions, as well as planning resources, to defend a target of attack. The decision maker can define strategies and actions to limit, in most cases, the expected losses.

For instance, for a specific attack strategy $a1$, a decision maker can decide to limit the losses or damages to a maximum of *L1* with a probability of at least 0.3, to *L2* with a probability of at least

[3] The method presented in this section has been published in [32]

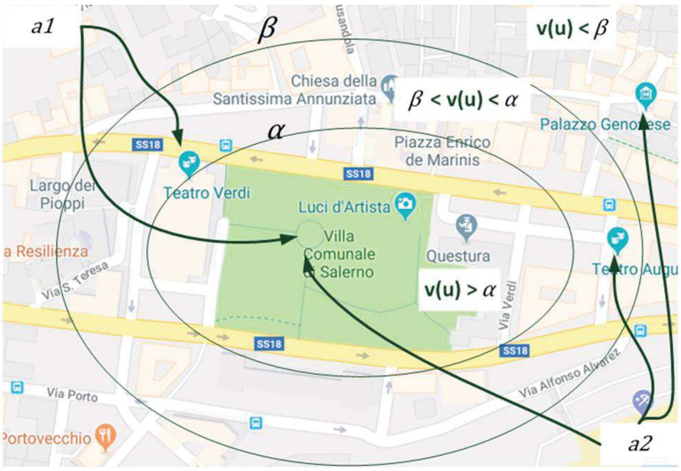


Figure 3.8: Target of attack hypotheses

0.5, to *L3* with a probability of at least 0.6. Similarly for other hypothesized attack strategies.

The objective of the method presented in this section is to support the decision maker in partitioning a target respecting the requirements mentioned above. Let us suppose the target of the attack is an urban area (see fig. 3.8). Let us suppose $a1$ and $a2$ are two attacks that can impact specific points of the urban area. Let be $v(u)$ an evaluation function for these points. If the value of v for a point of interest is greater than a threshold, $v(u) > \alpha$, the point is considered important and to protect with high priority. As such it can be included in a red zone. Similarly, if the assessment is below a threshold, $v(u) < \beta$, a point is considered less important, and consequently inserted into a green zone. The challenge is how to set α and β to maintain losses and damages within the limits set by the decision maker, discussed at the beginning of this section.

The method uses DRSA under uncertainty (see section 2.1.2) to perform analysis of threat scenarios. A threat scenario consists of an attack a_j, a set of expected losses on parts of the partition, $l(p_i, a_j)$, and a set of probabilities associated to these losses, $z^{'}(p_n, [a]_j)$. More formally: $TS_j = ([a]_j, < l(p_1, [a]_j), ..., l(p_n, [a]_j) >$

Table 3.9: Information table of PoI

	d1	d2	a1	a2
u1	3	4	1	0
u2	3	2	1	1
u3	1	2	1	1
u4	2	1	0	1

$, < z^{'}(p_1, [a]_j), ..., z^{'}(p_n, [a]_j) >)$ where $j = 1, ..., M$ (with M cardinality of the set of attacks) and $n = |P|$ is the number of parts of a partition.

The method to create and compare threat scenarios is reported in fig. 3.9. In the following we refer also to the definitions reported in section 2.1.2.

An information table, such as table 3.9, reports information on the objects of the universe described with a set of domain-specific and attack attributes that inform about the vulnerabilities of the objects of the universe.

The objects of the universe U can be, for instance, Points of Interest (PoI) of a city. The subset $D \subseteq Q$ characterizes the objects, $V \subseteq Q$ gives information on vulnerabilities of the objects. Table 3.9 reports an example consisting of four points of interest, two domain attributes, and two attack attributes.

The domain attributes, $d1$ and $d2$, characterize the objects in terms of performance, behaviour and so on. For instance, if objects are PoI of an urban area, these attributes can refer to information such as average number of persons in a building. The attack attributes, $a1$ and $a2$, describe the vulnerabilities of the objects. If we assume binary values for these attributes we can codify $2^n - 1$ threat scenarios. In the example of table 3.9, for instance, we have that $u1$ is vulnerable to the scenario whose attack is characterized by $a1 = 1$ and $a2 = 0$.

From this table we can construct granules of knowledge, which are parts p_i and equivalence classes $[a]_j$. The p_i are created from the domain attributes using an evaluation function $v(u)$. We employ 3WD [28] to execute a tri-partition of U on the basis of two

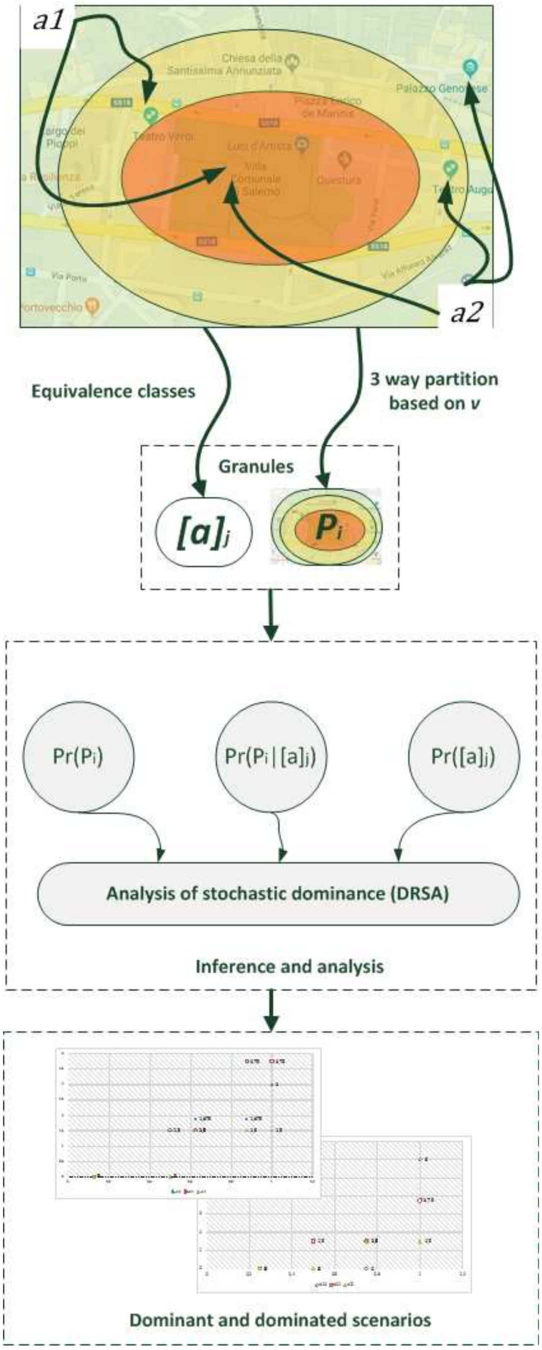

a1
a2
Equivalence classes
3 way partition based on v
Granules
[a]j
Pi
Pr(Pi)
Pr(Pi | [a]j)
Pr([a]j)
Analysis of stochastic dominance (DRSA)
Inference and analysis
Dominant and dominated scenarios

Figure 3.9: The secure partition method (elaborated from [32])

thresholds, α and β with $\alpha > \beta$. The equivalence classes $[a]_j$ are built on the basis of an equivalence relation over the attack attributes.

We use these granules of knowledge to derive probabilistic information to be used for analysis of dominance, as shown in the inference and analysis box of fig. 3.9 and, lastly, we reason about the results of the dominance analysis. These two phases are executed with the DRSA under uncertainty [57]. Let us clarify, also with reference to section 2.1.2, how we use DRSA analysis with p_i and $[a]_j$.

The set P of states of the universe is, in our context, a set of non overlapping parts covering all the objects of the universe that can be subject to an attack. If we assume a single attack model, just one object of the universe can be attacked. So the states associated to P are mutually exclusive, since only one part p_n can be subject to an attack. An a priori probability of p_n can be evaluated as $\lambda_n = \dfrac{|p_n|}{|U|}$ where $|.|$ is a cardinality measure.

The acts of the set A are attacks of threat scenarios. As already mentioned, in our model given n attributes of V we can have $2^n - 1$ scenarios. A scenario is represented with an equivalence class, let us call $[a]$, that contains the objects of the universe that are subject to the same threat. For instance, in the case of table 3.9, we have $[a]_{00} = \{\phi\}$, $[a]_{01} = \{u4\}$, $[a]_{10} = \{u1\}$, and $[a]_{11} = \{u2, u3\}$ where we included also the scenario of no attack ($[a]_{00}$).

The outcomes evaluation function for the threat scenarios evaluates the loss for a couple $(p_n, [a]_j)$. A loss L is evaluated as follows:

$$l(p_n, [a]_j) = L_{max} * Pr([a]_j)Pr(p_n|[a]_j) * (1 - E_r) \tag{3.5}$$

Eq. (3.5) is elaborated from [68]. In eq. (3.5) L_{max} denotes the maximum expected loss, $E_r \in [0, 1]$ measures the effectiveness of response and recovery actions, and $Pr([a]_j)Pr(p_n|[a]_j) = \dfrac{|[a]_j|}{|U|} \dfrac{|p_n \cap [a]_j|}{|[a]_j|}$ is a vulnerability index. The vulnerability index gives probability information on the objects in p_n that are subject to a specific threat.

Eq. (3.5) is used to evaluate the probabilities of eq. (2.20) and (2.21), and these last ones are used to evaluate eq. (2.22) and (2.23) giving us information on the stochastic dominance.

For the thesis, the evaluation of the method in [32] has been contextualised to a case study based on events extracted from the GTD. Results are reported in the section 4.2.

3.1.3 Resilience analysis of the target[4]

Attacks can have different consequences on a target and, to gain additional awareness, the decision maker should analyse the possible evolutions of threats. The objective of this phase is to understand the degree of resilience of the target, also considering the actions performed in the previous phase of secure partition to defend the target.

The starting point is a tri-partition of the target area or infrastructure performed with the secure partition method. The analysis and evaluation of attacks follow the principles of resilience. Resilience comes from the Latin *resilio* whose etymology is *re salire* that means going-up again. The term ontologically admits the going-down and this constitutes the core of this paradigm. With resilience we accept this risk of attacks and consider the ability to prepare for and adapt to changing conditions. Resilience includes *the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents*[5]. Resilience has different facets depending on the specific application domain. We briefly analyse in the following three domains: ecological, community and system.

In ecological study, resilience has a long history [69]. In this domain, resilience is the capability of an ecosystem to respond to perturbations caused by natural events or man-made disasters, and to respond and adapt. The ecological system may change state and, in some conditions, minute changes trigger extreme discontinuous responses that are not always reversible and the

[4] The method presented in this section has been published in [33]

[5] www.dhs.gov/what-security-and-resilience

system can not return to its previous state. This is refereed to as critical transition [70], and a challenge is the identification of indicators that allow to infer the critical transition [71] [72]. For the ecological domain, the works that are closer to the use of GrC methods are based on the adoption of fuzzy inference systems and fuzzy cognitive maps for prediction of changes and scenario analysis of ecological systems, e.g., [73] [74] [75], and the use of rough sets as data analysis tool for decision making for ecological sustainability, e.g., [76] [77].

The community based resilience is devoted to analyse and measure the resilience of a community. The focus in this case is very broad and includes crisis responses, sustainable developments in underdeveloped areas, social aspects. Community resilience includes also training humans to be resilient with organizational learning processes, and the definition of assessment methodologies and indicators, such as the Community Based Resilience Analysis (CoBRA) assessment methodology [78]. A paper that presents a quite complete summary of methods and approaches for community indicators is [79]. An interesting work that can show how GrC could play a role in community resilience is [80]. This work considers a correlation between holistic indigenous knowledge (a body of knowledge built up by a group of people through generations of living in close contact with nature and their ecosystems) and fuzzy logic as a way to explain how rules of thumb and other simple prescriptions can be used to deal with complexity of their community. With regards to indicators, there are results on fuzzy reasoning and fuzzy indicators for sustainable development [81] [82].

Lastly, there is the system resilience that is the perspective we are interested in this method. As mentioned in [83], system resilience can be determined by three capacities: *resistant* as the ability to prevent hazard and reduce damage, *absorptive* as the degree to which the system absorb the impact of a damage, and *restorative* as the ability to repair quickly and adapt.

With respect to resistant capacity, there is a wide literature presenting the adoption of rough sets and their extensions for reliability management and fault diagnosis, e.g., [84] [85], and on granules built with the tolerance relation, e.g., [86] [87]. Among these types of works, [88] uses DRSA for fault diagnosis in a smart grid. The adoption of DRSA is fostered also by us in the last phase of our approach. However, the technique is the same but the context of adoption is different. There is a substantial difference because we are not going to use DRSA as a stand-alone tool but we put DRSA into a framework for situation analysis. This is fundamental for our purposes because we must be able to discriminate situations (e.g. attacks or malfunctioning). Other works that can be related to the resistance capacity are based on fuzzy inference systems, e.g., [89].

With respect to the absorptive and restorative capacities we did not find several works. These capacities are very difficult to de-contextualize from the resilience concept. However, with respect to the restorative capacity, evolutionary algorithm can be used to re-plan systems and restore functionalities. Examples in power systems, including hybrid approaches that use computational intelligence, are reported in [90].

In this chapter, we consider the system perspective of resilience.

We need to use a model of resilience that has to be computationally tractable and, to this purpose, we consider the model defined in [27] that is based on the definition of resilience of a system provided by the National Academy of Science, i.e., the ability *to plan and prepare for, absorb, respond to, and recover from disasters and adapt to new conditions* [26]. The model correlates the concept of resilience to that one of critical functionality of a system. Given a system formalized as a graph $G(N, L)$, where N is a set of nodes and L is a set of links, the critical functionality, K, is defined as:

$$K(t; N, L, C) = \frac{\Sigma_{i \in (N,L)} w_i(t; C) \pi_i(t; C)}{\Sigma_{i \in (N,L)} w_i(t; C)} \tag{3.6}$$

where $w_i(t; C)$ is a measure of the relative importance of node or link i at time t, and $\pi_i(t; C)$ represents the degree to which a node or a link is active in the presence of an adverse event. An alternative interpretation defines $\pi_i(t;C)$ as the probability that a node or link i is fully functional. C is the set of temporal decision rules and/or strategies to be developed in order to improve the resilience of the system during its operation. An object $c \in C$ represents a configuration of the system.

Let E be a set of adverse events, the resilience $R = f(N, L, C, E)$ is defined as:

$$R \equiv R(K, E, [0, T_c]) = \frac{\frac{1}{|E|}\Sigma_E \int_{t=0}^{T_c} K(t; N, L, C)}{\int_{t=0}^{T_c} K^{nominal}(t; N, L, C)} \tag{3.7}$$

where $K^{nominal}$ is the value of the critical functionality when no external event is occurring, and T_c is the so-called control time that is the mean time occurring between two adverse events. Eq. (3.7) can be normalized and discretized to be computationally tractable. Let us suppose $K^{nominal} = 1$:

$$R = (\frac{1}{T_c})\frac{1}{|E|}\Sigma_E \Sigma_{t=0}^{T_c} K(t; N, L, C) \tag{3.8}$$

The definition of K depends on the specific target to analyse and on the objectives of the analysis.

Now that we have identified the computational model of resilience, let us describe what the proposed method does. The method uses granular structures to model the dependencies between nodes of a target, granular hierarchical models to evaluate the consequences of an attack considering these dependencies, and estimates a measure of resilience using DRSA.

i): Granular representation of dependencies. The issue of representation and modelling of dependencies, at least for Critical Infrastructures (CIs), has been investigated by Rinaldi et al. [91]. Their seminal work on interdependencies and cascading effects uses four general categories: *i)* Physical, a physical reliance on material flows from one infrastructure to another; *ii)* Cyber, a reliance on information transfer between infrastructures; *iii)* Geographic, a local environmental event affects components across multiple infrastructures due to physical proximity; and *iv)* Logical, a dependency that exists between infrastructures that does not fall into one of the previous categories.

We use the categorization proposed by Rinaldi et al. [91], and contextualize to the categories of Rinaldi et al. the formalization proposed in [92]. On this basis, let us consider two components (a, b) of a target and define:

- a physical dependency between a and b as a reliance of b on a: $a \rightarrow b$,

- a cyber dependency between a and b as a reliance of $f(b)$, where $f(.)$ means a functionality, on a: $a \rightarrow f(b)$,

- a geographical dependency between a and b as a proximity relation between a and b: $(a, b)_g = dist(a, b) < \varepsilon$. This is (the only one) reflexive relation, i.e. $(a, b)_g = (b, a)_g$,

- a logical dependency between a and b as the influence on an event of b due to an event on a: $E(a) \rightarrow E(b)$.

To represent and reason on dependencies based on the above mentioned four categories, we adopt a set of (four) binary relations [93]. Let $R \subseteq V \times U$ be a binary relation, $a \in V$ is related to $b \in U\ if (a, b) \in R$, denoted aRb. If $V = U$, R is a binary relation over U. In our case $R \in \{P, C, G, L\}$ meaning that is one among physical, cyber, geographical or logical relations. As reported by Lin et al. [93] a binary relation is different from an equivalence one. The equivalence relation is reflexive, symmetric and transitive while a binary relation does not satisfy these properties. We have already emphasized that, in our case, only the geographical dependency is reflexive. This difference between binary and equivalence relations has the consequence that partitions and granules formed with binary relations overlap.

To take into account all the four types of dependencies we use a family of granular structures, which is a collection of granular structures, and we include in this family a structure for each type of relation R. Thus, we define: $\mathbf{f}(GS(P), GS(C), GS(G), GS(L))$ where each GS is a collection of granules build as follow.

