Collective Intelligence for Risk Reduction: Theory, Implementation and Practical Application to Security Incident Response

Moufida SADOK
High Institute of Communication Technologies of Tunis
Email: Moufida.Sadok@isetcom.rnu.tn

Salah BENABDALLAH, PhD
High Institute of Communication Technologies of Tunis
Email : sba@supcom.rnu.tn

Humbert LESCA
Emeritus Professor
University of Grenoble, France
Laboratory CERAG UMR 5820 CNRS UPMF
http://www.veille-strategique.org

Abstract

The Collective Intelligence (CI) process is an adaptive process that helps companies to reduce business risk and cope with unstable and uncertain external events. In this paper a CI-methodology is proposed. It is based on an extended causal links approach that provides a theoretical framework to the representation, the manipulation, and the refinement of links to reconcile different views, to construct an intelligible vision, and to support the decision making in strategic management. A particular application of CI-methodology for risk reduction of digital aggressions in enterprise networks is presented. We also show the potentiality of using Internet technologies which can provide an efficient support to CI process and tools to competitive intelligence.

Key words:

Collective Intelligence, business intelligence, attacks security, incident response team

Acknowledgment:

The authors sincerely thank Prof. Noureddine BOUDRIGA, Professor of Telecommunications at SUP'COM (Ecole Supérieure des Communications), for his brilliant idea to develop the proposed model and write the article. Without his continuous contribution in this research, the article would not have been written.

Introduction

Collective intelligence is a process through which the enterprise is actively collecting environmental information, referred to as "weak signals" (Ansoff, 1975), to discover business opportunities, to increase anticipative capacity, and to reduce uncertainty. It is also a learning and adaptive process that helps companies reduce business risk and cope with unstable and unpredictable external events. Therefore, firms' competitiveness depends on firms' ability to monitor and to adapt to environmental conditions (Pfeffer& Salancik 1978; Venkatraman and Prescott, 1990; Daft et al., 1988).

Weak signals have been defined in the literature as fragmented, ambiguous, incomplete, and uncertain information (Blanco et al. 2003). The amplification or the zooming of these signals would help most of the time decision makers in identifying problems or improving decisions and analysis. As a result, it will reduce risk in decision making. The fields where the notion of risk is very important in decisions are investments, ICT products, stock market, and IT security attacks, etc. Particularly, in the domain of IT security attacks, the risk of cyber attacks continues to be high and the financial losses are increasing (Power, 2002 ; Richardson, 2003). The use of Internet and networked systems by the enterprises has increased the risk of security attacks which can disable temporarily their activities. Therefore, their competitive capacity would be reduced. To anticipate and to reduce such a risk, it is important to detect and to analyze weak signals related to IT security and collected through environmental scanning.

The reasoning through weak signals by creating links between fragmented information represents the intelligence process. This process conducted collectively in the enterprise is named Collective Intelligence (CI). It is the most important process to support efficiently the decision making and to improve the anticipation capacity. The complexity in different reasoning modes in performing CI requires that the typology of links cover a wide variety of types. Such types are semantic, probabilistic, or approximate links.

In that case, cognitive maps, particularly causal maps, offer a theoretical framework to represent the information and the different relating links. The causal maps presentation is based on nodes and arcs. Links provide a modeling flexible tool for reasoning, extending, and deciding on uncertain information represented by nodes. The nodes can contain weak signals information, actions, hypotheses and goals. The arcs represent dependency relations between the nodes.

The Internet technologies can provide an efficient support to the CI process. Internet mechanisms contribute to create an intelligent and dynamic storage of collected information by creating meaningful links to structured and organized information. In addition, the manipulation of links permits automatic deduction from hypotheses and deduction rules. The internet technology can also manage the data base by implementing appropriate reasoning heuristics to the stored links.

We present in this paper a CI-methodology for risk reduction in IT security based on an extended causal links approach integrating notions of sub-causal links rewriting, views reconciling and aiming to assist decision makers in strategic management. The main features of the model are the richness and the presentation of links, a reasoning engine over the links, and a modeling tool of links that assists in Collective Intelligence support system. Our approach is considered as the continuity of an initial work developed by Sadok et al. (2003). The proposed model has been applied in particularly to the incidence response activity in an enterprise network. This activity is based on the detection and amplified signals, an intelligent reasoning about information from these signals, and the creation of appropriate links between fragmented information. This activity is of a nature to generate non-repetitive and non programmable decisions. The decision is taken in

uncertain environment where the outcomes for the enterprise are important. The proposed Collective Intelligence process will naturally help achieve a quick response in the right moment and to improve the anticipation capacity.

This paper is organized into seven sections and a conclusion. The first section describes the Collective Intelligence process, its steps and its specificities and presents an extended model of CI process. The second section demonstrates the importance of using causal maps for the representation and the manipulation of links. The third section describes the importance of mediation process and how Internet technologies can support such process. The fourth section illustrates how the CI process can be adapted to the security incidence response. A conceptual reasoning model of links will be presented to support the activities of incidence response team. The fifth section demonstrates the steps of the model through a real case of security attacks. The last section presents a general framework of CI-methodology for risk reduction of digital aggression. Finally, the conclusion presents the principal results found with a discussion about future research work.

1. Collective Intelligence Process

One of the main organization tasks is described as an interpretation system that processes information from the external environment **(**Daft and Weick, 1984; Daft and Huber, 1987**)**. Interpretation is the process that translates events, develops models for understanding, brings out meaning, and assembles conceptual schemes among key managers. The interpretation system view deals with specialized information reception, equivocality reduction, and sense-making (Daft and Weick, 1984). Sense-making has been defined in the literature through different views. It is an interpretative process in which people assign meaning to ongoing events (Gioia and Chittipeddi, 1991). It is the amplification of weak signals and search for contexts within small details fitted together for sense making (Weick, 1995). It is considered as a creative and a collective method that can help the organization to give sense and see possibilities in the disorder that occurs (Choo, 2001; Ashmos et Nathan, 2002).

