REGIONAL DEPARTMENT
OF DEFENSE RESOURCES MANAGEMENT STUDIES

THE 6th EXPLORATORY WORKHOP

"INFORMATION RESOURCES MANAGEMENT - ISSUES, CHALLENGES AND FUTURE TRENDS"

ISSN: 2286 - 3060

ISSN-L: 2286 - 3060

COORDINATOR: Professor Habil Ph.D. eng. **CEZAR VASILESCU**

National Defense University "Carol I" Publishing House
Bucharest 2015

THE 6th EXPLORATORY WORKHOP
"INFORMATION RESOURCES MANAGEMENT - ISSUES, CHALLENGES AND FUTURE TRENDS"

WORKSHOP COMMITTEE:

Professor Habil eng. CEZAR VASILESCU, Ph.D.
Senior Lecturer Maria CONSTANTINESCU, PhD.
Senior Lecturer Aura CODREANU, PhD.
Lecturer Brînduşa POPA, PhD.

SESSION CHAIRMEN:

Professor Habil eng. CEZAR VASILESCU, Ph.D.
Senior Lecturer Maria CONSTANTINESCU, PhD.
Senior Lecturer Aura CODREANU, PhD.
Lecturer Brînduşa POPA, PhD.

THE 6th EXPLORATORY WORKHOP

"INFORMATION RESOURCES MANAGEMENT - ISSUES, CHALLENGES AND FUTURE TRENDS"

10 November 2015

Proceedings of the workshop unfolded during the

Information Resources Management Course

Conducted by the
Regional Department
of Defense Resources Management Studies

28 September – 20 November 2015

The content of the papers is in the entire responsibility of the author(s), and does not necessary reflecting the opinions of the Workshop Committee.

Braşov
ROMÂNIA

This page is intentionally left blank

C O N T E N T S

RESPONSIBILITY AND ACCOUNTABILITY IN A PERFORMANCE - BASED MANAGEMENT SYSTEM

Mikheil KAVTARADZE

INTRODUCTION

From times immemorial the human conducts labor activity. Even during the Stone Age the men and/or women already had been using the tools. Probably those primitive stone tools for hunting and gathering food were very effective and efficient at that time. Obviously early humans were using sophisticated thinking that's why every next "generation" of their tools and weapons was better than previous one. Using better tools and enhanced manners of working they had been obtaining more food. In other words the early humans somehow were focused on improving of performance. Human's trend of improvement is the active cause for further development of science, technology and social progress as well.

From the beginning to nowadays the humans permanently have been involved within collective works. Depending on historical period, social structure and level of progress the tribes, kingdoms or later on the states and organizations had various approaches and rules for conducting work. Though in any case from one side there are the leaders commanding or managing work and on the other hand the workers subordinated to them. Herewith there are defined some rights and obligations to arrange the relationship between leaders and workers.

Gradually with the social evolution and technological enhancement the organizations grew and reached high level of complexity. Especially at the end of 20th century while Information Technology advanced very fast the business processes became more complicated. Actually there was arisen situation in which everything was based on information, but Information Resources were not managed yet. Many large enterprises faced the problems with management and organizational performance. The existing approach of management was no more effective and efficient. Employees' roles and responsibilities were not clearly defined and present concept of accountability came to mean punishment. Thus high-performance organizations recognized the necessity of new approach to performance improvement. Accordingly they were interested in developing and deploying such kind effective systems that could help them to maintain high level of performance.

In order to arrange above mentioned problems USA signed the Government Performance and Results Act of 1993 (GPRA) and the Information Technology Management

Reform Act of 1996 (ITMRA) into law. As a matter of fact GPRA institutionalized the commitment to quality. Under GPRA federal agencies were required to develop strategic plans for how they would deliver high-quality products and services to the American people.

The strategic plans are the starting point for each federal agency to establish top-level agency goals and objectives, as well as annual program goals; define how it intends to achieve those goals; and demonstrate how it will measure agency and program performance in achieving those goals.

GPRA became the driving force for Performance Measurement and Performance-Based Management System as well as for assigning Responsibilities and Accountabilities within organizations.

I. THE CONCEPT OF PERFORMANCE MANAGEMENT

The United States of America has been the first country to recognize that Performance Management is a key element in the reform of the public and private sector as well. Today many countries are active in developing and using Performance Management. As a matter of fact these countries have many elements in common, but they also have a lot of differences at the same time. Consequently, each country must find its own approach, consistent with its needs and traditions. However, the countries initiating the development of a Performance Management system have a good opportunity to use the US experience and resources developed to assist in the effective and efficient implementation of GPRA. One of these resources is the publication of The Performance-Based Management Handbook produced by the Performance-Based Management Special Interest Group (PBM SIG). The handbook gives clear understanding about the Performance Management process.

This chapter contains the basic issues to understand what Performance Management means. However, it is worth noting that the concept of Performance Management and Performance Measurement are inextricably related and, hence, both are to be explained.

I.1. Performance Measurement

Performance Measurement and Performance Management are very closely linked to each other. Sometimes similarities and differences that exist between them cause some confusion. First of all, it must be underlined that Performance Measurement is a critical component of Performance Management. Actually, “as the common saying goes”, if you can’t measure performance you can’t manage it.

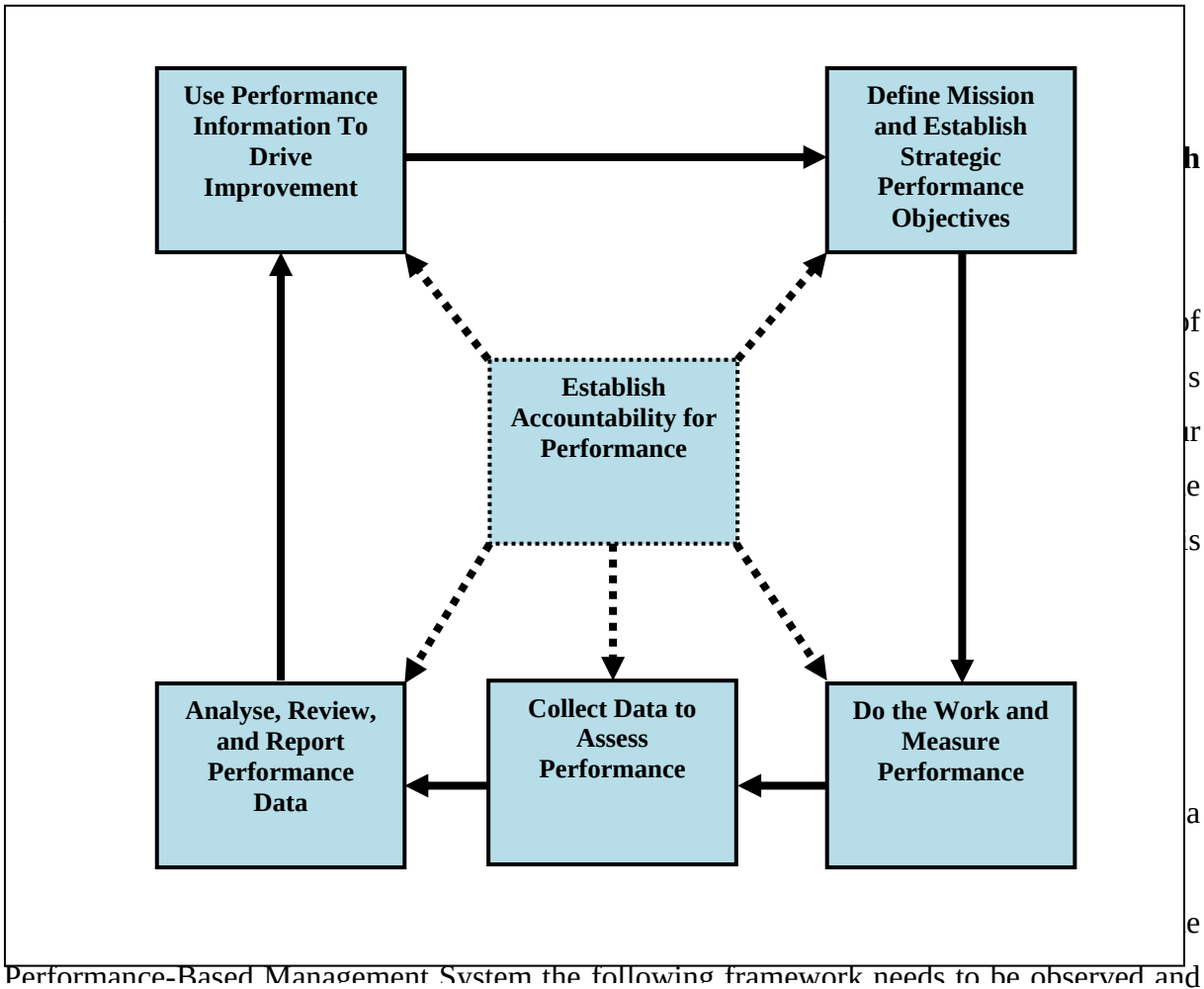
Performance Measurement is the comparison of actual levels of performance to pre-established target levels of performance. For effectiveness reasons, Performance Measurement must be linked to the organizational strategic plan. Performance-Based Management essentially uses performance measurement information to manage and improve performance and to demonstrate what has been accomplished.

I.2. Definition of Performance Management

There is no common definition for Performance Management. It refers to a process by which organizations align their resources, systems and employees to strategic objectives and

priorities. Performance Management focuses on the performance of an organization, employee and performance results (product or service). Herewith, the Performance Management System can be described as a set of interrelated activities and processes which ensure that goals are consistently being met in an effective and efficient manner.

According to The Performance-Based Management Handbook, "*Performance-Based Management is a systematic approach to performance improvement through an ongoing process of establishing strategic performance objectives; measuring performance; collecting, analyzing, reviewing, and reporting performance data; and using that data to drive performance improvement*."[1] This definition follows Performance-Based Management Framework (Figure 1).



Performance-Based Management System the following framework needs to be observed and

Figure 1. Performance-Based Management Framework
Performance-Based Management Special Interest Group (PBM SIG) – The Performance-Based Management Handbook

[1] Performance-Based Management Special Interest Group (PBM SIG) – The Performance-Based Management Handbook, Volume one , Establishing Performance-Based Management Program.

Step 1: Define organizational mission and strategic performance objectives;

Step 2: Establish an Integrated Performance Measurement System;

Step 3: Establish accountability for performance;

Step 4: Establish a process/system for collecting data to assess performance;

Step 5: Establish a process/system for analyzing, reviewing and reporting performance data;

Step 6: Establish a process/system for use performance information for drive improvement.

II. THE CONCEPT OF ACCOUNTABILITY

Performance Management and Accountability are closely linked. Performance is always related to accountability. Accountability is an often used word, but its concept is not easily understood. Unfortunately the commonly accepted and used definition of accountability doesn't exist. In this chapter we are going to discuss several views of accountability to find the answer to the following question: What is Accountability?

II.1. Responsibility and Accountability

Often, the word responsibility is used in conjunction with the word accountability. Some people equate them to each other and use them as a synonyms. Obviously, both of them are some kind of obligation but, they don't have the same meaning. Responsibility is the obligation to perform or act while Accountability is the obligation to answer for responsibilities. The Following view on Accountability expressed by the Auditor General of Alberta clearly shows the difference between these terms. *"Accountability is an obligation to answer for the execution of one's assigned Responsibilities. In simpler terms, Accountability is reporting."*[2]

II.2. Authority and Responsibility

Another key word used when discussing accountability is authority. We should make difference between it and responsibility to have clear understanding about concept of Accountability.

Authority is the right to act without prior approval from higher management. People in Authority have Responsibilities and they can delegate as well, although being responsible doesn't mean having authority. Authority is an assigned right, while Responsibility is delegated obligation.

II.3. Definition of Accountability

[2] Performance-Based Management Special Interest Group (PBM SIG) – The Performance-Based Management Handbook, Volume three , Establishing Accountability for Performance.

To achieve the good statement for definition we have to answer next question. What does it mean to be accountable to somebody and/or for something? From my point of view, if **A** is accountable to **B** for **A**'s performance, it means that **A** is obliged to inform **B** about **A**'s actions and decisions, to justify them, and to suffer punishment in the case of eventual misconduct.

The Performance-Based Management Handbook provides a common, understandable definition of subject. "*Accountability refers to the obligation a person, group, or organization assumes for the execution of authority and/or the fulfillment of responsibility. This obligation includes: Answering – providing an explanation or justification – for the execution of that authority and/or fulfillment of that responsibility, Reporting on the results of that execution and/or fulfillment, and Assuming liability for those results*."[3]

II.2. Key Aspects of Accountability

Accountability is multidimensional concept. Five key aspects shortly described below could be considered as dimensions of accountability.

Accountability Is a Relationship between a person in authority and a delegate in which both are accountable to each other. The person in authority is responsible for providing adequate direction, guidance, and resources as well as removing barriers to performance. The delegate is responsible for fulfilling its responsibilities.

Accountability Is Results-Oriented. It doesn't look at inputs and outputs, it looks at outcomes – performance results. In other words, it's more interested in quality than quantity.

Accountability Requires Reporting. Reporting means first providing an account of actions and results and second, providing tangible evidence of results. To be useful, the reporting must be timely, accurate, and complete.

Accountability Is Meaningless Without Consequences. It is an obligation to demonstrate and take responsibility for performance. Obligation indicates to consequences that could be positive (rewards) or negative (sanctions).

Accountability Improves Performance. The goal of accountability is to improve performance, not to place blame and deliver punishment. Accountability for performance have to be proactive, not reactive which led people to focus more on explaining their results rather than on achieving them.

II.3. Levels of Accountability

[3] Performance-Based Management Special Interest Group (PBM SIG) – The Performance-Based Management Handbook, Volume three , Establishing Accountability for Performance.

Theare are diverging theories on the levels of accountability. The question is if Accountability applies only to individuals, only to groups or both. The PBM SIG identifies

Figure 2. Five Levels of Accountability
Performance-Based Management Special Interest Group (PBM SIG) – The Performance-Based Management Handbook

five levels of accountability (shown in Figure 2): personal accountability, individual accountability, team accountability, organizational accountability, and stakeholder accountability. Personal Accountability is the foundation of all accountability. Starting with personal accountability, each level of accountability promotes the next, and no level of accountability can be established until the one below it hasbeen established. With regard to Stakeholder Accountability, which is shown with different color, the stakeholder is not responsible for ensuring that the levels of accountability below it are established and sustained. Rather the stakeholder is responsible for helping to determine organizational performance expectations and for holding the organization to account for its results.

Personal Accountability is an accountability relationship with oneself. In this relationship, the person looks to himself/herself for personal results and asks, „What can I do to improve the situation and make a difference?" In personal accountability, the individual looks within for answers instead of pointing fingers and placing blame on external factors. Some of the key aspects of personal accountability are honesty, integrity, ethicalness, morality, and reliability.

Individual Accountability refers to an accountability relationship within a work setting. It applies to both parties in the relationship – an authority (management) and a delegatee (the worker). The authority is responsible for providing adequate direction, guidance, and resources as well as removing barriers to performance. The delegatee is responsible for fulfilling its responsibilities. In this relationship, both are accountable to each other.

Team Accountability is a shared accountability wherein the group or team shares ownership for circumstances and performance results. Most organizational performance is accomplished by groups or teams. In the case of self-directed work teams, there is no „I", there is only „We". It is the group or team as a whole that provides the answering and reporting, not the individual. For example, a baseball or football team wins or loses a game, not the individuals on the team.

Organizational Accountability answers to what an organization actually accomplished inrelation to what it planned to accomplish. There are two types of organizational accountability:

• Internal Organizational Accountability referring to the establishment of the upward and downward flow of accountabilities between management and individuals and teams within the organization.

• External Organizational Accountability wherein the organization answers to its stakeholders on both its organizational performance and organizational behavior.

Stakeholder Accountability is located at the top of the accountability pyramid and shown in different color from the levels below it (Figure 2.). The reason of being that stakeholders (customers, shareholders, taxpayers, the general public, etc.) are not involved in the daily operations of the organization or the establishment of the internal organizational accountabilities. Rather, stakeholders provide input into the desired organizational outcomes, then leave it to the organization to achieve them, and then hold the organization to account for its results.

III. ESTABLISHING ACCOUNTABILITY FOR PERFORMANCE

Accountability doesn't happen by itself. It has to be established first through an accountability environment, then through an accountability framework.

III.1. Accountability Environment

The environment integrates accountability into the individual, team, and organizational performance systems. Accountability environment refers to the condition in which accountability canflourish. Specifically, an accountability environment is the condition in which individuals, teams, and organizations feel:

- Motivated to execute their authority and/or fulfill their responsibility;
- Stimulated to perform their work and achieve the desired results;
- Inspired to share (report) their results; and
- Willing to accept the liability for those results.

The optimal accountability environment is one of proactive accountability wherein the individual, team, and organization is focused on achieving great results rather than figuring out ways to explain away poor results.

For the most part, the accountability environment is established from the top down.

III.2. Requirements for an Accountability Environment

There are many requirements for the successful establishment of an accountability environment. These requirements are: Leadership, Transparency, Consequences, Reciprocation, Clarity, Consistency, Equity, Balance, Follow-Up, Trust and Ownership.

III.3. Barriers to the Accountability Environment

Barriers to the accountability environment are things that are counter-productive to establishing a healthy and effective accountability relationship. The most likely barriers that culd be faced to the organization include: Hidden Agendas, Favoritism, Lack of Leadership, Lack of Resources, Lack of Follow-Through, Lack of Clarity and Data Misuse.

III.4. Establishing a Framework for Accountability

When an individual or organization is assigned authority and/or delegated responsibility, they must provide a plan, execute the plan, and measure and report real results relative to that plan. The recipient of the report provides feedback, a new plan is developed, and the cycle begins again. This cycle provides the basic framework for accountability. As an example, the Accountability Framework described by Auditor General of Alberta (Figure 3.) is discussed below.