Given an universe U and a binary relation $R \in \{P, C, G, L\}$ over U, we use the formalism presented in [94] to define a granular structure GS as follows:

$$GS(R) = (g_R(x_1), g_R(x_2), ..., g_R(x_n)) \tag{3.9}$$

where

$$g_R(x_i) = \frac{p_{i1}}{x_1} + \frac{p_{i2}}{x_2} + ... + \frac{p_{in}}{x_n} \tag{3.10}$$

is the granule induced by x_i and + refers to union. For a fixed R we set $p_{ij} = 1 \ if \ (x_i, x_j) \in R$ and $p_{ij} = 0$ otherwise. Of course, $p_{ii} = 1$ and the fact that $(x_i, x_j) \in R$ can be known by design or discovered, in the case of CIs, with some of the techniques reported in [83]. Eq. (3.10) indicates the granule of all the components that depends from x_i for the specific relation R.

ii): Granular modelling of attacks. To take into account objects dependencies in the analysis of attacks evolutions, we propose an approach based on the fusion of different attack models, and use the hierarchical system modelling with GrC developed by Pedrycz et al. [95].

The idea is to model attacks that can follow a specific, and limited, path between a root and a target object, and then fuse two or more of these kinds of models when analysing attacks that can exploit several paths between a root and a target. We refer to these models as *local* and *global* models of attacks. The added value is that with the fusion it is possible to give analysts a rapid, even if abstract, information on the decrease of performance of a target object.

A global attack model can be obtained with the fusion of different local models with a hierarchical approach. Pedrycz et al. [95] have defined a method that can do this with GrC. The facets of originality of their results relate to the possibility of quantifying the diversity of local models via hierarchical granular architecture, and forming information granules emerging at higher levels of hierarchy.

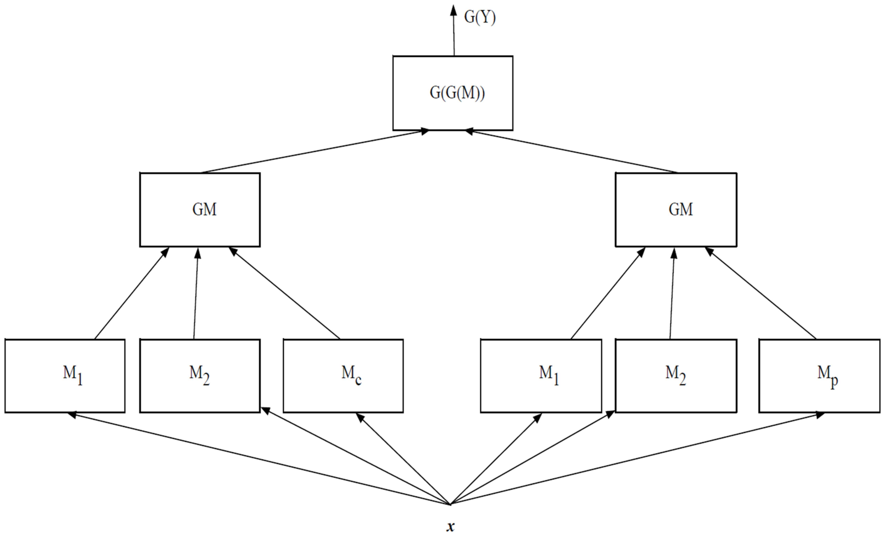


Figure 3.10: HSM from [95]

The approach can be easily understood by taking a look at fig. 3.10 from [95]. As we can see from fig. 3.10, there are some numeric models $M_1, ..., M_n$ that can be developed in different ways. These models are subject to a granular fusion to generate a Granular Model (GM), i.e., type 1 GM. Granular Models of type 1 can be further fused together to generate a higher level GM, i.e., type 2 GM. GMs are constructed with the principle of justified granularity [36] [96] aiming at designing information granules that are representative and meaningful, by finding a trade-off between two measures: coverage and specificity. In [95] authors report examples of the approach for fuzzy rule based models and neural networks.

Interested readers can refer to the cited works for more information on the principle of justified granularity and its application for hierarchical system modelling. Here we contextualize this approach to attack models and explain its added value, with a look at fig. 3.11 a) showing a target (i.e., a part of CI) where nodes 1 and 2 have a physical dependency from I, and node 3 has a cyber dependency from I. To improve the understanding, we label the dependencies between components, and introduce the following notation: we refer as V_{ij} to the $j-th$ vulnerability of the $i-th$ component of the target, and g_{Vi} as the information granule that granulates the vulnerabilities of a node.

Let us consider an attack exploiting some of vulnerabilities of the input I, e.g. $V_I = \{V_{I1}, V_{I2}\}$. The first of these vulnerabilities, when exploited, causes physical consequences to target node T, the second can cause cyber consequences to node T. With reference to some Smart Grid attacks presented and discussed in [97], we contextualize fig. 3.11 a) to a smart grid. Let us consider the node I as the attack entry point. Node I is a power control network, and I can be infiltrated inside a trusted perimeter by humans with an USB stick (this is V_{I1}) or can have a poorly configured firewall allowing network based intrusion (this is V_{I2}). Let suppose that I controls the power load distribution to a transmission node (1) and a service provider (2), and communicates with a metering device (3). The target T is a customer of a smart grid. The first attack path, $I-1-T$, may result in a power shortage to the customer, in the second $I-2-T$ the power shortage to service provider node may result in a failure to delivery apps and services for smart home load balancing, with the third $I-3-T$ path an attacker may inject false information and meter data. All the attacks have influence on the normal energy consumption of the customer.

Fig. 3.11 b) shows the numeric models we can develop in the analysed case. A model offers information on the chain of vulnerabilities, from the input to target node, that can be exploited. A model can be formalized in several way, such as by the if then rules:

$$if\ V_{I1}\ and\ V_1\ then\ V_{T1}$$
$$if\ V_{I2}\ and\ V_3\ then\ V_{T3}$$
$$if\ V_{I1}\ and\ V_2\ then\ V_{T2}$$

where the first relates to $M1$, the second to $M2$ and the third to $M1\_2$ of fig 3.11 b). We build granular models from these numeric ones. In this case we have two models $M1, M2$ exploiting a single dependency path, and a third $M1\_2$ following a hybrid

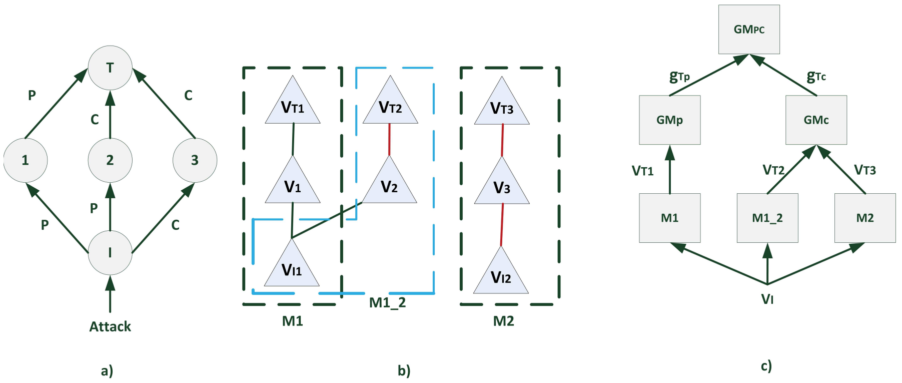


Figure 3.11: a) Part of a CI - b) Attack Trees - c) HSM (from [33])

path. From these models we can build the hierarchical granular system shown in fig. 3.11 c). The numeric models are granulated to form granular models of physical (GM_P) and cyber (GM_C) attacks. The outputs of these models are in the form of type 1 interval granules, i.e. $g_{V_{Tp}}$ and $g_{V_{Tc}}$ where p and c refer to physical and cyber, and can be fused to form a global attack model in the form of a type 2 interval granule.

The added value of using this approach to model attacks is twofold. First, we can have a concise but meaningful description of the impact on a target object if we build granular descriptors of the impact. In this way, an analyst can rapidly understand what s/he can expect in terms of minimum and maximum decreases of performances (interval granules), and can have this information also for separate types of attacks, e.g., by analysing specific local models of attacks. Second, if we are able to identify in a target, such as a large scale infrastructure, local models based on single dependency paths, we can better analyse and protect these paths because their complexity is reduced with respect to multi-dependencies paths.

However, real infrastructures usually are complex and include several paths among nodes that combines more dependencies. In the smart grid example discussed, this is the case of $M1\_2$. In these paths there are components that can break a dependency

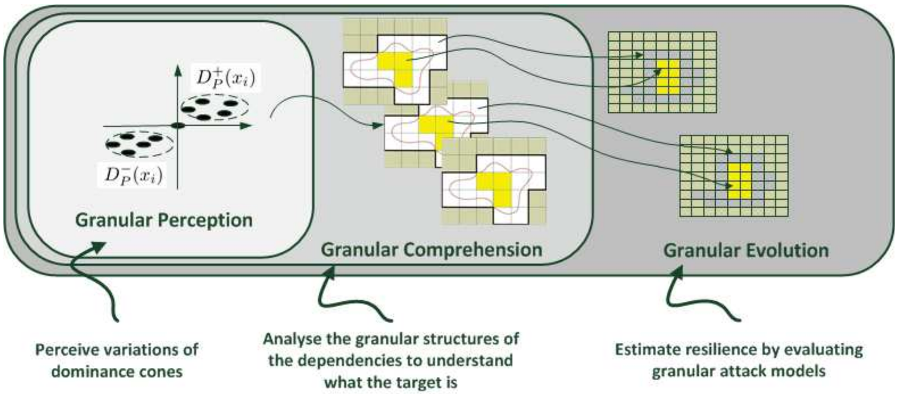

$D_P^+(x_i)$
$D_P^-(x_i)$
Granular Perception
Granular Comprehension
Granular Evolution
Perceive variations of dominance cones
Analyse the granular structures of the dependencies to understand what the target is
Estimate resilience by evaluating granular attack models

Figure 3.12: GSA for resilience (elaborated from [33])

path and start one or more paths based on a different dependency. Discovering these paths may be of interest because attackers, to reach a target node, may need to change their attack strategies. A formal procedure to discover these kinds of nodes/paths is left for future works.

iii): Resilience estimation. To estimate the resilience of the target, we use Granular Situation Awareness (GSA). The GSA has been defined in [25] starting from [98] and [6], and consists of the application of GrC in and across all the levels of a SA cognitive model. GSA offers a structured cognitive approach allowing operators to gain improved situation awareness, by combining GrC and Endsley's Situation Awareness (SA) [1] [99].

The GSA is shown in fig. 3.12 and interested readers can refer to [25] for a more detailed description of how GrC enforces each layer of the SA model. In the following, we just refer to the constructs we use for the case of resilience analysis that are: dominance classes (a.k.a. dominance cones, see section 2.1.2) as granules of knowledge in the GSA Granular Perception, and upper and lower approximations of dominance classes in the GSA Granular Comprehension phase.

The result of secure partition method of section 3.1.2 can be formalised as a decision table that classifies the components of the target in three ordered regions (RED, ORANGE and GREEN or also POS, BND, NEG). In each region resulting from the application of partition method, we can have further details if we build and analyse the dominance classes. This requires the application of DRSA [100] starting from a decision table. As mentioned in section 2.1.2, DRSA is an extension of rough set theory for multi-criteria decision analysis based on the definition of a dominance relation, which allows to deal with preference-ordered decision classes. DRSA has been adopted also for analysis of diagnosis in a smart grid [88], that is a case study similar to resilience, using the concept of approximation to make inference. Let be $\succeq_a$ a preference relation s.t. $x_i \succeq_a x_j$ means that x_i is preferable to x_j with respect to the attribute $a \in A$. If $x_i \succeq_a x_j$ for every $a \in A$, we say that x_i dominates x_j, i.e. $x_i D_A x_j$. For every object x_i, we can define a set of objects that dominates x_i and a set of objects that are dominate by x_i. These are respectively formalized in eq. (3.11).

$$\begin{aligned} D_A^+(x_i) &= \{x_j \in U | x_j D_A x_i\} \\ D_A^-(x_i) &= \{x_j \in U | x_i D_A x_j\} \end{aligned} \tag{3.11}$$

Now let be $D = \{d\}$ a set of decision attributes that, in our case, consists of the three ordered regions and makes a partition of the objects in three classes corresponding to the three regions defined with 3WD. Let $Cl = \{Cl_p, p \in P\}$ with $P = \{1, 2, 3\}$ be the set of decision classes / regions. According to DRSA, we can find upward union classes $Cl_p^{\geq} = \cup_{t \geq p} Cl_t$ that contain *all the objects at least of class* Cl_p and downward union $Cl_p^{\leq} = \cup_{t \leq p} Cl_t$ that contain *all the objects at most of class* Cl_p.

To clarify how we execute concept approximation in the comprehension level of GSA, we need to introduce the DRSA concepts of lower and upper approximations of these union classes. The knowledge being approximated is a collection of upward and downward unions of Cl and the granules of knowledge used for approximations are the dominance classes of eq. (3.11). Thus, given a set of attributes A, the lower and upper approximations of $Cl_p^{\geq}$ are defined as follows:

$$\begin{aligned}\underline{A}(Cl_p^{\geq}) &= \{x|D_A^+(x) \subseteq Cl_p^{\geq}\}\\ \overline{A}(Cl_p^{\geq}) &= \{x|D_A^-(x) \cap Cl_p^{\geq} \neq \phi\}\end{aligned} \tag{3.12}$$

Similar formulas are used for the lower and upper approximations of $Cl_p^{\leq}$:

$$\begin{aligned}\underline{A}(Cl_p^{\leq}) &= \{x|D_A^-(x) \subseteq Cl_p^{\leq}\}\\ \overline{A}(Cl_p^{\leq}) &= \{x|D_A^+(x) \cap Cl_p^{\leq} \neq \phi\}\end{aligned} \tag{3.13}$$

The quality of approximation can be measures with the following:

$$\gamma_A(Cl) = \frac{|U - ((\cup_p Bn(Cl_p^{\leq}) \cup (\cup_p Bn(Cl_p^{\geq})|}{|U|} \tag{3.14}$$

where, in eq. (3.14), $Bn(Cl_p^{\leq}) = \overline{A}(Cl_p^{\leq}) - \underline{A}(Cl_p^{\leq})$ is the boundary class of $Cl_p^{\leq}$ and $Bn(Cl_p^{\geq})$ is the analogous for $Cl_p^{\geq}$. Boundary classes contain objects that are doubtful. In fact, the quality of an approximation of eq. (3.14) is perfect, i.e. $\gamma_A(Cl) = 1$, only if boundaries are voids.

The value of using dominance and union classes is in the possibility of issuing early warning signals. According to the identified resilience model, any change in the attributes values of components affects the level of resilience. If we have classified in a proper way the components of a target infrastructure, until the dominance classes do not change we may consider these variations as normal system fluctuations. When dominance classes change, however, the classification is no more consistent, and upper and lower approximations of some union classes are different. The objects belonging to the boundary classes have to be carefully monitored because they are malfunctioning. So these object may be under attack and/or damaged.

To better understand the situation, the GSA comprehension level reasons on the granular structures of dependencies, and takes into consideration the granules of dependencies of the objects in the boundary region. This level recognizes what are the objects that depend from the objects in the boundary regions and can observe the attributes values of the dependent objects. If these are changed (i.e., they are lower), then the fault or the attack is evolving along a path of dependencies.

In a protection scenario, we can suppose the priority is to protect the most critical objects (i.e., the ones classified in a Red region). The comprehension level evaluates the possible paths to the objects of red region, and the evolution level projects the situation by evaluating the granular models of attack towards these objects. Since the granular models are in the form of interval granules, the critical functionality K of eq. (3.6) has to be evaluated using augmented operations for addition $\oplus$ and multiplication $\otimes$ with intervals:

$$K = \frac{\sum_{\oplus_{i \in (N,L)}} [w_i^-, w_i^+] \otimes [\pi_i^-, \pi_i^+]}{\sum_{\bigoplus_{i \in (N,L)}} [w_i^-, w_i^+]} \tag{3.15}$$

The same is true for eq. (3.8) for evaluation of R under the attack analysed (that is an event $e \in E$).

The method has been evaluated on a case study based on a Smart Grid, and readers interested to evaluation results can refer to [33]. However, to be applicable in the domain investigated in this thesis, the resilience analysis method requires further extensions and contextualization, starting from an appropriate definition of the critical functionality K. These activities are left for future works.

3.2 Comparison with other methods

We have mentioned the distinctive aspects of our methods in the section 1.1.2 (i.e., "What?"), in this section we compare our research results with other methods supporting the intelligence analysis stages.

In [101], Yager discusses the adoption of soft-computing techniques for intelligence analysis also considering the model of Situation awareness. He focused his work on the importance of multi-source data fusion with the support of fuzzy set and approximate reasoning techniques. In [102] he extends his results by considering data fusion based on several measures of "*possibility and certainty as a tool to enable an intelligence analyst to provide an answer in terms of an upper and lower bound on the truth of the hypothesis*". The idea behind the mentioned works is, essentially, similar to the one presented in this thesis which, as described, leverages the use of aggregation measures based on OWA and fuzzy theories and probability to build and reason on hypothesis.