Based on the previous definitions, Collective Intelligence (CI) constitutes an appropriate process for sense making. Lesca (2003), defines the CI process as the capability of the group to create significant links between uncertain, incomplete, scattered and fragmented information during interactions of individual and collective memories proceeded by inductive approach. The result of this operation can provide an efficient support to the decision making process by reducing the information ambiguity and the environmental uncertainty. In this section, the conceptual model of the CI process is presented, as described by Blanco et al. (2003). The extension of this model is then proposed to add more dynamic objects (or links), to reduce uncertainty, and to help controlling reasoning complexity.

1.1 Conceptual model of CI process

Two important phases have been identified to support the CI process (Blanco et al., 2003). Phase I is the regrouping of information according to certain criteria. Phase II is the creation of links between pieces of information within and between groups. These phases can be described as follows:

The Regrouping of Information: The regrouping of information assumes the existence of a classifying procedure according to certain criteria and the definition of links between stored information inside a regrouping. The regrouping of information provides a synthetic and generic informational storage. The classification of new information into existing or new groups related to a specific topic can be realized according to three types of criteria:

- Similarity criterion: similar information can be grouped whether they express the same idea or relate to the same theme (Moles, 1990; Weber, 1984; Conklin, 1987).
- Proximity criterion: the information has an approximate relation to the theme based on the common characteristics (Moles, 1990).
- Analogy criterion: the information can be grouped by direct or symbolic analogy when they are associated or based on observed resemblance.

The creation of links between Pieces of Information within and between Groups: The regrouping of information can be completed by creating links between pieces of information within and among existing groups. Lee and Lai (1991) have proposed, for example, seven types of links: the logically implied link, the support link, the denial link, the qualifying link, the presupposition link, the object to link and the answer link. Collective sense making phase, as another example, conveys the capability of the expert group to create and manipulate influence links: causality link, "object to" link, and "confirm to" link between scattered and fragmented information to provide possible operational fields for subsequent actions.

By analogy, the creation of links process can be compared to a puzzle game consisting in regrouping incomplete and disorderly pieces. However, the difference is that the process is not to rebuild something already existing. In addition, the actor/player does not have at his disposal the totality of pieces. The result of the process depends on the actor/player capability to add sense to uncertain, scattered, and fragmented information. The implementation of the conceptual model has shown the importance of providing practitioners with effective tool capable of tracing reasoning, storing various steps in CI process. This has been underlined in Blanco et al. (2003).

1.2 Model Extension

The conceptual model (Blanco et al., 2003) appears to be based on static links and can not take into consideration several important aspects, especially when environmental organization is hard to analyze or uncertain. Reasoning in the conceptual model appears to be a collective process, where decisions making is based on snapshots gathered at the end of the first phase and analyzed through the group intelligence available during the second phase. Therefore, the complexity and diversity of external events require a dynamic formulation of links and the establishment of variable parameters depending on time or context. In fact, theory has shown that:

- the interpretation process is inherently dynamic (Drazin et al., 1999), and
- the sense making teams see their work as continuous and dynamic (Ashmos et Nathan, 2002).

As a result, it requires that time factor and organization context explicitly be incorporated into the conceptual model to allow for more efficient interpretation. Incorporating time into this model increases the ability of researchers to propose more accurate sense creation, and possibly more robust decisions; while the collective intelligence continues to play an important role.

In addition, it has been found (Ashmos and Nathan, 2002) that sense making should integrate less linear reasoning, especially when CI teams are facing unstructured situations, high degree of equivocality, or uncompleted information, which may be encountered by an organization in managing risks, securing information assets, or building development strategies. For this reason, links should explicitly integrate approximation, incompletion, and probabilistic nature to the rational mental model. In addition, an iterative intelligent reasoning is needed to create the appropriate links. To this end, we propose an extended conceptual model composed of three phases. This model aims to amplify detected weak signals, analyze them, and react properly to the inherent risks.

Phase I: links initialization

Links initialization is considered as an initial phase. Its objective is to amplify detected weak signals and to set up the links capable of providing a clear picture of potential risk encountered by the enterprise as a result of the weak signals amplification. These links have to be able to trace and to comprehend the evolution of important environmental variables with the establishment of reasoning link typology to organize the available information with a significant meaning. This information is within the amplified weak signals, internal and external information, and the contribution of the CI actors.

Phase II: iterative reasoning about links

This phase is crucial in the CI process. During this phase, new links are inferred iteratively using existing links, tacit knowledge of CI actors, and supported by information retrieved from structural archives that are updated along the process. In addition, this phase gains from using appropriate heuristics and automatic transformation to create new links that will be presented later on in the paper.

Phase III: Satisfaction Criteria

This phase aims to check whether the iterative process has reached a clear knowledge of the risk encountered, a good understanding of the mechanisms that have generated the detected weak signals, and a global assessment of other potential related risks. At the end of this phase, a reactive process can be triggered to propose, if needed, the appropriate actions to reduce risk and to anticipate business decisions.

The implementation of the proposed extended model makes use of efficient tools available in Information and Communications Technologies (ICT) . This includes:

- a database for storing risk related information and all traced information generated during the reasoning phase of the CI process, and
- a knowledge base that stores all analyzed weak signals and traces all links inferred through the CI process.

Database and knowledge base provide an important support to ongoing CI process when it is assisted by intelligent retrieval mechanisms allowing approximation search, heuristics search, and automatic transformation of stored links.

2. Use of Causal Maps in the CI process

Causal maps provide a basis for representing a decision maker multiple perspective and help understanding how CI members organize their environments. Causal links that are used in this paper extend the causal maps developed by (Chaib-draa, 2002) by providing a probabilistic approach to cope with uncertainty, adding appropriate dependency relations between valuable information or actions that an agent can perform, and providing new operations to handle approximation between concepts.

