Extended Abstract

Cyberspace Information Security Incident Response Capability
A DOTMLPF-I approach

Paulo Jorge Baptista das Neves
Instituto Superior Técnico, Portugal

Abstract

Cyberspace has become thus valuable and critical. The Information is power, and who get the control of it will be able to control many other State and society critical assets. The importance to guarantee information availability, integrity and sometimes confidentiality, requires legal procedures and technical institutions under the States supervision, where the virtual space security and defense is organized.

Portugal is now starting to build the structures like the National Cyber Security Center or the military Cyber Defence Center that will allow to implement defence capabilities in its cyberspace.

Considering the present time and the opportunity concerning the construction of these Cyber Security and Cyber Defence structures, this paper aims to present a model for the implementation of an operational capability of information incident response and prevention of information security incidents, following the DOTMLPF-I[1] approach of the North Atlantic Treaty Organization (NATO) for the operational capabilities implementation.

Keywords: Cyberspace, Cyber Security, Cyber Defence, Incidents Management

1. Introduction

Cyberspace is a virtual space where more and more the mechanisms of fight for the supremacy of Information are processed. However, although its intangible nature, the actions that in it elapse also have translation in the physical space, being able to compromise infrastructures that supply and control critical services for society. Also in the cognitive plan the effects of what it happens in the Cyberspace affect and influence the people and society, namely through the control and manipulation of the "public opinion". We live in an information society with ubiquitous communications both on a personal level and at institutional level. States are increasingly dependent on electronic communication networks, where this feature is present in all sectors of society and the state itself. The Basic Services that support the Society, like Banking and Business among others, require constant information flow.

Cyberspace becomes so valuable and critical, leading naturally to its use for the exploration of illicit activities that threaten people, their individual property and to society as a whole. The Information is power. Who gets the control of it will be in conditions to control many other critical domains for the

[1] DOTMLPF-I – Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability

State and Society. The importance of ensuring the availability, integrity and sometimes the confidentiality of information, imposed on States the need to organize the defense of the virtual space through which all this information flows.

In order to develop the capabilities of Cybersecurity, the Portuguese government, following the recommendations of the European Union where each member state must implement a capability to respond to cybersecurity incidents, through the Decree-Law 69/2014 of May 9, decided to create the National Cybersecurity Center under the direct dependence on the National Security Authority.

In 2015 the Government of Portugal has defined the national security strategy for cyberspace, where are presented as strategic goals the promotion of "a conscious, free use, safe and efficient of the Cyberspace ", the protection “of fundamental rights, the freedom of expression, personal data and the citizens privacy", the strengthening of "cyberspace, critical infrastructures and national vital services security" and the assertion of "cyberspace as a domain of innovation and economic development ".[2]

Similarly, for Cyber Defence, following NATO recommendations adopted at the Summit of Wales in 2014, where was defined that each country through prevention, detection capacity, resilience and recovery, should develop a capacity of defence of their computer networks. The Portuguese Minister of national defence published the Decree No. 13692/2013 with the policy for the "political orientation for Cyber Defence", in which it is set the national defense structure of cyberspace, operationalized through a Cyber Defence Centre, depending on the Armed Forces General Staff Chief.

In the context of the above, to ensure cyber security capability, it is necessary to define a template for the construction of a computer security of information incident response capability in cyberspace. This research work proposes a model using the DOTMLPF-I approach, which is a methodology developed by the United States Department of Defence and adopted by NATO for the implementation of operational capacities.

To achieve this goal will be reviewed policies and procedures with regard to the most relevant existing rules on information security, with special attention to the necessary capability to respond to information security incidents. The DOTMLPF-I methodology will be applied to the construction of the aforementioned capability as well as how NATO has structured its operational capacity to respond to incidents, through the building of the NATO Computer Incident Response Capability (NCIRC). Another objective is to identify the main objectives for the various DOTMLPF-I areas, regarding the operation of a capability to respond to information security incidents in cyberspace, by collecting the opinion of reference professionals from the Cybersecurity area, using the written interviews methodology.