With an emphasis more closely linked to the assessment of the risk of terrorist attacks, approaches based on the creation and interpolation of fuzzy rules were used and validated on the GTD [12] [13]. These methods deviate from ours which are mainly aimed at reasoning on scenarios for the purpose of attributing hypotheses of attack on terrorist groups and identification of actions and strategies for the safe partitioning of attack targets.

The approaches that come closest to the aims and objectives of the methods proposed in this thesis concern the use of the Analysis of Competing Hypotheses (ACH). ACH allows decision makers to analyse and evaluate a set of competing hypotheses against a body of evidence that can support or contradict each hypothesis. The goal is to proceed step-by-step by rejecting hypotheses, accepting only those hypotheses that cannot be eliminated.

The ACH method has been integrated with the adoption of belief theory and subjective logic [103] to make recommendations on likelihoods of hypotheses based on uncertain knowledge about the evidence, with Bayesian theory [104] and Bayesian networks [15] to abstract and generalize ACH tables. ACH is part of a suite of methods, called Structured Analytic Techniques (SAT), supporting analysts and decision makers in a step-by-step process that mitigates the negative impact of cognitive biases.

Fig. 3.13 shows where we can position the research results also considering the above mentioned SAT.

The figure shows that our results can be positioned in the middle between SAT [10] and methods based on artificial intelligence, machine learning and big data analytic to support decision mak-

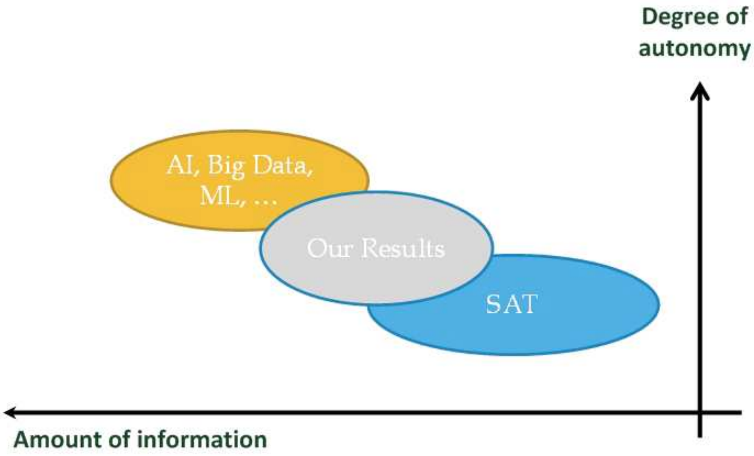


Figure 3.13: Positioning of research results

ing.

For instance, the analysis phases described in the previous sections can be executed with several SAT techniques combining Diagnostic and Imaginative thinking techniques, such as Analysis of Competing Hypotheses, Alternative Futures, Key Assumptions Check. These techniques can provide results also with a relative low amount of data and information (e.g., the suspect is a young male) but require the involvements of analysts and decision makers in several brainstorming activities. Furthermore, the knowledge is part of the decision maker.

On the other side, we have several methods for prediction and classification[6] that, however, require a large amount and adequate descriptions of data to produce results. In these cases, the degree of autonomy is higher and the involvement of analysts is not

[6] Just to limit to few results that have used real data for terrorism activities we mention: [105] using artificial neural networks and analytic hierarchy process; [106] using several classification algorithms (such as: KNN and SVM) for classification and prediction tasks; [107] using a modified version of k-means clustering algorithm; [108] proposing a machine learning method to evaluate the risk of terrorist attacks at a global scale on the basis of multiple resources, long time series and globally distributed datasets.

required in all stages.

The results achieved during this thesis period can be positioned in the middle.

The methods we propose share the aims (mainly of the SAT) of reducing cognitive biases during an analysis, and work on minimal set of data and information. As we will see in the chapter 4, for instance, the method to analyse and assess hypotheses provides results also when we reduce the original data set from 135 to 3 features. However, differently from SAT techniques, we do not require the involvement of analysts in all the phases. For instance, we do not need that the analyst makes explicit hypotheses, but we use numeric approaches. We create a list of alternative scenarios through OWA operators in phase 2 of the method to analyse and assess hypotheses and, then, these hypotheses are evaluated against the existing evidence using fuzzy probabilistic rough sets based on a Bayesian rough set model.

On the other hand, our methods have an advantage on classification and prediction approaches if we want to support analysts and decision makers in the early phases of a decision making process. The advantage comes from the possibility of using data and information also at a very coarse granularity, and from the fact that we can reason also on increases of information on the possibility that an event could occur rather than finding high probability rules, that could be impossible to derive considering also the minimal set of attributes used in our study.

Just to mention that we are not aware of the adoption of SAT for counter-terrorism analysis, at least on the basis of the data set used in this thesis (i.e., the Global Terrorism Database). Using the data in our conditions[7], we have done tests with rule induction algorithms. Specifically, we have tested a rule induction method from indiscernibility (i.e., rough set equivalence) classes and the implementation of CN2 algorithm for induction of decision rules implemented in the RoughSets R Package[8]. In our tests we split

[7] GTD in the 2012-2016 considering only groups perpetrating more than 1% of the total attacks. See chapter 4.

[8] https://cran.r-project.org/web/packages/RoughSets/RoughSets.pdf

our data in 60% training and 40% testing. In our conditions, a set of 94 rules was generated with CN2 algorithm with an accuracy of prediction for the test set of 0.325, and a set of 314 rules was generated with indiscernibility classes with an accuracy of prediction for the test set of 0.327. The most critical part of using decision rules is, however, the difficulty of prediction for attack patterns that are shared among different groups. As we are going to see in chapter 4, this limitation can be overcame with the adoption of the Bayesian rough set model.

Chapter 4

Experimental Results and Case Studies

This chapter reports the results of the experimentation and evaluation of the methods. Specifically, the analysis and assessment of hypotheses of section 3.1.1 has been experimented and evaluated on real data from the GTD. The secure partition of section 3.1.2 has been evaluated on a case study based on real events of the GTD.

GTD[1] is becoming a reference database for research and study activities related to the analysis of intentional terrorist attacks. It is an open source database of events concerning terrorist activities all around the world since 1970. This dataset contains information on more than 180,000 terrorism events, and considers 9 main attributes and several sub-attributes. The 9 main attributes are such as to cover the description of an event fairly completely, while the sub-attributes provide details. Sub-attributes values are not always available in the database.

The main attributes are: i) ID and Date; ii) Incident Information, iii) Incident Location, iv) Attack Information, v) Weapon Information, vi) Target/Victim Information, vii) Perpetrator Information, viii) Casualties and Consequences, and ix) Additional Information and Sources.

[1] `https://www.start.umd.edu/gtd/`

To evaluate our results with the GTD we have limited the events to five years (2012-2016) of terrorism activities, considered only groups perpetrating more than 1% of the total attacks in these five years, and excluded from our analysis the events that are not classified in the GTD (i.e., events for with the perpetrator is unknown).

The conditional attributes set C used for the evaluation consists of the following three categorical attributes:

- Attack Type (AT): describes the general method of attack. This attribute generally reflects a broad class of tactics used (e.g., a strategy). It has 9 values corresponding to 8 known types or tactics of attacks, and one level is reserved for unknown tactics.

- Target Type (TT): captures the general type of target/victim. It has 22 values corresponding to 20 types of general targets/victims, one value is reserved for "Other" types, and another one for unknown type.

- Weapon Type (WT): describes the general type of weapon used in the incident. This attribute has 13 values corresponding to 11 types of general weapons, one value is reserved for "Other" types, and another one for unknown type.

As we can see, we reduced the original feature set of GTD from 135 features to 3. Including only the three general attributes above mentioned, we have considered the most limited set of information related to attacks that we can suppose to have in the early stages of an intelligence analysis. Readers can refer to the GTD Codebook[2] for more information on the attributes.

In the time window 2012-2016, the total number of events correctly classified is 31819 and the number of perpetrators is 770. By considering groups perpetrating more than 1% of the total attacks, we have reduced the number of events to 23399 and perpetrators to

[2] https://www.start.umd.edu/gtd/downloads/Codebook.pdf

21. These groups perpetrated more than 73% of the total attacks in the 2012-2016. These groups are our decision classes:

$D = \{"g1: \ Al - Qaida\ in\ Iraq\ (AQI)"$
$"g2: \ Al - Qaida\ in\ the\ Arabian\ Peninsula\ (AQAP)"$
$"g3: \ Al - Shabaab\ (ALS)"$
$"g4: \ Bangsamoro\ Islamic\ Freedom\ Movement\ (BIFM)"$
$"g5: \ Boko\ Haram\ (BH)"$
$"g6: \ Communist\ Party\ of\ India\ -\ Maoist\ (CPI - Maoist)"$
$"g7: \ Donetsk\ People's\ Republic\ (DON)"$
$"g8: \ Fulani\ extremists\ (FE)"$
$"g9: \ Houthi\ extremists\ (HE)"$
$"g10: \ Islamic\ State\ of\ Iraq\ and\ the\ Levant\ (ISIL)"$
$"g11: \ Kurdistan\ Workers'\ Party\ (PKK)"$
$"g12: \ Maoists\ (MAO)"$
$"g13: \ Muslim\ extremists\ (ME)"$
$"g14: \ New\ People's\ Army\ (NPA)"$
$"g15: \ Palestinian\ Extremists\ (PE)"$
$"g16: \ Revolutionary\ Armed\ Forces\ of\ Colombia\ (FARC)"$
$"g17: \ Separatists\ (SEP)"$
$"g18: \ Sinai\ Province\ of\ the\ Islamic\ State\ (SIS)"$
$"g19: \ Taliban\ (TAL)"$
$"g20: \ Tehrik - i - Taliban\ Pakistan\ (TTP)"$
$"g21: \ Tripoli\ Province\ of\ the\ Islamic\ State\ (TIS)"\}.$

The probability distribution is $Pr = \{$
$0.01645, 0.03607, 0.10077, 0.01368, 0.08227, 0.01483, 0.02624,$
$0.01833, 0.03757, 0.18321, 0.03945, 0.04812, 0.01974, 0.04611,$
$0.01539, 0.01863, 0.01517, 0.01380, 0.21022, 0.02996, 0.01397\}$

Applying the procedure of evidence collection, described in section 3.1.1, we obtain the fuzzy GTD and similarity matrix reported in tables 1-2 and 3 of the Appendix A. The similarity matrix has been derived using the Gaussian kernel implementation of the package KRLS[3] in R, and values are rounded to the second decimal.

A detailed analysis of the terrorism phenomenon has not been done during the Ph.D period, and is not part of this thesis. How-

[3] https://cran.r-project.org/web/packages/KRLS/index.html

ever, we can highlight some points that are useful for the discussion and, at the same time, show how it is easy to comprehend interesting aspects of terrorist groups behaviours. Looking at table 1-2, we have an overview of the behaviour of the groups and can easily understand their preferences. For instance, we can observe that AQI has a strong preference for attack strategy 3 and, at the same time, this attack type is quite used by all the groups. We can observe an interesting exception, FE group that seems to have a particular behaviour centred on AT2, TT14 and WT5. Another distinctive trait is that one of PE being the only group using consistently WT9 (melee).

With reference to table 3, we have an overview of the similarity of groups. Considering only the information about attack patterns, we observe that the behaviours of AQAP and ALS are very difficult to discriminate, while clearly separable from the others seem to be the ones of FE and PE. However, if we look at table 4, which is the similarity matrix constructed using only attack types, their behaviours are similar with respect to the attack strategies. Other kinds of considerations can be done if we refer to similarity matrices based on other combination of attributes (that we have not reported in Appendix A but can be constructed following eq. (3.2)).

4.1 Evaluation of the method to assess hypotheses

The method described in section 3.1.1 has been evaluated on three cases where the hypotheses under analysis refer to: 1) a rare, 2) a distinctive, and 3) a combination of distinctive and common behaviours. The results are shown in fig. 4.1 that is divided in three parts, and allows to discuss results in the way illustrated with fig. 3.6. In fig. 4.1, values of α and β for different values of ε, as well as values of $Pr(\Omega|[g])$ that position groups in different regions, are not correctly scaled. The reader can refer to Appendix B presenting the tables with numeric values.

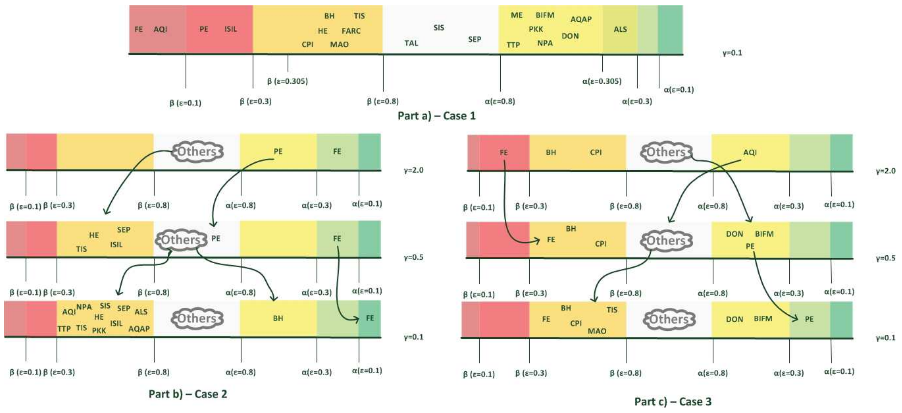


Figure 4.1: Results. Part a) refers to $< AT1, TT1, WT6 >$; Part b) refers to $< AT2, TT14, WT5 >$; Part c) refers to $< AT3, TT4, WT6 >$, $< AT2, TT4, WT9 >$ and $< AT2, TT14, WT9 >$ (from [31])

4.1.1 Case 1: A rare attack pattern.

The case considers an attack pattern that is rare in the dataset: $< AT1, TT1, WT6 >$. This represents the rarest event in our dataset, 1 out of 23399 events, and has been perpetrated by ALS. In this case, it makes no sense to derive different hypotheses Ω for different values of γ. The reason can be easily understood from the fact that this event is performed only by a group, and so the numerator of eq. (3.4) is 0 except when assessing the similarity between the TG and ALS. Different values of γ will only bring to different degrees of similarity between the two.

In other words, here the difference between hypotheses of *low* and *high* experience looses his meaning since only one group has experience on this pattern. So, let use derive Ω only for $\gamma = 0.1$ (only the membership degree is reported):

$\Omega_{optimistic} = \{0 \quad 0 \quad 0.00791 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0$
$0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0\}$.

As we can observe from Part a) of fig. 4.1, if the decision maker has to decide in the "realm" of strong (i.e., $\varepsilon \lesssim 0.1$) and positive (i.e., $\varepsilon \in [0.1, 0.3]$) evidence, s/he can only refuse the hypothesis that FE, AQI, PE and ISIL are perpetrators of the attack. In this realm, there is no evidence that a group can be positively associated to the hypothesis Ω. However, a very slight reduction in the support required for evidence (e.g., $\gamma = 0.305$) shows a positive classification for the group we expect that is ALS.

4.1.2 Case 2: A distinctive pattern.

This case considers an attack pattern that clearly characterizes the behaviour of a group. The pattern $< AT2, TT14, WT5 >$ clearly distinguishes FE from the others. This is a group active in Nigeria, and its behaviour appears to be strongly characterized by armed assaults to private citizens with firearms. More than the 72% of terrorism events of this group reflect this pattern. BH follows at a great distance with around 19% of events.

Let us derive Ω for $\gamma = 2$, $\gamma = 0.5$, and $\gamma = 0.1$:

$\Omega_{pessimistic} = \{0.067 \quad 0.016 \quad 0.020 \quad 0.046 \quad 0.019 \quad 0.018 \quad 0.034 \quad 0.075 \quad 0.022 \quad 0.016 \quad 0.021 \quad 0.018 \quad 0.023 \quad 0.022 \quad 0.037 \quad 0.015 \quad 0.032 \quad 0.033 \quad 0.019 \quad 0.023 \quad 0.015\}$

$\Omega_{modearted} = \{0.070 \quad 0.016 \quad 0.028 \quad 0.046 \quad 0.048 \quad 0.028 \quad 0.045 \quad 0.194 \quad 0.022 \quad 0.016 \quad 0.021 \quad 0.033 \quad 0.052 \quad 0.022 \quad 0.040 \quad 0.015 \quad 0.034 \quad 0.033 \quad 0.030 \quad 0.027 \quad 0.015\}$

$\Omega_{optimistic} = \{0.070 \quad 0.016 \quad 0.028 \quad 0.046 \quad 0.071 \quad 0.028 \quad 0.045 \quad 0.427 \quad 0.022 \quad 0.016 \quad 0.021 \quad 0.033 \quad 0.052 \quad 0.022 \quad 0.040 \quad 0.015 \quad 0.034 \quad 0.033 \quad 0.030 \quad 0.027 \quad 0.015\}$

Looking at the three hypotheses we can see that the degrees of similarity of some groups increase considerably from $\Omega_{pessimistic}$ to $\Omega_{optimistic}$. This is the case of BH (from 0.019 to 0.071) and FE (from 0.075 to 0.427). PE instead has a high value of similarity in the hypothesis $\Omega_{pessimistic}$ (i.e., 0.037) but this value does not increase significantly.

As we can observe from Part b) of fig. 4.1, for $\varepsilon = 0.3$, the group FE can be positively associated to all the three hypotheses and, as we move from $\gamma = 2$ to $\gamma = 0.1$, FE is confirmed also with a higher support of evidence (i.e., $\varepsilon = 0.1$). At the same time, we see a change in the regions of BH and PE. Fig. 4.1, in fact, shows also with arrows the movements of some groups. We can also note that, as we move towards the assessment of hypotheses that require more experience in perpetrating the attack, the decision maker succeeds in having indications (the orange area, barely noteworthy) of the fact that several groups can not be associated with the hypothesis of attack.