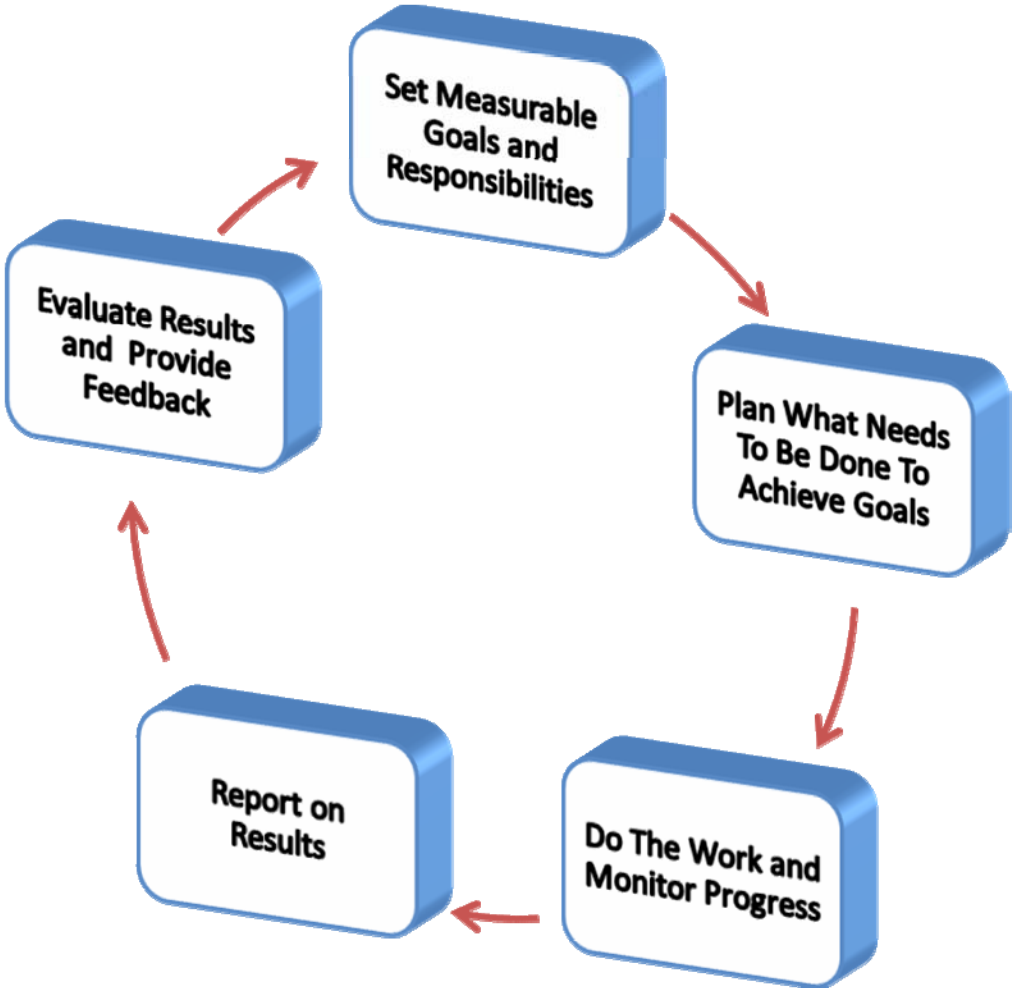


Figure 3. Auditor General of Alberta Framework for Accountability
Performance-Based Management Special Interest Group (PBM SIG) – The Performance-Based Management Handbook

The Framework cycle goes through the five steps and ensures the execution and fulfillment of the accountability obligations.

Step 1 – Set measurable goals, and responsibilities. Flowing from the strategic planning efforts, develop performance objectives, measures, and expectations. Identify roles and responsibilities in relation toachieving these expectations.

Step 2 – Plan what needs to be done to achieve goals. Identify what actions need to be taken by whom, at what time, and at what.

Step 3 – Do the work and monitor progress. Perform the work and measure its progress. Collect and analyze performance data.

Step 4 – Report on results. Prepare complete, understandable, and reliable reports on performance results and submit to pertinent entities in a timely manner.

Step 5 – Evaluate results and provide feedback. Evaluate results to determine what corrective actions need to be taken to improve performance or to determine what rewards should be given for efficient and effective performance.

III.5. Accountability Tools

Since accountability requires reporting, the focus of accountability tools is on reporting of performance – both intentions and results. Accountability tools include: Strategic Plans, Self-Assessments, Performance Agreements, Performance Reviews, Performance Plans, Management Controls, Accountability Reports, Equity Statements, Performance-Based Contracts, and Accountability Meetings.

CONCLUSION

Performance Management has become more than a necessity nowadays. Its major role is achieving organizational strategic objectives through performance planning. Performance-Based Management shares responsibility for performance improvement. Actually in the Performance-Based Management System, performance improvement becomes a joint responsibility between the organization and its stakeholders/customers or between the employee and their management.

Performance-Based Management System provides an excellent framework for accountability. This system ensures accountability for results. All actions, decisions, expenditures, and results can be easily explained, justified, and reported in the Performance-Based Management Framework.

Making this framework of Authority and Accountability active in the organization simply requires all employees to do their duty and to account to their superiors for what they have done. Giving and receiving an account of what has been done, and why, is the very important for organization because it enables people to take timely corrective action.

For making Accountability a key enabler of success leadership should recognize excellent work, apply administrative or disciplinary measures when required and deal promptly with issues in a fair and transparent manner.

Proper understanding of Accountability inside the organization is essential for effectiveness and eficiency of the organization."*When people are clear on who is responsible and accountable for what, they are better equipped to do their jobs ... Our approach must be know what works, change what doesn't. In short, it is our duty to learn and by learning to improve our ability to serve the country*."[4]

Establishing Performance-Based Management System should be the goal for organizations which are interested in performance improvment. Actually this model is „To be" condition for result-oriented performance. Although the organization first of all must evaluate existing approach of performance improvement („As is" condition). Afterwards should be developed and implemented the plan to achieve the goal. Consequently, established Performance-Based Management System continuously improves performance of your organization.

[4] Organization and Accountability – Guidance for Members of the Canadian Forces and Employees of the Department of National Defence, Second Edition, September 1999.

REFERENCES

1. Training Resources and Data Exchange Performance-Based Management Special Interest Group (PBM SIG) – The Performance-Based Management Handbook. A six-volume compilation of Techniques and Tools for Implementing the Government Performance and Results Act of 1993.

2. Organization and Accountability – Guidance for Members of the Canadian Forces and Employees of the Department of National Defence, Second Edition, September 1999.

3. Sigurður H. Helgason, Governance Iceland – Performance Based Accountability (http://siteresources.worldbank.org/PSGLP/Resources/PerformanceBasedAccountability.pdf)

4. http://alberta.ca/ags-policies-accountability.cfm

5. http://en.wikipedia.org/wiki/Performance_management

IMPLICATIONS OF OUTCOME ORIENTED PERFORMANCE MANAGEMENT IN DEFENSE ESTABLISHMENTS

Gigel ABAGIU

INTRODUCTION

Managing and measuring for outcomes presents many challenges for managers/leaders in defense establishments. What are the desired results of specific military action and/or service and what impact do these actions and services have on improving security conditions and overall military establishment activity? With the wide and frequently indistinct missions specific to military establishments, determining the desired outcomes can be easier said than done. The military leaders and managers are held accountable for a results-orientation that demonstrates how the outcomes of their specific decisions and activities contribute to the overall, higher-level group outcomes that public expect. Thus, implementing a results-oriented focus represents a desideratum and stands for an important shift in the way the military sector does business - an important shift in the nature of thinking, acting, and managing that moves away from a focus on process and regulations to a focus on outcomes and results. This shift is now taking place both within government and through independent organizations devoted to measuring specific community conditions.

The purpose of this paper is to analyze and identify the existing methods/procedures/guidelines of evaluating the performance based on outcomes at macro level, taking NATO as a case study because of its complexity and mixed structure of twenty eight members. In this respect, the aspect of individual performance was not covered for the reasons mentiond above. Given the complexity of the topic that requires through analysis and reflection, the current paper is to only provide a general overview. Also, contemporary theorists recognize that the connections between activities, events, motives, incentives, markets, and competencies are more complex than the normal sequential model used for current decision making (), and innovation occurs in networks of complementary as well as competitive agents, hence the emerging value-network.

Lastly, this paper is not intended to represent a rigorously base for further procedures or methods, but can represent a support for further discussions among specialists in the area of evaluation for military establishments.

CHAPTER I

BACKGROUND AND OVERVIEW

The purpose of this chapter is to set the present study in the context of major studies and theories of effective oriented performance measurement system(s). Looking into the origins of this system, it is well worth that experts and managers started to consider the necessity for performance measurement in 90s' but the subject was emphasized a decade later.

From a procedural perspective, to measure the performance outcome areas have to be defined and outcome measures have to be developed. The outcome measures have to be linked with planning and budgeting of the organization. After identification of the outcome areas, programs have to be assigned to these areas and create program outcome statement for each area. Then, is necessary to define outcomes that demonstrate success in each aspect of outcome statement in parallel with reflection of goals and programs in that area. If necessary these steps can be repeated to refine the process.

While government-sponsored performance measurement systems typically do not measure broader community outcomes, the main profiles of government organizations identified as serving the purpose of this paper that are applied at the US[1] level, and which do support outcome-oriented performance measurement systems, are:

- Washington State's Government Management Accountability and Performance (GMAP) Program ("a management approach at the leading edge of government-sponsored performance measurement").
- King County, Washington's "*AIMs High*" Program ("measuring performance is a hallmark of good governance")
- Oregon's Progress Board ("monitors state conditions through a set of economic, environmental, and community-related benchmarks")

[1] https://www.cob.org/documents/issues/kloby-report.pdf, accessed at 3 November 2015

Focusing on those government programs that are finding ways to make the connection between program specific performance measures and broader outcomes, the US experts were able to emphasize some of the strategies that managers are using to shift the emphasis to the big picture, or broader community issues and indicators.

When reflecting on what is required to change the resolution from program-specific performance measures, Michael Jacobson, Director of King County "AIMs High" performance measurement initiative notes "There needs to be two kinds of data that reflect what's going on in the world? We need to understand our relationship to the bigger picture. Some of the staff immediately understood the big picture relationship … others are more bureaucratically bound by what they are responsible for." The challenge highlighted is that one program or one department can influence an outcome but they cannot control it.

The following challenges of creating effective oriented performance measurement systems were identified by US experts[2]: Size of Staff Is Not Crucial to Success; Recruiting Enthusiastic Personnel Ready to Adapt and Learn is Essential; Political Support is Critical for Program Success; Culture Matters.

As recommendations the following were found out:

Recommendations for Designing an Outcome-Oriented System

- Capture intermediate program outcomes when designing outcome-oriented systems.
- In designing an outcome oriented system, demonstrate the link between program-specific indicators and community indicators.

Recommendations for Criteria for Selecting and Agreeing on Outcome Indicators

- Actionable indicators are more important than measures and plans.
- Select the most important indicators and avoid developing a cumbersome system.
- Seek community input to determine, revise, or draft new indicators.

Recommendations for Presenting and Reporting on Outcomes

- Adopt a plain language policy in reporting outcome.
- Present data around themes or desired outcomes.
- Highlight progress and let the data speak for itself.
- Use performance reporting as an opportunity to reflect and learn.
- Use the media to your advantage.
- Report on progress toward meeting community indicators periodically.
- Think about using the Information Technology (IT) capabilities.

Recommendations for Sustaining an Outcome Indicator System

- Build and sustain relationships with other service providers.

- Ensure that top leaders are meaningfully engaged.
- Institutionalize the process, build it in bureaucratically.
- Establish an expertise base and identity for performance measurement.

These challenges and recommendations identified by US experts can provide useful insights for military leaders and/or managers interested in broadening the focus of performance measurement efforts.

CHAPTER II

PERFORMANCE MEASUREMENT SYSTEM IN NATO

POLITICAL AND STRATEGIC LEVEL

This chapter will focus on existing models, at macro level, and will overview the efforts made by one of the most legitimate international actors in the field of security and military domain - North Atlantic Treaty Organisation (NATO)

At the fundamental level, NATO is a political body in the form of a treaty (treaties) between twenty-eight sovereign nations, each with a separate and distinct interest in how science and technology investments affect their national defense and industrial policies. Among each of those nations there are varied views about how economies should be organized and the role of science and technology investments in their respective economies. Within each of those nations there are institutions, military and civil, that have distinct although sometimes overlapping mission responsibilities, and there are complementary organizations such as industry, small-and-medium-sized enterprise, universities, laboratories, institutes, non-profits, non-governmental organizations, foundations, political parties, etc. that may hold a stake, or at least a point of view about science and technology investment portfolios. NATO is, of course, more than a treaty; it is an organization, a political body with practical tasks. As such there are internal structures intended to effect the collective will of the organization, including military and civil structures, governing bodies and an executive.

The evaluation systems hve to be in line with NATO's purpose, nature and fundamental security tasks (collective defense, crisis management and cooperative security) and linked with the central features of the security environment and provide guidelines for the adaptation of its military forces. All of these are defined in Alliance's Strategic Concepts, which are reviewed to take account of changes to the global security environment to ensure

[2] https://www.cob.org/documents/issues/kloby-report.pdf, accessed at 3 November 2015

the Alliance is properly prepared to execute its core tasks. Collective defense and part of the cooperative security are functioning on a reactive basis. All of these are depending of the amount allocated by the member states for defense and the better usage of this amount.

In an effort to reassure member states on the alliance's Eastern flank that felt threatened by Russia's aggressive action in Ukraine and feared that the collective defense commitment in Article 5 of the NATO treaty needed reconfirmation, NATO adopted a whole series of measures. In terms of their significance for NATO's development as a political and military alliance, two of these measures stand out. First, it is the adoption of the Readiness Action Plan (RAP) that encompasses a full array of military steps designed to enhance the deterrent value of NATO's military posture on its Eastern border. Second, it is a pledge by NATO's member states to aim at spending 2 percent of their respective gross domestic products (GDP) on defense within a decade.

While the Readiness Action Plan seeks to address the immediate security concerns stemming from an acute and evolving crisis in NATO's immediate vicinity, the two percent pledge is meant to address a more structural problem in the alliance: underfunding[3].

According to the overall trends to shift from an outcome oriented to an output oriented evaluation system, in 2011, the NATO Defence Policy and Planning Committee (DPPC) reached consensus on a list of new defense metrics (exemplified in *Annex 1 - Input / Output Metrics – Individual Nation's Fact Sheet – Denmark and Netherland*). These new metrics were approved by the North Atlantic Council in January 2012 to replace and expand on the input metrics and usability targets already in use by Allies. The final results were published in 2012, and have helped Allies to understand:

- How much they contribute to the Alliance;
- How this compares with the contributions of their peers; and
- Where the Alliance, as a whole, is particularly weak or strong.

NATO hopes that using these new defense metrics will provide Nations with a comprehensive picture of how and where resources are used and help foster political will for Nations so they may focus their efforts on NATO priorities and take on their fair share of responsibility.

Another current focus for NATO is the Connected Forces Initiative (CFI) which seeks to retain combat readiness and operational effectiveness through expanded training, exercise and better use of technology. An ambition of the CFI is that national capabilities and contributions are gradually linked into a federated coherent, accessible and operationally focused network. In order to achieve this, NATO must provide the structure and concepts to

achieve this goal. The Future Mission Network (FMN) is a current NATO concept to provide the structure for this ambition, while new concepts and experimentation in this federated environment will be required to develop this operationally focused information network and establish the synergies between NATO, the Nations and other stakeholders.

Through the NATO Defence Planning Process (NDPP), NATO identifies capabilities and promotes their development and acquisition by Allies, individually or together, so that it can meet its security and defense objectives.

The NATO Defence Planning Process (NDPP) main steps are:

1. Establish Political Guidance – a single unified one
2. Determine Requirements:
    - Identify Minimum Capability Requirements (MCR)
    - Conduct comparison between NATO/National capabilities and MCR
    - Capabilities to be maintained
    - Shortfalls
    - Surpluses
    - Prioritise Shortfalls
3. Apportion Requirements. Set Targets:
    - Distribute MCR throughout the Alliance → Targets to:
        - Single Nations
        - Groups of Nations
        - NATO (common funded)
4. Facilitate Implementation:
    - Assist and facilitate implementation of Targets
    - Focus on most critical capability shortfalls
5. Review Results
    - Assess Alliance Defence & Financial plans (national & collective efforts)
    - Conduct Suitability & Risk Assessment

All the concepts and processes mentioned above are part of the complicated and complex system of the Alliance with different evaluation performance systems divided horizontally (operational, exercises, capability development and so on) and vertically (different levels - political, strategic and operational and tactical). However a unique measurement system to incorporate all of these has not been defined and taking in consideration the complexity will be difficult to established one in near future.

[3] http://carnegieeurope.eu/2015/08/31/politics-of-2-percent-nato-and-security-vacuum-in-europe/ifig, accessed at

CHAPTER III

PERFORMANCE MEASUREMENT SYSTEM IN NATO

OPERATIONAL AND TACTICAL LEVEL

At the operational and tactical level, the official definition of analysis in NATO is: "The study of a whole by examining its parts and their interactions."[4] This is linked generally with a process used to thoroughly understand areas of activity identified to have potential for improvement. The results of analysis are used to support decisions that will result in enduring improvements, thus leading to a Lesson Learned (LL).

As well as its use in support of LL processes, analysis provides decision support to NATO in other areas. These include:

- Day to day operations to help the Commander and staff gain the best possible operational outcome. (Allied Command Operations Operational Analysis Cells);
- Capability Development to help select the future direction of NATO capability (Allied Command Transformation (ACT) Capability Development Cell and Defence Planners);
- Concept Development to help develop new ways of working and technology to support the future of NATO (ACT Future Capabilities Analysis Team);
- Training to help identify and fill training requirements in the best possible way. [Joint Warfare Centre (JWC) and Joint Forces Training Centre (JFTC)] .

From a procedural point of view the process of evaluating is linked mainly with the physical environment and allocation of resources mainly, but other specific environments or conditions such as morale, welfare and so on. While this study will not stress the LL procedures which are well defined and known, it will try to focus on the interaction between existing conditions and evolutions (*physical environment*) as well as allocation of resources.

---

8 November 2011

[4] http://www.jallc.nato.int/activities/jointanalysis.asp, accessed at 4 November 2015

The *physical environment* has always been important, and remains important for example, to select the timing or location of an operation, to reduce one's vulnerability or take advantage of an adversary's vulnerability, and to operate systems/weapons most effectively and efficiently.

Consequently, allies established Operation Planning Aids and Decision Support tools which require a fast and concise representation of both the *physical environment and allocation of resources*, in order to evaluate potential courses of action that are contingent upon these environmental conditions and uncertainty, an assessment of when and where additional data collection would provide more informed decision making, or conversely, when existing data is likely sufficient.

While substantive progress has been made on the various components required for a capability and cost-effectiveness, considerable work remains to integrate these components. Further, challenges remain in the quantification and propagation of uncertainty from field measurements through forecast models into application specific areas, and the portrayal of uncertainty as a risk (or opportunity) that can be managed, evaluated numerically to consider courses of action, and lead to optimal decisions.

Lastly in this regard, mechanisms are required for feedback between the decision maker and the design and operation of the complex heterogeneous data collection networks (and more generally to centralized data collection networks), including aids to decide when, where, and what *in situ* data (or additional data) is required and the fidelity required to achieve a reasonable / useable representation of the *physical environment.*

Nowadays, resources are generally limited, there is much to be gained by a superior ability to task limited assets while optimizing on the requirement of the operational decision maker and supporting military response and action. In this sense, the primary challenge to be addressed for different environments is this full-spectrum approach to improve decision and action, with an emphasis on feedback to inform further information requirements, which allow the both decision shapers and makers to identify and use resources better. Outstanding challenges remain in NATO's ability to effectively make use of all available resources, including information, to support operational decisions.

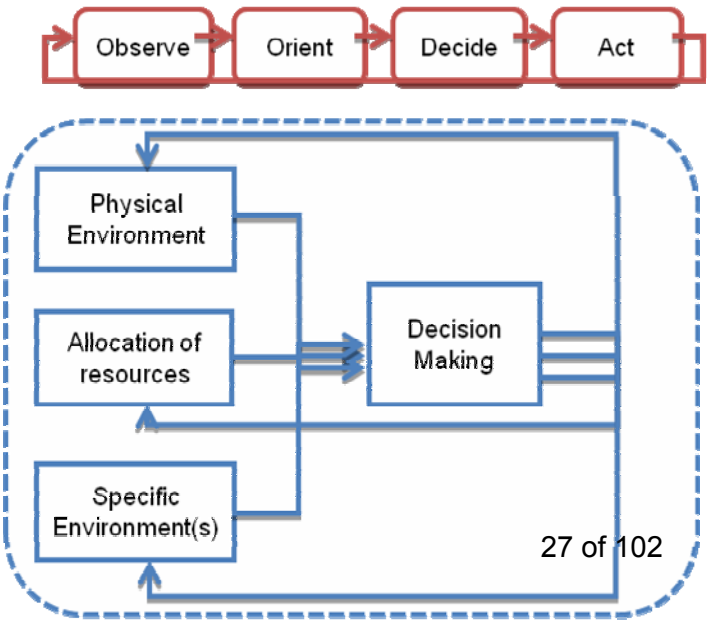


Fig. 1: This figure will emphasize decision making in military domain that is informed by knowledge of the physical environment (political, military) and allocation of resources and/or, at smaller scale, other specific environment which incorporates feedback between decision making and observational data requirements (analogous to the observe-orient-decide-act (OODA) loop

CONCLUSIONS

Measuring performance can be a discouraging task. The measurement challenge is complex through numerous and challenging burdens, programs and structures that appear to flout measurement, inadequate resources, political level of ambition, and networked vector systems. Add to that mix the expectation for more and better performance information related to broader community conditions and even the most seasoned public managers can feel overwhelmed. As discouraging as it may seem, implementing a fitted outcome oriented performance measurement system is a desideratum.