2.1 Causal Links Definition

We define a causal link CL as a directed and labeled graph by:

$$CL : (N, E , f: E \rightarrow [0,1], g: E \rightarrow \Delta) \qquad (1)$$

The components of this graph are a set N of nodes, a set E of arrows, a function f that associates every label with a probability value, and a function g that labels every edge with a dependency relation. A node represents a concept (e.g., hypothesis, goal), an action to be performed, or a valuable information appropriate for the CI member reasoning. An arrow represents a causal relation between concepts, or a dependency relation between actions. Let's consider a set Δ of dependency relations including causal relations, time dependency and output/input relations. We assume that Δ is defined at least by:

$$\Delta : \{ +, -, 0, \leq_t, OI\} \qquad (2)$$

where**,**

(+): means that node i has a positive effect on node j;
(–): means that node i has a negative effect on node j;
(0): means that node i has a no effect on node j;
($\leq_t$): means that node i should precede in time node j; and
(OI): (output/input relations) means that the output of node i is the input of node j

The first three relations were studied by Chaib-draa (2002). The last two relations have been added to cover part of the reasoning on situations, where risks and uncertainty are critical. Based on the above definition, the arrow represents a causal/dependency assertion of how one node can affect another along with a real value that measures the likelihood of the assertion. Probabilities associated with these relations are assumed, however, time dependent, that is, the probability value collected on a label can vary from one moment to another.

2.2 Causal Links Operations

The connection of nodes with arrows labeled by the above relations is the basic result in constructing reasoning about the node content. Therefore, such process is built on the notion of reasoning path. A path P from node n_1 to node n_s in a causal map is defined as a sequence of labeled arrows:

$$P: (n_1n_2), (n_2n_3),\ldots., (n_sn_{s+1}) \qquad (3)$$

Where (n_in_{i+1}) is an arrow characterized by its label as defined by equation (2).

Because nodes can contain concepts, actions and various information, one can consider that a node is a variable taking its value in a domain set. A mathematical model can be developed to determine the value of a node in a domain set and to compute paths automatically within the same causal link. We believe that the development of such a model will not be of the scope of the paper. However, the main features of our model will include:

1. Causal link representation: a CL is presented by a matrix. The (i , j)th component describes the causal assertion that provides the effect of node i on node j.
2. Composition of Causal Links: let C_1 and C_2 be two Causal Links having n nodes and p nodes ($n \geq p$). Then the composition of C_1 and C_2, say $C_1 * C_2$, is the CL obtained gathering all nodes and arrows together. Causal links, which are designed to show causal associations and actions dependencies, appear to provide useful tools for coping with reasoning about a global view developed for the need of analysis and decision in certain business activities. They allow prediction of future actions, explanation of past events, and anticipation of effects. Causal Links also offer ways of choosing among alternative actions. To this end, various operations on Causal Links can be implemented. Among the most important ones we can mention:

- Node replacement: this operation permits replacing a node by a network of nodes and links to clarify and to analyze the sub-implications of the node. Several methods can be used to accomplish this replacement. This includes (but not limited to) the node equivalence, the node approximation, the node restriction, and the node reduction. It is clear that applying a node replacement should be accompanied by the redefinition of the labels and end-nodes of arrows ending at or starting from the replaced node. An example of node replacement can be given by the reduction of the concept involved in a node and the appropriate modification of the labels of the links involved with the node.
- Sub-graph rewriting: this operation permits replacing a sub-network of nodes and arcs representing a particular view by an other network of nodes representing a relevant view that can be correctly integrated with the rest of the graph. The replacement of reasoning elements aims to enrich the global vision of the group, serves as an alternative view, or refines the reasoning process. There are several methods that can be used to accomplish this operation such as sub-CL rewriting, sub-CL hiding, sub-CL delete. In CI environment, all the above operations are important for decision making, mediations, and situation evaluation.

3. Reasoning Path construction: a traditional mathematical operation, based on the multiplication of matrices and the composition of relations, can be developed. If C is a causal link, then:

$$C^2 = C \,.\, C$$

$$C^n = C^{n-1} \,.\, C \qquad (4)$$

Where (.) stands for matrix multiplication, which implemented using the composition of relations as defined by:
If R and R' are relations on nodes occurring in set Δ, then the product R.R' states for all pairs of nodes that are related through another node using R and R'. For this reason, we say that C^2 is the set of paths of length 2 and C^n is the set of paths of length n. In the rest of this section, we demonstrate how Causal Links can be used in a CI process.

2. 3 Modeling CI activity

In CI environments, each member can choose a portion to reason about it. This process is often subject to problems of incompleteness, differences between members' views, and conflicts between them. A conflict occurs when two or more individuals build causal links that cannot apparently be conciliated. Therefore, methods such as mediation and negotiation are required to develop more compatible views/relations. Mediation enables the CI (system/support) member to reach with each conflicting member satisfying CL by proposing appropriate arrangements. Negotiation, in this case, means that CI members try to alter other causal links by persuading the causal links owners that they really need to these alterations. To perform mediation and negotiation, members may find it useful to visualize the structure of a CL and perform a dependency/causal based analysis where choices can be made in terms of consequences of assumed relations between actions and can be explained in terms of antecedent situations.

2.3.1 Reconciling differences

To integrate multiple causal reasoning sustaining the subjective view of each member, all concepts are coded (as nodes) in the same causal link, so that all views can be easily transformed into a unique matrix M of size n x n where n is the number of concepts. In this matrix, each element

$$m_{ij} = \ell_1, \ell_2, \ldots..,\ell_v$$

where v is the number of views, and ℓ_k is a label placed by the ith member on the arrow linking node i to j (as occurring in the ith view).
Matrix M allows the study of the following cases:

- Areas of complete consensus between members. These areas are characterized by multi-labels of the form. In that case, all members perceive the same causal effects.

$$m_{ij} = \ell, \ell, \ldots..,\ell$$

- Areas of partial consensus. These areas are characterized by similar perception of the causal effect between pairs of nodes in the areas. The probability values involved in labels are, however, different.
- Areas of non-agreement. These areas are characterized by conflicting labels perceived by members.