Finally will be proposed a model of information security incidents response, with the contributes by the technical teams of security of Information and Communication Technologies of the Navy, in order to create a sectoral CIRC clusters as part of the plan to build cyber defence capability in the armed forces, in accordance with the aforementioned Decree No. 13692/2013 of the national Minister of Defense. It is intended that the model presented can be easily applied to other State agencies or organizations, which have an identical dimension and structure of the Portuguese Navy.

[2] DR D. d., Estratégia Nacional de Segurança do Ciberespaço, DR, 1ª série, nº113, 12 de junho 2015, 2015

The future operationalization of this capacity in the Navy, according to the proposed model, will enable the validation and identification of susceptible of improvement points.

2. Standards and methodologies for incident response

In order to contribute to the information security, in particular efforts to ensure the quality of information through the premises of confidentiality, integrity, authenticity and availability in increasingly open and complex systems, there have been several normative recommending best practices. The existing rules are very broad and follow in detail all the processes in the various phases of architecture design of an Information System. Considering the scope of this work, the contribution of some of the most important standards and methodologies for of incident management will be examined in this section. We will begin by addressing the standards of the series 27000 ISO / TEC, specifically ISO 27002 and ISO 27035. It will also be analyzed framework Information Technology Infrastructure Library (ITIL), more oriented to the management of services, but also presents an approach for incident management. The United States and Europe have organizations that produce regulations relating to information security, thus the document SP 800-61 of the National Institute of Standards and Technology (NIST) in the US will be considered as a guide for the management of security incidents computers as well a guide to best practices for Incident Management from the European Union Agency for Network and Information Security (ENISA).

The analysis of the different standards showed an iterative nature of the frameworks that correspond to various phases of incidents treatment. In all the highlight of correct preparation for the Security Incident response is made. This preparation involves the creation and dissemination of security policies by creating predefined communication mechanisms for reporting events and / or incidents and safety record of the actions taken, and also referred to the necessary preparation and training of staff responsible for ensuring the management and treatment of incidents.

Upon detection of an event, either by personnel or automatically reported through the security platforms, there follows an analysis or screening phase, in which the events are sorted and some may even evolve into the condition of a security incident. In this situation it is important to analyze the impact that their occurrence will have on the organization's business and assign a corresponding treatment priority.

It follows the response phase or restraint, in order to eliminate the conditions that caused the event or incident. This phase aims a full replacement of services safely and should also proceed to the mitigation of vulnerabilities that somehow allowed their occurrence.

Technology also plays an important role in responding to security incidents. The use of correlation analysis platforms and events, together with data recording and storage systems, must be done in accordance with the legal requirements. Thus, the events recorded could be legally bind for future research and actions can be considered as valid evidence in any internal or judicial processes.

The iterative nature of the frameworks leads to the result of actions taken to be audited, through analysis of learned lessons. This eventually leads to a change in security policies or the review of

established procedures. All standards reveal the importance of communication with everyone involved, directly or indirectly, in the incident. This communication, whether internal, whether with external entities, it is essential to increase knowledge and awareness of the organization for security issues, helping to create relationships of trust between the parties.

The successful implementation of a capacity to respond to information security incidents is heavily dependent on the commitment with established security policies by the entire organization, especially of managers. The operation concepts of a capability to respond to information security incidents previously presented, together with the iterative process of the phases of incident handling, are fundamental to the model we want to display in this work. Stressing the structure presented by the ISO 27035 standard, with its five key stages ranging from the planning and preparation of actions, to organizational structure proposed based on the feedback information from learned lessons, proposed by ENISA for incident management.

3. The DOTMLPF-I methodology

The acronym DOTMLPF (Doctrine, Organization, Training, Material, Leadership, Personnel and Facilities) refers to the basic components of building an operational capability, developed by the US Defense Department (Department of Defense - DoD). It is an approach to the implementation of operational capabilities in order to identify gaps in their operation. In this basic model, the DoD would add another component, the Policies, aiming to add to this approach the search for common procedures among the various users in the use of new capacity. This new model is known for DOTMLPF-P. NATO adopted this basic model to implement new capabilities making only one change, replacing the concept of Policies for another to it very important, the Interoperability, emerging as the DOTMLPF-I acronym.