Inside the defense establishments the activities have been focused on alignment to political needs, security requirements, opportunities, priority shortfalls, and long-term capabilities as expressed through planning processes, both operational planning and defense planning. The differences between these two methods are influencing the evaluation methods and systems, taking in consideration that the operational planning is a reactive one and the defense planning are a proactive due to the development of capabilities on long term. Subsequently, performance measurement endeavours are stronger when they show the relationship between program-specific indicators and broader community outcomes.

In military establishment identifying broad outcome areas, assignment of programs and creation of the program outcome statement for each area are integrated in planning tools. The difficult part is to demonstrate success in each aspect of outcome statement for the reason that planning a tool to measure the performance during the execution is not realistic taking in consideration the long term planning and the uncertainty in situation evolution.

To sum up, for an efficient performance measurement it is worth identifying the right equation of evolution of conditions and parameters of the security environment and connections with strategic goals. Inside this equation, high risk and uncertainty specific to the military area, using more knowledge rather than more data, fairly allocating scarce resources and making good decisions have to be taken in consideration. A specific accent has to be put

on innovation which can be taken as an outcome that signals a new way of doing business in the military domain, and not only.

Finally, performance measurement can be used as a significant management instrument to stimulate committed civil/public servants, to get better decision making outcomes, build up programs and services, and enhance accountability to improve performance and achieve the desired (security) environmental conditions.

REFERENCES

1. Hatry, H. (1999). *Performance measurement: Getting results.* Washington, D.C.: Urban Institute Press.
2. McDavid, J.C., & Hawthorn, L.R.L. (2006). Performance measurement as an approach to evaluation. In *Program evaluation & performance measurement: An introduction to practice* . Thousand Oaks, CA: Sage.
3. www.nato.int
4. https://www.cob.org/documents/issues/kloby-report.pdf
5. http://www.jallc.nato.int/activities/jointanalysis.asp
6. http://carnegieeurope.eu/2015/08/31/politics-of-2-percent-nato-and-security-vacuum-in-europe/ifig
7. https://zoek.officielebekendmakingen.nl/blg-351973
8. http://www.ft.dk/samling/20121/almdel/fou/bilag/102/1218048.pdf

Annex 1

Input / Output Metrics – Individual Nation's Fact Sheet
Year: 2011

Denmark	Selected Indicator	Abs. value	Contribution (%)	NATO Guideline (%)	Rank
1. Percentage of Gross Domestic Product (GDP) on Defence	Defence Expenditures (current prices, mil. of national currency):	24,259	1.36	2	Middle
2. Percentage of Defence Expenditure on Major Equipment and Associated Research and Development	Major Equipment Expenditures (current prices, mil. of national currency):	2,348	9.68	20	Low
3A. Percentage of Implementation of Quantitative National Targets (Year: 2016)[1, 2, 3, 4, 5, 6]		-	60.18	100	Low
3B. Percentage of Implementation of Qualitative National Targets (Year: 2016)[7, 8, 9, 10]		-	47.90	100	Low
4A. Deployable Land Forces Personnel as a Percentage of Land Forces Personnel	Deployable Land Forces Personnel (unit):	5,546	57.77	50	Top
4B. Deployable Airframes as a Percentage of Airframes	Deployable Airframes (unit):	45	67.16	40	Top
4C. Deployable Vessels as a Percentage of Vessels	Deployable Vessels (unit):	8	72.73	80	Middle
5A. Sustainable Land Forces Personnel as a Percentage of Land Forces Personnel	Sustainable Land Forces Personnel (unit):	1,339	13.95	10	Top
5B. Sustainable Airframes as a Percentage of Airframes	Sustainable Airframes (unit):	7	10.45	8	Top
5C. Sustainable Vessels as a Percentage of Vessels	Sustainable Vessels (unit):	1	9.09	28	Middle
6A. Land Forces Personnel Deployed Abroad on NATO Operations as a Percentage of Deployable Land Forces Personnel	Land Forces Personnel Deployed Abroad on NATO Operations (unit):	1,387	25.01		Top
6B. Land Forces Personnel Deployed Abroad on non-NATO Operations as a Percentage of Deployable Land Forces Personnel	Land Forces Personnel Deployed Abroad on non-NATO Operations (unit):	182	3.27		Top
6C. Land Forces Personnel Deployed Abroad on NATO and non-NATO Operations as a Percentage of Deployable Land Forces Personnel	Land Forces Personnel Deployed Abroad on NATO and non-NATO Operations (unit):	1,569	28.28		Top
7A. Airframes Deployed Abroad on NATO Operations as a Percentage of Deployable Airframes	Airframes Deployed Abroad on NATO Operations (unit):	4	8.23		Top
7B. Airframes Deployed Abroad on non-NATO Operations as a Percentage of Deployable Airframes	Airframes Deployed Abroad on non-NATO Operations (unit):	0	0.28		Middle
7C. Airframes Deployed Abroad on NATO and non-NATO Operations as a Percentage of Deployable Airframes	Airframes Deployed Abroad on NATO and non-NATO Operations (unit):	4	8.51		Middle
8A. Vessels Deployed Abroad on NATO Operations as a Percentage of Deployable Vessels	Vessels Deployed Abroad on NATO Operations (unit):	1	9.38		Top
8B. Vessels Deployed Abroad on non-NATO Operations as a Percentage of Deployable Vessels	Vessels Deployed Abroad on non-NATO Operations (unit):	0	0.53		Middle
8C. Vessels Deployed Abroad on NATO and non-NATO Operations as a Percentage of Deployable Vessels	Vessels Deployed Abroad on NATO and non-NATO Operations (unit):	1	9.90		Top
9. Percentage of Immediate Response Force (IRF) Fulfilment		-	148.35	100	Top

[1] Base year: 2016.
[2] Reference: DPCS 2011 as of June 2011.
[3] Contributions two years later than requested: adjusted at 80%.
[4] Weighting system was used to address the relative magnitude of each force contribution.
[5] Only very limited assessment of quality of forces included.
[6] Does not assess readiness discrepancies unless significant.
[7] Measures degree of implementation of force goals (which seek to address qualitative shortfalls of forces) within the required timeframes.
[8] Can only be considered as a very rough measurement of the progress in transforming forces.
[9] Measurement is imprecise, especially for force goals with multiple requirements or for force goals with a very long implementation time.
[10] Weighting factor for each force goal takes into consideration effort and resources over the period of time required to implement it. However, it does not take into consideration that the level of effort to implement a force goal is different from nation to nation.

NETHERLANDS INPUT-OUTPUT METRICS YEAR 2013

Netherlands	Selected Indicator	Abs. Value	Contribution (%)	NATO Guideline (%)	Rank
1. Percentage of Gross Domestic Product (GDP) on Defence	Defence Expenditures (current prices, mil. of national currency):	7,777	1,29	2	Middle
2. Percentage of Defence Expenditure on Major Equipment and Associated Research and Development	Major Equipment Expenditures (current prices, mil. of national currency):	1,021	13,13	20	Middle
3A. Percentage of Implementation of Quantitative National Targets (Year: 2016)		-	97,81	100	Middle
3B. Percentage of Implementation of Qualitative National Targets (Year: 2016)		-	97,05	100	Top
4A. Deployable Land Forces Personnel as a Percentage of Land Forces Personnel	Deployable Land Forces Personnel (unit):	17680	65	50	Top
4B. Deployable Airframes as a Percentage of Airframes	Deployable Airframes (unit):	113	100	40	Top
4C. Deployable Vessels as a Percentage of Vessels	Deployable Vessels (unit):	24	100	80	Top
5A. Sustainable Land Forces Personnel as a Percentage of Land Forces Personnel	Sustainable Land Forces Personnel (unit):	2755	10,13	10	Middle
5B. Sustainable Airframes as a Percentage of Airframes	Sustainable Airframes (unit):	8	7,08	8	Middle
5C.Sustainable Vessels as a Percentage of Vessels	Sustainable Vessels (unit):	6	25	28	Top
6A. Land Forces Personnel Deployed Abroad on NATO Operations as a Percentage of Deployable Land Forces Personnel	Land Forces Personnel Deployed Abroad on NATO Operations (unit):	543	3,07	-	Low
6B. Land Forces Personnel Deployed abroad on non-NATO Operations as a percentage of Deployable Land Forces Personnel	Land Forces Personnel Deployed Abroad on non-NATO Operations (unit):	121	0,68	-	Middle
6C. Land Forces Personnel Deployed Abroad on NATO and non-NATO operations as a Percentage of Deployable Land Forces Personnel	Land Forces Personnel Deployed Abroad on NATO and non-NATO Operations (unit):	664	3,75	-	Low
7A. Airframes Deployed Abroad on NATO Operations as a Percentage of Deployable Airframes	Airframes Deployed Abroad on NATO Operations (unit):	4	3,54	-	Middle
7B. Airframes Deployed Abroad on non-NATO Operations as a Percentage of Deployable Airframes	Airframes Deployed Abroad on non-NATO Operations (unit):	0	0,00	-	-
7C. Airframes Deployed Abroad on NATO and non-NATO Operations as a Percentage of Deployable Airframes	Airframes Deployed Abroad on NATO and non-NATO Operations (unit):	4	3,54	-	Middle
8A. Vessels Deployed Abroad on NATO Operations as a Percentage of Deployable Vessels	Vessels Deployed Abroad on NATO Operations (unit):	0.5	2,06	-	Middle
8B. Vessels Deployed Abroad on non-NATO Operations as a Percentage of Deployable Vessels	Vessels Deployed Abroad on non-NATO Operations (unit):	0.5	2,06	-	Middle
8C. Vessels Deployed Abroad on NATO and non-NATO Operations as a Percentage of Deployable Vessels	Vessels Deployed Abroad on NATO and non-NATO Operations (unit):	1	4,13	-	Middle
9. Percentage of fulfilment of NATO Command Structure (NCS) positions		-	90	100	Middle
10. Percentage of Fulfilment of NATO Force Structure Headquarters		-	100	100	Top
11. Percentage of Immediate Response Force (IRF) Fulfilment		-	65,49	100	Middle
	= Investment				
	= Capabilities				
	= Actual Contribution				

AN OVERVIEW OF CRITICAL INFRASTRUCTURE PROTECTION IN GEORGIA

Giorgi MURADASHVILI

This paper aims to offer an overview of critical infrastructure protection in Georgia. Also consider international opinion and trends of critical infrastructure. With the development of technology the approach and vision to state security has changed. Critical infrastructure became one of the most important directions of the state's national security, In the past the focus of the critical infrastructure sector were physical facilities like local automated systems, which had not connection with the outside world, and the driving force was the human resource and, At present information and communication technologies (ICT) have the main role in the functioning of the critical infrastructure sectors. Critical sectors dependence on information technologies is growing with it increasing threats, therefore, the government should develop a plan for the protection of critical infrastructure and ensure its implementation.

I. OVERVIEW OF CRITICAL INFRASTRUCTURE

Critical infrastructure plays a vital role in Nation’s security. national economic security, national public health or normal functioning of society. There is no set standard list for the critical infrastructure sector. Each country determines what is part of its critical infrastructure. Determination of the critical infrastructure sectors depends on the country's assets, its internal resources, its international obligations (E.g. a member of NATO or the European Union), geographic location, and other factors. Country’s critical infrastructure are “Facilities and services whose assets, systems, and communication, whether physical or virtual, are considered so vital to the state that their failure may harm the country's security, national economic security, national public health or safety, or any combination thereof”[1] This definition is almost same for all states, and clearly illustrates the importance of critical infrastructure. It is important to clearly define critical infrastructure sectors, systems and network also identify interdependencies within a critical sector, between critical sectors and among data network asset. State should at first identify the critical sectors and then for each one of the critical sectors proceed with the identification of critical services, critical applications and finally critical information infrastructure assets.

[1] http://www.dhs.gov/what-critical-infrastructure

State should actually have the critical infrastructure protection ability and plan of action in crisis situations. An important part of the latter consists of an assessment of the risks. Critical infrastructure risks can be assessed in terms of the following:[2]

- Threats - such as natural disasters; physical violence; cyber attacks; terrorist acts
- Vulnerability - physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
- Consequence – effect of an event, incident, or occurrence

The state should identified risks, weaknesses and try to reduce them. When talking about risk assessment it is necessary to take into account the taxonomy of the critical infrastructure concept (e.g. physical; cyber; geographic critical and logical interdependencies).

Today, the emphasis is focused on cyber threats and information systems security, therefore it is important to develop a cyber security strategy, review the security policies and update them if necessary. Government should share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and promote learning and adaptation during and after exercises and incidents.

II. EVOLUTION OF THE TERM "CRITICAL INFRASTRUCTURE" US APPROACH

The term critical infrastructure dates back to 1980 in USA when the term and then concept of "infrastructure" were first formed and used. In this respect, the concept of infrastructure included the protection of the physical infrastructure with no standard or agreed definition[3]

The first Presidential Decision Directive of critical infrastructure was published in 1998 by President Clinton. The Presidential Decision Directive defined "critical infrastructure" as "*those systems and assets - both physical and cyber so vital to the nation that their incapacity or destruction would have a debilitating impact on national security*"[4]. Following the events of 9/11, the Bush administration released Executive Orders signed October 8, 2001 established the Office of Homeland Security. Among its duties, the office was to coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks.[5] On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7 clarifying executive agency responsibilities for identifying, prioritizing and protecting critical infrastructure. The Directive requires that Department of Homeland Security and other federal agencies collaborate with private sector entities in

[2] NIPP 2013 Partnering for Critical Infrastructure Security and Resilience
[3] https://www.fas.org/sgp/crs/RL32631.pdf Critical Infrastructure and Key Assets: Definition and Identification
[4] https://www.fas.org/sgp/crs/RL32631.pdf Critical Infrastructure and Key Assets: Definition and Identification
[5] https://www.fas.org/sgp/crs/RL32631.pdf Critical Infrastructure and Key Assets: Definition and Identification

sharing information and protecting critical infrastructure.[6] On February 12, 2013 President Barack Obama issued Presidential Policy Directive (PPD)-21, *"Critical Infrastructure Security and Resilience"*, which explicitly calls for the development of an updated national plan. It also identifies 16 critical infrastructure sectors.[7] At same time president issued executive order *improving critical infrastructure cyber security*, which calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cyber security information sharing and collaboratively develop and implement risk-based approaches to cyber security. As used in this order term, critical infrastructure means *"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters".*[8]

III. AN OVERVIEW OF CRITICAL INFRASTRUCTURE PROTECTION IN GEORGIA

Critical infrastructure in Georgia has become urgent since 2008.During the August war, the Russian Federation carried out concentrated and massive cyber-attacks, as well as land, air and naval borne attacks in parallel against Georgia. The attacks were mostly designed to block news sources. The information security systems were not ready for such an attack. This fact made it clear to the government that it was necessary to take action to establish the legal framework for the security of information systems and networks.[9] In 2009 the Data Exchange Agency (DEA) dea.gov.ge was established under the ministry of Justice. Its aim is to:

- Develop E-governance
- Establish a data exchange infrastructure
- Establish unified Government Network and ensure security
- Establish an information security policy and its implementation

DEA was the first organization which started to formulate the information security strategy for both the public and private sectors in Georgia. In 2011 under the Data Exchange Agency

[6] http://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031217-5.html
[7] https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
[8] https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[9] https://matsne.gov.ge/ka/document/view/89662

of the Ministry of Justice of Georgia a computer emergency response team cert.gov.ge[10] was formed which is responsible of handling critical incidents that occur within Georgian governmental networks and critical infrastructure.

The Law on "Information Security" was published in 2012.[11] The law promotes the effective implementation of information security, imposes duties and responsibilities of the public and private sectors in the field of information security, and defines information security policy and the state controls mechanism. In this law the term "critical infrastructure" was first used for the first time and its definition is as follows:

"Public and private entities whose information systems uninterrupted operation is so vital to the state that their incapacitation or destruction would have a debilitating effect on national security, national economic security, national public health or normal functioning of society"[12]

The law applies to both private and public areas that are the object of critical infrastructure protection. The list of critical infrastructure specific facilities was established by the Presidential Decree[13] in 2013 includes:

- Government Facilities Sector
- Transportation Systems Sector
- Healthcare and Public Health Sector
- Emergency Services Sector
- Financial Services Sector (Partially)

Critical infrastructure facilities must adopt internal rules which serve to enforce the provisions of this law and determine the organization's information security policy. The information security policy should meet the minimum requirements for the information security of the International Organization for Standardization (ISO) and the Information Systems audit and Control Association (ISACA) standards. Any critical infrastructure facility is required to establish a specific position called "information security officer" The law requires properties of information systems auditing and testing (penetration testing - Penetration testing the system stability and security check) audit and testing standards of the DEA sets. The law also defines 4 levels of information classification for the critical infrastructure facilities on the: confidential, restricted, unclassified and public.

[10] http://cert.gov.ge/
[11] https://matsne.gov.ge/ka/document/view/1679424
[12] https://matsne.gov.ge/ka/document/view/1679424
[13] https://matsne.gov.ge/ka/document/view/1867646

In 2003 by president was published Cyber Security Strategy and implementation action Plan of 2013-2015 periods.[14] Cyber Security Strategy is the cyber security of the main state policy document, which reflects the strategic objectives, basic principles, establishes action plans and objectives. Based on the strategy, the government will carry out measures that will assist state agencies, the private sector and civil society to function safely in cyberspace, electronic operations and implementation of business and economic activities of the country. Objectives of policy are:

- Research and analysis.
- The new legislative framework.
- Institutional coordination on cyber security.
- Public awareness and educational base.
- International cooperation.

DEA plays an important role in the protection of critical systems. It issues new regulations and rules, helping critical infrastructure facilities improve their security systems, but this assistance is limited only to consultation and training. As prescribed by the law, the government is only providing protection monitoring functions. Such an approach may be feasible and appropriate in countries where the ICT sector is well developed and critical infrastructure facilities can provide their own systems protection. Unfortunately, Georgia is not among these countries, it is a paradox but in Georgia the critical infrastructure list does not include such important facilities as Internet providers and electric energy and water supplies systems that belong to the private sector. At this stage, the state does not take responsibility for the critical infrastructure pertaining to the private sector. Nowadays, each private sector facility takes care of the cyber security of their existing resources, but they can voluntarily assume the duties and have same opportunity as critical infrastructure facility. There are lot of organization which are using this opportunity.

[14] https://matsne.gov.ge/ka/document/view/1923932

Conclusions and proposals

Currently, Critical Infrastructure Protection is not a new trend for Georgia. The government based on international experience and best practices and have good legislative base, but practical activities should be improved E.g. Promote learning and adaptation during and after exercises and incidents. Also government should clearly define critical infrastructure sectors, systems and network and identify interdependencies within. however, we should take into account the fact that the only state's effort would be scant. Critical infrastructure protection responsibilities should be divided between government and the facilities itself.