4.1.3 Case 3: A combination of distinctive and common patterns.

This case combines a very common pattern, $< AT3, TT4, WT6 >$, with two patterns, $< AT2, TT4, WT9 >$ and $< AT2, TT14, WT9 >$, that characterize with different degrees the group PE. The first pattern is shared among all the groups but FE, and characterizes mainly the groups BIFM and DON. Let use see how the 21 groups of our universe are characterized with respect to these patterns looking at table 4.1 that reports $\mu_{AT2TT4WT9}$, $\mu_{AT2TT14WT9}$ and $\mu_{AT3TT4WT6}$. The membership values are evaluated as described in section 3.1.1.

We can see that PE has the highest value of $\mu_{AT2TT4WT9}$, and BIFM and DON have the highest values of $\mu_{AT3TT4WT6}$

Let us derive Ω for $\gamma = 2$, $\gamma = 0.5$, and $\gamma = 0.1$, and see Part c) of fig. 4.1.

$\Omega_{pessimistic} = \{0.068 \quad 0.035 \quad 0.034 \quad 0.079 \quad 0.023 \quad 0.007 \quad 0.056 \quad 0.005 \quad 0.046 \quad 0.041 \quad 0.041 \quad 0.017 \quad 0.040 \quad 0.039 \quad 0.038 \quad 0.048 \quad 0.053 \quad 0.063 \quad 0.032 \quad 0.039 \quad 0.034\}$

$\Omega_{modearted} = \{0.068 \quad 0.059 \quad 0.060 \quad 0.135 \quad 0.026 \quad 0.015 \quad 0.096 \quad 0.022 \quad 0.058 \quad 0.053 \quad 0.070 \quad 0.024 \quad 0.063 \quad 0.042 \quad 0.073 \quad 0.056 \quad 0.063 \quad 0.108 \quad 0.040 \quad 0.060 \quad 0.034\}$

$\Omega_{optimistic} = \{0.068 \quad 0.071 \quad 0.069 \quad 0.204 \quad 0.026 \quad 0.015 \quad 0.145 \quad 0.022 \quad 0.058 \quad 0.053 \quad 0.087 \quad 0.027 \quad 0.063 \quad 0.042 \quad 0.196 \quad 0.056 \quad 0.063 \quad 0.131 \quad 0.040 \quad 0.060 \quad 0.034\}$

In the cases $\gamma = 2$ and $\gamma = 0.5$ for values of $\varepsilon \leq 0.3$ we can not positively support our hypotheses, and can exclude only FE in the scenario of pessimistic analysis for $\varepsilon = 0.3$. If we require a lower support of evidence, however, we can obtain some informa-

Table 4.1: Membership degrees of the patterns (from [31])

	$\mu_{AT2TT4WT9}$	$\mu_{AT2TT14WT9}$	$\mu_{AT3TT4WT6}$
AQI	0	0	0.1117
AQAP	0	0.0071	0.3744
ALS	0	0.0178	0.3668
BIFM	0	0	0.55
BH	0.0119	0.0119	0.1278
CPI	0	0.0576	0.0375
DON	0	0	0.4691
FE	0.0093	0.0233	0
HE	0	0	0.2332
ISIL	0	0.0124	0.2312
PKK	0.0033	0	0.3879
MAO	0	0.0684	0.0941
ME	0.0433	0.0433	0.2121
NPA	0	0	0.1974
PE	0.4306	0.2806	0.1056
FARC	0	0	0.2133
SEP	0	0	0.2169
SIS	0	0	0.3808
TAL	0.0096	0.0096	0.22
TTP	0	0	0.2839
TIS	0	0	0.1315

tion if we look at how the groups move when analysing the three scenarios. Let us focus on the groups highlighted in the regions corresponding to $\varepsilon = 0.8$ (the orange and yellow ones).

AQI in the analysis of the scenarios move from POS to BND. If we look at table 4.1 we observe that the membership values of the three patterns under analysis for AQI are respectively 0, 0, and 0.1117 so it presents a low degree of experience in using these patterns. What differs AQI from other groups that are in a similar situation is the availability of evidence in its favour: specifically the strong dominance of $AT3$ for AQI (see table 1 of Appendix A) that, in case we require a low support of evidence (e.g., $\varepsilon = 0.8$), allows to classify AQI in a POS zone. However, as soon as we move towards the analysis of scenarios denoted by moderated and optimistic hypotheses, AQI loses this characteristic at the expense of other groups, such as BIFM, DON and PE, which are classified in the POS zone. These three appear to be the groups with more experience on the adoption of at least one of patterns under analysis, as we can see also from table 4.1, with PE that is confirmed also for $\varepsilon = 0.3$.

Another interesting analysis is that one related to FE which is ruled-out in the pessimistic hypothesis, because it has no experience in the most common pattern of this case. As soon as we perform moderate or optimistic analysis (which weigh more on the single pattern than on their combination), the decision to exclude FE becomes less certain.

4.1.4 Errors and Accuracy

We evaluated results with respect to error and accuracy metrics, in the positive region (labelled as POS) and in the negative one (labelled as NEG). In the first case, we evaluate the ability of the method to correctly accept groups as perpetrators in the various hypotheses tested (pessimistic, moderate and optimistic). In the second case, we evaluate the ability to reject groups that cannot be considered perpetrators. We have used a confusion matrix, implemented in the R caret package[4], to obtain measures of *sensitivity* (*Sen*), *specificity* (*Spec*), *precision* (*Pre*), *recall* (*Rec*). These measures can be defined in terms of True Positive (t_p), False Positive (f_p), True Negative (t_n) and False Negative (f_n) classes as follows: $Sen = Rec = \frac{t_p}{t_p+f_n}$, $Spec = \frac{t_n}{t_n+f_p}$ and $Prec = \frac{t_p}{t_p+f_p}$. We report also combinations of these measures in terms of *f-measures* $F1 = 2\frac{Pec*Rec}{Prec+Rec}$ and *balanced accuracy* $BA = \frac{Sen+Spec}{2}$. Table 4.2 reports the confusion matrices for hypotheses testing in the positive and negative regions.

Table 4.2: Confusion matrices for the Hypotheses testing in *POS* and *NRG* regions (from [31])

			Truth	
		POS	BND	NEG
	POS	t_p	f_p	f_p
	BND	f_n	t_n	t_n
	NEG	f_n	t_n	t_n
			Case POS	
Prediction				
		POS	BND	NEG
	POS	t_n	t_n	f_n
	BND	t_n	t_n	f_n
	NEG	f_p	f_p	t_p
			Case NEG	

The Truth is derived from the GTD. For Case 1, it is easy to derive: ALS is the positive class because it is the only group that executed the attack behind this case. All the other groups are negative classes. For Case 2 and Case 3, this last one combines three patterns, it is not so trivial to define a ground truth because all the 21 groups executed the attacks behind the cases, and we need to identify positive and negative classes on the basis of the degree of experience in executing the patterns. The degree of experience is assessed as the relative frequency (rf) of

[4] https://cran.r-project.org/web/packages/caret/caret.pdf

adoption of the patterns by the groups. Specifically: we consider high experience if a group has a $rf \geq 1.5$ the mean of all the relative frequencies ($mean(rf)$), moderated experience if $rf \geq mean(rf)$, and low experience if $rf \geq 0.5 mean(rf)$. In order to include a BND region, even if narrow, we considered boundary classes the groups that are in a narrow neighbourhood of the three thresholds mentioned above. Thus, for example, in the optimistic case, we consider boundary the groups that have a $rf \in [1.4\, mean(rf),\ 1.6\, mean(rf)]$. Therefore, groups with $rf > 1.6 mean(rf)$ will be positive classes for the ground truth, and groups with $rf < 1.4 mean(rf)$ will be negative classes. Similarly, for the moderated and pessimistic cases. The relative frequencies for case 2 and case 3 are shown in fig. 4.2 where a red dashed line indicates the value of $mean(rf)$, the blue refers to 1.5 $mean(rf)$ and the black to 0.5 $mean(rf)$. The relative frequencies of Case 3 combine the three patterns, and Case 1 is not shown since only ALS executed the attack behind this case. We report here the boundary classes, so that a reader can easily identify the positive and negative classes from fig. 4.2: $BND_{case2\ Pess}\{$ MAO, PE, TAL, TTP $\}$, $BND_{case2\ Mod} = BND_{case2\ Opt}\{\phi\}$, $BND_{case3\ Pess}\{$ AQI, BH, MAO, ME $\}$, $BND_{case3\ Mod}\{$ ISIL SEP $\}$, $BND_{case3\ Opt}\{$ BIFM $\}$.

Fig.4.3 shows the performance measures when we move from Pessimistic to Optimistic analysis, and from positive support of evidence (i.e., $\varepsilon = 0.3$) to indications (i.e., $\varepsilon = 0.8$). Only results for $\varepsilon = 0.3$ (0.305 for the case 1) and $\varepsilon = 0.8$ are reported in fig.4.3. For the Case 2, however, the results for $\varepsilon = 0.1$ are the same of $\varepsilon = 0.3$.

Case 1 is based on a rare pattern. The evaluation of results for Case 1 POS is good for $\varepsilon = 0.305$, but worsens by $\varepsilon = 0.8$. This can be observed also looking at fig. 4.1 where we note that some groups belonging to negative classes appear in the POS region. This is motivated by the fact that the evidence, on which we base the assessment of the hypotheses, takes into account the overall similarity (not limited to the specific pattern analysed) of the groups. Thus, when we lower the support level of evidence,

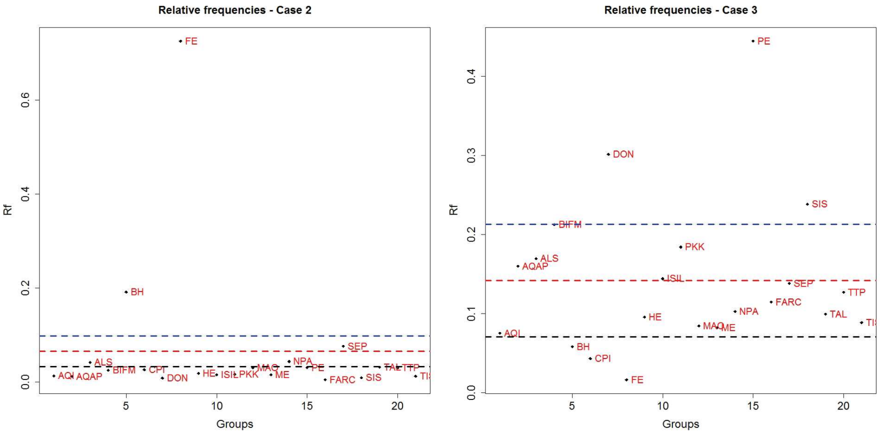


Figure 4.2: Relative Frequencies of adoption of the patterns behind Case 2, left-hand side, and Case 3, right-hand side (from [31])

our method reports information about the groups that have a behaviour most similar to ALS. For Case 1 NEG, on the other hand, there is a slight improvement in moving from $\varepsilon = 0.305$ to $\varepsilon = 0.8$, and this because further true negative classes are predicted. The BA for this case is always > 0.5.

Case 2 considers only a distinctive pattern. In general, we observe that the results are positive as regards the attribution of the hypothesis in POS cases, worse in NEG cases (except for the optimistic $\varepsilon = 0.8$, with good results for both). To this end, we observe that the measure of specificity is generally low in the NEG case, and also the sensitivity is very low in the NEG case for $\varepsilon = 0.3$. The low sensitivity indicates errors in the capacity of correctly identifying the groups that cannot be associated to the event (that are, in the NEG case, the true positive samples). This can be observed also looking at fig. 4.1 where we note that the NEG region for $\varepsilon = 0.3$ has no groups inside. The specificity measure indicates an error in rejecting group that can be associated to the pattern (that are the true negative samples in the NEG case). The reason is that several groups fall in the BND region.

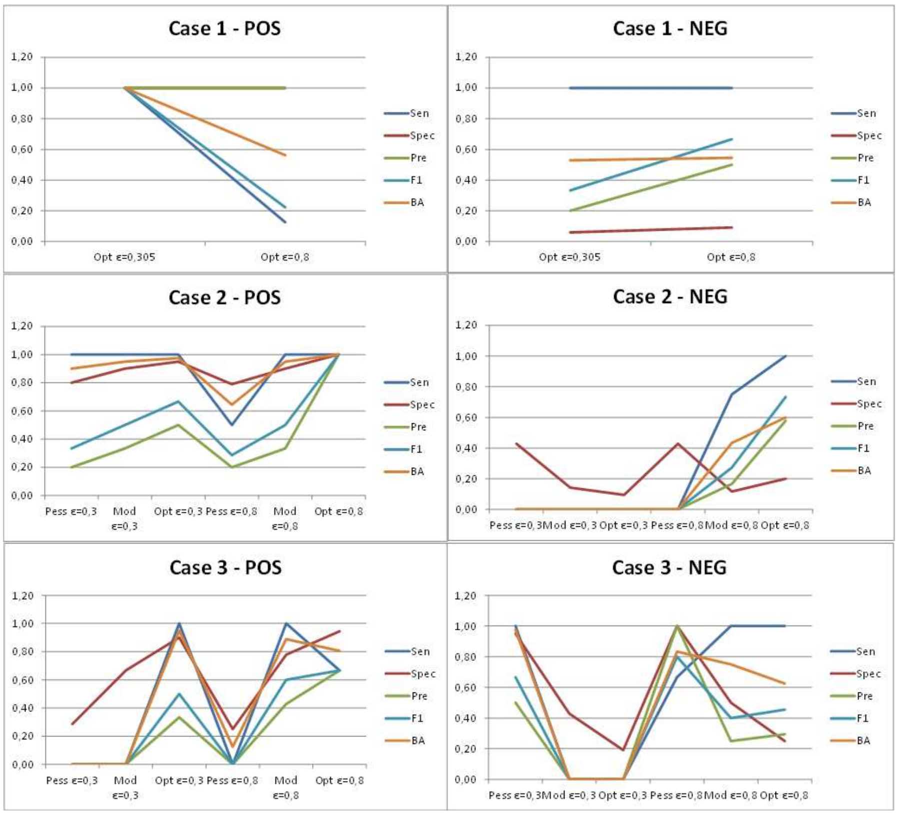


Figure 4.3: Results evaluation (from [31])

Case 3 combines three patterns. The results appear to be better in the case of attribution of positive cases if we assume an optimistic analysis (execution of one among the patterns) while it is the opposite for pessimistic (an ”and” among the patterns) where the results are better as regards the attribution of negative cases.

4.2 Evaluation of the secure partition method

A wide number of events of the GTD includes attacks perpetrated in villages or urban areas targeting private citizens and properties (i.e., TT14), military (i.e., TT4), business (such as restaurant, caf, stores, i.e., TT1). An attack pattern of this type is, for example, the one discussed in case 2 of section 4.1, $< AT2, TT14, WT5 >$ referring to an armed assault attack strategy (AT2), with firearms (WT5) towards private citizens and property (TT14).

The secure partition method presented and described in section 3.1.2 has been evaluated on a case study built on top of these kinds of events.

Let us suppose the hypothesis under analysis relates to an armed assault in a city, with firearms towards citizens, police or business. Suppose, moreover, that the attack strategy can be implemented through the use of guns or rifles and/or arson. The threat scenarios that can be generated refer to: *i)* armed assault with guns and rifles; *ii)* armed assault based on arson; *iii)* combination of both cases.

The area under analysis consists of eight points of interest that are modelled by two descriptive attributes: a Capacity (C) and a degree of importance (I). C refers to the number of people usually present in or near the building, I refers to a degree of importance of the building (or point of interest) in relation also to its perceived image.

The case study can be modelled with the information table of table 4.3, where C and I are the domain attributes. Let us suppose ATM and Car rental service are protected by metal detectors to detect firearms such as guns, the other points of interest are not equipped with such devices. Instead, the last four points of interest are equipped with Fire protection systems, so they are less vulnerable to arson. Let be $a1$ a threat based on arson and $a2$ based on the adoption of guns or riffles. To model these situations, we use the two attack attributes, $a1$ and $a2$, as follows: 00 means no attack, 10 means that assault based on arson, 01 means assault based on guns or riffles, and last, 11 means a combination of arson and guns / riffles.

Table 4.3: Case study for urban area

	C	I	a1	a2
Hospital	200	0,8	1	1
ATM	100	0,2	1	0
Car hire service	154	0,4	1	0
Church	300	0,9	1	1
Tea Garden	145	0,6	0	1
Police	164	0,9	0	1
Hotel	130	0,7	0	1
School	185	0,8	0	1

The decision maker wants to partition the city to limit the losses to 5 casualties in most cases. S/he decides to divide the area in three regions and applies three different levels of protection: high for the red zone, medium for the orange and low for the green. These levels correspond to three different values of E_r, as reported in Table 4.4. Of course, values of E_r are implemented with different resources employed to protect the area, and are associated with different costs (usually higher for higher values of E_r).

In the following, we refer to the red, orange and green zones also as POS, BND, and NEG, respectively. Let us last suppose that the maximum damage in a region (in terms of causalities) is 30.