Particular multi-labels are called unilateral views. They express unilateral estimation of the causal effect between two nodes, say i, j. In that case the multi-label m_{ij}, is written as:

$$m_{ij} = 0,\ldots., 0, \ell, 0,\ldots,0 \quad \text{and} \quad \ell \neq 0$$

Reconciling differences will focus on three main issues:

1. Achieve a shared definition/meaning of all concepts, actions, and valuable information;
2. Eliminate the areas of non-agreement using negotiations or further investigation using information technology tools; and
3. Reduce the number of unilateral views and areas of partial consensus by attempting to shorten differences.

A mediator can help achieving the above issues. The database and knowledge base mentioned in the previous Section 2 represent also an appropriate tool to support all issues and problems dealing with mediation. Moreover, a formal model to support the relational manipulation, the representation of causal links, and the integration of subjective views can be implemented to support mediation activities.

2.3.2 Decision making

After reconciling differences and mediation, the different beliefs are transformed into a unique graph, which can be analyzed to solve undetermined decisions. The decision making problem can be stated as follows: Given a causal link including one or more decision and a goal (i.e., concepts or actions inserted in the causal link as a node), which decision should be taken and which should be rejected to achieve the goal?

To achieve this, the agent (or mediator) involved in the causal link should compute the complete causal relations linking the decisions to the goal (all paths connecting decisions to the goal). Generally, decisions initiating only positive effects are kept and decisions initiating negative paths are rejected. Conflicting paths lead to undetermined decisions. Solving it is a hard task. It can be achieved using various techniques, including:

- Deleting negative segments within the path produced by a particular decision. Practically, this means that the goal is evaluated under hypothetical situation.
- Deleting positive paths; by doing so, the impact of a given decision without considering positive impacts can be better analyzed.

- Probability compensation. We suppose that the impact of a decision on the goal produces a positive effect that is more valuable then what this decision can impact negatively, then the decision is retained.
- Choosing among alternative decisions. This can be achieved through addition information related to business management, for example.

Finally, if decision can be made/achieved, the view under discussion should be refined using a process conducted by the mediator. The refinement process aims to add more concepts, logics and information.

3. Mediation Management

3.1 Mediator Role

The previous section shows the importance of mediation in CI process. The mediator negotiates with each of the participants in conflict to reach a mutually satisfying arrangement. The mediator constructs and analyzes a new matrix that represents all the nodes and the relations which are relevant to the situation in order to identify potential conflicts. CI mediation in security risks is a set of actions developed within CI process that aims:

- To help members to construct individual views of the situation,
- To reconcile individual views,
- To help to construct and to analyze collective causal map, and
- To refine collective views.

Mediation can be controlled by a mediator whose role is animation, convergence to collective actions, construction of decision alternatives, and concept/information retrieving. The mediator can add, reduce or delete constructed links and information selections. Thus, the mediator needs efficient tools to support the relational manipulation and the representation of causal links. In addition, he needs efficient search engine to retrieve complementary information stored in internal or external database. To solve problems and integrate different views, the mediator must have several skills in order to accomplish his role efficiently. The major appropriate skills are pedagogy, credibility, trust, communication, and coordination. Mediation actions depend on business activities and goals, environment constraints and threats, and CI members' skills and implication. A core set of actions should include:

- Validation of concepts, actions and decisions (represented by the nodes),
- Consolidation, update, manipulation of links (represented by the arcs),
- Construction of all paths that support collective decision making,
- Construction of heuristics to reduce collective decision complexity, and
- Control the refinement process of collective views.

3. 2 Management Tools

Recent literature has shown the importance of ICT in the creativity process. Several studies have demonstrated, for example, that information technologies can support significant group creativity (Massetti, 1996; Wierenga et Bruggen, 1998) and improve the quality of the organizational intelligence (Huber, 1990). Models have been proposed to describe the impact of the internet on the quality of a competitive intelligence process (Teo, 2000; Teo & Choo, 2001). We have found that the Internet technology offers advanced mechanisms that can provide efficient support to CI process. Four majors mechanisms of Internet are appropriate. They are:

1. An approximate search engine by using semantic links (Greenberg, 2003), dependence and hierarchical links, and advanced links, such as hyperlinks, URL addresses: In fact, the classic classification in databases presents several insufficiencies. It is characterized by the existence of determinist and static links between stored information. Therefore, it limits the possibilities of enhancement and crosschecking essential for significant generation. The Internet technologies can respond to theses needs by using hypertext storage mechanisms of information (static links, exact/approximate search).

2. The manipulation of dynamic links by using an inference engine: These engines permit automatic deduction from hypotheses and deduction rules and approached deduction rules based on semantic or probabilistic links. The Internet technology can also manage the database implementing appropriate reasoning heuristics to the stored links. Thus, Internet mechanisms contribute to create an intelligent and dynamic storage of collected information efficiently and rapidly by creating useful links to structured and organized information into hierarchical structures.

3. Control mechanisms access that involves the implementation of corporate control policies for end user authentication, access to corporate resources, and authorization to perform specific actions: These mechanisms guarantee the traceability of accesses and all operations performed on enterprise resources. These mechanisms permit also the definition of an access policy to stored knowledge and a search tool for requested information. This approach permits thereby a capitalization of corporate knowledge when comments formulated by experts are linked with corresponding information illustrated by the evolution of collective learning.

4. Computation support that can manage heuristics with relative rapidity and flexibility which can positively affect team reaction.

The CI process supported by Internet technologies presents attractive qualities that may interest decision makers to develop an anticipative capacity. These qualities include reliability, flexibility and generality. In fact, this process guaranties an acceptable reliability by permitting the traceability of the information and reactivity. The flexibility will be in terms of adaptability to information structure modification and adaptability to structural modification of decision rules. Finally, this process verifies general conditions in terms of applicability to different types of problems or activities.

4. CI Process for Digital Aggressions Reduction

To measure the collective intelligence process efficiency in terms of reliability, flexibility and generality, we propose an application to detect attacks on enterprise local area networks. The CI process in the network security is a particular information system to help the protection of company resources. This process allows detecting automatically the classified attacks in different sites. The same process allows detecting non classified attacks through the analysis of weak signals detected by detection control systems, to evaluate the potential losses, and to prepare the appropriate and rapid response to these attacks. The non classified attacks require the generation of certain type of decision non repetitive and non programmable. Decision making requires creative reasoning activity based on links. In addition, these attacks and the generation of links from the collective intelligence process have to be memorized to make the security incident response process richer.

