Design of a Case-Based Reasoner for Information Security in Military Organizations

José Borges[1], José Martins[1], Jorge Andrade[1], Henrique dos Santos[2]
[1] Academia Militar – CINAMIL, Lisboa, Portugal
[2] Universidade do Minho – DSI, Guimarães, Portugal
jose.borges@academiamilitar.pt
jose.carloslm@gmail.com
jorge.andrade@academiamilitar.pt
hsantos@dsi.uminho.pt

Abstract

Information security is concerned with the protection of information, which can be stored, processed or transmitted within critical information systems of the organizations, against loss of confidentiality, integrity or availability. Protection measures to prevent these problems result through the implementation of controls at several dimensions: technical, administrative or physical.

A vital objective for military organizations is to ensure superiority in contexts of information warfare and competitive intelligence. Therefore, the problem of information security in military organizations has been a topic of intensive work at both national and transnational levels, and extensive conceptual and standardization work is being produced. A current effort is therefore to develop automated decision support systems to assist military decision makers, at different levels in the command chain, to provide suitable control measures that can effectively deal with potential attacks and, at the same time, prevent, detect and contain vulnerabilities targeted at their information systems.

The concept and processes of the Case-Based Reasoning (CBR) methodology outstandingly resembles classical military processes and doctrine, in particular the analysis of “lessons learned” and definition of “modes of action”. Therefore, the present paper addresses the modeling and design of a CBR system with two key objectives: to support an effective response in context of information security for military organizations; to allow for scenario planning and analysis for training and auditing processes.

Keywords: conceptual model for information security, case-based reasoning, decision support system, method of attack, information security controls.

1. Introduction

Nowadays we are assisting to an increasing dependence of organizations (military, governmental or other civil institutions) on the use of information systems (IS) to collect, store and manipulate internal data, which is critical for their activities. This data accumulates information ranging from confidential activities, to employee information or research projects, just to mention a few. Therefore, information is a critical asset that needs to be protected from potential threats and attacks, and secured with respect to possible infrastructure vulnerabilities.

Information security (InfoSec) is generally concerned with the protection of information, which is stored, processed and transmitted through IS that rely on both private and public networks, and at the same time to assure its availability to authorized users. The fundamental properties of InfoSec (ISO/IEC 27001, 2013; Posthumus & Solms, 2004; Siponen & Oinas-Kukkonen, 2007) can be summarized as: to prevent loss of confidentiality; to ensure data integrity; to assure data availability to authorized users.

The vectors to provide InfoSec rely on three factors (Posthumus & Solms, 2004): technological, which allows storage, processing, and transmission of information; human, namely the users who can access information through either public or private networks; business process that rely on the use of data.

A vital objective for military organizations is to ensure superiority, including in contexts of information warfare and competitive intelligence. New military concepts have been emerging over the past two decades: information superiority (Alberts, Garstka, Hayes & Signori, 2001); information warfare (Arquilla & Ronfeldt, 1999); defensive battle (Chesla, 2004). The key point of these concepts is that information is seen as simultaneously a weapon and a target (Hutchinson, 2003).

Therefore, the problem of InfoSec in military organizations, so-called Computer Network Operations, has been a topic of intensive work at both national and transnational levels, and extensive conceptual and standardization work is being produced. Computer Network Operations (JP 3-13, 2006) enable organizations to protect, defend, and respond to cyber threats and adversaries by leveraging information in three areas of network operations: computer network attack, which focuses on the offensive aspects of cyber warfare and the ability to disrupt or destroy an adversary's computer and information capabilities; computer network defense, which leverages information to prevent, identify, analyze, monitor, and respond to cyber attacks; computer network exploitation, which supports the area of computer network attack by gathering the necessary intelligence and information to proliferate effective attacks.