The text presents the military perspective on each of the different areas that shows this DOTMLPF-I methodology relevance to the build an operational capability, so is important to define the concept of capacity. According to the NATO definition, an operational capability is the possibility of a military commander be able to run a specific set of actions, identifying the effects needed to fulfill a certain goal. This definition follows that an operational capability is complex and is not just a question of material or procedures, basically, a holistic approach as the DOTMLPF-I is necessary for the success of their development and implementation.

The following is the analysis based on the different DOTMLPF-I dimensions concepts, related to the implementation of an operational capability of incidents response within the Cybersecurity perspective and its interpretation as applied by the NATO NCIRC concept, allowing to understand some of the key aspects to implementing a capability of this nature. Doctrine reliefs the importance of being defined legislative principles that will frame the action of response incident team, towards to its objectives and its scope of action. The Organization is very important particularly in coordination and communication capability inside the organization. In this point it is highlighted the levels of structure adopted by NCIRC, which allows the separation between the technical level, the coordination and the community of users of information systems. The Training stands out the importance to conduct international exercises that allow you to test and develop skills in the decision making, coordination, information sharing and technical skills. The Material in incident response capability is relevant in the

way that there must be the necessary means for the cyberspace monitoring with detection mechanisms and event logs analysis, which eventually level up to incidents, providing the means to monitor over there all its life cycle. Leadership highlights the importance of the higher levels of organization management being involved in the whole process of the capability building, supporting their development, motivated by operational needs, providing the necessary human and material resources. For this capability to be effective, the resources at staff level must assure the education and training that allow successfully achieve the goals listed in Doctrine and it is also very important be able to ensure the teams stability. Interoperability is assumed as vital in the building of an effective Incident Security Response Capability. The complexity of many cyber-attacks means that only a concerted action of various entities allow their mitigation. Sharing information and knowledge is crucial in building of a Cyberspace situational awareness. True interoperability is realized only if there are considered two key elements: the existence of strong relationships of trust between the various players that contribute to Cybersecurity and compatible communication mechanisms (secure communication platform, taxonomy, common, etc.).

3.1 Interviews with reference professionals in the Cybersecurity field

After reviewing the DOTMLPF-I dimensions based on the concepts related to the implementation of an operational capability of incident response and its interpretation based on their application under the NATO NCIRC, it is intended, as part of this research work, collect opinion from reference professionals from the cybersecurity information area for identifying the key elements involved in building an Information Security Incident Response capability that can be applied in Navy's Information Security Incidents Response Center or even other in other civil organizations, seeking to build this capability.

To collect these opinions we used the written interview method in a variant of a semi directive interview. The interview guide is oriented in order to obtain the opinion of respondents on the subject, following a DOTMLPF-I analytical perspective. Eight questions were prepared, one for each dimension, where it is intended to identify the factors that the respondent considers essential (critical) for the operation of an Information Security Incident. To analyze the information obtained from interviews, content analysis methodology was used.

The interviews results allow us to identify that one of the most critical factors is Doctrine. This should be used to define the strategic aim to be achieved and what are the standards, principles and procedures to adopt. It is also of high importance the unequivocal identification of the capacity target community and what services will be provided to this community. Finally, the definition of an internal and external communication policy and the definition of the security basic concepts for the organization.

The Organization has been also identified as one of the most critical dimensions for the successful implementation of this capability in particular factors such as technical skills, considering the specificity of the various areas and services to provide within the framework of Operation ability to respond to information security incidents. The organizational framework is also critical because the organization must ensure full independence of working teams for the vulnerability analysis, detection and response to incidents, from the technical department responsible for the administration and

management of the systems configuration, including security platforms. Depending on the size of the structure responsible for this capability, some specific support services may not be resident in their own capacity and may be provided by other institution departments. In this case, the legal aid have a big relevance not only to support the contested nature of employees' actions or from other organizations, whether collaborating in the development of standards and policies in terms of their legal validation. Another service that cannot be internal to this capability is the Public Relations team, which, by their specificity, can be shared, with advantage to the organization itself, so the interdepartmental coordination is of great importance.