In fact, the attack is any actions that compromise the information security (Stallings, 2000). The findings of the annual report of CSI/FBI confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting (Power, 2002; Richardson, 2003). The Internet connection is increasingly cited as a frequent attack point.

The most severe attacks detected are virus, network access and abuse of internet use, companies' intrusion of the information system, denial of service, and non authorized access by internal users. These attacks resulted in large financial losses of the surveyed companies. These important losses added to the increasing numbers and complexities of attacks have pushed companies to develop efficient policy based in particular on the reactivity of the security incident response team (IRT).

4.1 IRT main Tasks

The security incident response team (IRT) is in charge to identify attacks by analyzing weak signals collected by detection systems, to reduce the impact of the attacks, and to make the appropriate decision to protect the sensitive resources of the enterprise. An IRT has to react within the framework of a defined security policy that can be integrated within collective intelligence process. The important tasks accomplished by IRT are:

1. notification (temporary memorization): each incident must be identified in time and communicated to concerned persons or appropriate departments (Van Wyk and Forno, 2001; Schultz and Shumway, 2002; Kruse and Heiser, 2002) .
2. analysis: the objective is to describe the causes of this accident and the consequences and to determine any eventual links with previous incidents (Allen, 2001 ; Sokol and Curry, 2000).
3. reaction: the IRT reaction must be concrete to stop or to limit the impact of the incident taking into the account the enterprise specific activity. This reaction has to be quick, efficient and realized collectively (Sokol and Curry, 2000; Mandia and Prosise, 2001;).
4. documentation and traceability (memorization): each security incident has to be documented in specific format and published in web sites where the results can be accessed at any time.

To support the IRT activities, database with link generation is necessary for the analysis of the attacks. This database contains two components. The first component supplies complete information on classified attacks in generic web sites or in enterprise internal sites. The second component contains links between the attacks with useful information related to weak signals analysis, enterprise resources, and decision making alternatives.

4.2 Adapting CM techniques to the activity of the IRT

The CM model presentation is based on nodes and arcs. The nodes represent actions, hypotheses, information, and goals. In the case of network security, actions include, but are not limited to:

- intrusion or misuse action,
- unauthorized access, and
- obtain unauthorized information or execute unauthorized operation.

Hypotheses include decisions or countermeasures to be achieved on the network system or on the information system. Goals represent statements such as:

- asset X is facing a specific attack,
- system X is appropriately protected, or
- attack X is identified

Concept and information nodes represent weak signals (as detected by the organization's sensor network) or any useful information that helps detecting, analyzing, and responding to potential

attacks. The arcs indicate the types of influence relating two nodes. There are five types of influential relations between nodes:

1. The positive relation (+) indicates that the node n_1 is necessary to improve, to favor, to strength, to activate, to aid, or to make possible the node n_2. In the network security, a first collected information can indicate a potential risk that can activate a certain action.
2. The negative relation (–) indicates that the node n_1 prevents, obstructs, makes difficult, or inhibits the node n_2. For example, if node n_1 is a countermeasure and node n_2 represents a possible action, then relation (–) relates the effect of the countermeasure on the proposed action.
3. The neutral relation (0) indicates that there is no influence between nodes.
4. The (OI) relation between $n_1$and n_2 indicates that the output of n_1 is the input of n_2. Such input includes an IP address, a password, unauthorized information, etc.
5. The ($\leq_t$) arc indicates dynamic relation between the realization of the two nodes contents depending on time. In our case, the time constitutes an important variable to establish a significant relation between collected or stored information in order to detect an eventual attack.

Specific rules for digital aggression are important to construct the definitive scenario of a digital attack. To reduce the reasoning complexity, the ICT can be used to access useful websites known to be well documented for providing information about all known attacks (e.g. CERT website, Allen, 2001). The ICT support can limit the number of candidate attacks and contribute to converge views during the reconciling process. Various operations such as node replacement or sub-graph rewriting are appropriate in network security case to define the attack scenario. Sub-graph rewriting is, in this case, getting more details on the node/subnet content. This includes for example the description of the scenario of actions that an attack can perform to achieve its objectives.

4.3 IRT Puzzle Model

To assist the IRT work, this paper proposes a model supported by Internet technologies called IRT-puzzle model. It is composed of five modules (Figure 1) as follows:

1. Information memorization module: it is used to memorize collected information including weak signals, attack features and intermediate CM.
2. Information multi-criteria reconciling module: it uses exact/approximate search operators to permit progressively the construction and the refinement request until the process actors are satisfied with generated view. Negotiation is then performed to achieve a high level of agreement among CI members.
3. Construction puzzles module (or refining CM construction): it represents the phase of reasoning about links. A CI group can either achieve a reasonable conclusion with CM, or start a process of reconstructing the CM through constructing links from the memory or building new links. In the case of creation of new links, the actors can process link association automatically provided by the ICT tools and derived from association with stored links after the use of the search engine. Otherwise, they construct the links by themselves according to their own reasoning.
4. Handling process module: it permits real time management of the different information in the database and created links. The process manager can add, reduce or delete constructed links and information selections.
5. Exacted/approximated search module: it permits the extraction of local and external information according to influence and semantic links.