Some examples of disruptive effects due to methods of attack targeting IS from sovereign states are: the *Snowden's Case*, which has triggered a wide discussion in the media and several security forums; the cyber attack launched against Estonia in April and May 2007, which led to the shutdown of several State activities (Tikk, 2008); the conflict in Georgia in 2008 (Tikk, Kaska, Rünnimeri, Kert, Talihärm & Vihul, 2008). Additionally, the increasing capacity of some countries to conduct cyber warfare and computer network operations (Andress & Winterfeld, 2011; TRADOC-PAM 525-7-8, 2010) completely justifies an integrated approach to InfoSec in military organizations.

All these factors demand for new approaches to InfoSec in order to promote and develop processes for InfoSec in military organizations that strength capacities to act both reactively and preemptively. The focus of such processes has to be the possible modes of action of an opponent (i.e. their methods of attack). A model for InfoSec (Martins, Santos, Dias & Borges, 2014; Martins, Santos, Nunes & Silva, 2012; Martins, Santos, Rosinha & Valente, 2013) guided by some principles of war and taking into account known modes of action provides the identification of: the main methods of attack that can occur; the baseline for controls baseline applied in military organizations; the security controls applied by attack methods and validation the their effectiveness, according to the specific method of attack.

A major effort today is being directed into developing automated decision support systems to assist military decision makers at different levels in the command chain, and to provide suitable control measures that can effectively deal with potential attacks and, at the same time, prevent, detect and contain vulnerabilities targeting at military IS.

The concept of the *Case-Based Reasoning* (CBR) methodology and process (Aamodt & Plaza, 1994; Kolodner, 1993) outstandingly resembles some classical military processes and doctrine, in particular the analysis of *lessons learned*, which is equivalent to *case-based interpretation* and *learning from success and failures*, and the definition of *modes of action*, which is equivalent to *case-based problem-solving*. Therefore, the present paper addresses the modeling and design of a CBR system with two key objectives: to support an effective response in context of InfoSec for military organizations; to allow for scenario planning and analysis for training and auditing processes. The conceptual framework proposed in this paper can also be applied for InfoSec in civil organizations.

The literature in CBR (David & Plaza, 1997) describes several successful applications. Some recent application examples, just to cite few, are: InfoSec risk analysis (Bang, Kim & Hwang, 2008); health sciences (Bichindaritza & Marling, 2006); support of strategic decisions in business (Surma, 2010).

The remainder of this paper consists of three sections. Section two revises a conceptual model for information security and the integration of CBR within this framework. The third section addresses the conceptual design of the case-based reasoner in terms of the typical CBR cycle, and as well the design of a case representation layout for information security methods of attack. Finally, the last section presents some conclusions and future work.

2. A conceptual Model for Information Security

In the present context, information is defined (JP 3-13, 2006) as existing data in any form and shape, which is assigned a meaning, after having been organized in a useful manner, in order to impart a meaningful message to the recipients of its use.

Information security (ISO/IEC, 2013) is an inherent quality of information, which indicates to what extent that property of security exists in that information, which is materialized in means that preserve it from eventual attack methods.

An *attack method* (Howard & Longstaff, 1998; Pfleeger & Pfleeger, 2007) is any action(s) supported in tools that are used to exploit the vulnerabilities of the main components of IS, with the purpose of, directly or indirectly, achieving the security properties of information and consequently producing operational effects.

The *Operational effects* are the main objectives of military nature to achieve by an opponent, in order to contribute to information superiority in an information warfare environment.

The information security conceptual model (Martins, Santos, Dias & Borges, 2014; Martins, Santos, Nunes & Silva, 2012; Martins, Santos, Rosinha & Valente, 2013) that is described in this section is based on international standards for information security management (ISO/IEC 27001, 2013), the military security standards that have been applied in the Portuguese Army (PDE 2.09.00, 2010), the security doctrine of NATO (AAP-6, 2009), and the Certified Information System Security Professional (Harris, 2008). The proposed model can be used by the Portuguese Army, or other organizations, to provide sets of controls that give the best response to information attacks or threats within their systems information networks. Therefore it aims at contributing for improving InfoSec in general organizations while applying principles and procedures inspired by the military organization.