The dimensions of Training and Personnel emerge as critical and closely related to each other. It is extraordinarily important to identify the people who have the right profile that is able to properly act under pressure, with good ability to work cooperatively and ease of communication. The organization must clearly identify the skills that are necessary, given the objectives to achieve, providing conditions for learning and consolidation of knowledge, using the training actions that may be internal or external nature. Even having the right people with the proper education, to have a real operational capability is necessary to ensure its continued training. The dynamic nature of threats and the multiplicity of factors that may affect information security, require trained teams, desirably in environments that follow as closely as possible the actual scenarios that could affect the organization. The existence of training exercises in a multi-organization environment, in addition to other exclusively internal, are very important to establish important relationships of trust and communication channels to test the horizontal level between CSIRTs'. At the Material dimension is important to ensure the proper tools having the concern to be more holistic in terms of systems architecture and services, and instead of focus in the tool itself. These tools should allow the capacity of monitoring network traffic and forensic analysis of artifacts complying with the legal requirements of evidence-gathering.

In an information security incidents response capability is natural that arise often situations of complex nature and great psychological pressure. In this context, also the Leadership was considered as a factor of critical nature. Leadership in this case can be considered at two different levels. On the one hand we have the Leadership level of the organization itself, which should be one of the main supporters of the action of incident response teams, thus giving greater internal relevance to the incident response capability, acting as a facilitator in the implementation policies and procedures, not always popular or well understood by the constituent community. From another perspective, it is necessary to consider the role of Leadership at the operational level, directly coordinating teams to ensure this capability. In this context, the leader must have a strong background in security and be recognized for its technical expertise. In addition to these technical qualities, it must also have a high capacity of decision, because, once again, the possibility of great critical situations to information security, where the response time and the timely decision can make all the difference in severity of compromise of the information systems. Finally, it is also important that the leader has the ability to realize the "state of mind" of its teams and have the ability to motivate, even in situations of great stress or less positive results.

In terms of Facilities, the most important will be to ensure that there exists the necessary security conditions (physical, electrical, environmental) to ensure the integrity and availability of information, namely the database incidents registration.

The last dimension analyzed was the Interoperability and also it presents as critical to the construction and operation of this capability. As stated in the context of Training, considering the dynamic and comprehensive nature of the threats, the effective response to incidents needs a lot of a concerted actions that often go beyond the boundaries of the organization. Considering the sensitive nature of the issues related to information security, security teams from different organizations tend to operate in closed mode, however, there is an increasing awareness that they can only be effective if working in a cooperative environment. Communication between security teams from different organizations, sharing knowledge and experience, allows us to establish trust relationships, contributing to an overall knowledge of what is happening in cyberspace, establishing a virtual monitoring network whose main product will be the production of early warnings that would allow preventative actions related to many global attacks. The standardization of processes and a common taxonomy is fundamental to have an effective communication. Currently the effort is made by all, through the establishment of organized meetings between security teams from various organizations, as exemplified by nationwide network of CSIRT.

4. Building model for an Information Security Incident Response Capability

Following the guideline of DOTMLPF-I methodology that underlies this work, we intend to address the various aspects that make up an Information Security Incident Response Capability, to propose a model that would be applicable to the Portuguese Navy but that would be likely to extrapolated to other similar organizational structures, in terms of size, whether in the organization structure of their information systems. This model will be based on the best practices and recommendations drawn from standards and methodologies previously presented and in the analysis to the NATO NCIRC adopted model and the conclusions drawn from interviews with experts. It is intended that the model would be more than a compilation of the results obtained, so the proposed model is also the result of reflection conducted by the author in this particular area of information security.