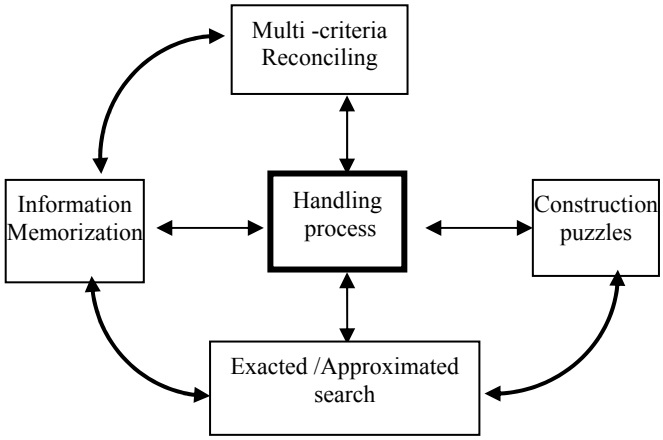

Figure 1 : IRT Puzzle Model

5. Case study: Web Defacement (French Connection)

To demonstrate the IRT puzzle model, we apply it to an example of a security attack. The example, web defacement, is taken from Schiffman, (2001). It describes the case of a publicly traded, medium-sized software company which is subjected to an attack of a web server. The company is an IT company where the computers, software, intranet, and internet are the main production tools. Any attacks on these tools would suspend the enterprise activities. Therefore, it will result in major financial losses that may bankrupt the company. In fact, the hacker posted a link to the company's defaced web site along a snide message mocking about its security in Yahoo! Message board that was supposed to be about investments in the company. As a result, the company's stocks have fallen down.

Signal Analysis: attack description

The help desk of the company has received a telephone call from a customer that the hackers had apparently attacked the company's web site on Friday night. The person in charge of the help desk at that time checked out the web and had indeed found that the web site has defaced. He founds the following message:

The script attack: *"you, my friendz, are completely owned. I'm here, your security is nohere. Someone should check your system security coz you sure aren't."*

From analyzing the attack detection, it can be noticed that the customer (end user) reporting the attack, was an outsider to the company. This implies that the company does not have monitoring tools for its main activities. It is really a serious gap in the management process.

The CI process has started from the telephone call of the customer. This telephone call is treated as a weak signal since it is reported by an entrusted source and the competence and the analysis capabilities of the user are unknown to the company. However, the message cannot be disregarded. Therefore, the IRT should start analyzing the signal and developing a consistent view that can lead either to decide that a serious attack was really performed, that the flaw revealed by the message is a limited alert, or that there is no attack. This analysis procedure is the first step in constructing the puzzle.

The IRT staff began to research Web defacement attacks. They found that the web server that was attacked hosted an older web site with an old page, which was noticed by no one for several hours. The system logs on the hacked system offered no evidence of an attack. In addition, the operating system (NT) event log did not have any entries during the days prior to or during the dates and times in question. The company decided to ignore this signal since there was no evidence of an attack. This shows a problem in the analysis capabilities of the IRT. It is because the IRT has

used a reasoning approach based on the following causal map (Figure 2), which represents the view that the IRT members have built according to their capacities.

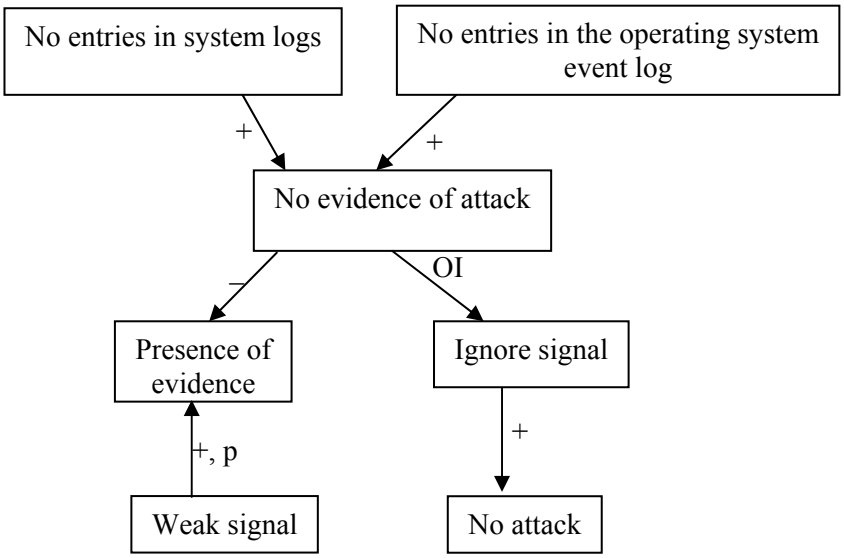

Figure 2: Causal Map of the IRT

The probability p measures the likelihood of an attack. A good reasoning process should have noticed that the relationship between "no evidence of attack" and "ignore signal" and the relationship between "no evidence of attack" and "presence of evidence" could not be accepted and that, the probability p should be estimated efficiently during the weak signal amplification step based on members knowledge and ICT capacities. Therefore, the reconciling step did not achieve an efficient view during the global view construction.

After the weekend, the lack of skills was pointed out and the problem got worse since the attack has been published in Yahoo! Message board. It has resulted in an embarrassment to the company credibility. The IRT staff has then decided to analyze in more details the problem. That is amplifying the signal reported by the end user. As a result, they discovered that the web server software they were using had a well-known bug that easily allowed attackers to take control of the machine. This discovery has created the first input information that is stored in the information memorization module. The second input information is that the server was inside the network when it was compromised. Creating a link between these two pieces of information will result in a third inferred information that the attacker could now have backdoors to any system inside the network, as well as copies of sensitive data and passwords.

Once the IRT staff knew the probable method of entry, and identified the bug, they began to piece together the attack. They started constructing the different part of the puzzle. The bug relies on the ability to execute a system shell, a program called *cmd.exe*, in order to execute commands on the Web server. The IRT staff found that if this bug was used, evidence of the attack would be in the Web server log files. They collected all the log files from the web server and imported them into a database for analysis. Once the attacker had a better understanding of the environment, the attack began.

The following causal map (Figure 3) attempts to give the collective construction of the attack scenario. Two relations play an important role in the decision process to recover from the attack. They are:

1. Relation $\leq_t$: states the "web server defacement" should preceded by the execution of commands "cmd.exe". The log file shows all executed commands with their time execution.

2. Relation OI: states that the "web server defacement" cannot be realized without getting information on existing backdoors.

For the sake of clarity of our case study, we have omitted the related views that the IRT members can build for the prevention and mitigation.