Planning Method for Information Security

The planning method for InfoSec is proposed in this section based on the following components:

- a reasoner that allows for the identification of possible methods of information attacks, carried out using the vectors of physical, human or technological infrastructure attack (Martins, Santos, Nunes & Silva, 2012);
- a framework of categories of InfoSec controls (security dimensions: organizational, physical and environmental, human, and technological) (Martins, Santos, Rosinha & Valente, 2013);
- a decision process triggered by the attack vectors of an opponent, and the possible effects of InfoSec controls (prevent, detect, deter, deflect, recover or react);

- the analysis of processes from military organization.

Framework Model

In order to derive a conceptual model for InfoSec, the following propositions are considered:

1. The InfoSec is built on the basis of possible methods of attack of an opponent, carried out in the attack vector: physical, human and technological infrastructure (Martins, Santos, Nunes & Silva, 2012).
2. The security controls are integrated into the major categories of InfoSec, according to the dimensions of security: organizational, physical and environmental, human and technological (Martins, Santos, Dias & Borges, 2014).
3. The desired effects from applying InfoSec controls are to prevent, detect, deter, deflect, recover or react to an attack method (Pfleeger & Pfleeger, 2007).
4. The planning of InfoSec is based on lessons learned (PDE 0.32.0, 2012), or rather aims at selecting, retrieving and adapting ongoing solutions attack methods or InfoSec incidents that have occurred, that resemble the situation.

Given the specificity of the military organization, the design of an InfoSec planning method takes into account the most important principles of war applied in the planning and conduct of military operations (Couto, 1988). The principles of war are under military laws, which were for centuries, and are still considered in military doctrine, as the key elements in operational planning, being fundamental to the characterization of the specificity of the planning of military operations (Couto, 1988). The adaptation of these principles to the planning of InfoSec method is presented in Table 1.

Table 1: Principles of war adapted to the information security context

Principles of War	Goal
Economy of Force	The InfoSec controls implemented must protect the greatest number of attack methods and ensure maximum possible effects (i.e. prevent, recover).
Maneuver	The controls implemented should ensure protection of the main vector of attack, defense in depth and mutual support between them.
Unity of Command	The method of planning should ensure integration of all management levels in military organizations, through a common sight in the planning, implementation (includes maintenance, monitoring and audits) and cohesion of controls applied.
Security	The planning method should allow planning actions to obtain information about an opponent in order to anticipate its modes of action.
Offensive	The planning method should allow offensive action within the InfoSec, rather than react. Simultaneously should allow anticipating the possible methods of attack an opponent and exploit its vulnerabilities.

The conceptual model that implements the method of planning InfoSec is implemented in a military organization according to the process illustrated in figure 1, and matches the requirements for quality management systems in ISO/IEC 9001 (Martins, Santos, Rosinha & Valente, 2013).

The goal is to select efficient combinations of InfoSec controls, to deal with an enemy attack, and definition of the baseline InfoSec to be implemented in order to avoid, in the information warfare, environment the information superiority of the adversary.

The inputs are: security components, which consist of a model of attack methods and the framework of categories of InfoSec controls; a decision matrix for InfoSec; the analysis of the military organization processes. The outputs are a baseline of security controls for information and the InfoSec controls for the perpetrated attack method.

In order to provide process control detailed documentation is required: documental evidence of the operational procedures; reports of attack cases, with lessons learned in military organizations where the method is applied; reports of planned and unannounced audits. Further documentation should be provided regarding:

validated methods of attack and information security framework; plan of information security; policy information security; technical information security policies; operational procedures; registration of the evidence of the case and the controls implemented.

The coordination is performed by the chain of command of the military organization, while the responsible for the process is the security officer by authority delegation of the Commander in the military organization. The effective use of such framework requires: an automated case-based reasoner; experts in the fields of InfoSec; automated processes of gathering evidence of InfoSec in military organizations (i.e., incidents).