Let be v an evaluation function for the objects that evaluates

Table 4.4: Areas and E_r values (extracted from [32])

Zone	E_r
Red Area (POS)	0.8
Orange Area (BND)	0.5
Green Area (NEG)	0.2

Table 4.5: Probabilistic information (from [32])

	$[a]_{00}$	$[a]_{10}$	$[a]_{01}$	$[a]_{11}$
$Pr([a])$	0	0,25	0,5	0,25
$Pr(POS \mid [a])$	0	0	0,5	1
$Pr(BND \mid [a])$	0	0	0,5	0
$Pr(NEG \mid [a])$	0	1	0	0

each object, u_i, as a normalized capacity multiplied by the degree of importance of the point: $v(u_i) = \dfrac{C(u_i)}{max(C)} * I(u_i)$

In a first phase, the decision maker decides to accurately protect church, hospital, police building and school, and includes these objects in a red area. S/He decides for a medium level of protection for hotel and tea garden, including them in an orange area. For the other two objects, s/he decides for a lower level of protection by placing them in a green area. The three zones are shown in fig. 4.4 where in the $RED = POS = \{Churc, Hospital, Police, School\}$, $ORANGE = BND = \{Hotel, Tea\ Garden\}$ and $GREEN = NEG = \{ATM, Car\ Hire\}$ that correspond to $\beta = 0.25$ and $\alpha = 0.45$ (where POS is $v(u) \geq \alpha$ and NEG is $v(u) \leq \beta$).

The four attacks are represented by the equivalence classes:
$[a]_{00} = \{\phi\}$,
$[a]_{10} = \{ATM, Car\ Hire\}$,
$[a]_{01} = \{Tea\ Garden, Police, Hotel, School\}$
$[a]_{11} = \{Hospital, Church\}$.

From these granules, we can derive the probabilistic information, reported in table 4.5, to be used for analysis of threat scenarios.

Let us evaluate the expected losses with eq. (3.5) of section

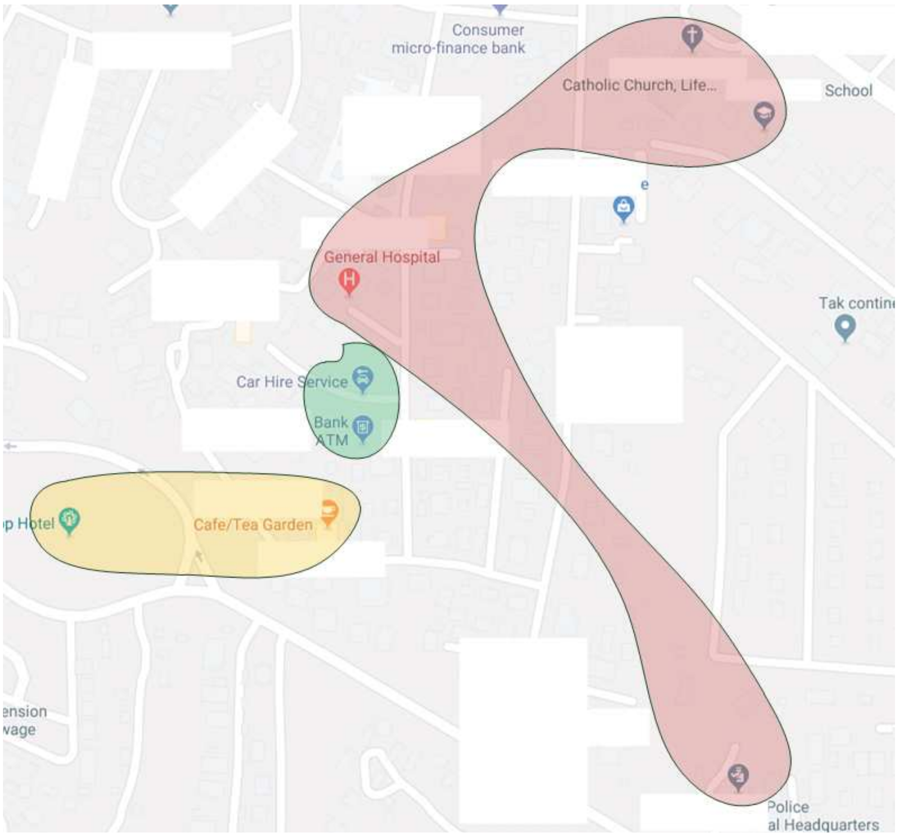


Figure 4.4: Area partition.

Table 4.6: Expected losses (from [32])

	$[a]_{00}$	$[a]_{10}$	$[a]_{01}$	$[a]_{11}$
POS	0	0	1.5	1.5
BND	0	0	3.75	0
NEG	0	6	0	0

Table 4.7: Probabilities $z^{'}$ (from [32])

	$[a]_{00}$	$[a]_{10}$	$[a]_{01}$	$[a]_{11}$
POS	1	0.75	0.75	1
BND	1	0.75	1	0.5
NEG	1	1	0.25	0.5

3.1.2, where we use $L_{max} = 30$ and E_r values as in table 4.4, and the vulnerability indexes can be evaluated with the values of table 4.5. The expected losses are reported in the table 4.6.

For our application, we can reason in pessimistic terms (i.e., losses); therefore, we can perform the analysis of stochastic dominance using $z^{'}$ and $\rho^{'}$. To evaluate the probabilities $z^{'}$, we apply eq. (2.21) where the a priori probability distribution values λ_y refer to the three regions obtained with 3WD: $\lambda = \{\lambda_{POS}, \lambda_{BND}, \lambda_{NEG}\} = \{\frac{4}{8}, \frac{2}{8}, \frac{2}{8}\}$. The values of $z^{'}$ are reported in table 4.7

Following eq. (2.23), the values of $\rho^{'}$ are in table 4.8, which can also be represented with fig. 4.5. In fig. 4.5, the values of ordinates are losses ($\rho^{'}$) and the abscissas are probabilities.

Fig.4.5 can be analysed with the following interpretation:

Table 4.8: $\rho^{'}$ values (from [32])

	$[a]_{00}$	$[a]_{10}$	$[a]_{01}$	$[a]_{11}$
0.25	0	0	0	0
0.5	0	0	1,5	0
0.75	0	0	1,5	1,5
1	0	6	3,75	1,5

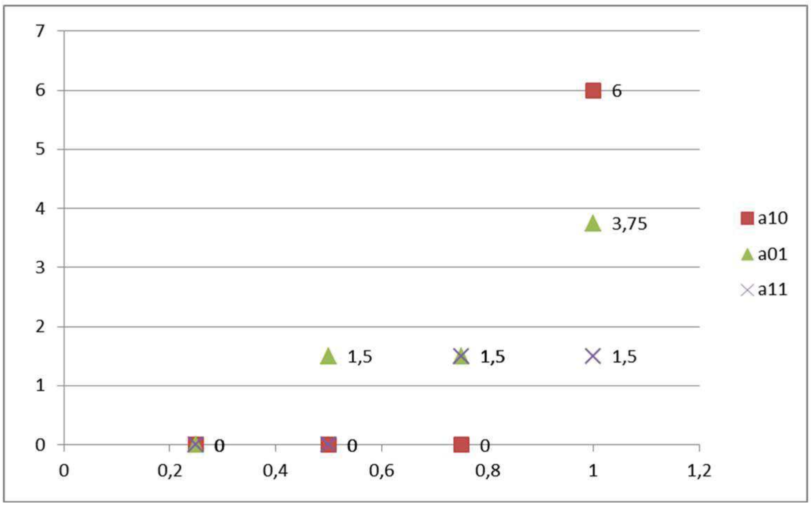


Figure 4.5: Case: $\beta = 0.25$ and $\alpha = 0.45$ (elaborated from [32])

- the values of $\rho^{'}$ corresponding to abscissa 1 are certain and read as follows: in the case of threat $[a]_{01}$, the expected loss is definitely 3.75; in the case of threat $[a]_{10}$, the expected loss is definitely 6; and in the case of threat $[a]_{11}$, the expected loss is definitely 1.5.

- the values of $\rho^{'}$ corresponding to abscissa 0.75 are highly probable values and read as follows: in the case of threat $[a]_{01}$, the expected loss is at most 1.5 with a probability of at least 0.75; in the case of threat $[a]_{10}$, the expected loss is at most 0 with a probability of at least 0.75; and in the case of threat $[a]_{11}$, the expected loss is at most 1.5 with a probability of at least 0.75.

The threat scenarios of the case $\beta = 0.25$ - $\alpha = 0.50$ are the following: $TS_{10} = ([a]_{10}, < 0, 6 >, < 0.25, 1 >)$, $TS_{01} = ([a]_{01}, < 0, 1.5 >, < 0.25, 0.75 >)$, and $TS_{11} = ([a]_{11}, < 0, 1.5, 3.5 >, < 0.25, 0.5, 1 >)$. The last TS is interpreted as follows: in case of attack $[a]_{11}$, the expected loss is 0 with a probability greater than 0.25, the expected loss is at most 1.5 with a probability greater than 0.5, and the expected loss is at most 3.5 in any case.

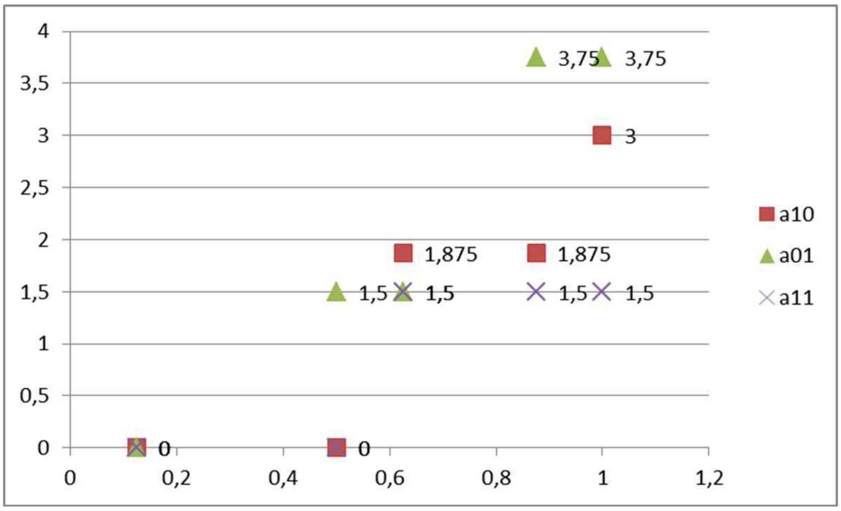


Figure 4.6: Case: $\beta = 0.20$ and $\alpha = 0.50$ (elaborated from [32])

4.2.1 Quality of partition.

The decision maker could make other choices. It could decide to increase the resources available for protection of a point of interest and move it, for example, from a BND region to a POS. This involves a new partition of the objects with the creation of new granules and, consequently, different values of $\rho^{'}$. As regards the case analysed in the previous section, s/he could decide to expand the BND area to include the points: Car Hire Service, Police and School. S/he could decide to leave only ATM in the NEG area, and Church and Hospital in the POS one. With our evaluation function, v, this corresponds to setting $\alpha = 0.20$ and $\beta = 0.50$. Under these conditions, the DRSA analysis leads to a different result shown in the fig. 4.6.

Analysing fig. 4.6, one might be tempted to say that the new situation is better than that one represented in fig. 4.5. It emerges, in fact, that in fig. 4.6 the certainties report minor losses compared to fig. 4.5. However, a deeper analysis denies this result. It is observed, in fact, that the losses expected from $a01$ attack are higher for higher probability values in the case shown in fig.4.6.

To support the decision maker in the analysis phases, it would be useful a measure able to provide indications on the quality of a partition, as a whole and with respect to the single threats, starting from basic granules (parts and equivalence classes). This measure depends on the level of protection applied in the parts of P and on the vulnerability index of the parts. Let us define the quality of the partition P with respect to the attack $[a]_j$ as:

$$\begin{aligned}&Q_{[a]_j}(P) = Q_{[a]_j}(POS) + Q_{[a]_j}(BND) + Q_{[a]_j}(NEG) = \\ &(1 - E_r)_{POS} Vi_{[a]_j}(POS) + (1 - E_r)_{BND} Vi_{[a]_j}(BND) + \\ &(1 - E_r)_{NEG} Vi_{[a]_j}(NEG)\end{aligned} \tag{4.1}$$

where the subscript POS refers to the positive region, $Vi_{[a]_j}(POS) = Pr([a]_j)Pr(POS|[a]_j)$ is the vulnerability index of the positive region with respect to the attack $[a]_j$, and $(1 - E_r)_{POS}$ is its level of protection. The same description applies to the subscripts NEG and BND. We assume the level of protection is homogeneous in a region, i.e., it is the same for all the objects in the region. An overall measure of quality for the partition is:

$$Q(P) = \sum_{[a]} Q_{[a]}(P). \tag{4.2}$$

The measure of quality has to be minimized. In fact, under the assumption of homogeneous levels of protection, it minimizes the vulnerability indexes of the three regions. Eq. (4.1) and eq. (4.2) can be considered as contextualizations of the usual forms of the quality of a partition, such as the one reported in [109]: $Q(P) = \omega_{POS}Q(POS) + \omega_{BND}Q(BND) + \omega_{NEG}Q(NEG)$, where the weights ω refer to $(1 - E_r)$, and the quality of a region is measured with the vulnerability index.

Eq. (4.1) depends on a specific attack $[a]$, since it is clear that the vulnerability indexes of the three regions are dependent on how these regions are vulnerable to a specific attack. In eq. (4.2), the vulnerability indexes of the three regions do not depend on the attacks. This result is intuitively correct since, under uncertainty conditions, an overall measure such as eq. (4.2) considers the fraction of all objects that are vulnerable to all attacks and how they are protected and can be formally proved by expanding eq. (4.2). Thus, eq. (4.2) can provide only relative information and has to be used in combination with eq. (4.1) to allow reasoning and decision making.

Tables 4.9 and 4.10 report the quality measure for the two cases.

Table 4.9: Quality measures for $\beta = 0.25$ - $\alpha = 0.40$

	Overall	a10	a01	a11
POS	0,1	0	0,05	0,05
BND	0,125	0	0,125	0
NEG	0,2	0,2	0	0
	0,425	**0,2**	**0,175**	**0,05**

Table 4.10: Quality measures for $\beta = 0.20$ - $\alpha = 0.50$

	Overall	a10	a01	a11
POS	0,05	0	0	0,05
BND	0,3125	0,0625	0,25	0
NEG	0,1	0,1	0	0
	0,4625	**0,1625**	**0,25**	**0,05**

As we can observe, the overall quality is better in case $\beta = 0.25$ - $\alpha = 0.4$. The movements of Car Hire Service (from the NEG to BND), Police and School (from POS to BND), lead to a BND region that is more vulnerable in the case $\beta = 0.20$ - $\alpha = 0.50$. The cost associated to the two cases is, however, different. In the case $\beta = 0.25$ - $\alpha = 0.4$, the cost is higher since we have four objects in the POS area compared to the two of case $\beta = 0.20$ - $\alpha = 0.50$, and the values of E_r in the POS area are higher than the ones in the BND and NEG areas. This means that more resources have to be deployed for the protection of the target area.

The decision maker can avoid this additional cost if s/he has more precise information about the threat. As can be observed from the values of the quality measure for the individual threats, in fact, if one were reasonably convinced of an arson attack, case $\beta = 0.20$ - $\alpha = 0.50$ offers a higher quality at a lower cost.

We have assumed homogeneous levels of protection for the three areas that are related to the three values of E_r of Table 4.4. This assumption is not mandatory and, indeed, is not always the best choice. Different values of E_r can also be used when the decision maker is satisfied by the probability distribution of the outcomes and wants only to reduce the expected losses. Let us consider case $\beta = 0.20$ - $\alpha = 0.50$. In this case, the $BND = \{Tea\ Garden, Hotel, Police, School\}$ with four objects vulnerable to $[a]_{01}$ and 1 object vulnerable to $[a]_{10}$. The decision maker can set E_r in a non-homogeneous way as follows:

$$E_r(POS) = \begin{cases} 0.8 & if\ [a]_{11} \\ 0.2 & otherwise \end{cases}$$

$$E_r(NEG) = \begin{cases} 0.8 & if\ [a]_{10} \\ 0.2 & otherwise \end{cases}$$

$$E_r(BND) = \begin{cases} 0.8 & if\ [a]_{01} \\ 0.4 & otherwise \end{cases}$$

and the quality is:

$Q(P_{0.20-0.50}) = 0.2 * Vi_{[a]_{10}}(NEG) + [0.2 * Vi_{[a]_{01}}(BND) + 0.6 * Vi_{[a]_{10}}] + 0.2 * Vi_{[a]_{11}}(POS) = 0.2 * 0.125 + [0.2 * 0.5 + 0.6 * 0.125] + 0.2 * 0.25 = 0.25$

which is lower.

Chapter 5

Conclusions and future works

The work carried out in the Ph.D period has led to the definition of three approximate reasoning methods that can support decision makers in the initial phases of a counter-terrorism analysis process. The GrC techniques used, which are mainly based on extensions of the rough set model, have provided satisfactory results and the 3WD models have confirmed their ability to reduce the cognitive effort related to the interpretation of results for decision-making purposes.

One of the main problems encountered during the study is the scarcity of real data in the application sector chosen for this thesis. With the exception of the GTD and a few others (e.g., for crime analysis) not many data sets are available. This problem has been very serious with regard to experimentation and validation of the method for resilience analysis.