In terms of Doctrine the model identifies the goal to be achieved by building the capability to respond to information security incidents, as well which are the target community that will interact with this capability and the principles and procedures that will serve as based for their actions. As basic documents are considered the "National Strategy for Security in Cyberspace", the order of the Minister of Defence No. 13692/2013, in which publishes the "Guideline policy for cyber defense" and is still considered as doctrinal the military publications PEMGFA 301 and APC 16.

Regarding to the Organization, the model follows closely the structure adopted by NATO NCIRC, with 3 different levels of intervention. A first level responsible for the governance and coordination of Navy cyber defense, a second level essentially technical and operational which includes

incident response and a third level corresponding to the constituent community, including the local authorities responsible for the operation and security of information systems.

Training always comes up as one of the key areas when the objective is to establish and maintain an effective and efficient operational capability. In this dimension, the proposed model takes advantage of the training actions at national and international levels. In view of its military nature, the primary goal is to ensure the participation of Navy Information Security Incident Response Center, coordinated by Naval Command, in conjunction with the Cyber Defence Centre in NATO's annual exercise "Cyber Coalition" whose main goals are the training of ability to Decisions, Coordination, Information Sharing and Technical Skills training in. At the national level we highlight the cyber defense exercise of the Portuguese Army, “Cyber Perseu”, which, in editions of 2013 and 2014, was open to the other branches of the armed forces and the civil community and therefore is also an important training opportunity to consider for Navy Incident Response Center.

In the Material field there are some assumptions that are essential to mission success. The Navy Incident Response Center must have the monitoring capacity of all security platforms that protect the Navy information and communication systems, assuming a key role the existence of a Security Information and Events Management (SIEM) equipment to ensure the correlation of events received from various platforms. Equally critical is the existence of a platform that allows logging of security events. These events, eventually, could escalate to incident. The registration of all actions performed by the team during the following / treatment of the event / incident from its detection to resolution is required for future procedure analisys. Also important are the media which allow contact with the constituent community, between different levels of responsiveness to incidents and other external teams.

Leadership is presented from the perspective of technical / operational coordination of Navy Incident Response Center. The leader of this group should be someone with recognized technical skills, coordination of team work, with enough experience and that has a current knowledge of the problems related to information security. Based on its own experience, skills and training, he must have the power to decide on the incidents management, particularly its escalation to other entities, be the point of contact with external entities to the Navy, for exclusively technical matters and establishing itself as a reference for the other team members.

The Personnel dimension is presented as one of the most critical in the construction of an incident response capability. The focus is on the selection of reliable elements, a profile to work together in stressful situations, with the necessary skills and appropriate training, to carry out the various tasks associated with this capability. This work identified and characterized four different roles according to their functions, namely the Coordinator of the Unit, the Forensic Analyst, the Incident Manager and Incident Monitor.

Regarding the Facilities, is all about the necessary infrastructures to the building up of this capability, these can be summarized in providing a physical space that ensures the necessary physical and environmental security conditions in accordance with the level of the processed security classification as well as the space needed for the operation of the Navy Incident Response Centre in its various actions.

The Interoperability emerges as a critical dimension to this capability as such the model ensures the interoperability basis with Centers of other armed forces branches, with the Cyber Defense Center and through this or directly, with the elements of the CSIRT network and the Cybersecurity National Center, not forgetting the relationship with the incoming NATO directives coming from the NCIRC. In order to ensure these conditions, this model proposes the use of Request Tracker platform for Incident Response (RTIR), already adopted by the Cyber Defense Center and quite popular among the national CSIRT community, which already includes an entire management workflow the incidents. As a complement, the Navy Incident Response Centre will also adopt the taxonomy released by the National Cyber Security Center to facilitate interaction with other CSIRT as well its active participation in the organization and development of dissemination actions and multi-disciplinary working groups, on the various aspects related to Cybersecurity and Security Event Management, either under NATO or civil society.