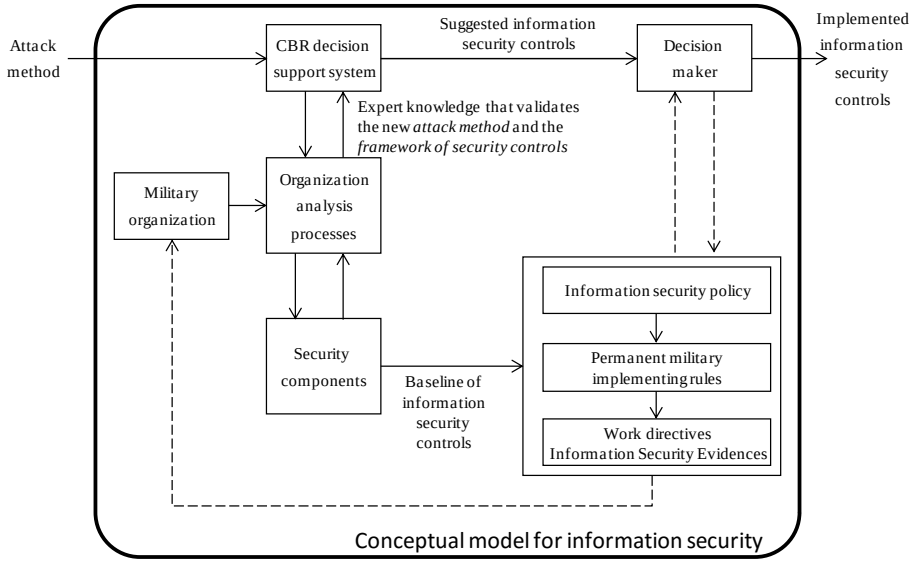

Fig. 1: Conceptual model for information security in military organizations [Adapted from (Martins, Santos, Dias & Borges, 2014; Martins, Santos, Nunes & Silva, 2012; Martins, Santos, Rosinha & Valente, 2013)]

As shown in figure 1, the CBR decision support system will provide (suggested) set of controls to the decision maker, and will receive feedback from the organization InfoSec experts, therefore it directly interacts with the main organization processes. These will allow for the bookkeeping of cases, which are stored in the case base, with respect to problem descriptions and successful/unsuccessful solutions. The conceptual model for InfoSec planning within military organization in an information warfare environment has the following characteristics:

1. Considers the principles of war and military security ("need to know", "least privilege", "responsibility, loyalty and trust" and "the defense in depth").
2. Facilitates its operationalization through the chain of command, by: centralized planning and efforts orientation by attack method; all organization levels; security capabilities (dimensions and categories of controls) and skills of employees (security controls).
3. Allows an agile management that enables simulate and anticipate attack methods (interconnection with the model of attack models), and facilitate the inclusion of new categories and InfoSec controls.
4. Supports the management of InfoSec lessons learned concerning to incidents of InfoSec, taking into consideration that there is no single "recipe" of InfoSec for all military organizations.
5. And finally, enables all employees to raise awareness for InfoSec, through a single view, i.e. shared model for all employees.

The proposed planning method complies with the principle of Unity of Command by ensuring the integration of management levels of the military organization, which provides a common view of InfoSec to all employees and "cohesion" of measures to be applied. The proposed planning method is also guided by the principles of Security and Offensive; the model of attack methods allows, both friend and foe, planning actions of obtaining information and offensive.

The conceptual model of InfoSec planning, supported by the propositions already focused and the principles of war, allows answering the following operational issues: how can a method of attack on information from a military organization contribute to an opponent achieving information superiority; what are the targets that a particular method of attack can explore and a determined target that can be exploited by attack methods;

what is the minimum baseline of InfoSec controls to military organizations; what is the contribution of a particular security check to protect the military organization of a particular attack method or set of methods of attack to information.

3. Conceptual Design of a Case-Based Reasoner for Information Security

Case-based reasoning (Aamodt & Plaza, 1994; Kolodner, 1993) is a methodology that has emerged from artificial intelligence and can provide reasoning and learning to support decisions for new problems. The key idea of this methodology is to reuse knowledge collected from past cases, which are described in terms of problem attributes and respective solution, to provide solutions to a new problem. Interestingly, this concept is closely related with processes that have been applied in military organizations for ages, namely *lessons learned* and *modes of action*.