Although the results presented have been validated in application scenarios aimed at supporting the stages of an intelligence analysis cycle, the proposed methods and tools can be applied in other scenarios, such as crime investigations and evidence-based medicine. In general, the methods presented in this thesis can be applied in cases of analysis and assessment of hypotheses related to events (e.g., counter-terrorism, organized crime, adverse events in medicine). In particular, they are such to support the phase of analysis of the hypothesis. This phase is, in general, complex and influenced by cognitive biases and wrong mental models of the analyst. Our methods allow to refine hypotheses according to different situations and assess the refined hypotheses with respect to available evidence. This last one is also created starting from available data.

The proposed methods present some limitations that will be investigated in future works.

In particular, in the method of analysis and assessment of terrorism hypotheses, we assume that information sources are trusted and does not weigh their information differently. So, this method is very vulnerable to the threat of deception, and need to integrate a technique to evaluate "*completeness and soundness of available information sources*" such as the quality of information check of [29]. A second limitation relates to the lack of diagnosticity of evidence. In fact, we question ourselves about the hypotheses because we generate different situations but we trust the evidence that should support or not support these hypotheses. Lastly, to deal with big data, we aim to extend our method in order to allow the derivation and refinement of hypotheses starting from data streams and supporting the combination of structured (i.e., the GTD) and not structured data (e.g., social media content) to improve the phase of evidence creation. Of course, this requires also different technological choices such as the adoption of the Lambda Architecture. For instance, an architecture based on Apache Kafka (to collect data from different sources) and Apache Spark (designed to handle massive data and to enable both batch and stream-processing methods) could support all the phases of the proposed approach, except for the final decision dashboard that should be implemented by using Web technologies interacting with the results provided by Apache Spark.

The method for secure partition is sensitive to the number of scenarios that can be generated, as result of the previous method, from a hypothesis under investigation. Also in this case, a better integration of this method with some structured analytic techniques, such as analysis of competing hypotheses (ACH) and devil's advocacy, can help in preparing and filtering scenarios. The adoption of granules of knowledge in the inference phase allows us to have approximate solutions to our problem of zone partitions, which are analysable at different levels of granularity. Accordingly, the decision maker can decide whether to concentrate on dominant scenarios or on the whole set of alternative possible attacks. However, the decision maker has to be aware of the inherent uncertainty regarding the use of GrC.

With regards to the resilience analysis method, its main limitations for applications to real CI have been already discussed in [33]. Similar considerations can be repeated for the applications sector of this thesis. We mention, for instance, the issues of modelling and representing dependencies among potential targets of an urban area under attack. While it appears clear that there can be a logical dependency between a military target (e.g., a police station) and civil ones (e.g., private properties) since an attack to the first may cause a reduction of the protection for the second, it is quite challenging to properly quantify this phenomenon. To a certain extent, a similar problem is related to the correct definition of critical functionality, K, to be used in the resilience model. Also, the nature of the dependencies may be fuzzy rather than crisp and, in this case, we have to refine the approach for granular representation of dependencies by using fuzzy granular structures.

Lastly, the complexity of the phenomenon under investigation will require an additional study devoted to analyse and evaluate the integration of other datasets with the GTD.

Bibliography

[1] M. R. Endsley, “Toward a theory of situation awareness in dynamic systems,” *Human factors*, vol. 37, no. 1, pp. 32–64, 1995.

[2] N. A. Stanton, P. M. Salmon, G. H. Walker, and D. P. Jenkins, “Is situation awareness all in the mind?” *Theoretical Issues in Ergonomics Science*, vol. 11, no. 1-2, pp. 29–40, 2010.

[3] M. Endsley and W. Jones, “Situation awareness, information dominance, and information warfare (united states air force armstrong laboratory technical report 97-01),” 1997.

[4] L. A. Zadeh, “Toward a theory of fuzzy information granulation and its centrality in human reasoning and fuzzy logic,” *Fuzzy sets and systems*, vol. 90, no. 2, pp. 111–127, 1997.

[5] Y. Yao, “A triarchic theory of granular computing,” *Granular Computing*, vol. 1, no. 2, pp. 145–157, 2016.

[6] V. Loia, G. DAniello, A. Gaeta, and F. Orciuoli, “Enforcing situation awareness with granular computing: a systematic overview and new perspectives,” *Granular Computing*, vol. 1, no. 2, pp. 127–143, 2016.

[7] S. Krasmann and C. Hentschel, “situational awareness: Rethinking security in times of urban terrorism,” *Security Dialogue*, vol. 50, no. 2, pp. 181–197, 2019.

[8] H. H. Willis, “Using risk analysis to inform intelligence analysis,” *Wiley Handbook of Science and Technology for Homeland Security*, pp. 1–10, 2008.

[9] L. Krizan, "Intelligence essentials for everyone," JOINT MILITARY INTELLIGENCE COLL WASHINGTON DC, Tech. Rep., 1999.

[10] R. J. Heuer Jr, R. J. Heuer, and R. H. Pherson, *Structured analytic techniques for intelligence analysis.* Cq Press, 2010.

[11] G. D'Aniello, A. Gaeta, M. Gaeta, V. Loia, and M. Z. Reformat, "Application of granular computing and three-way decisions to analysis of competing hypotheses," in *Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on.* IEEE, 2016, pp. 001 650–001 655.

[12] S. Jin, J. Ge, and J. Peng, "Terrorism risk assessment using hierarchical bidirectional fuzzy rule interpolation," in *2016 IEEE 15th International Conference on Cognitive Informatics & Cognitive Computing (ICCI* CC).* IEEE, 2016, pp. 403–410.

[13] ——, "A new fuzzy rule interpolation approach to terrorism risk assessment," in *Violent Extremism: Breakthroughs in Research and Practice.* IGI Global, 2019, pp. 351–372.

[14] Y.-C. Ko and H. Fujita, "An evidential analytics for buried information in big data samples: Case study of semiconductor manufacturing," *Information Sciences*, vol. 486, pp. 190–203, 2019.

[15] M. Valtorta, J. Dang, H. Goradia, J. Huang, and M. Huhns, "Extending heuers analysis of competing hypotheses method to support complex decision analysis," in *Proceedings of the International Conference on Intelligence Analysis.* Citeseer, 2005.

[16] Y. Yao, "Three-way decision and granular computing," *International Journal of Approximate Reasoning*, vol. 103, pp. 107–123, 2018.

[17] J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, "Anomaly detection based on zone partition for security protection of industrial cyber-physical systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 5, pp. 4257–4267, 2018.

[18] M. McBride and R. Mitchell, "A zoning algorithm for dynamic cyber zone defense," in *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*. IEEE, 2017, pp. 1–6.

[19] F. Karbalaei and H. Shahbazi, "Determining an appropriate partitioning method to reduce the power system dimensions for real time voltage control," *International Journal of Electrical Power & Energy Systems*, vol. 100, pp. 58–68, 2018.

[20] C. Zhang and J. E. Ramirez-Marquez, "Protecting critical infrastructures against intentional attacks: a two-stage game with incomplete information," *IIE Transactions*, vol. 45, no. 3, pp. 244–258, 2013.

[21] L. Zhang and G. Reniers, "Applying a bayesian stackelberg game for securing a chemical plant," *Journal of Loss Prevention in the Process Industries*, vol. 51, pp. 72 – 83, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0950423017310239

[22] E. Jenelius, J. Westin, and Å. J. Holmgren, "Critical infrastructure protection under imperfect attacker perception," *International Journal of Critical Infrastructure Protection*, vol. 3, no. 1, pp. 16–26, 2010.

[23] V. M. Payappalli, J. Zhuang, and V. R. R. Jose, "Deterrence and risk preferences in sequential attacker–defender games with continuous efforts," *Risk Analysis*, 2017.

[24] D. Wu, H. Xiao, and R. Peng, "Object defense with preventive strike and false targets," *Reliability Engineering & System Safety*, vol. 169, pp. 76–80, 2018.

[25] V. Loia, A. Gaeta, and F. Orciuoli, *Ambient Intelligence: A Perspective of Granular Computing.* Wiley Encyclopedia of Electrical and Electronics Engineering, 2017, pp. 1–15. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8356

[26] S. L. Cutter *et al.*, “Disaster resilience: A national imperative,” *Environment: Science and Policy for Sustainable Development*, vol. 55, no. 2, pp. 25–29, 2013.

[27] A. A. Ganin, E. Massaro, A. Gutfraind, N. Steen, J. M. Keisler, A. Kott, R. Mangoubi, and I. Linkov, “Operational resilience: concepts, design and analysis,” *Scientific reports*, vol. 6, 2016.

[28] Y. Yao, “Three-way decisions and cognitive computing,” *Cognitive Computation*, vol. 8, no. 4, pp. 543–554, 2016.

[29] R. J. Heuer, *Psychology of intelligence analysis.* Jeffrey Frank Jones, 1999.

[30] W. Chang, E. Berdini, D. R. Mandel, and P. E. Tetlock, “Restructuring structured analytic techniques in intelligence,” *Intelligence and National Security*, vol. 33, no. 3, pp. 337–356, 2018.

[31] H. Fujita, A. Gaeta, V. Loia, and F. Orciuoli, “Hypotheses analysis and assessment in counter-terrorism activities: a method based on owa and fuzzy probabilistic rough sets,” *IEEE TFS. (Accepted).*

[32] ——, “Improving awareness in early stages of security analysis: A zone partition method based on grc,” *Applied Intelligence*, vol. 49, no. 3, pp. 1063–1077, 2019.

[33] H. Fujita, A. Gaeta, V. Loia, and F. Orciuoli, “Resilience analysis of critical infrastructures: A cognitive approach based on granular computing,” *IEEE Transactions on Cybernetics*, vol. 49, no. 5, pp. 1835–1848, May 2019.

[34] J. T. Yao, A. V. Vasilakos, and W. Pedrycz, “Granular computing: perspectives and challenges,” *IEEE Transactions on Cybernetics*, vol. 43, no. 6, pp. 1977–1989, 2013.

[35] W. Pedrycz, A. Gacek, and X. Wang, “Clustering in augmented space of granular constraints: A study in knowledge-based clustering,” *Pattern Recognition Letters*, vol. 67, pp. 122–129, 2015.

[36] W. Pedrycz and W. Homenda, “Building the fundamentals of granular computing: a principle of justifiable granularity,” *Applied Soft Computing*, vol. 13, no. 10, pp. 4209–4218, 2013.

[37] L. Livi and A. Sadeghian, “Data granulation by the principles of uncertainty,” *Pattern Recognition Letters*, vol. 67, pp. 113–121, 2015.

[38] ——, “Granular computing, computational intelligence, and the analysis of non-geometric input spaces,” *Granular Computing*, vol. 1, no. 1, pp. 13–20, 2016.

[39] Z. Pawlak, “Rough sets,” *International journal of computer & information sciences*, vol. 11, no. 5, pp. 341–356, 1982.

[40] Q. Zhang, Q. Xie, and G. Wang, “A survey on rough set theory and its applications,” *CAAI Transactions on Intelligence Technology*, vol. 1, no. 4, pp. 323 – 333, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2468232216300786

[41] Y. Yao, “An outline of a theory of three-way decisions,” in *Rough Sets and Current Trends in Computing*, J. Yao, Y. Yang, R. Słowiński, S. Greco, H. Li, S. Mitra, and L. Polkowski, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 1–17.

[42] ——, “Three-way decisions with probabilistic rough sets,” *Information Sciences*, vol. 180, no. 3, pp. 341 – 353, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025509004253

[43] ——, “Probabilistic rough set approximations,” *International Journal of Approximate Reasoning*, vol. 49, no. 2, pp. 255 – 271, 2008, special Section on Probabilistic Rough Sets and Special Section on PGM06. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0888613X07001491

[44] ——, “The superiority of three-way decisions in probabilistic rough set models,” *Information Sciences*, vol. 181, no. 6, pp. 1080 – 1096, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025510005645

[45] ——, "Three-way decisions with probabilistic rough sets," *Information Sciences*, vol. 180, no. 3, pp. 341–353, 2010.

[46] X. Deng and Y. Yao, "An information-theoretic interpretation of thresholds in probabilistic rough sets," in *International Conference on Rough Sets and Knowledge Technology.* Springer, 2012, pp. 369–378.

[47] C. Gao and Y. Yao, "Determining thresholds in three-way decisions with chi-square statistic," in *International Joint Conference on Rough Sets.* Springer, 2016, pp. 272–281.

[48] J. P. Herbert and J. Yao, "Game-theoretic rough sets," *Fundamenta Informaticae*, vol. 108, no. 3-4, pp. 267–286, 2011.

[49] D. Slezak and W. Ziarko, "The investigation of the bayesian rough set model," *International journal of approximate reasoning*, vol. 40, no. 1-2, pp. 81–91, 2005.

[50] D. Slezak, "Rough sets and bayes factor," in *Transactions on Rough Sets III.* Springer, 2005, pp. 202–229.

[51] D. Dubois and H. Prade, "Rough fuzzy sets and fuzzy rough sets," *International Journal of General System*, vol. 17, no. 2-3, pp. 191–209, 1990.

[52] D. S. Yeung, D. Chen, E. C. Tsang, J. W. Lee, and W. Xizhao, "On the generalization of fuzzy rough sets," *IEEE Transactions on fuzzy systems*, vol. 13, no. 3, pp. 343–361, 2005.

[53] Q. Hu, D. Yu, Z. Xie, and J. Liu, "Fuzzy probabilistic approximation spaces and their information measures," *IEEE transactions on fuzzy systems*, vol. 14, no. 2, pp. 191–201, 2006.

[54] X. R. Zhao and B. Q. Hu, "Fuzzy probabilistic rough sets and their corresponding three-way decisions," *Knowledge-Based Systems*, vol. 91, pp. 126–142, 2016.

[55] L. A. Zadeh, "Probability measures of fuzzy events," *Journal of mathematical analysis and applications*, vol. 23, no. 2, pp. 421–427, 1968.

[56] S. Greco, B. Matarazzo, and R. Slowinski, "Rough approximation of a preference relation by dominance relations," *European Journal of operational research*, vol. 117, no. 1, pp. 63–83, 1999.

[57] S. Greco, B. Matarazzo, and R. Słowiński, "Dominance-based rough set approach to decision under uncertainty and time preference," *Annals of Operations Research*, vol. 176, no. 1, pp. 41–75, 2010.

[58] H. Levy, "Stochastic dominance and expected utility: survey and analysis," *Management science*, vol. 38, no. 4, pp. 555–593, 1992.

[59] R. R. Yager, "On ordered weighted averaging aggregation operators in multicriteria decisionmaking," *IEEE Transactions on systems, Man, and Cybernetics*, vol. 18, no. 1, pp. 183–190, 1988.

[60] ——, "Owa aggregation with an uncertainty over the arguments," *Information Fusion*, 2019.

[61] ——, "Generalizing variance to allow the inclusion of decision attitude in decision making under uncertainty," *International journal of approximate reasoning*, vol. 42, no. 3, pp. 137–158, 2006.

[62] Q. Hu, L. Zhang, D. Chen, W. Pedrycz, and D. Yu, "Gaussian kernel based fuzzy rough sets: Model, uncertainty measures and applications," *International Journal of Approximate Reasoning*, vol. 51, no. 4, pp. 453–471, 2010.

[63] B. Moser, "On the t-transitivity of kernels," *Fuzzy Sets and Systems*, vol. 157, no. 13, pp. 1787–1796, 2006.

[64] ——, "On representing and generating kernels by fuzzy equivalence relations," *Journal of machine learning research*, vol. 7, no. Dec, pp. 2603–2620, 2006.

[65] R. R. Yager and M. Z. Reformat, "Looking for like-minded individuals in social networks using tagging and e fuzzy sets," *IEEE Transactions on Fuzzy Systems*, vol. 21, no. 4, pp. 672–687, 2013.

[66] G. D'Aniello, A. Gaeta, M. Gaeta, V. Loia, and M. Z. Reformat, "Collective awareness in smart city with fuzzy cognitive maps

and fuzzy sets," in *2016 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE).* IEEE, 2016, pp. 1554–1561.

[67] R. J. Heuer Jr, "Improving intelligence analysis with ach," 2005.

[68] W. L. McGill, B. M. Ayyub, and M. Kaminskiy, "Risk analysis for critical asset protection," *Risk Analysis*, vol. 27, no. 5, pp. 1265–1281, 2007.

[69] C. S. Holling, "Resilience and stability of ecological systems," *Annual review of ecology and systematics*, vol. 4, no. 1, pp. 1–23, 1973.

[70] M. Scheffer, S. R. Carpenter, T. M. Lenton, J. Bascompte, W. Brock, V. Dakos, J. Van De Koppel, I. A. Van De Leemput, S. A. Levin, E. H. Van Nes *et al.*, "Anticipating critical transitions," *science*, vol. 338, no. 6105, pp. 344–348, 2012.

[71] V. Dakos, S. R. Carpenter, E. H. van Nes, and M. Scheffer, "Resilience indicators: prospects and limitations for early warnings of regime shifts," *Philosophical Transactions of the Royal Society B: Biological Sciences*, vol. 370, no. 1659, p. 20130263, 2015.

[72] M. Scheffer, S. R. Carpenter, V. Dakos, and E. H. van Nes, "Generic indicators of ecological resilience: inferring the chance of a critical transition," *Annual Review of Ecology, Evolution, and Systematics*, vol. 46, pp. 145–167, 2015.

[73] J. Ascough, H. Maier, J. Ravalico, and M. Strudley, "Future research challenges for incorporation of uncertainty in environmental and ecological decision-making," *Ecological modelling*, vol. 219, no. 3, pp. 383–399, 2008.