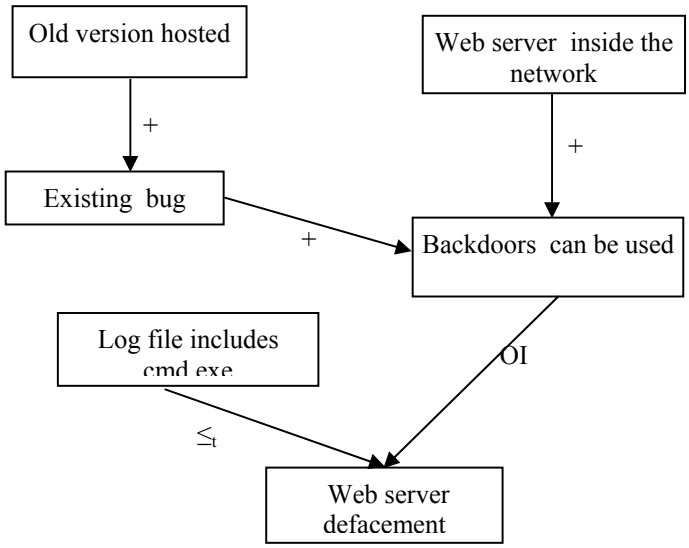

Figure 3: Collective Construction of Scenario Attack

This graph is represented through a matrix (figure 4) where 1, 2, 3, 4, 5, and 6, represent respectively "Old version hosted", "Web server inside the network", "Existing bug", "Backdoors can be used", "Log file includes cmd.exe", "Web server defacement".

$$C = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 0 & 0 & + & 0 & 0 & 0 \\ 0 & 0 & 0 & + & 0 & 0 \\ 0 & 0 & 0 & + & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & OI \\ 0 & 0 & 0 & 0 & 0 & \leq_t \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

Figure 4 : Matrix Presentation of the Graph

The analysis of the C^n, $n \geq 1$, shows that only paths of length 1, 2, and 3 can be provided. Only one path of length 3 is available, it links "Old version hosted" to "Web server defacement" nodes. It shows the indirect affect the existence of an old version can have on the defacement of the web server.

6. Toward a structured CI-methodology for risk reduction of digital aggression

The structured CI-methodology is defined by three majors steps where each step is divided into sub steps. It permits the exploitation of weak signals information to reduce risk of digital aggression and to develop an anticipative capacity. It satisfies five criteria which are recommended to support a structured methodology:

1. The structured CI-methodology contains a sequence of three steps. Every step is clearly defined, and the output of every step is clearly determined.
2. The different steps are accompanied by tools support which is necessary to validate and to test the results obtained by every step.
3. The structured CI-methodology verifies the condition of the coherence of the different reasoning mechanisms, the concepts and the results.
4. The structured CI-methodology for risk reduction of digital aggression can be extended to treat other types of risks (such as investment risk, stock market, etc.). Thereby, the structured CI-methodology for risk reduction offers a general framework to trait several types of risks with the respect of a certain condition of replication.
5. The structured CI-methodology represents a simple and direct method makes it possible to attain a specific objective. In fact, it is based on several mechanisms such as reconciliation and refinement of views and heuristics susceptible to reduce the complexity of reasoning.

The three steps of the structured CI-methodology for risk reduction of digital aggression are presented as follows:

- **Weak signals collection and strengthening:** this step is described by Ansoff (1975) as a "graduated response through amplification and response to weak signals". It contains:

1. The detection of weak signals: The digital aggressions begin every time by the detection of weak signals. However, the detection is complex and difficult. The detection of weak signals supposes placing sensors to detect, to filter, and to provide information to the appropriate persons or departments.
2. The amplification of weak signals: the analysis of this information may lead to extract, collect meaningful information that can be of great help to detect anomalies or vulnerabilities related to the weak signals in the network system
3. The Collection of complementary information: to complete the analysis of the amplified signals, this step is important and necessary to identify the problem and decide to develop a detailed action plan. The plan starts by identifying links between collected and stored information.

- **Modeling the scenario aggression:** During this step, the CI members develop their views by identifying the nodes and their contents. Then, they analyze and create links between the identified nodes in order to have more intelligible vision. The generation of static links can be automated since there is no intelligence in creating them. For example, identifying causal links between two information is considered static links. Inferred links are created by inference from facts and rules using heuristics or other search approaches. The reasoning is based on generated links from knowledge base or inferred from the existing knowledge or created by collective intelligence. The combination of static and dynamic links will construct the complete scenario of attack. The step of modeling the scenario aggression is supported by several mechanisms permitting the reconciliation and the refinement of members' views. The role of a mediator is very important during this step in order to solve conflicts, integrate views and validate the global vision of the CI group.

- **Responding to aggression and anticipating risks:** this step represents the decision making phase. The CI members assess the direct or indirect damages and implications of the attack and

evaluate the immediate actions to respond. The mitigation will enhance the team capacities to identify weak signals appropriate to similar problems and to anticipate the appropriate protective measures (such as human skills resources and modification of security policy).

Conclusion

In this paper, we have proposed structured methodology for a general CI process that is able to conduct decision making in a risky environment by analyzing and reducing all business risks related to uncertain activities including numerical aggressions. This methodology extends some of the CI processes proposed in the literature (e.g. Blanco et al., 2003). It also provides theoretical tools for the description of views, member reasoning and process reconciliation. The foundations of a mediator role has been developed by adding new features and tools to the model proposed by Chaib-draa (2002) which is based on causal map paradigm. These features help addressing uncertain deductions, temporal issues, contradicting hypotheses, and converging heuristics. We have found the methodology developed in this paper well suited to analyze, to react to, and to prevent security incidents in enterprise networks. In this context, the work of an IRT is modeled. The reconciliation is adapted to the context of internal and external intrusions/anomalies and the availability of dynamic information sources reporting on attacks. Finally, we have shown an implementation of our model through a real example. This model is now under validation at the Tunisian National Digital Certification Agency where it is daily used in IRT activity.