The conceptual design of a problem-solving CBR system to provide decision support for information security within military organizations is addressed in this section. The dimensions for InfoSec (Martins, Santos, Nunes & Silva, 2012; Martins, Santos, Rosinha & Valente, 2013) are: organizational, physical, human and technological. The possible effects on InfoSec (Martins, Santos, Nunes & Silva, 2012; Martins, Santos, Rosinha & Valente, 2013) are: react; recover; deflect; deter; detect; prevent. The best set of controls, which result from acting on the InfoSec dimensions, that will attempt to mitigate the effects on InfoSec is the main goal of this CRB system.

The initial set of information describing the cases, which are stored into the case base, will result from different sources, namely: organization's own past experience; international standards; best practices within both the military and civil organizations.

CBR Cycle

The CBR cycle (Aamodt & Plaza, 1994) is adapted to fit into the conceptual model for information security in military organizations, which in the previous section is represented in figure 1. Figure 2 represents the CBR cycle with the required modifications.

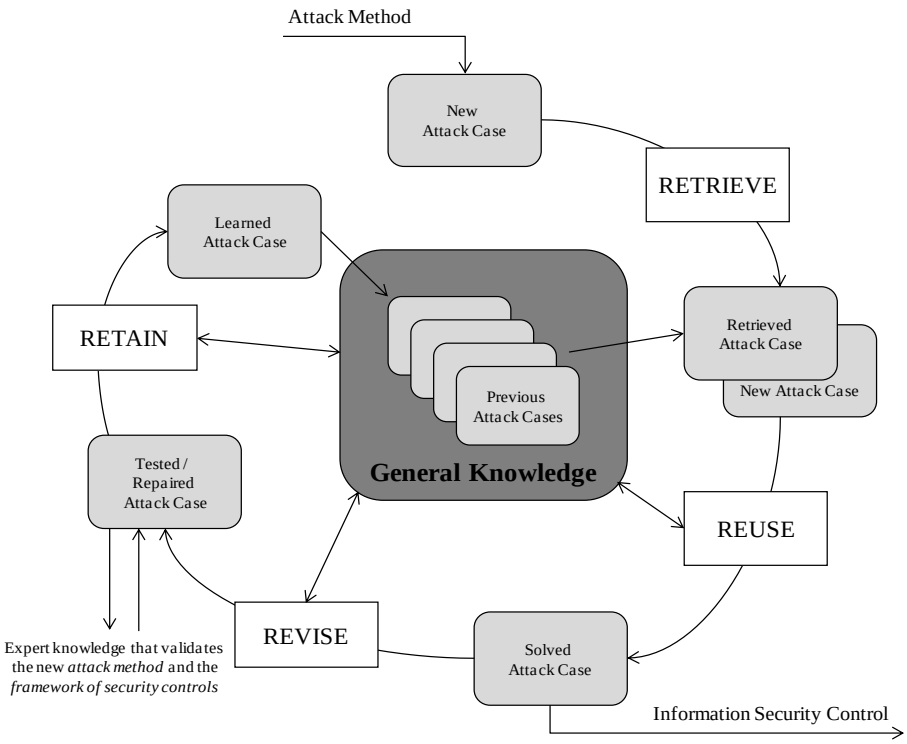

Fig. 2: CBR cycle applied to information security (Adapted from (Aamodt & Plaza, 1994))

The traditional steps for the CBR cycle are adapted to the present case: CBR retrieves cases with feasible attack methods in the case base; decision makers may directly reuse the solution, which consists of a set of controls for InfoSec, that is coded in these retrieved cases; decision makers may revise the solution according to the outcome of the case, upon application of the control set; upon validation by domain experts, CBR retains successful cases, together with solutions, in the case base, therefore retaining it for future reference.