[74] Y. Cai, G. Huang, Q. Tan, and B. Chen, "Identification of optimal strategies for improving eco-resilience to floods in ecologically vulnerable regions of a wetland," *Ecological Modelling*, vol. 222, no. 2, pp. 360–369, 2011.

[75] E. H. Meesters, R. P. Bak, S. Westmacott, M. Ridgley, and S. Dollar, "A fuzzy logic model to predict coral reef development under nutrient and sediment stress," *Conservation Biology*, vol. 12, no. 5, pp. 957–965, 1998.

[76] M. Makowski and H. Nakayama, *Natural Environment Management and Applied Systems Analysis.* IR-01-021, 2001.

[77] E. Demartini, A. Gaviglio, and D. Bertoni, "Integrating agricultural sustainability into policy planning: A geo-referenced framework based on rough set theory," *Environmental Science & Policy*, vol. 54, pp. 226–239, 2015.

[78] A. E. Quinlan, M. Berbés-Blázquez, L. J. Haider, and G. D. Peterson, "Measuring and assessing resilience: broadening understanding through multiple disciplinary perspectives," *Journal of Applied Ecology*, vol. 53, no. 3, pp. 677–687, 2016.

[79] "An adaptive learning process for developing and applying sustainability indicators with local communities," *Ecological Economics*, vol. 59, no. 4, pp. 406 – 418, 2006.

[80] F. Berkes and M. K. Berkes, "Ecological complexity, fuzzy logic, and holism in indigenous knowledge," *Futures*, vol. 41, no. 1, pp. 6–12, 2009.

[81] L. A. Andriantiatsaholiniaina, V. S. Kouikoglou, and Y. A. Phillis, "Evaluating strategies for sustainable development: fuzzy logic reasoning and sensitivity analysis," *Ecological Economics*, vol. 48, no. 2, pp. 149–172, 2004.

[82] Y. A. Phillis and L. A. Andriantiatsaholiniaina, "Sustainability: an ill-defined concept and its assessment using fuzzy logic," *Ecological economics*, vol. 37, no. 3, pp. 435–456, 2001.

[83] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," *Reliability engineering & System safety*, vol. 121, pp. 43–60, 2014.

[84] M. Dohnal, "Rough sets in reliability engineering," *Microelectronics Reliability*, vol. 32, no. 4, pp. 539–543, 1992.

[85] Q. H. Wang and J. R. Li, "A rough set-based fault ranking prototype system for fault diagnosis," *Engineering applications of artificial intelligence*, vol. 17, no. 8, pp. 909–917, 2004.

[86] X. Yan, Z. Zhang, and W. Cheng, "Intelligent fault diagnosis based on granular computing," in *Granular Computing, 2008. GrC 2008. IEEE International Conference on.* IEEE, 2008, pp. 712–717.

[87] Z. ZHANG, X. YAN, and W. CHENG, "Granular computing with application to fault diagnosis [j]," *Journal of Xi'an Jiaotong University*, vol. 9, p. 008, 2009.

[88] S. Rawat, A. Patel, J. Celestino, and A. L. M. dos Santos, "A dominance based rough set classification system for fault diagnosis in electrical smart grid environments," *Artificial Intelligence Review*, vol. 46, no. 3, pp. 389–411, 2016.

[89] A. Azadeh, V. Ebrahimipour, and P. Bavar, "A fuzzy inference system for pump failure diagnosis to improve maintenance process: The case of a petrochemical industry," *Expert Systems with Applications*, vol. 37, no. 1, pp. 627–639, 2010.

[90] V. Miranda, D. Srinivasan, and L. M. Proenca, "Evolutionary computation in power systems," *International Journal of Electrical Power & Energy Systems*, vol. 20, no. 2, pp. 89–98, 1998.

[91] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems*, vol. 21, no. 6, pp. 11–25, 2001.

[92] D. D. Dudenhoeffer, M. R. Permann, and M. Manic, "Cims: A framework for infrastructure interdependency modeling and analysis," in *Proceedings of the 38th conference on Winter simulation.* Winter Simulation Conference, 2006, pp. 478–485.

[93] Z. Chen, T.-Y. T. Lin, and G. Xie, "Knowledge approximations in binary relation: granular computing approach," *International Journal of Intelligent Systems*, vol. 28, no. 9, pp. 843–864, 2013.

[94] Y. Qian, H. Cheng, J. Wang, J. Liang, W. Pedrycz, and C. Dang, "Grouping granular structures in human granulation intelligence," *Information Sciences*, vol. 382383, pp. 150 – 169, 2017.

[95] R. Al-Hmouz, W. Pedrycz, A. Balamash, and A. Morfeq, “Hierarchical system modeling,” *IEEE Transactions on Fuzzy Systems*, 2017.

[96] W. Pedrycz, “From numeric models to granular system modeling,” *Fuzzy Information and Engineering*, vol. 7, no. 1, pp. 1–13, 2015.

[97] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, “Cyber–physical security of a smart grid infrastructure,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[98] G. DAniello, A. Gaeta, V. Loia, and F. Orciuoli, “A granular computing framework for approximate reasoning in situation awareness,” *Granular Computing*, vol. 2, no. 3, pp. 141–158, 2017.

[99] M. R. Endsley, *Designing for situation awareness: An approach to user-centered design.* CRC Press, 2011.

[100] S. Greco, B. Matarazzo, and R. Slowinski, “Rough sets theory for multicriteria decision analysis,” *European journal of operational research*, vol. 129, no. 1, pp. 1–47, 2001.

[101] R. R. Yager, “Soft computing for intelligence analysis and security decisions: multi-source fusion,” in *NAFIPS 2005-2005 Annual Meeting of the North American Fuzzy Information Processing Society.* IEEE, 2005, pp. 228–232.

[102] ——, “Fuzzy set methods for uncertainty management in intelligence analysis,” *International journal of intelligent systems*, vol. 21, no. 5, pp. 523–544, 2006.

[103] S. Pope and A. Josang, “Analysis of competing hypotheses using subjective logic,” QUEENSLAND UNIV BRISBANE (AUSTRALIA), Tech. Rep., 2005.

[104] K. A. Duncan and J. L. Wilson, “A multinomial-dirichlet model for analysis of competing hypotheses,” *Risk Analysis: An International Journal*, vol. 28, no. 6, pp. 1699–1709, 2008.

[105] A. Kengpol and P. Neungrit, “A decision support methodology with risk assessment on prediction of terrorism insurgency distribution range radius and elapsing time: An empirical case study in thailand,” *Computers & Industrial Engineering*, vol. 75, pp. 55–67, 2014.

[106] G. M. Tolan and O. S. Soliman, “An experimental study of classification algorithms for terrorism prediction,” *International Journal of Knowledge Engineering-IACSIT*, vol. 1, no. 2, pp. 107–112, 2015.

[107] S. B. Salem, S. Naouali, and M. Sallami, “A computational cost-effective clustering algorithm in multidimensional space using the manhattan metric: application to the global terrorism database,” *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 11, no. 6, pp. 703–708, 2017.

[108] F. Ding, Q. Ge, D. Jiang, J. Fu, and M. Hao, “Understanding the dynamics of terrorism events with multiple-discipline datasets and machine learning approach,” *PloS one*, vol. 12, no. 6, p. e0179057, 2017.

[109] C. Gao and Y. Yao, “Actionable strategies in three-way decisions,” *Knowledge-Based Systems*, vol. 133, pp. 141–155, 2017.

Appendix A - Fuzzy GTD and Similarity Matrix

Table 1: FuzzyGTD 2012-2016 (from [31])

	AT1	AT2	AT3	AT4	AT5	AT6	AT7	AT8	AT9	TT1	TT2	TT3	TT4	TT5	TT6	TT7	TT8	TT9	TT10	TT11
g1	0,02	0,11	0,86	0,00	0,00	0,00	0,00	0,00	0,01	0,06	0,07	0,23	0,11	0,00	0,00	0,00	0,01	0,00	0,00	0,00
g2	0,17	0,27	0,37	0,00	0,00	0,08	0,01	0,00	0,08	0,02	0,14	0,11	0,45	0,00	0,00	0,02	0,01	0,00	0,01	0,00
g3	0,09	0,32	0,37	0,01	0,01	0,07	0,02	0,00	0,13	0,06	0,13	0,08	0,47	0,00	0,01	0,01	0,01	0,00	0,01	0,00
g4	0,01	0,36	0,56	0,00	0,00	0,03	0,01	0,00	0,03	0,07	0,04	0,03	0,55	0,00	0,00	0,00	0,01	0,00	0,00	0,00
g5	0,03	0,45	0,32	0,00	0,01	0,07	0,07	0,00	0,06	0,05	0,06	0,11	0,13	0,00	0,00	0,00	0,04	0,00	0,00	0,00
g6	0,04	0,18	0,29	0,00	0,02	0,24	0,19	0,01	0,02	0,16	0,14	0,22	0,04	0,00	0,00	0,00	0,02	0,00	0,00	0,00
g7	0,00	0,30	0,47	0,00	0,00	0,11	0,05	0,00	0,06	0,03	0,05	0,04	0,64	0,00	0,00	0,01	0,01	0,00	0,03	0,00
g8	0,02	0,81	0,00	0,00	0,00	0,09	0,05	0,00	0,02	0,00	0,03	0,02	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,00
g9	0,02	0,09	0,54	0,00	0,00	0,14	0,02	0,00	0,18	0,04	0,05	0,03	0,23	0,00	0,01	0,01	0,03	0,00	0,05	0,00
g10	0,02	0,07	0,66	0,00	0,00	0,12	0,01	0,00	0,11	0,05	0,03	0,12	0,23	0,00	0,00	0,00	0,00	0,00	0,01	0,00
g11	0,02	0,33	0,43	0,00	0,00	0,07	0,08	0,00	0,06	0,04	0,04	0,25	0,39	0,00	0,00	0,00	0,06	0,00	0,00	0,00
g12	0,03	0,22	0,41	0,00	0,01	0,16	0,12	0,01	0,03	0,11	0,12	0,28	0,09	0,00	0,00	0,00	0,01	0,00	0,00	0,00
g13	0,06	0,27	0,46	0,00	0,00	0,07	0,05	0,01	0,07	0,07	0,06	0,13	0,21	0,00	0,02	0,03	0,04	0,00	0,01	0,00
g14	0,04	0,45	0,20	0,01	0,02	0,10	0,14	0,00	0,04	0,17	0,07	0,10	0,49	0,00	0,00	0,00	0,00	0,00	0,00	0,00
g15	0,01	0,74	0,11	0,00	0,00	0,00	0,03	0,12	0,00	0,02	0,00	0,18	0,43	0,00	0,00	0,00	0,00	0,00	0,00	0,00
g16	0,02	0,17	0,63	0,00	0,00	0,06	0,07	0,00	0,05	0,08	0,03	0,25	0,21	0,00	0,01	0,00	0,00	0,01	0,00	0,00
g17	0,05	0,36	0,48	0,00	0,00	0,03	0,06	0,00	0,01	0,19	0,12	0,20	0,22	0,00	0,00	0,01	0,04	0,00	0,00	0,01
g18	0,04	0,23	0,57	0,01	0,00	0,11	0,01	0,00	0,03	0,03	0,02	0,36	0,38	0,00	0,00	0,01	0,01	0,00	0,00	0,00
g19	0,06	0,29	0,39	0,00	0,00	0,09	0,03	0,00	0,13	0,02	0,10	0,38	0,22	0,00	0,00	0,00	0,01	0,00	0,00	0,00
g20	0,12	0,31	0,46	0,00	0,01	0,06	0,01	0,00	0,02	0,04	0,07	0,25	0,28	0,00	0,00	0,02	0,04	0,00	0,01	0,00
g21	0,03	0,06	0,32	0,02	0,01	0,36	0,06	0,00	0,13	0,09	0,04	0,09	0,13	0,00	0,00	0,03	0,01	0,00	0,01	0,00

Table 2: FuzzyGTD 2012-2016 - Continued (from [31])

TT12	TT13	TT14	TT15	TT16	TT17	TT18	TT19	TT20	TT21	TT22	WT1	WT2	WT3	WT4	WT5	WT6	WT7	WT8	WT9	WT10	WT11	WT12	WT13
0,00	0,00	0,42	0,02	0,01	0,02	0,00	0,01	0,03	0,01	0,00	0,00	0,00	0,00	0,00	0,12	0,87	0,00	0,00	0,00	0,00	0,00	0,00	0,01
0,00	0,00	0,09	0,01	0,00	0,07	0,00	0,00	0,02	0,04	0,02	0,00	0,00	0,00	0,00	0,40	0,47	0,00	0,01	0,01	0,00	0,00	0,00	0,11
0,01	0,00	0,16	0,01	0,00	0,01	0,00	0,01	0,02	0,00	0,00	0,00	0,00	0,00	0,00	0,33	0,47	0,00	0,01	0,02	0,00	0,00	0,00	0,16
0,00	0,00	0,11	0,01	0,00	0,00	0,00	0,03	0,09	0,07	0,00	0,00	0,00	0,00	0,00	0,28	0,68	0,00	0,00	0,00	0,00	0,00	0,00	0,03
0,00	0,01	0,46	0,07	0,02	0,01	0,00	0,02	0,03	0,00	0,00	0,00	0,00	0,00	0,00	0,42	0,42	0,00	0,08	0,01	0,00	0,00	0,00	0,07
0,00	0,00	0,24	0,01	0,05	0,01	0,00	0,07	0,03	0,00	0,01	0,00	0,00	0,00	0,00	0,34	0,32	0,00	0,18	0,06	0,00	0,00	0,00	0,10
0,01	0,00	0,15	0,01	0,00	0,00	0,00	0,02	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,19	0,66	0,00	0,01	0,02	0,00	0,00	0,00	0,13
0,00	0,00	0,91	0,02	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,88	0,00	0,00	0,05	0,02	0,00	0,00	0,00	0,04
0,01	0,00	0,41	0,02	0,00	0,06	0,00	0,01	0,01	0,00	0,03	0,00	0,00	0,00	0,00	0,12	0,58	0,00	0,01	0,00	0,00	0,00	0,00	0,30
0,00	0,01	0,40	0,03	0,00	0,05	0,00	0,01	0,03	0,01	0,00	0,00	0,00	0,00	0,00	0,10	0,69	0,00	0,01	0,01	0,00	0,00	0,00	0,19
0,00	0,00	0,10	0,01	0,00	0,03	0,00	0,01	0,03	0,03	0,00	0,00	0,00	0,00	0,00	0,27	0,54	0,00	0,08	0,00	0,00	0,00	0,00	0,11
0,00	0,00	0,20	0,00	0,02	0,01	0,00	0,04	0,10	0,00	0,01	0,00	0,00	0,00	0,00	0,32	0,43	0,00	0,09	0,07	0,00	0,00	0,00	0,09
0,01	0,00	0,25	0,09	0,00	0,02	0,00	0,02	0,02	0,02	0,00	0,00	0,00	0,00	0,00	0,30	0,50	0,00	0,03	0,04	0,01	0,00	0,01	0,11
0,00	0,00	0,10	0,00	0,01	0,00	0,00	0,01	0,04	0,00	0,00	0,00	0,00	0,00	0,00	0,60	0,23	0,00	0,10	0,00	0,00	0,00	0,00	0,08
0,00	0,00	0,28	0,02	0,00	0,00	0,00	0,04	0,03	0,00	0,00	0,00	0,00	0,00	0,00	0,12	0,11	0,00	0,07	0,59	0,11	0,00	0,00	0,00
0,00	0,00	0,06	0,00	0,00	0,00	0,00	0,10	0,07	0,18	0,00	0,00	0,00	0,00	0,00	0,16	0,68	0,00	0,06	0,00	0,00	0,00	0,00	0,10
0,00	0,01	0,12	0,02	0,00	0,00	0,00	0,01	0,03	0,04	0,01	0,00	0,00	0,00	0,00	0,40	0,50	0,00	0,08	0,00	0,00	0,00	0,00	0,02
0,00	0,01	0,10	0,02	0,00	0,01	0,00	0,00	0,04	0,01	0,00	0,00	0,00	0,00	0,00	0,30	0,61	0,00	0,01	0,02	0,00	0,00	0,00	0,06
0,01	0,00	0,18	0,01	0,00	0,01	0,00	0,01	0,04	0,00	0,00	0,00	0,00	0,00	0,00	0,36	0,44	0,00	0,02	0,01	0,00	0,00	0,00	0,16
0,01	0,00	0,13	0,03	0,00	0,07	0,00	0,01	0,01	0,00	0,03	0,00	0,00	0,00	0,00	0,39	0,58	0,00	0,01	0,00	0,00	0,00	0,00	0,03
0,00	0,00	0,45	0,02	0,00	0,10	0,00	0,00	0,03	0,01	0,00	0,00	0,00	0,00	0,00	0,17	0,34	0,00	0,02	0,05	0,00	0,00	0,01	0,42