References

Allen J. H. (2001), The CERT guide to system and network security practices, Addisson Wisley.

Ansoff, I. (1975), "Managing strategic surprise by response to weak signals " *California Management Review*, Vol.18 (2): 21-33.

Ashmos D.P. et Nathan M.L. (2002), "Team sense-making: a mental model for navigating uncharted territories", *Journal of Managerial Issues*, Vol. XIV, n°. 2, Summer.

Blanco S., Caron M.L. et Lesca H., (2003) "Developing capabilities to create collective intelligence within organizations", *Journal of Competitive Intelligence and Management,* Volume 1, Number 1, Spring: 80-92.

Chaib-draa, B. (2002), "Causal maps: Theory, Implementation, and Practical Applications in Multiagent Environments", *IEEE Transactions on Knowledge and Data Engineering,* Vol. 14, N°. 6, November/December.

Choo, Ch. W. (2001), The knowing organization as learning organization, Education & Training, Volume 43, number 4/5, pp. 197-205.

Choo, Ch. W. (2002), Information Management for The Intelligent Organization : the art of scanning environment, Information Today, Inc. Medford, NJ.

Choo, Ch. W., Deltor B. et Turnbull D. (2000), Web Work: information seeking and knowledge work on the World Wide Web, Kluwer Academic Publishers, Dordrecht, The Netherlands, 236 p.

Conklin J. (1987), "Hypertext: an Introduction and Survey", *IEEE Computer,* 20(9): 17-41.

Daft, R.L. ; Sormunen, J. et Parks, D. (1988), "Chief executive scanning, environmental characteristics, and company performance : an empirical study ", *Strategic Management Journal*, Vol. 9.

Daft, R.L. and Weick K.E. (1984) "Toward a model of Organizations as Interpretation systems", *The Academy of Management Review,* Vol. 9, n° 2.

Daft, R.L. et Huber G., (1987) "How Organizations Learn: a communication framework", *research in the Sociology of Organizations,* Vol. 5, p. 1-36.

Drazin R., Glynn M.A. et Kazanjian R.K. (1999), "Multilevel theorizing about creativity in organizations: a sensemaking perspective", *Academy of Management Review,* Vol. 24, n° 2.

Gioia, D. A. and Chittipeddi K. (1991), "Sense-making and Sense giving in Strategic Change Initiation", *Strategic Management Journal*, Vol. 12.
Greenberg, J. (2003), "The semantic Web", *Bulletin of the American Society for Information Science and Technology,* May/April.
Huber, G. P. (1990), "A theory of the effects of advanced information technologies on organizational design, intelligence, and decision making", *Academy of Management Review*, Vol. 15 (1).
Kruse W. G., Heiser J. G., (2002), *Computer Forensics, Incident Response Essentials,* Reading, MA: Addison-Wesley.
Lee J. and K. Lai (1991), "What's in Design Rationale ?" *Humain-Computer Interaction,* 6 (3&4).
Lesca H. (2003) – Veille stratégique La méthode L.E.*SCAnning*. Ed. ems Management et société, 190 p.
Mandia K. and Prosise Ch., (2001), *Incident Response: Investigating Computer Crime,* Berkeley, CA: Osborne/McGraw Hill.
Massetti, B. (1996), "An empirical examination of the value of creativity systems on idea generation", MIS Quarterly, March.
Moles A. (1990), "Abaques de regnier" pp. 255-228 in *les Sciences de l'imprécis.* Paris, FR† : Editions du Seuil.
Pfeffer, J. and Salancik, G. (1978), The external control of organizations, New York: Harper & Row.
Power R. (2002), "2002 CSI/FBI Computer Crime and Security Survey", *Computer Security Issues & Trends*, Vol. VIII, No. 1, Spring.
Richardson R., (2003), "2003 CSI/FBI Computer Crime and Security Survey", *Computer Security Instiute,* Eight Annual.
Sadok M., Benabdallah S. and Lesca H. (2003), "Apports Différentiels de l'Internet pour le Veille Anticipative : Application au cas de Réponse aux Atteintes à la Sécurité des Réseaux d'Entreprise", 8th Colloque of AIM, May 2002, Grenoble.
Schiffman, M. (2001), *Hackers Challenge: Test Your incident response Team skills using 20 Scenarios,* Berkley, CA: Osborne/McGraw Hill.
Schultz E. and Shumway R., (2002), Incident Response: A Strategic Guide to Handling System and Network Security Breaches, *Indianapolis, IN: New Riders Publishing.*
Sokol M. and Curry D. A., (2000), "Security Architecture and Incident Management for E-business", Atlanta, GA: Internet Security Systems, http://www.iss.net/support/documentation/whitepapers/technical.php
Stallings W. (2000), Network Security Essentials : Applications and Standards, Prentice Hall.
Teo, T.S.H. (2000), " Using the Internet for competitive intelligence in Singapore ", *Competitive Intelligence Review*, Vol. 11(2).
Teo, T.S.H. et Choo, W. Y. (2001), "Assessing the impact of using Internet for competitive intelligence", *Information Management*, Vol. 39.
Van Wyk, K. R. and Forno R., (2001), *Incident Response,* Sebastopol, CA: O'Reilly & Associates, Inc.
Venkatraman, N. and Prescott, J. E. (1990), "Environment-strategy coalignment: An empirical test of its performance implications", *Strategic Management Journal*, Vol. 14.
Weber C. E. (1984), "Strategic Thinking: Dealing with Uncertainty", *Long Range Planning,* 17(5): 60-70.
Weick, K.E. (1995), *Sensemaking in Organizations,* Sage Publications, Thousand Oaks, CA.
West-Brown M. J., Stikvoort D. et Kossakowski K. P (1998), *Handbook for Computer Security Incident Response Teams (CSIRTs)*, Carnegie Mellon University/Software Engineering Institute, December.
Wierenga B. et Bruggen G. H. (1998), "The dependent variable in research into the effects of creativity support systems: quality and quantity of ideas", *MIS Quarterly*, March.