References:

http://www.dhs.gov/what-critical-infrastructure
NIPP 2013 Partnering for Critical Infrastructure Security and Resilience
https://www.fas.org/sgp/crs/RL32631.pdf Critical Infrastructure and Key Assets: Definition and Identification
https://www.fas.org/sgp/crs/RL32631.pdf Critical Infrastructure and Key Assets: Definition and Identification[1] https://www.fas.org/sgp/crs/RL32631.pdf Critical Infrastructure and Key Assets: Definition and Identification
http://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031217-5.html
https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
https://matsne.gov.ge/ka/document/view/89662
http://cert.gov.ge/
https://matsne.gov.ge/ka/document/view/1679424
https://matsne.gov.ge/ka/document/view/1679424
https://matsne.gov.ge/ka/document/view/1867646
https://matsne.gov.ge/ka/document/view/1923932

CRITICAL INFRASTRUCTURE PROTECTION IN ROMANIA. A CIMIC PERSPECTIVE

Eusebiu INCULET

INTRODUCTION

Critical infrastructure definition

A country's critical infrastructures are the specific facilities, services and informational systems that are vital to its national security, economy, public health, and for the security and well functioning of the Government itself. The failure or destruction of such critical infrastructures could heavily weaken or threaten the latter. As such, both the management and protection of critical infrastructures go hand in hand.[1]

It is important to note that infrastructures are not critical in themselves, but that accurate analysis needs to be carried on all infrastructures in order to identify those of significant importance. Critical infrastructures are called as such because[2] they:

- ✓ are unique amongst other systems and infrastructures
- ✓ have a vital input on the functionality of other systems and infrastructures
- ✓ cannot be replaced in their role for assuring the security and functionality of other systems and infrastructures
- ✓ are particularly vulnerable to internal and external conditions and can be threatened or attacked.

Critical infrastructures can be physical (roads, wires, pipelines etc), cosmic (satellites and orbital stations) and virtual (virtual telecommunication systems, networks, databases). Computer networks are particular in this respective sense, as they involve both physical and virtual side.

Different countries use different means to evaluate and to define what represent for each of it the vital assets. In order to generally define the overall assets that are essential for the functioning of a society and/or an economy it emerged the term **Critical infrastructure**. This term is used by governments to describe, most commonly, the facilities associated with the following domains[3]:

---

1 Steiner, Nicolae. Andriciuc, Radu. *Infrastructura critica. Vulnerabilitatile si protectia ei.* Bucuresti, 2010. http://www.academia.edu/4377219/Consid_priv_protectia_infrastructurii_critice

2 Alexandrescu, Grigore. Vaduva Gheorghe. *Infrastructuri critice. Pericole, amenintari la adresa acestora. Sisteme de protectie*. Editura Universităţii Naţionale de Apărare „Carol I". 2006. http://cssas.unap.ro/ro/pdf_studii/infrastructuri_critice.pdf

3 https://en.wikipedia.org/wiki/Critical_infrastructure

- ✓ electricity generation, transmission and distribution;
- ✓ gas production, transport and distribution;
- ✓ oil and oil products production, transport and distribution;
- ✓ telecommunication and IT;
- ✓ water supply (drinking water, waste water/sewage, stemming of surface water);
- ✓ agriculture, food production and distribution;
- ✓ heating (e.g. natural gas, fuel oil, district heating);
- ✓ public health (hospitals, ambulances);
- ✓ transportation systems (fuel supply, railway network, airports, harbors, inland shipping);
- ✓ financial services (banking, clearing);
- ✓ security services (police, military).

Civil-military cooperation (CIMIC)

As a part of the modern society, defense establishment have it own perspective about the critical infrastructure. The very nature and scope of modern military operations provides significant challenges across the entire spectrum of conflict or crisis intervention. To prepare and equip for these challenges it is important to consider and allow for the civil dimension in the military planning process. For this reason, NATO states developed a tool (capability) to interact, analyze, evaluate and deal with civil dimension within the specific Area of Operations (AOO). This tool was called Civil-military cooperation (CIMIC).

In conflict, crisis or civil disaster, the state or condition of the civil infrastructure may be significantly affected. The degree to which this is the case will vary from that where there is no significant change to that where components of the civil infrastructure may have been rendered totally ineffective (be it by either military action or natural disaster). In order to evaluate the real situation on the field, CIMIC modules are using an important instrument named *CIMIC Assessment*. The purpose of a CIMIC Assessment is to provide the military commander with a means of examining the status of a specific Area of Responsibility (AOR) or Area of Interest (AOI) in order to identify critical shortfalls or capability gaps in the civil environment that may affect his mission, or that of the opposing force or forces.

1. CONCEPTUAL DELINEATIONS

Critical infrastructure – general overview

For civilian society and for government's critical infrastructure represent each asset associated with the domains that they decided that are essential to the social stability, wealth and development of the country. Generally, those peculiar domains are described at the Critical infrastructure definition and, are linked with all common assets used by the majority of the society in the specific age of developing.

Because the Critical infrastructure is vital for states, each of it develops own concept, doctrine or specific programs with the aim of protection the critical infrastructure against the different risks, threats or actions/incidents that may affect it. All of these actions taken in order to protect the Critical infrastructure are well known as *Critical infrastructure Protection* (CIP). It is very clear that, even for the most developed countries, is impossible to protect the entire infrastructure at the same time so that, as a result, the need to identify and to prioritize which one of the Critical infrastructure will be protected and in what order. Taking into consideration all these aspects is obvious that prevention have a huge importance also. States entities in charges with *Critical infrastructure Protection* are made a lot of planning regarding how to prevent a failure of a critical infrastructure asset and how to protect a critical infrastructure asset if an incident occurs at it. These plans can be Contingency Plans or Situational Plans made for a specific incident at a specific period of time.

Critical infrastructure – a CIMIC perspective

From civil-military cooperation perspective critical infrastructure represents each asset associated with the domains that they decided that are essential to the mission accomplishment within the specific AOR or AOO. In order to evaluate the critical infrastructure from military point of view and to have an accurate picture of the situation within a specific zone, CIMIC modules from the force HQ are starting the process of CIMIC Assessment using those factors that they are consider to be critical important or only important in the area. Taking into consideration civilian perspective and the military one it is obviously that *critical infrastructure* as an entire can be the same both for civilian and for military but the reference time is different for military than for

civilian. Considering this, is normal for military to analyze and to protect critical infrastructure during crisis situation and war more than during peacetime.

Critical Factors

Whether or not factors are considered critical will be situation dependent and must be defined by the force. That said, there are a number of factors that may be estimated likely to be included within this category. CIMIC analyze made using specific TTP (techniques, tactics, procedures) has identified five of these factors and incorporated them into a checklist (see figure no.1) in order to provide a tool to assist in CIMIC Assessment process. These factors are as follows:

(1) Water

(2) Sanitation

(3) Power

(4) Health

(5) Food.

It is important to stress that not all of the above factors will be critical in all operations but are situation dependent. On the other hand, factors not included in this may be critical. A good example of this may be shelter that is likely to be critical in many humanitarian operations and in scenarios where large numbers of DPREs (Displaced Persons, Refugees and Evacuees) are present.

Additional Factors

The list of additional factors that are not considered critical, but may also be included within CIMIC Assessment is almost limitless. The question as to whether or not these factors will be incorporated and if so, to what degree, will be situation dependent and may turn on some of the following questions[4]:

(1) How relevant is the factor to the military mission?

(2) What resources are available to conduct the assessment?

(3) How much time is available to conduct the assessment?

(4) How valuable is the information for use as a normality indicator?

(5) Could the factor become critical in the future?

(6) How detailed/broad does the commander require the assessment to be?

The checklist that is made for this purpose provides additional factors that may be considered (see figure no.2). This list is not exhaustive and that not all of the factors listed will be relevant in all situations or operations.

CIMIC Assessment Process

Concerning the assessment process there are a number of considerations that must be addressed. These include the following:

Information Collection.

[4] Civil military cooperation (CIMIC) Manual, SMG P.F.A. 5.3, BUCURESTI, 2011

In order to conduct an assessment the force must have the capability to collect and process the necessary information. This may include the employment of specialist staff. Sources may include the use of governmental and civil organization as well as the media, the Internet, libraries, archives and software. Formations should also check with their higher command and other formations to check what work or information may already have been gathered in order to avoid unnecessary duplication. The characteristics of accuracy and relevance are of specific relevance here as is the requirement for a consistency in approach across the AOO/AOI.

Checks.

In order for the information to be of any value the process must incorporate some form of system that will be able to analyze the information gathered. As such, when designing the assessment process it is important to ensure that such a system is built in at the outset that will be of use, not purely in order to validate the assessment but to filter out irrelevant information.

Monitoring.

It is also essential that the process can be monitored. In order to achieve this, a comprehensive reports and returns mechanism should be designed into the process. This will not only facilitate the movement of information once gathered in order to ensure that the appropriate level of visibility is achieved but it will also allow for tracking.

Co-ordination.

Co-ordination of effort and resources while collecting and assessing information for the assessment is also vital. This is linked with visibility and represent a function of the CIMIC staff at all levels.

In order to foresee and to manage the civil urgencies NATO utilize Civil Emergency Planning (CEP)[5]. The aim of Civil Emergency Planning in NATO is to collect, analyze and share information on national planning activity to ensure the most effective use of civil resources for use during emergency situations.

CEP represents a network of civil experts located across the Euro-Atlantic area which allows Allies and Partner nations to deal with the consequences of crisis, disaster or conflict.

CEP includes coordination of humanitarian support, flood relief, infrastructure protection and response to terrorist attacks with chemical, biological, radiological agents.

Requests for assistance are addressed to the Euro-Atlantic Disaster Response Coordination Centre[6], based at NATO Headquarters, which will match the offers of assistance from contributing nations with the requests of the stricken nation.

[5] http://www.nato.int/cps/en/natohq/topics_49158.htm
[6] http://www.nato.int/cps/en/natohq/topics_49158.htm

Figure no.1: **CIMIC assessments – critical factors checklist**[7]

CRITICAL FACTORS CHECKLIST		
WATER	o Locations o Facilities o Serviceability o Supply o Availability o Treatment o Pollution o POCs o Shortfalls o Civil Implications o Military Implications	
SANITATION	o Locations o Facilities o Serviceability o Treatment o POCs o Shortfalls o Civil Implications o Military Implications	
POWER	o Locations o Facilities o Distribution Network o Serviceability o Supply o Availability o Dependency o Resources Requirement o Human Resources o Fuel Type o Reserves o Hazardous Issues o POCs o Shortfalls o Civil Implications o Military Implications	
HEALTH	o Locations o Facilities o Availability o Diseases o Human Resources o Medical waste o Hygiene o POCs o Shortfalls o Civil Implications o Military Implications	
FOOD	o Availability o Supply o Distribution o POCs o Shortfalls o Civil Implications o Military Implications	

[7] Civil military cooperation (CIMIC) Manual, SMG P.F.A. 5.3, BUCURESTI, 2011

Figure no.2: **CIMIC assessments – aditional factors checklist**[8]

ADDITIONAL FACTORS – CHECKLIST		
GEOGRAPHICAL	o Key Physical Features o Population o Resources o Water o Neighbouring Countries o Climate	
ECONOMIC	o Industry o Resources o Power o Agriculture o Income o Wealth o Labour o Transportation o Communications o Technology o Banking/Financial System o Markets o Institutions/Organisations o Utilities o Wages o Inflation/Price Mechanisms o Standards	
POLITICAL	o Political System/Structure Administration o Legislation o Legal System o Judiciary o Law Enforcement o Civil Defence o Civil Emergency Services Institutions/Organisations o International Affairs	
SOCIAL	o History o Population o Language o Ethnic Groups o Religion o Health o Disease o Sanitation o Shelter o Education o Social Structure o Welfare o Social Ethics o Philosophy/Values o Cultural Issues Arts/Monuments/Archives o Media	

[8] Civil military cooperation (CIMIC) Manual, SMG P.F.A. 5.3, BUCURESTI, 2011

2. DIFFERENT PERSPECTIVE ON CRITICAL INFRASTRUCTURE MANAGEMENT (USA, EU)

United States of America

The term "critical infrastructures" began to be used in 1980s in the United States, where a history of attacks and threats on the country's values and objectives have led to the inauguration of the Presidential Commission for the Protection of Critical Infrastructures. It initially focused on three main industries: electricity, communications and computers. However, following the increase in terrorist attacks such as the 1993 World Trade Center bomb attacks and the 2001 fall of the twin towers led to the United States proposal that an international partnership should be agreed upon in order to collaboratively face globalized vulnerabilities and attacks.

At the end of 2001, the US launched the Executive Order for the Protection of Critical Infrastructures[9]. Its Patriot Act[10] of 2001 defined critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Two years later, the US tackled cyber security too with the National Strategy of Securing the Cyber Space, where it expanded the notion of critical infrastructures to include water and food management, public health, medical emergency responses, national defence, chemical and toxic substances management etc. This lead to international agencies such as NATO and the EU to also acknowledge the importance of such critical infrastructures and of partnerships for securing them.

The federal government has developed a standardized description of critical infrastructure, in order to facilitate monitoring and preparation for disabling events. The government requires private industry in each critical economic sector to:

- ✓ Assess its vulnerabilities to both physical or cyber attacks
- ✓ Plan to eliminate significant vulnerabilities
- ✓ Develop systems to identify and prevent attempted attacks
- ✓ Alert, contain and rebuff attacks and then, with the Federal Emergency Management Agency (FEMA), to rebuild essential capabilities in the aftermath.

According to the federal government standardized description of critical infrastructure, the National Infrastructure Protection Plan (NIPP)[11] defines critical infrastructure sector in the US.

[9] https://en.wikipedia.org/wiki/Critical_infrastructure_protection/ Presidential directive PDD-63 on the subject of Critical Infrastructure Protection.
[10] https://en.wikipedia.org/wiki/Patriot_Act
[11] https://en.wikipedia.org/wiki/National_Infrastructure_Protection_Plan

Presidential Policy Directive 21 (PPD-21)[12], issued in February, 2013 entitled Critical Infrastructure Security and Resilience mandated an update to the NIPP. This revision of the plan established 16 critical infrastructure sectors and assigns the following agencies sector-specific coordination responsibilities:

1. Chemical - Department of Homeland Security
2. Commercial Facilities - Department of Homeland Security
3. Communications - Department of Homeland Security
4. Critical Manufacturing - Department of Homeland Security
5. Dams - Department of Homeland Security
6. Defense Industrial Base - Department of Defense
7. Emergency Services - Department of Homeland Security
8. Energy - Department of Energy
9. Financial Services - Department of the Treasury
10. Food and Agriculture - Department of Agriculture
11. Government Facilities - Department of Homeland Security and General Services Administration
12. Healthcare and Public Health - Department of Health and Human Services
13. Information Technology - Department of Homeland Security
14. Nuclear Reactors, Materials, and Waste - Department of Homeland Security
15. Transportation Systems - Department of Homeland Security and Department of Transportation
16. Water and Wastewater Systems - Environmental Protection Agency

CIMIC/Civil affairs

The CIMIC equivalent in USA defense forces is called Civil Affairs.

Civil affairs in the United States Armed Forces are civil-military operations (CMO) use of military force to control areas seized from the enemy (or a third party), minimize insurgency or civil interference with military operations, and maximize civil support for military operations[13].

Case study – Katrina hurricane

In late August 2005, Hurricane Katrina moved into the Gulf of Mexico and began to strengthen into a massive storm. When it made land fall near the end of the month, Hurricane Katrina produced a storm surge and flooding that necessitated one of the largest search and rescue operations in U.S. history.

It took the National Guard troops less than four hours after the storm landfall to have forces on the ground, in the water, on the streets, and in the air. These state National Guard troops, along with

[12] https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience
[13] https://en.wikipedia.org/wiki/History_of_civil_affairs_in_the_United_States_Armed_Forces

guard soldiers from many other states, were placed in all areas along the coast, with a concentrated effort in the New Orleans area. These troops conducted many operations in the area including evacuation assistance, law enforcement activities, and search and rescue operations.

As the response activities continued, the resources of the local, state and regional agencies (including the National Guard) were quickly overreached. The National Response Plan (which was in effect during Hurricane Katrina), states that U.S. Department of Defense support during a domestic emergency is normally provided only when local, state, and other federal forces are overwhelmed, and it is requested by the lead federal agency responding to the event[14]. Once the request was made by the Federal Emergency Management Agency (FEMA) and Department of Defense (DoD), after a evaluation in terms of legality, readiness, lethality, risk, cost, and appropriateness, approved the request few other procedural steps were done in order to allow DoD active military members to intervene.

The active military duty response was large and the units began arriving and conducting many types of operations in the search and rescue area. Active duty forces from all branches of the armed services were deployed to the area and were all working under JTF-Katrina. The most immediate of the active duty forces support came from medical aircraft providing medical support to the area. Only two days after Hurricane Katrina made landfall, medical aircraft operations were underway and the USS Bataan arrived to provide additional support to relief efforts. This ship produced large quantities of fresh water, which was distributed throughout the region. It also addressed immediate medical needs because it is equipped with 600 hospital beds. Additionally, the USS Bataan has its own helicopters which are used for rescue missions.

In addition to the USS Bataan, several other Navy ships were sent from Norfolk, Virginia, including a rescue and salvage vessel and the USS Iwo Jima. By the fourth day after landfall of the storm, the 82nd Airborne Division out of Fort Bragg, North Carolina, and the 1st Cavalry Division out of Fort Hood, Texas, were placed on alert and arrived to the area two days later. As mentioned earlier, much has been reported about the slow response of the DOD to the Katrina disaster, but only one week after the storm hit the gulf coast, DOD assets in the affected area included more than 17,000 active duty personnel, 20 US ships, 360 helicopters, and 93 fixed wing aircraft. This was an extremely quick response for that amount of movement[15].

Among all the involved forces use of Civil Affairs Groups (CAG) was absolutely critical to enhance the ability to implement enablers for recovery beyond the search and rescue effort. As a lesson learned it was stressed that: “Experienced CAG officers, used to working with a stressed civilian leadership (people who are in the survival mode), are invaluable assets.”[16]

European Union

[14] Homeland Security Presidential Directive-5

[15] http://www.drj.com/articles/online-exclusive/reserve-response-to-search-and-rescue-operations-following-hurricane-katrina.html

[16] https://www.hsdl.org/?view&did=457055, MARFOR Katrina Staff Lessons Learned

Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of the EU. An adequate level of protection must be ensured and the detrimental effects of disruptions on the society and citizens must be limited as far as possible.

For the European Union, this became a top priority following terrorist attacks such as those in Madrid (2004) and London (2005), which lead to the immediate call for global strategies in protecting critical infrastructures. In 2004 the EU had already established the European Programme for Protecting Critical Infrastructures and in 2005 it launched CIWIN - Critical Infrastructure Warning Information Network in order to provide communication and warning disseminations to all its member states.

In Europe the "European Programme for Critical Infrastructure Protection" (EPCIP) refers to the doctrine or specific programs created as a result of the European Commission's directive EU COM786 from 2006 which designates European critical infrastructure that, in case of fault, incident, or attack, could impact both the country where it is hosted and at least one other European Member State. Member states are obliged to adopt the 2006 directive into their national legislation. The EPCIP is supported by regular exchanges of information between EU States in the frame of the CIP Contact Points meetings[17].

A key pillar of this programme is the 2008 Directive on European Critical Infrastructures. It establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection (fig. no.3). The Directive has a sectoral scope, applying only to the energy and transport sectors[18].