5. Conclusion

This research work about Information Security and Law in Cyberspace is presented with the objective of defining a model for building an Information Security Incident Response Capability. Based on the concepts employed in NATO for the building of new operational capabilities, the study is centered around a number of different dimensions, which as a whole enables a holistic analysis of the problem, identifying the critical elements for the success of the mission and identifying potential vulnerabilities that may exist. These dimensions are the Doctrine of the Organization, Training, Material, Leadership, Personnel, Facilities and Interoperability.

Addressing the issue of cyber threats and how these could compromise the information security of the people, states and even infrastructures which support society critical services, there was the need to edify military and civilian structures in order to protect the quality of information, structures capable of respond to these incidents and recovery the systems.

The analysis of several existing standards and methodologies related to incident management, allowed us to identify commonalities in approach to this issue, demonstrating the need for existence of an iterative framework, with several well defined key stages for the construction of the model.

This work intends to present itself as innovative by addressing the Cybersecurity issues doing it in a DOTMLPF-I perspective. To better frame the issue in this perspective, it was held analyzed the NATO Computer Security Incident Response Capability, along several dimensions identifying their most critical components and anticipate some of the problems that may arise during its construction.

In order to enrich the information presented and with a main concern that the proposed model have a high adhesion to reality, there was realized a set of interviews with professionals if recognized capability in the cybersecurity area, that made a decisive contribution to the choices made in the preparation of the proposed model.

We conclude this research work with the effective presentation of a model that allows the building of a capability to respond to information security incidents. The DOTMLPF-I approach proved to be very effective in identifying the key elements for building an organizational structure of this nature, with a strong operational component. It also allowed to identify what elements can be presented as

critical in its construction and shows the greatest risks that present themselves to their completion, such as, for example, the need to have competent personnel (in number and properly trained) for the tasks required for the implementation of capacity.

Bibliography

ACQuipedia. (30 de junho de 2005). *DOTMLPF.P Analysis*. Obtido em 29 de outubro de 2014, de ACQuipedia: https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=d11b6afa-a16e-43cc-b3bb-ff8c9eb3e6f2

Arraj, V. (2010). *ITIL, The Basics.*

Bardin, L. (2003). *L' analyse de contenu.* Paris: Presses Universitaires de France.

DR, D. d. (2013). *Orientação Política para a Ciberdefesa, DR, 2.ª série — N.º 208 — 28 de outubro de 2013* . Lisboa: Assembleia da República.

DR, D. d. (2014). *Instalação do Centro Nacional Cibersegurança, DR, 1.ª série — N.º 89 — 9 de maio de 2014* . Lisboa: Assembleia da República.

DR, D. d. (2015). *Estratégia Nacional de Segurança do Ciberespaço, DR, 1ª série, nº113, 12 de junho 2015.* Lisboa: Assembleia da República.

ENISA. (2010). *Good Pratice Guide For Incident Management.* Obtido de enisa.europa.eu: https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management/at_download/fullReport

JANET. (s.d.). *RTIR incident handling work-flow.* Obtido em 17 de janeiro de 2015, de bestpractical.com: https://www.bestpractical.com/static/rtir/janet-workflow.pdf

Killcrece, G., & Ruefle, R. (2008). *Creating and Managing Computer Incident Response Capability (CSIRTs).* Pittsburg: Carnegie Mellon University.

Killcrece, G., Kossakowski, K., Ruefle, R., & Zajicek, M. (2003). *Organizational Models for Computer Security Incident Response Teams (CSIRTs).* Pittsburg: Carnegie Mellon.

NATO. (2002). *NATO COMPUTER INCIDENT RESPONSE CAPABILITY (AC/322-D/0056).* NC3B.

NATO. (2002). *NCIRC - CONCEPT OF OPERATIONS (AC/322-N/0797).* NC3B.

NATO. (13 de 10 de 2014). *Wales Summit Declaration.* Obtido de nato.int: http://www.nato.int/ cps/en/natohq/official_texts _112964.htm

Quivy, R., & Campenhoudt, L. (1998). *Manual de investigação em ciências sociais.* Lisboa: Gradiva.