The process described by the CBR cycle is similar to that of *lessons learned* and *modes of action* in military context, or others used within the human problem solving domain.

The Representation of a Case for Information Security

The case codifies existing operational knowledge about a given problem, which in the present paper is an attack method, through the association of information about the problem, i.e. the model of attack methods, and the solution, i.e. the framework of InfoSec controls. As stated in the previous section, the main goal for the present conceptual model for InfoSec is to select efficient combinations of InfoSec controls, to deal with enemy attacks.

The Content of Problem Representation

The problem representation for the case encodes the state of the problem (Kolodner, 1993). In the present paper the problem description consists of the identified model of attack methods (Martins, Santos, Nunes & Silva, 2012; Martins, Santos, Rosinha & Valente, 2013). The variables of this model identify possible attackers, threats and attack methods (i.e. the actions, tools/weapons) and targets that can be achieved to affect the fundamental properties of InfoSec (i.e. confidentiality, integrity and availability) directly or indirectly by exploiting the vulnerabilities of the major components in the IS. Goals and constraints are added to the problem description to provide useful information to help the decision maker characterizing the cases, although they are not directly used by the reasoner. The goals and features are restricted to countable finite sets that are codified into numeric values in order to enhance the performance of the retrieve step, which is based on search and match throughout the case base. All these sets were validated by a panel of information security experts (Martins, Santos, Nunes & Silva, 2012).

Problem Features

Attacker.
Individual, or group of individuals, internal or external to the organization, that with the execution of one or more methods of attack, seek to aim the fundamental properties of information security in to order to accomplish an operational objective (FM 100-06, 1996; Howard & Longstaff, 1998). The feature *attacker* may assume one the following values: (1) amateur; (2) professional; (3) organization; (4) state; (5) internal; (6) natural disasters.

Threat.
Potential cause of an incident of information security, which can result in damage to the system or organization (ISO/IEC 27001, 2013). The feature *threat* may assume one the following values: (1) interception; (2) interruption; (3) modification; (4) fabrication; (5) destruction; (6) disclosure.

Action.
Activity that causes an event in a system (i.e. application) and the possible change of its state (Howard & Longstaff, 1998). In terms of information security, actions may cause information security incidents. The feature *action* may assume one the following values: (1) physical; (2) electronic deception; (3) electronic attack; (4) human intelligence (HUMINT); (5) imagery intelligence (IMINT); (6) signals intelligence (SIGINT); (7) measurement and signature intelligence (MASINT); (8) open source intelligence (OSINT); (9) technical intelligence (TECHINT); (10) counter intelligence; (11) observe; (12) perception managing; (13) probe; (14) scan; (15) flood; (15) authenticate; (16) bypass; (17) spoof; (18) read; (19) copy; (20) steal; (21) modify; (22) delete.

Tools.
Means, weapons or resources that are used to exploit the vulnerabilities of critical assets of an organization, i.e. the targets (Howard & Longstaff, 1998). The feature *tools* may assume one the following values: (1) physical means; (2) means of psychological operations; (3) electromagnetic means; (4) means to capture sounds; (5) means of intelligence; (6) information exchange; (7) user command; (8) script or program; (9) autonomous agent; (10) toolkit; (11) distributed tool; (12) data tap.

Target.
Logical entities (i.e. account, information/data); physical entities (i.e. computer, network); human resources of the organization (i.e. decision-makers, experts); means of transmitting information (i.e. the wiring, electromagnetic radiation, sound waves); physical infrastructure (i.e. facilities, data centre, meeting rooms), or rather, all of the critical assets of an organization which achieve directly or indirectly, confidentiality, integrity and availability of information (Howard & Longstaff, 1998; ISO/IEC 27001, 2013). The feature *target* may assume one the following values: (1) facilities and equipment; (2) people; (3) physical documents; (4) electromagnetic spectrum; (5) sound waves; (6) communication devices; (7) storage devices; (8) account; (9) process; (10) information; (11) component; (12) computer; (13) network; (14) internetwork.