The Directive also requires owners/operators of designated ECI to prepare Operator Security Plans (advanced business continuity plans) and nominate Security Liaison Officers (linking the owner/operator with the national authority responsible for critical infrastructure protection).

Civil-military cooperation

European Union did not have it own defense force but some nations (mainly Great Britain and France) provide forces for Common Security and Defence Policy (CSDP). For this reason to utilise the defense forces within EU border and hence CIMIC component of it is the EU nations decision. But the very changing environment (midle east refugees flow, increasing number of the terorist attacks etc) can lead to a different aproach. But so far EU planned and conducted ten civilian and five military missions across the word and have ongoing ten civilian and seven military missions. The main goal of each of these missions represented a relief effort and civilian critical infrastructure reconstruction within the country/countries of deployment.

[17] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm
[18] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm

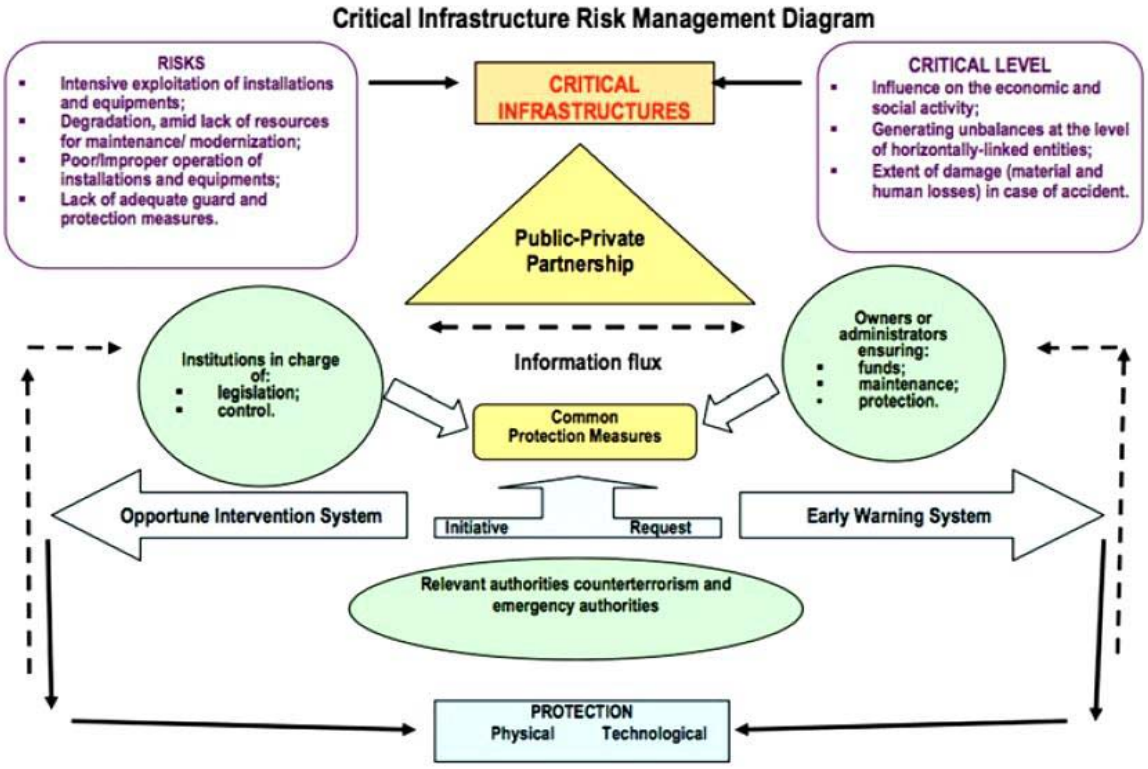


Figure no. 3: EU Infrastructure Risk Management Diagram[19]

3. MANAGEMENT OF THE ROMANIAN CRITICAL INFRASTRUCTURE

(Legal framework)

3.1. Accountable entities

[19] Alessandro Lazari, European Critical Infrastructure Protection, Springer International Publishing Switzerland, 2014: 79

Romania responded to the European Union and its Directive 2008/114/CE[20] that proposed all EU members to develop legislation and activities that would identify, manage, develop and secure critical infrastructures on their territories.

Romania first launched the emergency ordinance OUG number 98/201021 that was later approved into legislation as law 18/2011[22].

This law defines a national critical infrastructure similar to definition offered previously in this paper but also introduces the term "European critical infrastructure", defined as a national system or facility whose failure or perturbation would affect at least two EU member states.

According to the national legislation the Coordination Centre for Protecting Critical Infrastructures (CCPIC) from the Minister of the Internal Affairs (MAI) is nominated as the primary structure responsible for the security of the Critical infrastructure in ROMANIA. This is a national agency overseen by the PM and his/her state counselor.

The CCPIC is the primary agency that ensures that all the activities implemented in accordance to European law (specifically, directive 2008/114/CE) and the national law (namely, the OUG 98/2010 and its approval to law 18/2011) follow the purpose of developing and securing Romania's critical infrastructures.

The agency is also an intermediary in communicating and maintaining partnerships with similar EU bodies, the European Commission itself, NATO etc.

All this activities conducted by the CCPIC agency are leaded by the Government Decision 718 from 13 July 2011(HG 718)[23] which defined The National Strategy for Protecting Critical Infrastructures.

The strategies identify and define some terms and elements that affect our National Critical Infrastructures:

- ✓ ***Vulnerabilities***, defined as situations, processes and phenomena that either delay the critical infrastructure's capability to react to risks, threats and aggressions or in fact favors their emergence.
- ✓ ***Risks*** are defined as particular contexts, elements or situations (internal and external) that favor the creation of a direct threat.
- ✓ ***Threats*** are then considered capabilities, intentions, strategies and plans that aim to destabilize critical infrastructures by means of gestures, attitudes, or direct actions. The result of threats can include instability, insecurity and dangers of the critical infrastructures and the authorities and citizens relying on them.

[20] Centrul de Coordonare a Protectiei Infrastructurilor Critice. http://ccpic.mai.gov.ro/directiva.html
[21] Avocanet.ro http://www.avocatnet.ro/content/articles/id_22140/OUG-nr-98-2010-privind-identificarea-desemnarea-si-protectia-infrastructurilor-critice.html
[22] Monitorul Oficial: Strategia nationala privind protectia infrastructurilor critice (pdf) http://ccpic.mai.gov.ro/docs/HGR718_2011.pdf
[23] Idem 13

✓ ***Aggressions*** are defined as attacks (military, cybernetic) that target the weakening or failure of critical infrastructures, with serious consequences for the everyday life.

Based on these types of security issues, emerged four major strategic objectives of the national strategy on critical infrastructures, as follow:

✓ To assure that there is a unitary approach on how they are identified, assessed and managed

✓ To develop an early-warning system by integrating all existing networks and informational capabilities

✓ To correctly evaluate all possible vulnerabilities and make sure they are addressed properly

✓ To cooperate on the local, regional, national and international level on the topic of critical infrastructure security.

Within the law, CCPIC assumes several important roles. First, it connects public authorities and the owners, administrators or operators of the national critical infrastructures in order for them to carry annual evaluations concerning the status of the identified critical infrastructures, as well as submit similar evaluations to the European Commission once every two years. Public authorities are various ministries or public services institutions while the owners, administrators and operators can be, for example, private telecommunications providers or public energy providers. Second, together with similar institutions in the EU and with the European Commission, CCPIC is involved in discussions for creating supplementary protection measures at EU level, based on each member state's input.

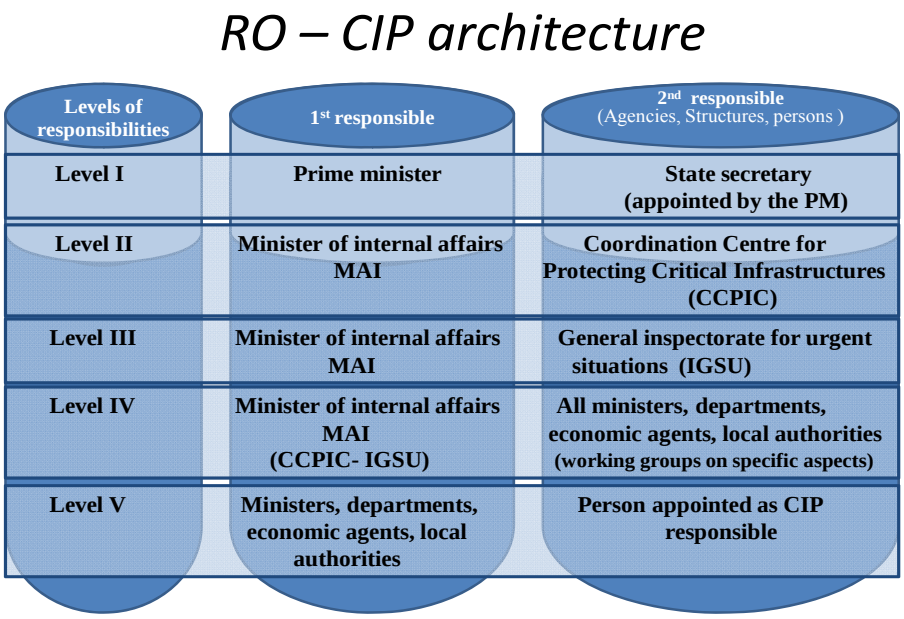
The task of identifying critical infrastructures as such is itself complex. There are strict criteria in assessing whether an infrastructure should or should not be considered critical.[24]

This involves, for example, calculating the number of people that would be harmed (physically) if that infrastructure would fail or be attacked, or the economical impact it would have (services/products being halted, loss of jobs), and finally to what degree would people mistrust the Government as a result of that failure or attack (because mistrust can directly affect the Government's proper functionality). These various criteria are not cumulative, meaning that if an infrastructure tick's just one major impact from the criteria listed, it is considered critical. If it is the case, the CCPIC can alert the European Commission if it identifies a particular infrastructure outside the country (in another EU member state), that nevertheless could heavily impact Romania in case of failure or attacks. Then research, discussions and assessments will be carried by both countries and the European Commission and, if it is the case, the respective infrastructure will be named a European Critical Infrastructure. According to the law, Romania also has the duty to inform all other EU member states about its national critical infrastructures, particularly those that

[24] Idem 13

can affect them directly. If it is the case, a national critical infrastructure will become a European critical infrastructure following discussions and assessments from the EU member states involved[25].

3.2. Critical infrastructure protection architecture



3.3. The place of CIMIC in the Critical infrastructure architecture

Romanian CIMIC role is defined in CIMIC Doctrine and CIMIC Manual, each of it providing the legal framework for creation and utilization of CIMIC structures. There are underlined the main CIMIC functions during peacetime, crisis and war:

- ✓ Civil-military Liaison
- ✓ Support to the Civil Environment
- ✓ Support to the Force.

In real life (daily activities) CIMIC is dealing with activities connected with CIP, within the assigned AOR, by:

- ✓ Creating and updating data bases
- ✓ Assessments upon the overall situation and particular situations
- ✓ Liaison with the local authorities representative and the Inspectorate for Urgent Situations (ISU) representative
- ✓ Common planning with the local authorities and the Inspectorate for Urgent Situations (ISU) representative for CIP when disasters, hazardous phenomena or attacks occurs (Joint Contingency Plans-JCP)
- ✓ Participating, at the local authorities request based on the JCP, or after the MoD approval in some particular cases that are not covered by the JCP, at interventions and relief efforts.

[25] *Marius Laurentiu ROHART,* Overview of Critical Infrastructures Protection in Romania, BRASOV, Nov 2014

4. CONCLUSIONS

As the inter-connectivity of our globalized world continues to increase, Critical Infrastructure Protection seeks to satisfy its role by different ways of approaches watching efficiency on one hand and consolidation of the security on the other.

Critical Infrastructure Protection represents a domain that requests a permanent analyzing, monitoring, evaluation, anticipating and improvement.

Critical infrastructure Protection is an ongoing activity, dealing with risk management and designing, implementing and monitoring the countermeasures necessary to be taken to avoid/reduce the risk. The visibility of these activities for mass media and hence for society it depends of the period of time when assets from Critical infrastructure need protection and who on earth will provide the protection measures.

During peacetime the entities dealing with CIP are governmental authorities/agencies conducting especially the prevention aspects. All these aspects of CIP are routine activities and have a low level of visibility for public opinion. Anyway the most visible and spectacular CIP activities are those interventions when incidents occur. On this phase the CIMIC participation in CIP or for providing the basic needs associated with Critical infrastructure is very unlikely because of limitations in terms of law and capabilities. Only for very clear reasons (big disasters as massive floods, enormous snowfall, and huge earthquake etc), central governments can decide to utilize the CIMIC capabilities on national territory.

During crisis or conflicts CIP involved both Host Nation governmental authorities and CIMIC modules from defense entities involved into conflict. From the timeline the CIMIC implication is very high at the beginning of crisis/conflict (CIMIC assessments and recommendations), decreasing during the phase of military operations/actions and rise up again during post conflict/transition phase (relief and support for reconstruction effort).

5. REFERENCES

1. Steiner, Nicolae. Andriciuc, Radu. *Infrastructura critica. Vulnerabilitatile si protectia ei.* Bucuresti, 2010. http://www.academia.edu/4377219/Consid_priv_protectia_infrastructurii_critice
2. Alexandrescu, Grigore. Vaduva Gheorghe. *Infrastructuri critice. Pericole, amenintari la adresa acestora. Sisteme de protectie*. Editura Universităţii Naţionale de Apărare „Carol I". 2006. http://cssas.unap.ro/ro/pdf_studii/infrastructuri_critice.pdf
3. https://en.wikipedia.org/wiki/Critical_infrastructure
4. http://www.nato.int/cps/en/natohq/topics_49158.htm
5. Civil military cooperation (CIMIC) Manual, SMG P.F.A. 5.3, BUCURESTI, 2011

6. https://en.wikipedia.org/wiki/Critical_infrastructure_protection/ Presidential directive PDD-63 on the subject of Critical Infrastructure Protection.
7. https://en.wikipedia.org/wiki/Patriot_Act
8. https://en.wikipedia.org/wiki/National_Infrastructure_Protection_Plan
9. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience
10. https://en.wikipedia.org/wiki/History_of_civil_affairs_in_the_United_States_Armed_Forces
11. Homeland Security Presidential Directive-5
12. http://www.drj.com/articles/online-exclusive/reserve-response-to-search-and-rescue-operations-following-hurricane-katrina.html
13. https://www.hsdl.org/?view&did=457055, MARFOR Katrina Staff Lessons Learned
14. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm
15. Alessandro Lazari, European Critical Infrastructure Protection, Springer International Publishing Switzerland, 2014: 79
16. Centrul de Coordonare a Protectiei Infrastructurilor Critice. http://ccpic.mai.gov.ro/directiva.html
17. Avocanet.ro http://www.avocatnet.ro/content/articles/id_22140/OUG-nr-98-2010-privind-identificarea-desemnarea-si-protectia-infrastructurilor-critice.html
18. Monitorul Oficial: Strategia nationala privind protectia infrastructurilor critice (pdf) http://ccpic.mai.gov.ro/docs/HGR718_2011.pdf
19. *Marius Laurentiu ROHART,* Overview of Critical Infrastructures Protection in Romania, BRASOV, Nov 2014

PROJECT MANAGEMENT METHODOLOGIES: A COMPARATIVE OUTLOOK

Ion STRIŞCĂ

INTRODUCTION

Do we need a methodology?

Let's accept it - doing "Project Management" merely means that the Project Manager, acting or assigned, is doing it for him/her. He/she is paid for the ability to "come to the finish" on time and with the right result. The rest, from the point of view of senior management (chief, commander, etc.) is sometimes no more than an obscure ritual.

A project management methodology, when used properly, reduces uncertainty. However, this is nothing more than a "map and compass" in this "journey" since, it is useless without the proper skills and the desire to use them.

The methodology, as such, cannot make a successful manager, as well as the rejection of him/her does not necessarily mean the failure of the project. In simple and short walks the map can never be required. In the same time no one will indulge to be involved in a more or less serious traveling without navigation. If the horizon of the project starts to be enveloped with thick fog and your team starts to stray from the route, then it is preferable that the project's success depends not only on good luck and intuition.

In order to achieve some goals and planned results within a defined schedule and with a certain cost, a manager uses a project oriented approach. Regardless of which field or which trade, there are assortments of methodologies to help managers at every stage of a project from the initiation stage, to implementation and to closure.

Thus, a methodology is a model, which project managers use for the design, planning, implementation and achievement of their project objectives. There are different project management methodologies that can be used to fulfill different projects.

This paper will try to figure out differences and similitude of some of the main and common Project Management methodologies used by different governs, organizations, companies, etc.

The most known and used Project Management methodologies, especially in both governmental and private IT sector, that are described in this paper are, as follows:

1. The so-called "**PMBOK**" (Project Management Book of Knowledge) method
2. PRINCE2 (**PR**ojects **IN C**ontrolled **E**nvironments).

I. PROJECT RELATED CONCEPTS. CURRENT PROJECT DEFINITIONS

Before going deep let’s start with the beginning. What a project is not? What is the project?

First of all a project is not a routine action that has to be done and repeated over and over. So, to "develop a software" - is not a project. The project is, for example, "to create and implement an information system by 1st of March of the following year."

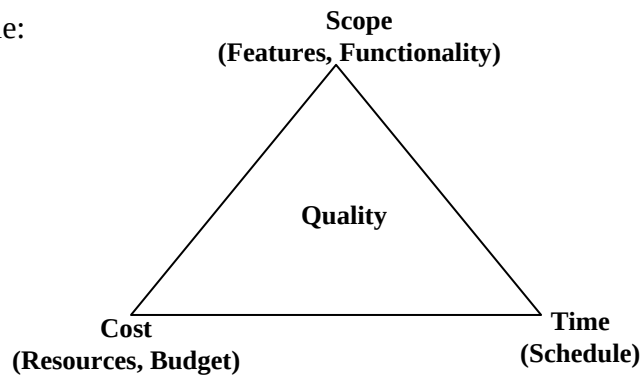
One of the simplest definition states: the project is all that has "a beginning, an end and purpose." So, when we are involved in the launch of a new project - it is always about something "final" and has a goal.

Project Management Institute define project as "*a temporary endeavor undertaken to create a unique product, service or result.*"

The PRINCE2 definition of a project can be found in the PRINCE2 Manual - Managing Successful Projects with PRINCE2 and reads: "*a project is a temporary organization that is created for the purpose of delivering one or more business products according to an agreed Business Case*."

So, the main goal of project management is to apply knowledge, skills and specialized techniques to fulfill projects in an effective and efficient way. This means achieving project goals on-time, on-budget and with the required functionality and quality. However, it is not important just to meet these goals and constraints, but also to determine the optimal allocation of resources needed to meet the goals and complete the project.

There are three main project constraints: scope, time and cost. Scope is achieved by the activities that need to be done in order to complete the project; time is the amount of time available to complete the project, while cost represents the resources, first of all financial, but not limited to these, available for the project. Neither of them can be changed without affecting the other two. The relationship between them is best understood on the project management triangle:



A large scope of work would result in increased project duration and higher cost. Small budget (cost) would increase time and reduce the scope. Finally, a tight deadline would result in reduced scope as well as increased cost of the project.

Nowadays the final result of work, especially in IT sector, but not limited to this, is not limited to a single product. There are different needs and often a unique product or service is delivered to consumers. The process of creating that unique product or service is called a project. So, project management is the process of managing projects.

II. PROJECT METHODOLOGIES

A *methodology* is a set of guidelines or principles that can be tailored and applied in a specific situation. In a project domain it might be a specific approach, forms, templates, and even a checklist used overall project life cycle. Despite this, it is not defined as a cookbook approach for project success.