Table 3: Similarity Matrix - AT, TT, WT (from [31])

	g1	g2	g3	g4	g5	g6	g7	g8	g8	g10	g11	g10	g13	g14	g15	g16	g17	g18	g19	g20	g21
g1	1	0	0	0,02	0	0	0,01	0	0,06	0,32	0,02	0,02	0,04	0	0	0,12	0,02	0,05	0,01	0,03	0
g2	0	1	0,8	0,27	0,09	0,06	0,26	0	0,06	0,04	0,47	0,16	0,36	0,17	0	0,08	0,32	0,27	0,31	0,52	0,02
g3	0	0,8	1	0,34	0,14	0,06	0,41	0	0,11	0,06	0,53	0,16	0,45	0,18	0	0,08	0,31	0,24	0,31	0,39	0,03
g4	0,02	0,27	0,34	1	0,03	0,01	0,63	0	0,04	0,07	0,36	0,04	0,19	0,03	0	0,16	0,19	0,28	0,06	0,26	0
g5	0	0,09	0,14	0,03	1	0,17	0,02	0	0,05	0,03	0,12	0,22	0,37	0,07	0	0,02	0,21	0,04	0,2	0,16	0,04
g6	0	0,06	0,06	0,01	0,17	1	0,01	0	0,04	0,02	0,09	0,63	0,22	0,04	0	0,04	0,18	0,04	0,2	0,09	0,1
g7	0,01	0,26	0,41	0,63	0,02	0,01	1	0	0,08	0,08	0,35	0,03	0,16	0,02	0	0,09	0,09	0,21	0,06	0,16	0,01
g8	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
g9	0,06	0,06	0,11	0,04	0,05	0,04	0,08	0	1	0,65	0,09	0,09	0,26	0	0	0,1	0,04	0,07	0,08	0,07	0,23
g10	0,32	0,04	0,06	0,07	0,03	0,02	0,08	0	0,65	1	0,09	0,08	0,23	0	0	0,22	0,05	0,13	0,06	0,09	0,06
g11	0,02	0,47	0,53	0,36	0,12	0,09	0,35	0	0,09	0,09	1	0,31	0,51	0,09	0	0,3	0,5	0,61	0,49	0,62	0,02
g12	0,02	0,16	0,16	0,04	0,22	0,63	0,03	0	0,09	0,08	0,31	1	0,51	0,04	0	0,17	0,46	0,22	0,54	0,34	0,07
g13	0,04	0,36	0,45	0,19	0,37	0,22	0,16	0	0,26	0,23	0,51	0,51	1	0,05	0	0,24	0,55	0,34	0,48	0,58	0,07
g14	0	0,17	0,18	0,03	0,07	0,04	0,02	0	0	0	0,09	0,04	0,05	1	0	0	0,11	0,02	0,07	0,06	0
g15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
g16	0,12	0,08	0,08	0,16	0,02	0,04	0,09	0	0,1	0,22	0,3	0,17	0,24	0	0	1	0,21	0,4	0,14	0,24	0,01
g17	0,02	0,32	0,31	0,19	0,21	0,18	0,09	0	0,04	0,05	0,5	0,46	0,55	0,11	0	0,21	1	0,34	0,41	0,64	0,01
g18	0,05	0,27	0,24	0,28	0,04	0,04	0,21	0	0,07	0,13	0,61	0,22	0,34	0,02	0	0,4	0,34	1	0,39	0,61	0,01
g19	0,01	0,31	0,31	0,06	0,2	0,2	0,06	0	0,08	0,06	0,49	0,54	0,48	0,07	0	0,14	0,41	0,39	1	0,51	0,04
g29	0,03	0,52	0,39	0,26	0,16	0,09	0,16	0	0,07	0,09	0,62	0,34	0,58	0,06	0	0,24	0,64	0,61	0,51	1	0,01
g21	0	0,02	0,03	0	0,04	0,1	0,01	0	0,23	0,06	0,02	0,07	0,07	0	0	0,01	0,01	0,01	0,04	0,01	1

Table 4: Similarity Matrix - AT (from [31])

	g1	g2	g3	g4	g5	g6	g7	g8	g8	g10	g11	g10	g13	g14	g15	g16	g17	g18	g19	g20	g21
g1	1	0,12	0,11	0,33	0,05	0,05	0,23	0	0,33	0,63	0,17	0,16	0,24	0,01	0	0,62	0,22	0,45	0,14	0,22	0,04
g2	0,12	1	0,93	0,59	0,65	0,5	0,74	0,04	0,5	0,34	0,77	0,72	0,85	0,49	0,08	0,47	0,73	0,65	0,89	0,89	0,32
g3	0,11	0,93	1	0,67	0,79	0,49	0,83	0,06	0,51	0,33	0,87	0,74	0,89	0,59	0,12	0,47	0,79	0,64	0,98	0,85	0,31
g4	0,33	0,59	0,67	1	0,59	0,26	0,86	0,02	0,46	0,46	0,83	0,59	0,84	0,31	0,07	0,71	0,93	0,83	0,71	0,83	0,14
g5	0,05	0,65	0,79	0,59	1	0,42	0,71	0,19	0,23	0,14	0,82	0,59	0,68	0,86	0,33	0,28	0,76	0,42	0,76	0,67	0,17
g6	0,05	0,5	0,49	0,26	0,42	1	0,53	0,02	0,38	0,23	0,54	0,82	0,52	0,46	0,04	0,31	0,39	0,39	0,54	0,43	0,65
g7	0,23	0,74	0,83	0,86	0,71	0,53	1	0,03	0,61	0,5	0,96	0,87	0,96	0,46	0,08	0,7	0,9	0,86	0,89	0,86	0,33
g8	0	0,04	0,06	0,02	0,19	0,02	0,03	1	0	0	0,05	0,02	0,03	0,28	0,76	0	0,04	0,01	0,04	0,03	0
g9	0,33	0,5	0,51	0,46	0,23	0,38	0,61	0	1	0,86	0,51	0,62	0,65	0,13	0,01	0,75	0,43	0,72	0,6	0,5	0,47
g10	0,63	0,34	0,33	0,46	0,14	0,23	0,5	0	0,86	1	0,39	0,47	0,53	0,06	0	0,87	0,37	0,75	0,41	0,43	0,27
g11	0,17	0,77	0,87	0,83	0,82	0,54	0,96	0,05	0,51	0,39	1	0,85	0,95	0,58	0,11	0,62	0,94	0,76	0,91	0,87	0,28
g12	0,16	0,72	0,74	0,59	0,59	0,82	0,87	0,02	0,62	0,47	0,85	1	0,86	0,47	0,05	0,63	0,72	0,74	0,8	0,75	0,52
g13	0,24	0,85	0,89	0,84	0,68	0,52	0,96	0,03	0,65	0,53	0,95	0,86	1	0,44	0,07	0,74	0,91	0,88	0,93	0,93	0,32
g14	0,01	0,49	0,59	0,31	0,86	0,46	0,46	0,28	0,13	0,06	0,58	0,47	0,44	1	0,38	0,14	0,49	0,22	0,54	0,43	0,16
g15	0	0,08	0,12	0,07	0,33	0,04	0,08	0,76	0,01	0	0,11	0,05	0,07	0,38	1	0,01	0,11	0,03	0,1	0,08	0,01
g16	0,62	0,47	0,47	0,71	0,28	0,31	0,7	0	0,75	0,87	0,62	0,63	0,74	0,14	0,01	1	0,63	0,89	0,55	0,63	0,23
g17	0,22	0,73	0,79	0,93	0,76	0,39	0,9	0,04	0,43	0,37	0,94	0,72	0,91	0,49	0,11	0,63	1	0,78	0,81	0,92	0,18
g18	0,45	0,65	0,64	0,83	0,42	0,39	0,86	0,01	0,72	0,75	0,76	0,74	0,88	0,22	0,03	0,89	0,78	1	0,71	0,82	0,29
g19	0,14	0,89	0,98	0,71	0,76	0,54	0,89	0,04	0,6	0,41	0,91	0,8	0,93	0,54	0,1	0,55	0,81	0,71	1	0,85	0,36
g29	0,22	0,89	0,85	0,83	0,67	0,43	0,86	0,03	0,5	0,43	0,87	0,75	0,93	0,43	0,08	0,63	0,92	0,82	0,85	1	0,24
g21	0,04	0,32	0,31	0,14	0,17	0,65	0,33	0	0,47	0,27	0,28	0,52	0,32	0,16	0,01	0,23	0,18	0,29	0,36	0,24	1

Appendix B - Tables with numerical values of the experimentation

Table 5: $< AT1, TT1, WT6 >$ (from [31])

		$\alpha = 0.00792$	$\alpha = 0.00265$	$\alpha = 0.00261$	$\alpha = 0.001$
	$Pr(\Omega\mid[g])$	$\beta = 7.97982e-05$	$\beta = 0.00024$	$\beta = 0.00024$	$\beta = 0.00064$
		$\varepsilon = 0,1$	$\varepsilon = 0,3$	$\varepsilon = 0,305$	$\varepsilon = 0,8$
g1	0.00004	NEG	NEG	NEG	NEG
g2	0.00231	BND	BND	BND	POS
g3	0.00261	BND	BND	POS	POS
g4	0.00188	BND	BND	BND	POS
g5	0.00058	BND	BND	BND	NEG
g6	0.00038	BND	BND	BND	NEG
g7	0.00222	BND	BND	BND	POS
g8	0.00000	NEG	NEG	NEG	NEG
g9	0.00041	BND	BND	BND	NEG
g10	0.00018	BND	NEG	NEG	NEG
g11	0.00129	BND	BND	BND	POS
g12	0.00046	BND	BND	BND	NEG
g13	0.00101	BND	BND	BND	POS
g14	0.00138	BND	BND	BND	POS
g15	0.00009	BND	NEG	NEG	NEG
g16	0.00043	BND	BND	BND	NEG
g17	0.00093	BND	BND	BND	BND
g18	0.00079	BND	BND	BND	BND
g19	0.00066	BND	BND	BND	BND
g20	0.00100	BND	BND	BND	POS
g21	0.00040	BND	BND	BND	NEG

Table 6: $< AT2, TT14, WT5 >$ $\gamma = 2$ (from [31])

	$Pr(\Omega\|[g])$	$\alpha = 0.1834$ $\beta = 0.0022$ $\varepsilon = 0,1$	$\alpha = 0.0696$ $\beta = 0.0067$ $\varepsilon = 0,3$	$\alpha = 0.0273$ $\beta = 0.0176$ $\varepsilon = 0,8$
g1	0.0263	BND	BND	BND
g2	0.0205	BND	BND	BND
g3	0.0207	BND	BND	BND
g4	0.0243	BND	BND	BND
g5	0.0195	BND	BND	BND
g6	0.0192	BND	BND	BND
g7	0.0239	BND	BND	BND
g8	0.0746	BND	POS	POS
g9	0.0185	BND	BND	BND
g10	0.0185	BND	BND	BND
g11	0.0209	BND	BND	BND
g12	0.0196	BND	BND	BND
g13	0.0201	BND	BND	BND
g14	0.0208	BND	BND	BND
g15	0.0359	BND	BND	POS
g16	0.0202	BND	BND	BND
g17	0.0208	BND	BND	BND
g18	0.0211	BND	BND	BND
g19	0.0196	BND	BND	BND
g20	0.0207	BND	BND	BND
g21	0.0181	BND	BND	BND

Table 7: $< AT2, TT14, WT5 >$ $\gamma = 0.5$ from [31]

	$Pr(\Omega\|[g])$	$\alpha = 0.2471$ $\beta = 0.0033$ $\varepsilon = 0,1$	$\alpha = 0.0986$ $\beta = 0.0098$ $\varepsilon = 0,3$	$\alpha = 0.0394$ $\beta = 0.0256$ $\varepsilon = 0,8$
g1	0.0276	BND	BND	BND
g2	0.0281	BND	BND	BND
g3	0.0288	BND	BND	BND
g4	0.0304	BND	BND	BND
g5	0.0380	BND	BND	BND
g6	0.0319	BND	BND	BND
g7	0.0304	BND	BND	BND
g8	0.1921	BND	POS	POS
g9	0.0215	BND	BND	NEG
g10	0.0204	BND	BND	NEG
g11	0.0289	BND	BND	BND
g12	0.0308	BND	BND	BND
g13	0.0301	BND	BND	BND
g14	0.0263	BND	BND	BND
g15	0.0394	BND	BND	BND
g16	0.0253	BND	BND	NEG
g17	0.0305	BND	BND	BND
g18	0.0283	BND	BND	BND
g19	0.0301	BND	BND	BND
g20	0.0294	BND	BND	BND
g21	0.0237	BND	BND	NEG

Table 8: $< AT2, TT14, WT5 >$ $\gamma = 0.1$ (from [31])

	$Pr(\Omega \mid [g])$	$\alpha = 0.2829$	$\alpha = 0.1162$	$\alpha = 0.0470$
		$\beta = 0.0039$	$\beta = 0.0117$	$\beta = 0.0306$
		$\varepsilon = 0,1$	$\varepsilon = 0,3$	$\varepsilon = 0,8$
g1	0.0277	BND	BND	NEG
g2	0.0287	BND	BND	NEG
g3	0.0297	BND	BND	NEG
g4	0.0308	BND	BND	BND
g5	0.0482	BND	BND	POS
g6	0.0343	BND	BND	BND
g7	0.0307	BND	BND	BND
g8	0.4234	POS	POS	POS
g9	0.0220	BND	BND	NEG
g10	0.0207	BND	BND	NEG
g11	0.0296	BND	BND	NEG
g12	0.0323	BND	BND	BND
g13	0.0321	BND	BND	BND
g14	0.0276	BND	BND	NEG
g15	0.0397	BND	BND	BND
g16	0.0255	BND	BND	NEG
g17	0.0320	BND	BND	BND
g18	0.0286	BND	BND	NEG
g19	0.0311	BND	BND	BND
g20	0.0304	BND	BND	NEG
g21	0.0249	BND	BND	NEG

Table 9: $< AT2, TT4, WT9 >$, $< AT2, TT14, WT9 >$ and $< AT3, TT4, WT6 >$ for $\gamma = 2$ (from [31])

	$Pr(\Omega \vert [g])$	$\alpha = 0.2737$ $\beta = 0.0038$ $\varepsilon = 0,1$	$\alpha = 0.1116$ $\beta = 0.0112$ $\varepsilon = 0,3$	$\alpha = 0.045$ $\beta = 0.0293$ $\varepsilon = 0,8$
g1	0.0463	BND	BND	POS
g2	0.0362	BND	BND	BND
g3	0.0364	BND	BND	BND
g4	0.0438	BND	BND	BND
g5	0.0290	BND	BND	NEG
g6	0.0269	BND	BND	NEG
g7	0.0431	BND	BND	BND
g8	0.0054	BND	NEG	NEG
g9	0.0404	BND	BND	BND
g10	0.0415	BND	BND	BND
g11	0.0369	BND	BND	BND
g12	0.0310	BND	BND	BND
g13	0.0350	BND	BND	BND
g14	0.0361	BND	BND	BND
g15	0.0374	BND	BND	BND
g16	0.0402	BND	BND	BND
g17	0.0350	BND	BND	BND
g18	0.0384	BND	BND	BND
g19	0.0332	BND	BND	BND
g20	0.0361	BND	BND	BND
g21	0.0352	BND	BND	BND

Table 10: $< AT2, TT4, WT9 >$, $< AT2, TT14, WT9 >$ and $< AT3, TT4, WT6 >$ for $\gamma = 0.5$ (from [31])

		$\alpha = 0.3487$	$\alpha = 0.1514$	$\alpha = 0.0627$
	$Pr(\Omega\|[g])$	$\beta = 0.0053$	$\beta = 0.0158$	$\beta = 0.0411$
		$\varepsilon = 0,1$	$\varepsilon = 0,3$	$\varepsilon = 0,8$
g1	0.0566	BND	BND	BND
g2	0.0558	BND	BND	BND
g3	0.0563	BND	BND	BND
g4	0.0699	BND	BND	POS
g5	0.0381	BND	BND	NEG
g6	0.0370	BND	BND	NEG
g7	0.0694	BND	BND	POS
g8	0.0222	BND	BND	NEG
g9	0.0536	BND	BND	BND
g10	0.0543	BND	BND	BND
g11	0.0550	BND	BND	BND
g12	0.0428	BND	BND	BND
g13	0.0499	BND	BND	BND
g14	0.0472	BND	BND	BND
g15	0.0716	BND	BND	POS
g16	0.0557	BND	BND	BND
g17	0.0502	BND	BND	BND
g18	0.0562	BND	BND	BND
g19	0.0459	BND	BND	BND
g20	0.0527	BND	BND	BND
g21	0.0443	BND	BND	BND

Table 11: $< AT2, TT4, WT9 >$, $< AT2, TT14, WT9 >$ and $< AT3, TT4, WT6 >$ for $\gamma = 0.1$ (from [31])

	$Pr(\Omega\|[g])$	$\alpha = 0.3786$ $\beta = 0.0061$ $\varepsilon = 0,1$	$\alpha = 0.1688$ $\beta = 0.0179$ $\varepsilon = 0,3$	$\alpha = 0.0708$ $\beta = 0.0465$ $\varepsilon = 0,8$
g1	0.0573	BND	BND	BND
g2	0.0638	BND	BND	BND
g3	0.0648	BND	BND	BND
g4	0.0875	BND	BND	POS
g5	0.0399	BND	BND	NEG
g6	0.0389	BND	BND	NEG
g7	0.0876	BND	BND	POS
g8	0.0222	BND	BND	NEG
g9	0.0553	BND	BND	BND
g10	0.0556	BND	BND	BND
g11	0.0623	BND	BND	BND
g12	0.0453	BND	BND	NEG
g13	0.0540	BND	BND	BND
g14	0.0509	BND	BND	BND
g15	0.1881	BND	POS	POS
g16	0.0605	BND	BND	BND
g17	0.0548	BND	BND	BND
g18	0.0629	BND	BND	BND
g19	0.0488	BND	BND	BND
g20	0.0581	BND	BND	BND
g21	0.0455	BND	BND	NEG