Vulnerabilities.
Characteristics of critical assets (targets) of an organization, which consist of weaknesses that can be exploited by an attacker to execute a method of attack (ISO/IEC 27001, 2013). The feature *vulnerabilities* may assume one the following values: (1) physical; (2) human; (3) processes; (4) design; (5) implementation; (6) configuration.

Properties of information.
Inherent quality of information, which indicates to what extent that property of security, exists in that information (ISO/IEC 27001, 2013). The feature *properties of information* may assume one the following values: (1) confidentiality; (2) integrity; (3) availability.

Operational effects.
Main purposes, or objectives, of military nature to achieve by an opponent, in order to contribute to information superiority, in an information warfare environment. The feature *Operational Effects* may assume one the following values: (1) information (2) collection; (3) protection; (4) intrusion; (5) destruction; (6) simulation; (7) financial.

The Content of Solutions

The solution for a given problem encompasses the set of objects that achieve the goals set forth in the problem description, taking into account the specified constraints and other specified contextual features (Kolodner, 1993). In the current setting, the solutions are framed by the framework of categories of information security controls. Security controls are resources used to mitigate, i.e. reduce or remove, vulnerabilities affecting critical assets. The definition of controls needs to consider two vectors (Martins, Santos, Dias & Borges, 2014): dimensions of information security (according to the attack vectors); desired effects from applying InfoSec controls when reacting to one or more methods of attack.

It is important to consider in the identification and selection of these security controls the following criteria: (i) control is necessary to ensure the protection of one or more dimensions of InfoSec against possible attack methods used by an opponent. This is because control of InfoSec can be implemented to protect information from one or more methods of attack and possibly with different goals; (ii) control is specific (single) and should be measured qualitatively or quantitatively; (iii) the implementation of a control is achievable within a time period acceptable to the organization, and realistic when compared to the criteria defined by the military organization.

Dimensions.
(1) organizational, (2) physical and environmental, (3) human, (4) technological.

Effects.

(1) prevent, (2) detect, (3) deter, (4) deflect, (5) recover, (6) react.

The Content of Case Outcome

The case outcome gives feedback about the result from applying a given solution. Typically, the fields of interest are: success (yes/no); evaluation, which is the case grading, defined in the interval [0, …, 1] regarding the merit of solution; justification; execution time.

Case Representation for an "Attack Method"

Table 2 represents the structure for the "attack method" case that will be used in the case-based reasoner.

Table 2: Case representation for an "Attack Method"

Attack Method Case	Problem: Goal: Constraints: Situation: Attacker: Threat: Action: Tools: Target: Vulnerabilities: Properties of information: Operational effects:
	Solution: Set of controls: Justification: Dimensions: Effects:
	Outcome: Success: Evaluation: Explanation: Execution time:

4. Conclusions

This paper describes the conceptual design of a case-based reasoner to support decision makers in providing a set of information security controls to deal with potential attacks to information systems in organizations.

A model for information security was presented, and as well its adaptation to CBR. In particular, this paper addresses the integration of CBR into the conceptual model for information security in military organizations, and the design of a case representation for an information security attack method.

Future work will necessarily address the implementation of the case-based reasoner to provide information security controls, and the tests within operational environment.

References

1. AAP-6 (2009). NATO Glossary of Terms and Definitions
2. Aamodt, A., & Plaza, E. (1994). "*Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches*", Artificial Intelligence Communications 7, no. 1 (1994): 39-52.