Project Management shows various project life cycle approaches, which any newcomer or project manager can work with. It can be found over a dozen of different project management methodologies, which can be used for a lot of purposes. A superficial look shows they have the common basic “building blocks”, which can be tailored to suit the organization. In different domains, such as construction, energy, education, social, government, or information technology there are common factors that can be universally applied.

On the other hand, development of a single universal project management methodology is not as practical as it seems, reality proves there is more than one way to manage it. The methodology choice depends on the project type, size, complexity, duration, and organization, even all methodologies have the same main scope: to prevent problems and ease the project development. There is no one-size-fits-all methodology.

Project Management Methodologies developed from a less complex reality of smaller, more easily controlled projects. However, present day projects are often larger and more complex and involve significantly greater risks. Managing a complex project is more difficult than managing its projects’ individual parts. Methodology can ensure the right projects will be done in a right way at the right time, and the benefits will be identified and measured.

Key advantage of using a methodology and associated processes is that the risk of failure is reduced.

Use of the Project Management Methodology allow organisation to treat projects comprehensively, systematically, and in an integrated manner for acceptable risk. It is

necessary to provide confidence to customers, partners and top management that the organization can manage large projects and deliver them efficient. The methodology enables the organization to realistically assess the risks and difficulties that large projects encompass, ensures early recognition and put in place the strategies needed to minimize and overcome them.

The alternative of allowing different methodologies or no methodology is often inefficiencies, higher costs, longer schedules and of course higher risk. Consistency means having a standard way of managing all projects. It ensures that all aspects of the project are considered, evaluated and documented.

The methodology should start with the business processes before starting the project and should look at projects as part of a portfolio of endeavors that the business wants to achieve. In addition the methodology should look at projects that are part of a programme and treat them as such because there are different requirements in that scenario.

Most known and used key project management methodologies may be considered:

PMBOK - presents a set of standard terminology and guidelines (a body of knowledge) for project management.

PRINCE2 - takes a process-based approach to project management.

Agile was developed for projects requiring significant flexibility and speed and is comprised of "sprints" – short delivery cycles. Agile may be best-suited for projects requiring less control and real-time communication within self-motivated team settings. Agile is highly iterative, allowing for rapid adjustments throughout a project.

Information Technology Infrastructure Library (ITIL) - this methodology is a collection of best practices in project management. ITIL covers a broad aspect of project management which starts from the organizational management level.

Waterfall (Traditional) - is the legacy model for software development projects. This methodology has been in practice for decades before the new methodologies were introduced. In this model, development lifecycle has fixed phases and linear timelines. Waterfall allows for increased control throughout each phase but can be highly inflexible if scope changes may be anticipated later.

Critical Path Method (CPM) is a step-by-step methodology used for projects with interdependent activities. It contains a list of activities and uses a work-break-down structure (WBS), a timeline to complete and dependencies, milestones and deliverables. It outlines critical and non-critical activities by calculating the "longest"

(on the critical path) and “shortest” (float) time to complete tasks to determine which activities are critical and which are not.

When evaluating methodologies, these are only a few of the many factors that should be carefully considered: organizational strategic goals, constraints, stakeholders involved, risks, complexity, project size & cost, and key business drivers.

III. ENTITIES INVOLVED IN PROJECT MANAGEMENT

Project management is a team work, and in today's modern society it relies on the principal players of the team taking responsibility and accountability for those aspects of the project they have been charged with. All teams need a leader, so the principal role has to be played by the one commonly referred to as the **Project Manager**, with primary task to ensure that the Project Team completes the project. The Project Manager develops the Project Plan with the team and manages the team’s performance of project tasks. It is also the responsibility of the Project Manager to ensure acceptance and approval of deliverables from the Project Sponsor and Stakeholders. The Project Manager is responsible for communication, including status reporting, risk management, escalation of issues that cannot be resolved in the team, and, in general, making sure the project is delivered in budget, on schedule, and within scope.

The **Project Team** members are responsible for executing tasks and producing deliverables as outlined in the Project Plan and directed by the Project Manager, at whatever level of effort or participation has been defined for them.

The **Executive Sponsor/Project Sponsor** is a manager with demonstrable interest in the outcome of the project who is ultimately responsible for spending authority and resources for the project.

Stakeholders are all those groups, units, individuals, or organizations, internal or external to the organization, which are impacted by, or can impact, the outcomes of the project, with an interest in the project and have something to either gain or lose as a result of the project. This includes the Project Team, Sponsors, Steering Committee, Suppliers, Customers who will be affected by the change in Customer work practices due to the new product or service; Customer managers affected by modified workflows or logistics; Customer correspondents affected by the quantity or quality of newly available information; and other similarly affected groups.

Key Stakeholders are a subset of Stakeholders who, if their support were to be withdrawn, would cause the project to fail.

The **Steering Committee** generally includes management representatives from the key organizations involved in the project oversight and control, and any other key stakeholder groups that have special interest in the outcome of the project. Depending on how the project is organized, the steering committee can be involved in providing resources, assist in securing funding, act as liaisons to executive groups and sponsors.

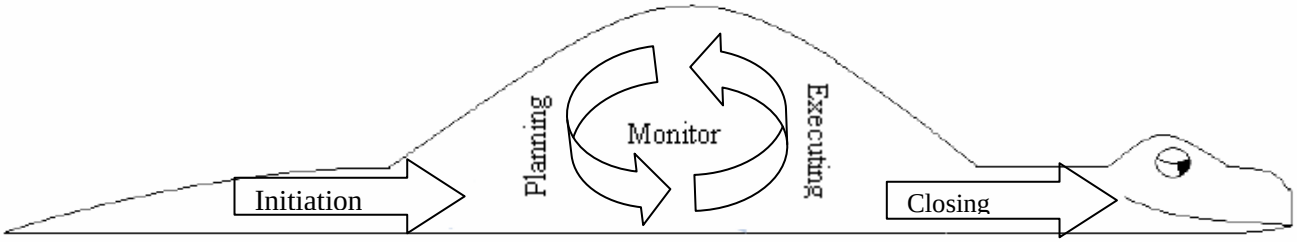
Customers comprise the business units that identified the need for the product or service the project will develop. Customers can be at all levels of an organization.

Suppliers / Vendors are contracted to provide additional products or services the project will require.

IV. PROJECT MANAGEMENT BOOK OF KNOWLEDGE (PMBOK)

Project Management Institute publishes A Guide to the Project Management Body of Knowledge (PMBOK Guide), which describes project management practices that are common to "most projects, most of the time." Developing the most common and traditional project management methods existed before it includes the following ideas:

The beginning of the project is called „Initiation" and the ending is „Closing". Between these two events are located (nonlinear) the planning, the execution of works and the "monitor and control". The non-linear characteristics appear because these processes are consistent, but iterative. So, once planned the project starts running, but as the work is doing, the monitoring brings the need for changing. Initial plans are adjusted, and the further monitoring is going on for them. And so on, and so on. In this way we can imagine the life cycle of the project as a „snake":



Sometimes, the „snake" can include several cycles of planning, executing and monitoring/controlling; in these cases the projects include several phases.

Typically the process of managing projects can be divided into five phases:

1. **Initiating**

This phase is the one most often given the least attention, but this phase scopes the project. During the initiation phase, it is carefully analyzed whether the project will bring

some benefits to the organization or not. The main documents elaborated during this phase are Project Charter and Preliminary Project Scope Statement. Also, all the activities taken in order to win the project, such as the negotiation with the client and other pre-sale activities, take place in this phase.

2. Planning

Planning can be considered the most important part of project management. Failure to plan the project time, cost and resources properly may result in not completing the project scope or financial loss. On the other hand, with a good plan, half of the job is done and it is likely that the project would be completed successfully.

During the planning phase is developed the project management plan. The planning processes also identify and better define the project scope, project cost, and schedule the project activities that occur within the project. As new project information is discovered, additional dependencies, requirements, risks, opportunities, assumptions, and constraints will be identified or resolved.

Project planning usually includes the following main activities:

- Determine how to plan (level of detail or rolling wave)
- Develop the scope statement
- Select the planning team (personnel involved)
- Identify deliverables and creating the work breakdown structure
- Identify the activities needed to complete those deliverables and networking the activities in their logical sequence (WBS)
- Estimate the resource requirements for the activities
- Estimate time and cost for activities
- Develop the schedule
- Develop the budget
- Risk analyzing
- Plan Purchases and Acquisitions
- Gain formal approval to begin work

3. Executing

In this phase, the processes required to complete the work defined during the planning phase are executed. Resources and tasks are distributed; personnel involved are informed of their responsibilities where each member of the team has their own assignments within the given schedule for each activity. The most important task during this phase is to optimally coordinate people and resources in order to complete the project goals.

The main processes within this phase are:

- Direct and Manage Project Execution
- Perform Quality Assurance
- Acquire and develop Project Team
- Information Distribution
- Request Seller Responses and select them

4. Monitoring and controlling

During the monitoring and controlling phase, the execution of the project is observed and monitored regularly, identifying the potential problems or variances from the project plan on time and fixing them promptly. Monitoring and controlling includes:

- Measuring the ongoing project activities (where we are)
- Monitoring the project variables (cost, effort, scope, etc.) according to the project management plan and the project performance baseline (where we should be)
- Identify corrective actions to address issues and risks properly (How can we get on track again)
- Influencing the factors that could circumvent integrated change control so only approved changes are implemented.

5. Closing

Closing is the formal ending of the project. It is the last phase of the project management process and it usually starts after all the project tasks have been completed and consist of hand off the completed product to customer (client, etc.) or close a cancelled project. Closing usually includes administrative activities, such as archiving the project files and marking project as completed, contract closure (completing all points written in the contract) and formally informing the project team about completing the project. Optionally, this phase also includes the post-implementation review, which consists of looking at things that went well and analyzing things that went bad on the project in order improve work efficiency and effectiveness on future projects.

V. PROJECTS IN CONTROLLED ENVIRONMENTS (PRINCE2)

This methodology emphasis on quality management, control and organization of a project with consistency and review to align with the demanded objectives. PRINCE2 is a certification program for practitioners in the methodology who are accredited, qualified through training. PRINCE2 emphasis on dividing the project into manageable and controllable stages. It is a process-driven project management methodology. It is based on seven principles: continued business justification, learn from experience, defined roles and

responsibilities, manage by stages, manage by exception, focus on products and tailored to suit the project environment.

PRINCE2 method includes eight management processes, which are further defined in 45 sub-processes. The processes include:

1. Starting Up a Project
2. Initiating a Project
3. Directing a Project
4. Controlling a Stage
5. Managing Product Delivery
6. Managing Stage Boundaries
7. Closing a Project
8. Planning

Some sources don’t include the planning as a separate process, due to fact it is included in almost all other processes.

This method includes also eight Components that support the mentioned Processes:

1. Business Case
2. Organization
3. Plans
4. Controls
5. Risk Management
6. Quality in a Project Environment
7. Configuration Management
8. Change Control

Also PRINCE2 allows the use of most techniques existing in project management theories and best practice, but there are three techniques specifically addressed within it: Product-Based Planning, Change Control and Quality Review.

VI. A COMPARISON OF PMBOK AND PRINCE2

PMBOK and PRINCE2 are considered scalable methodologies, which can be tailored to suit the specific requirements and constraints of the project and the environment.

PRINCE2, as a method and a certification, is adopted in many countries worldwide, including the UK, western European countries, and Australia.

The PMI and its certification, the PMP, are most popular in the UK, USA and the rest of the world. Since the PMI's PMBOK is a collection of recognized good practices, while

PRINCE2 is more practical, that makes Project Team easier to understand where to start and to stop. PRINCE2 also covers most the PMBOK concepts through Industry Practical Method. PMP is further from realistic then PRINCE2, being more as a knowledge.

PMBOK is not intended to tell people how to do any of the techniques or use any of the tools described. It only lays out the processes, how they link together and the tools and techniques that can be invoked.

PMBOK provides information on: Procurement, Earned Value management, Time Management, Communication Management, HR Management, whereas PRINCE2 doesn't cover these topics. But PRINCE2 provide focus on the Business Case, Products/Product-Based Planning, Project Assurance, strong process model, defining project management steps, clear roles and responsibilities, Management by Exception. PRINCE2 answer the question: How do I apply best practice Project Management Concepts in a project?

VII. MATRIX FOR COMPARISON

SIMILARITIES:

– World known project management methodologies;

- Scalable to project size;
- Can be fitted to different project types and scopes;
- There are provided trainings and certification.

DIFFERENCIES:

- PMBOK has a knowledge based approach to project management, while PRINCE2 is a process-based methodology;
- PMBOK describes core practices and a wider range of techniques that can be applied to manage a project, while PRINCE2 defines **what** must be done, **when** and **how** it must be done and by **whom** over the life of a project;
- PMBOK is a non-prescriptive methodology, PRINCE2 is prescriptive, but tailorable;
- PMBOK focuses on the project manager's role, while PRINCE2 defines the roles of everyone involved in a project.

CONCLUSIONS

The projects have common characteristics that can be formalized into a structural process, which allows managing projects more effectively. Each phase can typically be brought to closure in some logical way, before the next project phase begins and each phase results in discrete milestones or deliverables, which provide the starting point for the next phase.

Using wrong Project Management Methodology or even no methodology at all can cause:

- Schedule and cost slippages
- Miscommunication within the team
- Wasting time on administrative tasks with no purpose
- Project management burnout
- Project failure

One can consider that PMBOK and PRINCE2 are competitors, but they complement each other, can be used in conjunction for effective Project Management, considering PMBOK as a comprehensive source of information about all aspects of best practice Project Management and PRINCE2 as a practical Project Management methodology.

Defense establishments can use PMBOK to be interoperable with government and national organization, considered “de facto” national standard Project Management Methodology and PRINCE2 methodology when have to succeed international projects, especially run by or within NATO umbrella.

REFERENCES

1. Project Management Professional Study Guide, Kim Heldman,Wiley Publishing.
2. PRINCE2™ Foundation – Participant Guide, Boston University;
3. ITS Project Management Methodology, v 2.1, ITS Project Management Group, University of California Santa Cruz;
4. Comparing PRINCE2 with PMBoK®, R. Max Wideman, AEW Services;
5. IT Project Management – An effective system from “zero” in any organization, Ivan Selikhovkin

METEO TRAINING AND MENTORING PROGRAMME (2012 – 2014) AT KABUL INTERNATIONAL AIRPORT

Dorin PODIUC

INTRODUCTION

This paper is dedicated to METEO team, which laid the foundation of the Meteorological Aeronautical Service, on Kabul International Airport.

The objective of transferring the airport functions to the Afghan authorities is not a new project.
Recently, in September 2010, KAIA[1] Meteo Office started training several Afghan civilians, as indicated by the HQ IJC FRAGO 447-2010 and directed by Commander KAIA. The training ended in April 2011 without the objectives being met.
That experience, however, provided lessons learned which enable the existing project to have a successful result.
The Training and Mentoring Programme is designed to provide the knowledge and skills to the future Kabul Airport Meteo Team, enabling them to meet the standards and recommended practices and to create a safe meteorological environment for air operations.
The Programme will not provide the trainees with the experience, which will be acquired along the time.

This plan allows training a maximum of 12 subjects in the next 2 years with a high level of skills provided that MoTCA[2] is able to select good candidates in due time so that the course timeline does not suffer major delays.
The creation of an Afghan Civil Aviation Authority and the establishment of a State Meteo Policy is an important step to approach Afghanistan aviation sector to the International Civil Aviation Organization standards and provides the guidelines for the aviation industry in the country.
In addition, for an Airport Meteo System to be efficient the involvement and support of the higher management is vital and Kabul International Airport is not an exception. Kabul Airport Administration is responsible to provide airport users a safe working environment for an efficient operation and therefore shall support the Airport Meteo Team in achieving that objective.
The projects designed for the rehabilitation of Kabul International Airport must be seen as an opportunity for change. The present Training and Mentoring Programme is the first step for such hard objective.

[1] KAIA- Kabul International Airport
[2] Ministry of Transport and Civil Aviation

I. Course Administration and Policies

I.1 Meteo Training and Mentoring Programme Staff

Programme Director
ISAF[3] KAIA AIR OPERATIONS GROUP COMMANDER
Course Director
ISAF KAIA CHIEF METEO OFFICE
Course Manager
HIGHEST RANKING ISAF KAIA METEO INSTRUCTOR
Course Instructors
ISAF KAIA METEO INSTRUCTORS
ISAF KAIA FORECASTERS AND OBSERVERS
Course Supporting Instructors
ISAF METEO STATION

I.2.Program Management

The Meteo Training and Mentoring Programme is established under the directives set on the Transition Plan for Airport Activities approved by NATO JFC Brunssum and agreed upon with the Ministry of Transportation and Civil Aviation (MoTCA) of the Government of the Islamic Republic of Afghanistan (GIROA).
The terms and conditions of the Programme are described in the Letter of Agreement between ISAF and MOTCA on Transition of Airport Operational Functions at Kabul International Airport signed on the 23rd August 2011.
The Administration of the Training and Mentoring Programme is defined as follows:

The **Programme Director** reports directly to KAIA Commander. The Programme Director is responsible to:

- oversee the progress of the Course,
- report the progress of the Course to the higher Chain of Command,
- review the Weekly and Monthly Training Reports,
- communicate and coordinate with Kabul Airport Management, HQ Aviation Development and MOTCA on matters related to this Programme,
- decide on the elimination of trainees from the Programme in close coordination with MOTCA.

The **Course Director** reports directly to the Programme Director. The Course Director is responsible to:

- oversee the progress of the Course in a daily basis,
- decide on immediate actions at his level for the normal conduction of the Course,
- report to the Programme Director on issues requiring immediate attention and/or decision from higher levels of the Chain of Command,
- present the Weekly and Monthly Reports to the Programme Director,
- act on the disciplinary matters defined on paragraph E of the Course Policies.
- manage the trainees and instructor's schedules during OJT, in order not to impact with KAIA METEO primary mission,

[3] International Security Assistance Force

- coordinate with appropriate agencies their availability for study visits in the interest of trainees knowledge,

The **Course Manager** reports directly to the Course Director. Besides acting as Instructor, the Course Manager is also responsible to:

- establish the training plan and necessary updates based on the trainees progress and objective achievement,
- ensure the training is conducted in accordance with the parameters defined in this document,
- ensure the training is documented on a daily basis,
- provide the Course Director with a daily update on the activities, concerns and needs,
- prepare and perform the assessments in close coordination with the Instructors,
- prepare and deliver the Weekly and Monthly Training Reports to the Course Director.

The **Course Instructors** report to the Course Manager. The Instructors are responsible to:

- prepare and provide the training in accordance with the parameters set in the Training Plan,
- provide the Course Manager with a daily report on the activities conducted, the objectives achieved and the results of the daily trainees evaluation.

The trainees report directly to the Course Manager. Trainees responsibilities and privileges are explained in the Course Policies.

I.3. Course Documentation

A Personal Folder will be created for each trainee where all individual information regarding the trainee will be kept.
A Daily Report archive will be updated in digital format by the Instructors. This digital archive will be available for the Course Director at the NU network. A hardcopy of a Daily Training Report (*refer to Annex A1*) will also be available upon request.
Weekly Training Report (*refer to Annex A2*) will be produced documenting the training conducted along the week and the individual performance of each trainee based on the Daily Activity Reports. This report will be sent every Friday by electronic mail to the Course Director.
Monthly Training Report (*refer to Annex A3*) will be produced documenting the overall training conducted monthy and the individual performance of each trainee based on the Weekly Training Reports. This report will be sent at the each month by electronic mail to the Course Director. The data will be used in the Monthly Report sent to the Programme Director not later than the 5th day of the month.
Trainee Feed-back Report *(refer to Annex A4))* will be produced regularly at every 10 days of classes or at anytime a trainee feels the need to provide a written feed-back in regard to the training activities. This report will be incorporated in the trainee's personal folders.
All documentation is kept at KAIA Meteo Office. Documentation can be released to MOTCA Supervisors on request, upon approval from the Programme Director.