3. Alberts, D., Garstka, J., Hayes, R., & Signori, D. (2001). *Understanding Information Age Warfare*, CCRP Publication Series, Washington, United States of America.
4. Andress, J., & Winterfeld, S. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Syngress Media Inc.
5. Arquilla, J., & Ronfeldt, D. (1999). "*The Advent of Netwar: Analytic Background*", Studies in Conflict & Terrorism, 22(3), 193-206.
6. Bang, Y. H., Kim, J. G., & Hwang, J. G. (2008). "*CBR (Case-Based Reasoning) Evaluation Modeling for Security Risk Analysis in Information Security System*", International Conference on Security Technology.
7. Bichindaritza, I., & Marling, C. (2006). "*Case-based reasoning in the health sciences: What's next?*", Artificial Intelligence in Medicine 36(2).
8. Chesla, A. (2004). "*Information Security: A Defensive Battle*", Information Security Journal: A Global Perspective, 12(6), 24-32.
9. Couto, C. (1988). *Elementos de Estratégia*, Vol. I, Instituto de Altos Estudos Militares, Lisboa (in Portuguese).
10. David, L., & Plaza, E. (1997). "*Case-Based Reasoning Research and Development*", Proceedings of the Second International Conference on Case-Based Reasoning. Berlin: Springer Verlag.
11. FM 100-06 (1996). Information Operations, Washington, Headquarters, Department of the Army.
12. Harris, S. (2008). CISSP All-in-One Exam Guide, Fourth Edition, McGraw-Hill, New York, United States of America.
13. Howard, J. D., & Longstaff, T. A. (1998). "A Common Language for Computer Security Incidents", Sandia Report: SAND98-8667, Sandia National Laboratories.
14. Hutchinson, W. (2003). "*The Changing Nature of Information Security*", Paper read at 1st conference of the Information Security Management, Australian.
15. ISO/IEC 27001 (2013). Information technology – *Security techniques – Information Security Management Systems – Requirements*.
16. JP 3–13 (2006). *Joint Doctrine for Information Operation*, United States of America.
17. Kolodner, J. (1993). *Case-Based Reasoning*, San Mateo, Morgan Kaufmann.
18. Martins, J., Santos, H., Dias, M., & Borges, J. (2014). "*Planning Method of Information Security for Military Organizations*", Paper read at 13th European Conference on Cyber Warfare and Security ECCWS-2014, Piraeus, Greece.
19. Martins, J., Santos, H., Nunes, P., & Silva, R. (2012). "*Information Security Model to Military Organizations in Environment of Information Warfare*", Paper read at 11th European Conference on Information Warfare and Security, Laval, France.
20. Martins, J., Santos, H., Rosinha, A., & Valente, A. (2013). "*Information Security Military Standards versus ISO 27001 - A Case Study in a Portuguese Military Organization*", Paper read at 12th European Conference on Information Warfare and Security, Jyväskylä, Finland.
21. PDE 2.09.00. (2010). Estudo do Espaço de Batalha pelas Informação (IPB), Ministério da Defesa Nacional, Exército Português (in Portuguese).
22. PDE 0.32.00 (2012). *Lições Aprendidas*, Ministério da Defesa Nacional, Exército Português (in Portuguese).
23. Pfleeger, C., & Pfleeger, S. (2007). Security in Computing, Prentice Hall, 4th ed, USA.
24. Posthumus, S., & Von Solms, R. (2004). "*A Framework for the Governance of Information Security*", Computers & Security, 23(8), 638-646.
25. Siponen, Mikko, & Oinas-Kukkonen, Harri (2007). "*A Review of Information Security Issues and Respective Research Contributions*", ACM SIGMIS Database, 38(1), 60-80.
26. Surma, J (2010). "*Case Based Reasoning for Supporting Strategy Decision Making in Small and Medium Enterprises. Successful Case-based Reasoning Applications – I*", Studies in Computational Intelligence (305) 83-96.
27. Tikk, E. (2008). "*National Defense Policies for Cyber Space – Background and Effect of the Estonian Cyber Attacks (Cooperative Cyber Defence Centre of Excellence)*", presentation in Military Academy, Lisboa, Portugal.
28. Tikk, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm, A.-M., & Vihul, L (2008). Cyber Attacks Against Georgia: Legal Lessons Identified, NATO Unclassified Report v1.0. Tallin, Estonia: Cooperative Cyber Defense Centre of Excellence.
29. TRADOC-PAM 525-7-8 (2010). *Cyberspace Operations - Concept Capability Plan 2016-2028*, The United States Army's.