I.4. Course Policies

A new LOA between COMKAIA and MoTCA will be written to take into account the liability of each party as well as administrative policies regulating the leaves and working hours. In this context, course policies will be described in this document as a guideline

awaiting this new LOA to be in effect. Until that time, the following procedures will be applied.

A. SELECTION OF CANDIDATES

The selection of candidates to attend the Training and Mentoring Programme shall start as soon as the Meteo positions have been allocated in the Kabul Airport Tashkeel.
A pool of candidates, preferably a number between the double and the triple of the positions allocated in the Tashkeel for Meteo shall be provided by MOTCA, ensuring the selected candidates fulfil as a minimum, the following requisites:

- Education at High School Level – Grade 12
- Meteorological / Aviation background
- Good command of English (Understanding, Speaking, Reading and Writing)
- Driver License
- Good physical and psychological condition

The pool of candidates will be subjected to an individual evaluation based on:

- Test on general meteorological, geographical, physics, maths concepts (40% weight for final result);
- Individual interview with the applicants (30% weight for final result);
    - The interview board will include the Course Director, the Course Manager and a MOTCA representative;
- Applicant's curriculum (30% weight for final result);
    - The Curriculum's evaluation criteria will take into consideration the following factors:
        - Education
        - English Level
        - Experience in meteorology
        - Computer skills

A final list of candidates will be established based on the overall results.
The candidates with the higher scores will fulfill the allocated positions. In case of unavailability of a selected candidate at the start of the Programme, his/her position will be occupied by following the final list established.

B. TRAINEES RESPONSIBILITIES

The trainees selected to integrate the Meteo Training Program will abide by the Policies underlined in this document during the duration of the Program and will report directly to the Course Manager on any technical, operational and administrative matters related with the Programme.
The trainees will also abide by the Afghan National applicable rules prescribed in Afghan Labor Law and Civil Servants Law.
MOTCA will be notified in regard to administrative requirements such as duty schedules, leave periods, disciplinary actions and absences.
Additionally, during the duration of the Training and Mentoring Programme the trainees are responsible to:

- Report to the training sessions in a good physical and psychological condition,
- Attend punctually to the scheduled training sessions,
- Report to the training sessions with the supporting material as requested by the instructors,
- Commit entirely with the training and endeavor all efforts to reach the programmed objectives;

- Present the tasks, studies and reports assigned to be performed on the dates established,
- Comply with the directives set by the Instructors and described in this Document,
- Notify the Course Manager of any absence as prescribed on the paragraph C. *Absences From Training* below,
- Maintain a professional and respectful behavior towards the instructors, colleagues and others in the performance of the job,
- Maintain in good conditions all material provided along the Programme.

C. ABSENCES FROM TRAINING

As employees of the Ministry of Transportation and Civil Aviation (MOTCA), the trainees' absences will be regulated by the Labour Law and Civil Servants' Law appropriate Articles in regard to the Public Leave (Official Holidays), Urgent Leave and Recreational Leave.
All scheduled absences must be previously coordinated between the trainee and the Course Manager who will notify the Course Director. However, in order to reduce the impact on the training and allow an adequate planning of the lessons/tasks, annual leave will be granted to the trainees at regular intervals.
Clear definitions of justified and unjustified absences as well as sick leave are included in the paragraphs below.

1. Justified absence

A justified absence is a scheduled absence from training sessions which has been coordinated and approved by the Course Manager and MOTCA Supervisor or an unscheduled absence, as described in d) which has been immediately reported to the Course Manager. The following absences are considered justified:

a) Annual Leave,
b) Public Leave (Official Afghan Holidays),
c) Leave due to Marriage,
d) Death of direct Relatives and Birth of a child, provided a certificate is presented to MOTCA and the Course Manager.

2. Unjustified absence

An unjustified absence is the non-attendance to training sessions without prior notification and approval from the Course Manager.
Unjustified absenteeism might lead to the elimination from the training Programme.

3. Sick Leave

The cases of sick leave will be treated in accordance with Article 52 of the Afghanistan Labor Law, with the exception of paragraph (2). During the time the trainee is under the Training Programme, absence from training sessions for more than 2 (two) consecutive days must be justified by a medical certificate, otherwise, it will be considered as unjustified leave.
It does not relieve the trainee from the responsibility to inform the Course Manager by the most expeditious mean of his/her state of health and the impossibility to report for training.

4. Punctuality

Trainee's punctuality will be monitored and recorded in the Daily Training Report. Knowing that unpredictable situations might occur, especially in the access to the airport, it is required that trainees inform immediately the Course Manager of any delay to attend the training session.

D. WORKING HOURS AND HOLIDAYS DURING THE TRAINING PROGRAMME

During the theoretical training phase, the training sessions will normally take place from 08:30 to 12:30 from Saturday to Wednesday for a total of 20 (twenty) working hours per week. However, training sessions may be conducted from 08:30 to 16:30 when deemed necessary to comply with the initial training plan (trainee absence, security measures, etc.). Coordination will be achieved with MOTCA regarding the working times during the Holy Month of Ramadan (August).
During the OJT phase, the training sessions will be in an 8 hours daily basis for a total of 40 (forty) working hours per week. Eventual extensions on the working hours may occur during periods of Hajj flights, snow season, airport constructions or unusual procedures when deemed suitable for the training objectives. Compensatory rest time will be granted following the extension.

Thursday and Friday are considered as week-end days. Trainees will also be entitled to the Afghan Official Holidays. One week leave for every 2 months of training will be provided in a total of 6 weeks to match the requirements of the Afghan Labour Laws.
All working hours will be recorded in a daily basis.

E. DISCIPLINARY ACTIONS

A system of Awards and Penalties will be implemented along the Training Programme as a motivation incentive.
Awards and Penalties will be recorded in the trainee's personal folder and included in the Weekly and Monthly Reports.

- **Awards**

Awards will be given in form of Certificates. The objective is to create a healthy competition between the trainees and motivate them towards the training objectives. The Awards will be as follows:

- Certificate of Accomplishment: awarded to the trainees at the successful completion of Modules 3 to 15.
- Certificate of Accomplishment with Merit: awarded to the trainee(s) having obtained an average score of at least 80% in a Module. This Certificate will be awarded in lieu of the Certificate of Accomplishment.

NOTE: *The above mentioned Certificates of Accomplishment are exclusively an internal procedure applicable during the duration of the Training and Mentoring Program conducted by ISAF. These Certificates are not and do not grant any kind of official recognition to the certificate's holder.*

- **Penalties**

The Penalties, as the Awards, have the objective of motivating the trainees towards the Programme and their responsibilities.
The Penalties will be given in form of Verbal Warning, Warning and Reprimand Letters and will be recorded in the trainee's personal folder and included in the Weekly and Monthly Reports. Warning and Reprimand Letters require immediate notification to MOTCA Supervisor. The Penalties will apply as follows:

- **Verbal Warning**: Issued when non-compliance with the Training Programme Policies occurs for the first time.
- **Warning Letter**: Issued when recurring non-compliance with the Training Programme Policies occurs following a Verbal Warning.
- **Reprimand Letter**: Issued when the trainee having received a Warning Letter, reoccurs in similar action or behavior. A Reprimand Letter may also be given without being preceded by an Warning Letter in situations where the gravity of the situation so dictates, such as:

- Improper behavior towards colleagues, instructors or other persons during training sessions;
- Improper behavior to take advantage of his/her position as Meteo personnel in own profit;
- Deliberate acts to damage material or documentation;
- Deliberate actions which has or might jeopardize the safety of persons or damage equipment;

F. ELIMINATION

Elimination from the Training Programme will be considered whenever a trainee:

- Has received a second Reprimand Letter;
- Continuously demonstrate difficulties to reach the proposed objectives and no improvement is demonstrated or anticipated;

The elimination from the Training Programme is the Programme Director's decision in coordination with ISAF HQ Aviation Development and MoTCA.

I.5. Training Program Requirements

A. AIM OF THE METEO COURSE

The aim of the present Meteo Course is to prepare the trainee for the further observer and forecaster jobs on Kabul International Airport and not only, in the accomplishment of their duties as Meteo personnel.
This course has also been constructed in order to provide the Meteo trainees with a solid knowledge allowing them to acquire further specific knowledge in the Meteo domain.

B. CONSIDERATIONS

The challenges presented by an Airport such as Kabul International Airport require motivated, well-trained and knowledgeable personnel. Besides these characteristics, the trainee shall possess good communications skills and the ability to interact with people from very different backgrounds.
The total duration of the training, including theoretical and On-the-Job Training (OJT) is expected to be a total of 700 hours.
The duration of the theoretical phase is expected to have a total of 570 hours.
The duration of the OJT and supervised practice is expected to have a total of 130 hours.
In order to optimize Meteo human resources with the main goal to train the maximum number of trainees till the start of 2015, it's expected to have simultaneous courses running in different phases; theoretical and OJT.

C. LOGISTIC AND ADMINISTRATIVE SUPPORT

1) Logistic Support

In order to conduct the Meteo Course, the following logistic support is required:

- Allocation of a space (office) at the Civilian Airport side is essential in order to build the Meteo Office. Part of the OJT portion will be conducted in the office simultaneously with theoretical training. The allocation of the space must occur not later than the end of the 1st Course;
- Office furniture – detailed request will be submitted according to the available office space;
- Two desktop computers. One computer shall be programmed in Arabic and the other in English. Preferably, both computers shall operate in Win7 and have installed Microsoft Office (Office 2007 or 2010), Adobe Reader, PDF Creator, Compressor program (WinZip, NX PowerLite) and CD/DVD burning drive;

- Internet access;
- One laptop computer with similar programs as mentioned above for the desktop computers;
- One external hard drive, preferably with 1TB;
- One USB pen Drive with 8GB memory;
- One Multifunction Colour Printer;
- One Digital Still Camera with 8GB memory card;
- One Digital Voice Recorder;
- One laminating machine;
- One paper-cutting machine;
- One telephone for internal call and capability for external calls;
- One cell phone;
- One binding machine (for binder rings);
- One whiteboard 90cmx120cm;
- One calendar board 60cmx120cm;
- One pin board cork 90cmx120cm;
- Two radios (programmed for communications within airport facilities, including TWR);
- One measuring wheel;
- One vehicle;
- Perishable office items (pens; paper; binders; clips; laminating pouches; binder rings; staplers; puncher (two holes); board markers and board eraser);
- ICAO[4] Annexes and Documents;

2) Administrative Support

In order to conduct the Meteo Course, the following administrative support is required:

- Allocation of positions for Meteo personnel in Kabul Airport Tashkeel – Condition *sine qua non* to start the Programme;
- Total availability of the trainees – Trainee shall not be expected to work in any other department or service;
- Payment of salary according to Afghan Laws;
- Access to meteo designated Airport areas for each trainee and Instructors;
- Screening and Vetting process for the selected candidates.

II. Training Plan

II.1. Timetable and Teaching Methods

The objective of the Meteo Training and Mentoring is to provide the trainee with the knowledge and skills, in accordance with International Civil Aviation Organization (ICAO) Standards and Recommended Practices which enable them to perform a forecaster and observer job at Kabul International Airport and not only.

After completion of the training, the applicants will be able to perform, as MOTCA employees, the duties of Meteo personnel, as listed:

- Analyzing, assimilating and interpreting current atmospheric conditions and other meteorological products to prepare forecasts of expected weather conditions;
- Providing required meteorological and designated/related atmospheric information to ground and aircrew personnel;

[4] International Civilian Aviation Organization

- Developing procedures and computer programs to enhance the clarity, accuracy and usefulness of weather products;
- Providing climatologically data to Meteorological Office personnel;
- Maintaining a weather watch;
- Preparing prognostic charts and forecasts;
- Providing weather forecast briefings;
- Producing weather warnings and contacting the required personnel in a timely manner to maintain safe operations;
- Coordinating and maintaining liaison with other meteorological organizations;
- Producing reference and training material for office use;
- Conducting and planning training for aircrew members;
- Issues aviation weather information as well as other designated areas, according to
- WMO[5] standards, i.e. TAF[6]s, METAR[7]s;
- Perform observer duties if required;
- To perform upper air sounding as required.
- Providing the required meteorological observations and designated/related atmospheric information at KAIA and its surroundings using a variety of meteorological equipment
- Interpreting standards and regulations as they apply to weather observation and reporting
- Interpreting atmospheric data measurement apprising the forecaster and other concerned personnel on significant changes in the actual weather situation
- Assisting the forecaster in the preparation of weather information and disseminating products to local and long line customers
- Providing, in the absence of a forecaster, observed weather warnings to avoid loss of base equipment and prevent injury to personnel
- Performing preventive maintenance on meteorological equipment
- Ensuring the proper functioning of the meteorological communications, data and graphics display systems
- Providing input for the formulation or revision of directives and regulations.

The Meteo training is divided in 13 (thirteen) Modules. All Modules complement each other and will be enriched with the trainee OJT experience.

With the purpose of clarification, the training methods refer to:

- Lecture: A straight talk or exposition, possibly using visual or other aids, but without group participation other than questions, usually at the conclusion.
- Lesson: A training technique incorporating a number of instructional techniques designed to ensure the participation of the trainee in reaching the specified objectives.
- Case study: A training technique in which a real or fictional situation or series of events are presented to the trainee for his/her analysis and consideration of possible solutions or problems identified. The findings in a real situation can be compared with what actually occurred. In the Training Syllabus, the exercises and tasks mentioned are considered case study.
- Supervised Practice: equals to On-the-Job training.

Training will be based on International Civil Aviation Organization (ICAO) Standards and Recommended Practices set in ICAO Documents and Annexes.

[5] World Meteorological Organization

[6] Terminal Airport Forecast

[7] Meteorological Airport Report

The structure of the present Training Plan allows the acquisition of knowledge at different rates being adaptable to each trainee. The plan can be adjusted in accordance with the trainees' needs and problems encountered within the timeframe of the mentoring Programme.

II.2. Meteo Courses Contents

METEOROLOGIST/FORECASTER

MODULE 1 - Aviation History and Organizations – WMO/ICAO
At the end of the Module, the student will be able to describe and differentiate the organizations affecting the operation of civil and military aviation worldwide, in Afghanistan in general and in Kabul in particular. The subjects include:

- Aviation History
- World Meteorological Organization (WMO)International Civil Aviation Organization (ICAO)
- International Civil Aviation Organization (ICAO)

MODULE 2 - Reviewing knowledge of mathematics and physics required to study Meteorology
At the end of the Module, the student will be able to operate with mathematics and physics formulas used in Meteorology the subjects include:

- Mathematics
- General Physics and Chemistry

MODULE 3 – Specialized scientific knowledge
At the end of the Module the student shall be able t o understand physical processes of the atmosphere, basically attempts to describe the atmospheric processes through mathematical equations, understand and perform a study of heat to work transformation (and the reverse) in the earth's atmospheric system in relation to weather.
The subjects include:

- Physical Meteorology
- Dynamic Meteorology
- Thermodynamics of the atmosphere

MODULE 4 – Specialized knowledge (Synoptic Meteorology)
At the end of the Module, the student will be able to make maps of soil correlation with altitude to develop weather forecasts. The subjects include:

- Air masses
- Atmospheric fronts
- Atmospheric Pressure field forms : Cyclone
- Atmospheric Pressure field forms : Anticyclone
- Atmospheric Pressure field forms : Practice
- Altitude charts
- Altitude charts : practice
- Weather forecast : practice

Supporting Documents:
ICAO Annex 3 – *Meteorological Services for International Air Navigation*
ICAO Doc 8896 – *Manual of Aeronautical Meteorological Practice*
ICAO Doc 9328 – *Manual of Runway Visual Range Observing and Reporting Practices*

MODULE 5 – Climatology
At the end of the Module, the student shall be able to establish the mechanisms by which factors cause the formation of different types of climate, know the latitude and longitude distribution of major weather elements, understand the major climate classifications and the main climates of The Earth, identify the main characteristics of the Afghanistan climate and how they influence general weather forecasts, make assessments on climate change.
The subjects include:

MODULE 6 – Aeronautical Meteorology
At the end of the Module, the student will be able to describe the meteorological phenomena affecting aviation. The subjects include:
- Meteorological phenomena
- Meteorology and Aviation
- Meteorological reports
- Exercise

MODULE 7 – Hydrometeorology
At the end of the Module, the student will be able to describe the relationship between meteorological variables and the maximum precipitation reaching the ground The subjects include:
- Extreme rain fall
- Deposits of snow and water reserves

MODULE 8 – Computers
At the end of the Module, the student will be able to have the necessary skills to work with computer. The subject includes:
- Computer
- Software

MODULE 9 – Radar & Satellite remote sensing
At the end of the Module, the student will be able to interpret & use satellite & radar pictures to forecast weather. The subject includes:
- Radar pictures
- Satellite pictures

MODULE 10 – Atmospheric pollution
At the end of the Module, the student will be able to describe Atmospheric pollution and causing factors. The subject includes:
- Pollution factors
- Derived implication

MODULE 11 – Weather observation
At the end of the Module, the student will be able to make accurate observation. This subject includes:
- Temperature
- Wind
- Pressure
- Cloud coverage & ceiling
- Phenomena

MODULE 12 – Aeronautical Telecommunications
At the end of the Module, the student will be able to use telecommunication systems. The subject includes:

- Organization of aeronautical / meteorological telecommunications.

MODULE 13 – Weather briefings for Flight Crew Members
At the end of the Module, the student will be able to elaborate an Weather briefing for Flight Crew Members. The subject includes:

- Briefing requests

Practical lessons (OJT)
The trainee will conduct series of tasks under the supervision of a Trainer. This part of the program is effectively the OJT.
The tasks are programmed to train the trainee in accordance with the requirements of his/her job description.

Meteorological Technicians/ OBSERVERS & MET-BRIEFFERS

Module 0 – Course Introduction
At the end of the Module, the student will be able to describe the Meteorological Training Program, his/her responsibilities and goals. The subject includes:

- Instructors and students
- Course introduction
- Course Policy
- Course Content

MODULE 1 - International Organizations – WMO/ICAO
At the end of the Module, the student will be able to describe and differentiate the organizations affecting the operation of aviation worldwide. The subjects include:

- World Meteorological Organization (WMO)
- International Civil Aviation Organization (ICAO)

MODULE 2 - Introduction to geophysics
At the end of the Module, the students will have knowledge about the Solar System and planet Earth. The subjects include:

- The Solar System
- The Earth
- Earth Forces
- Earth movements
- Solar radiation and the Earth
- Circulation in the atmosphere
- The Oceans
- Measurement of Time

MODULE 3 – Climatology
At the end of the Module, the student will have knowledge of the fundamental concepts of Climatology and how to collect and processing climatological data. The subjects include:

- Fundamental concepts in Climatology.
- Statistics concepts in Climatology.
- Climate classifications
- The Climate of Afghanistan.

- Climatology and Aeronautical activity.

MODULE 4 – Meteorological Instruments and Methods of Observation
At the end of the Module, the student will be able to make accurate observation. The subjects include:

- General topics about meteorological observations
  Meteorological instruments/equipments
- Visibility
- Temperature
- Wind
- Humidity
- Pressure
- Cloud coverage & ceiling
- Meteorological observation practice

Supporting Documents:
ICAO Annex 3 – *Meteorological Services for International Air Navigation*
ICAO Doc 8896 – *Manual of Aeronautical Meteorological Practice*
ICAO Doc 9328 – *Manual of Runway Visual Range Observing and Reporting Practices*

MODULE 5 – Meteorological Codes
At the end of the Module, the student will be able to code and decode aviation and synoptic messages. The subjects include:

- Code & decode messages according to WMO formats
- Code and decode METARs and TAFs

MODULE 6 – Radar & Satellite remote sensing
At the end of the Module, the student will be able to interpret & use satellite & radar pictures to forecast weather. The subjects include:

- Radar pictures
- Satellite pictures

MODULE 7 – Physic and Dynamic Meteorology
At the end of the Module, the student will be able to characterize the atmosphere and describe, characterize and recognize thermodynamic processes and thermodynamic phenomena that occur in the atmosphere. Relate the observed phenomena with dynamic causes. The subjects include:

- Atmosphere components
- Vertical structure of the Atmosphere
- Heat exchanges in the Atmosphere
- Temperature
- The Moist air
- Adiabatic processes and atmospheric stability
- Air turbulence.
- Temperature inversions.
- Clouds
- Precipitation
- Fog
- Thunderstorms
- Tornados

- The Dynamic behavior of the Atmosphere - The Wind

MODULE 8 – Synoptic Meteorology
At the end of the Module, the student will have the basic knowledge on the various meteorological weather patterns and systems. The subject includes:
- Air masses
- Fronts
- Barometric configurations : Cyclonic and anticyclonic
- Analyse Synoptic Charts

MODULE 9 – Aeronautical Meteorology
At the end of the Module, the student will be able to describe the meteorological phenomena affecting aviation. The subject includes:
- Meteorological phenomena dangerous for aviation.
- Altimetry.
- Meteorological visibility.
- Meteorological information for aeronautic.
- Meteorological codes
- Aeronautical operations and meteorology.

MODULE 10 – Rawin and Digicora
At the end of the Module, the student will be able to work with the Rawin equipment and perform an altitude observation. The subject includes:
- Altitude Station
- Meteorological equipment / sounding

MODULE 11 – Aeronautical Telecommunications
At the end of the Module, the student will be able to use telecommunication systems. This subject includes:
- Organization of aeronautical / meteorological telecommunications.

MODULE 12 – Weather briefings for Flight Crew Members
At the end of the Module, the student will be able to elaborate an Weather briefing for Flight Crew Members. The subject includes:
- Briefing requests

Practical lessons (OJT)
The trainee will conduct series of tasks under the supervision of a Trainer. This part of the program is effectively the OJT.
The tasks are programmed to train the trainee in accordance with the requirements of his/her job description.

III. ASSESSMENT EVALUATION

Trainees and Trainers must be aware that the main objective of performing an assessment is to determine the quality of knowledge and skills so adequate corrections may be made to overtake any deficiencies, if necessary.

A correct assessment will contribute to better quality training and will help in the planning of the next training session in accordance with trainees' needs.
Prior to any assessment, trainees must be made fully aware of the objectives and the areas or subjects the assessment is covering.
The assessments conducted along this Training and Mentoring Programme will be mostly conducted with a formative objective. Summative assessment will also be conducted especially for the theoretical part of the Programme.
An assessment may be carried out in a number of ways. The methods used during this Course are:

- **Oral questioning** – conducted by the instructor based on objective questions and answers, as part of the training items for that training session.

Oral questioning will mostly be used during the classroom lessons and supervised practice. Oral questioning will be used to identify the strengths and weaknesses in order to help planning following training sessions with the objective of consolidating the trainee's knowledge or overtake detected learning difficulties.

- **Written questioning** – conducted using printed questions with multiple-choice selections, true or false and fill-in-blank questions. This assessment will be summative and the test will be graded.

Trainees will normally be informed of the written assessment at least four (4) days in advance. Written assessments will be graded from 0% to 100%.
Whenever the score obtained is less than 75%, the trainee will be given the opportunity to retest and must score 75% or more so his progress is considered Satisfactory or above.

NOTE: When a retest occurs, the final score will never be greater than 75%, regardless of the score obtained in the retest.
Written assessments covering the subjects of the previous day lessons might be conducted without prior notification, in order to evaluate the quantity and quality of the information retained.

- **Supervised Practice Assessment** – conducted to determine the trainee's skills, knowledge, initiative and judgment on performing an assigned task. In the context of this Training and Mentoring Programme, the tasks are depicted on Module 13.

Trainees will be subject to a constant evaluation while in supervised practice. The results will grade from UNSATISFACTORY to VERY GOOD.

- **OJT Assessment** - conducted to determine the trainee's skills, knowledge, initiative, judgment, attitude and communication while performing OJT. This evaluation method must always take into consideration if the trainee has faced a similar situation previously.

At this stage of training, it is expected that the trainees will be able to respond to meteo related issues with minor assistance from the instructors.
The results will grade from UNSATISFACTORY to VERY GOOD.

When an assessment is performed, the performance shall be classified as:

- **VERY GOOD**: trainee shows no weaknesses and is consistently well above the level expected.
- **GOOD**: trainee commits almost no mistakes and deliberately uses own initiative, imagination and professional competence. Maintains the expected level of effort and achievement.

- **SATISFACTORY**: trainee's performance generally satisfies the training requirements and objectives, but not more.
- **MEDIOCRE**: trainee's overall performance does not meet the training objectives.
- **UNSATISFACTORY**: trainee's performance demonstrates lack of commitment to the training.

In MEDIOCRE and UNSATISFACTORY evaluations, the facts leading to such result must be detailed in the evaluation.

The result of the evaluation shall always be discussed with the trainee as well as the steps to improve his/her performance. Trainee's feedback is mandatory in MEDIOCRE and UNSATISFACTORY evaluations.

Besides knowledge and skills, trainee's attitude, assiduity and willpower will also be the subject of constant evaluation and will be included in the Activity Reports.

As trainees are evaluated on their performance, the training will also be subject to the trainees' evaluation at the end of each module or phase (theoretical and OJT). Each trainee will fill a feedback questionnaire.

IV.TRAINING SYLABUS

According:

-WMO-No.49, Technical Regulations, Vol I • Chapter 4 – Education and Training • Definition of BIP-M and BIP-MT • Chapter 5 – Qualification and Competency

-WMO-No.1083, Manual (replaced WNO-No.258) – implementation guidance

-WMO-No. 1083- Manual on the Implementation of Education and Training Standards in Meteorology and Hydrology

CONCLUSIONS

„NATO, ICAO, and US Federal Aviation Administration (FAA) cooperation in Afghanistan has been vital in moving forward the complex, multi-faceted problem regarding the handover of responsibility of KAIA from ISAF to GIRoA. The recruitment and retention issues that have plagued previous plans to grow capacity in key specialist areas have now been resolved.
Through a concerted effort between ISAF and MoTCA, the publication/endorsement of the TASHKIL[8] and TAS[9] created the real opportunity to grow the necessary skills and experience and finally, to start the process of transition. This should be regarded as the first step of many but is vital if transition is ever to be achieved.
For example, rehabilitation and normalization of the aviation sector and infrastructure/ equipment issues are equally important for the process to be completed.
We have assessed that, whilst a small initial investment in terms of manpower is required (just 3 mentors), the savings are significant (more than 8 CE Posts). A further 8 CE posts will be saved once the Afghan personnel have assumed the leadership and supervisory roles bringing the total saving to more than 10 CE posts. As a result, NATO will save a big amount of money (e.g: an average monthly payment for an ICC(International civilian consultant) is around 7, 500 Euro; for an Afghan LCH is between 500 $ and 1200$ depends on the field.
However, even if the Plan seems to be achievable, there are some challenges and a certain grade of risk which from my point of view, can hamper or delay the implementation of the Transition Plan, such us:
- willing of the Afghan side to be really involved in the Transition Plan.
- TAS/ Payment issues:
– to retain the Afghan personnel trained and qualified by ISAF trainers;
– to retain the Afghan personnel graduated from CATI[10]
- availability of the trainees for the training program;
- additional tasks out of the OJT program to be given by MoTCA, for trainees;
- quality and experience of the majority of the Afghan personnel is very low in comparison with ISAF personnel (especially ICCs);
- problem to find the suitable Afghan candidates, due to the very limited percentage of the people with a high school degree (almost 90% of the Afghan population are illiterates).
The ultimate goal of this project is to ensure the trainees acquire the knowledge and skills required to perform the duties as Meteo Personnel contributing for the approach of Kabul International Airport to ICAO meteo standards ” (KABUL INTERNATIONAL AIRPORT (KAIA) TRANSITION PLAN: CASE STUDY ON HUMAN RESOURCES MANAGEMENT (HRM) Capt. cder. Marius PETRE,)

[8] Organizational chart
[9] Budget
[10] Civil Aviation Training Institute

REFERENCES

The following supporting documentation is used to provide theoretical and OJT.
ICAO and WMO PUBLICATIONS
ICAO:
Annex 1 – Personnel Licensing
Annex 2 – Rules of the Air
Annex 3 – Meteorological Service for International Air Navigation
Annex 4 – Aeronautical Charts
Annex 5 – Units of Measurement to be used in Air and Ground Operations
Annex 10 – Aeronautical Telecommunications
ICAO Abbreviation and Codes (Doc 8400)
Manual of Aeronautical Meteorological Practice (Doc 8896)
WMO:
-WMO-No.49, Technical Regulations, Vol I • Chapter 4 – Education and Training • Definition of BIP-M and BIP-MT • Chapter 5 – Qualification and Competency
-WMO-No.1083, Manual (replaced WNO-No.258) – implementation guidance
-WMO-No. 1083- Manual on the Implementation of Education and Training Standards in Meteorology and Hydrology

Documentation from other Sources
Afghanistan Aeronautical information Publication
Letter of Agreement between ISAF and MoTCA on Transition of Airport Functions
Afghan Labor Law
Afghan Civil Servants Law
Information was retrieved from the following websites for the purpose of the present Program:
International Civil Aviation Organization (ICAO) official website
European Organization for the Safety of Air Navigation (EUROCONTROL) official website
Ministry of Transport and Civil Aviation of the Islamic Republic of Afghanistan official website

AN OVERVIEW OF CRITICAL INFRASTRUCTURE PROTECTION IN ROMANIA

Ioan Marian STREZA

INTRODUCTION

The world as we know it now and in which we live involves risks that we cannot eliminate, but we can control and reduce them to acceptable levels. To reduce risks and keep them under control, first we need to identify them with all the factors that influence them and take appropriate protective and preventive measures.

The emergence of the concept of critical infrastructure worldwide, its development and adoption of Community legislation creates major responsibilities to the Romanian government for creating the legal framework needed to develop activities in the field of critical infrastructure protection. "*Identification, optimization and securing critical infrastructure is an unquestionable priority for both managers of systems and processes as well as their opponents, i.e. for those who seek to attack, destabilize and destroy the targeted systems and processes. Critical infrastructures are critical and are not only due to attacks or attacks, but also because of other causes, some of them difficult to detect and analyze. Usually, especially after the terrorist attacks of 11 September 2001 on the World Trade Center and the Pentagon, it is considered that are or may become critical infrastructure against terrorist attacks and other threats, especially asymmetrical*."

In this context protection of critical infrastructure (CI) is a topic of great interest to the authorities of the Member States and the European Union. The concern of national governments and the European Commission focuses on developing procedures and methodologies for identifying and taking measures for the protection of critical infrastructure, as the negative impact of malicious human actions (here we include organized crime, terrorism and cyber attacks), and natural disasters (hurricanes, tornadoes, earthquakes, tsunamis, landslides, floods, etc.) and technological accidents affecting many communities around the world.

Romania managed to clearly define the terms and expressions used in this matter, the responsible public authorities, identification procedure by public authorities in charge of

critical infrastructures which may be designated as national critical infrastructure / European Critical Infrastructure (ICN / ICE) creating the legal framework national activities in the area. In turn responsible authorities or ministries have developed internal order to establish sectorial criteria and critical thresholds related to ICN sector - national critical infrastructure. It was also created the Centre for Coordination of Critical Infrastructure Protection (CCPIC) under Ministry of Internal Affairs, that is responsible for organizing and conducting activities necessary to implement the Ordinance, namely the establishment of cooperation between the responsible public authorities and non-governmental structures. Also specifies that CCPIC ensure national contact point in relations with other Member States, European Commission, NATO and other international structures and management CIWIN at national level.

I. COMPARATIVE OUTLOOK ON CRITICAL INFRASTRUCTURE DEVELOPMENT CONCEPT

I.1 The emergence of the concept of critical infrastructure worldwide and European

The unprecedented increase in the last 20 years, of the risks, dangers and threats to the vital objectives of states and international organizations, along with their increasing number and vulnerability led to the emergence of a new concept known as critical infrastructure.

This kind of infrastructure exists everywhere in the world and, of course, in each country and within each physical or virtual system in all areas of human activity.

The first studies in the field have identified objectives deemed "critical", but since the 80s phrase "critical infrastructure" was first used formally in July 1996 when US President Bill Clinton, issued "Executive Order nr. 13010 for Critical Infrastructure Protection "of the need to adopt effective measures to prevent and combat possible attacks on critical information structures type. According to the "preamble" of this document, "... that part of the national infrastructure which is so vital that destruction or making it incapable of functioning can seriously diminish or defend the US economy ". The document stated that the critical infrastructure includes: telecommunications, electricity system and water supply, gas and oil deposits, finance and banks, emergency services (medical, police and fire) and the continuity of government.

This is the first legal document that defines critical infrastructure and lists its components and puts in place a mechanism for handling the matter.

In Europe, in the general context of increasing terrorist threats, as well as a more pragmatic approach of responding in times of disaster, in June 2004 the European Council asked for the preparation of an overall strategy to protect critical infrastructures. In response, on 20 October 2004, the Commission adopted a Communication on critical infrastructure protection in the fight against terrorism which put forward suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures.

On 17 November 2005 the Commission adopted a Green Paper on a European programme for critical infrastructure protection which provided policy options on the establishment of the programme and the Critical Infrastructure Warning Information Network.

The responses received to the Green Paper emphasised the added value of a Community framework concerning critical infrastructure protection. The need to increase the critical infrastructure protection capability in Europe and to help reducing vulnerabilities concerning critical infrastructures were acknowledged. The importance of the key principles of subsidiarity, proportionality and complementarity, as well as of stakeholder dialogue was emphasised.

In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a European programme for critical infrastructure protection ('EPCIP') and decided that it should be based on an all hazards approach while countering threats from terrorism as a priority. Under this approach, man-made, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority.

In April 2007 the Council adopted conclusions on the EPCIP in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders while welcoming the efforts of the Commission to develop a European procedure for the identification and designation of European critical infrastructures ('ECIs') and the assessment of the need to improve their protection.

On 8 December 2008 has been issued the Directive 2008/114 / EC of the European Union which stipulates the responsibility of Member States to identify critical infrastructures within national borders and establish and manage specific safeguards, the stated purpose of contributing to the protection of persons.

This Directive constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection.

The primary responsibility for the protection of ICE rests for the Member States and the owners / operators of infrastructure.

For the purposes of this Directive the following terms:

a. „critical infrastructure" means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;
b. 'European critical infrastructure' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant

impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure;

c. 'risk analysis' means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure;
d. 'sensitive critical infrastructure protection related information' means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations;
e. 'protection' means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability;
f. 'owners/operators of ECIs' means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive.

I.2. The concept of critical infrastructure in Romania

In Romania the first official approach to the concept appears in the Order no. 660 of 22 November 2005 the Ministry of Economy and Trade Order approving the "Guidelines for identification of critical infrastructure in the economy" published in Official Gazette no. 1099 of 6 December 2005.

Unfortunately, however, the guide did not make any reference to define the terminology to quantitative criteria or the methodology used for the identification of critical infrastructure. It summed up the importance delineate targets, already covered by legislation, of critical infrastructure that would be established at the level of each economic operator. Also it established selection criteria of critical infrastructure in the economy and scopes within its competence, limited to four fields: defence production, the industrial production, the energy and mineral resources.

Although Directive 2008/114 / EC of the European Union was issued on December 8, 2008, Romania fails to create a legal framework to harmonize this issue until on 3 November 2010 by the adoption by the government of Emergency Ordinance Government No. 98 on the identification, designation and protection of critical infrastructures. In the motivation of the urgent adoption of the ordinance are exposed the following:

- "Given that ensuring an adequate level of protection of critical infrastructure is essential for economic development, support of vital functions of society and the safety of citizens, and that adopting such legislation urgently could harm national security thanks significantly impact generated by the inability to maintain those functions to create the legal framework for the protection of critical infrastructure,

- Having regard to the obligation of transposition until 12 January 2011, the provisions of Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, published in the Official Journal European Union no. L 345 of 23 December 2008,

- Taking account of the need for the deadline specified a set of laws indispensable process of implementation of the Directive,

- Taking into account the procedures for the identification and designation of European Critical National Infrastructure and to be achieved by that date,

- Whereas the completion of the secondary normative framework, i.e. covering specific procedures is being conditioned by the existence of primary regulation on the protection of critical infrastructure, given that the delay fulfilment of correct transposition and full of Directive 2008/114 / EC of 8 December 2008 Romania will seriously harm consisting hinders access to EU funds made available by the European Commission's program of prevention, preparedness and management of the consequences of acts of terrorism and other security risks for 2007-2013, blocking the closure possibilities timely agreements between Romania and Member States of the European Union involved in the designation of European critical infrastructures, failure to complete the deadline of the process for the identification and designation of critical infrastructure and, consequently, lead to the triggering of the European Commission procedure infringement against Romania since the late conclusion of the bilateral / multilateral agreements with Member States of the European Union for the designation of critical infrastructure would put Romania in a position to forgo immediately informed and comprehensive overview of possible trans boundary effects disastrous due to disruption of facilities, services or vital systems Romania, on the territory of those Member States, coordinated and integrated implementation of measures at European level for the protection of critical infrastructure, as well as tools for limiting and eliminating the negative consequences of the disruption or destruction of such infrastructures. "

Government Emergency Ordinance no. 98 is approved by Law no. 18 of 11 March and clearly defines terms and expressions used this issue as follows:

a) *national critical infrastructure*, hereinafter ICN an asset, system or part thereof located on national territory, which is essential for maintaining vital functions of society, health, safety, security, welfare or economic status of persons and whose disruption or destruction would have a significant impact nationally because of the failure to maintain those functions;

b) *European critical infrastructure*, hereinafter referred to as ICE - a national critical infrastructure whose disruption or destruction would have a significant impact on at least two Member States of the European Union, hereinafter referred to as Member States. The significance is assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector relationships of dependence on other types of infrastructure;

c) *Critical infrastructure protection*, 'the PIC - any activity that aims at ensuring the functionality, continuity and integrity ICN / ICE to deter, mitigate and neutralize a threat, risk or vulnerability. In a non-exhaustive list, PIC includes activities successively on the assessment and risk analysis, ensuring the protection of classified information, development of security plans for operators of critical infrastructure, referred to as PSO, establishing liaison officers and the embodiment of communications, and exercises, reports, documents prepared revaluations and updates;

d) *Risk analysis* - analysing significant threat scenarios to assess the vulnerability and the potential impact of disruption or destruction of ICN / ICE;

e) *The responsible public authorities* - public authorities set out in Annex. 1;

f) *Owners / operators / managers* ICN / ICE are those entities responsible for investments in an asset, system or part thereof designated as ICN or ICE, according to the ordinance, and / or operation / management of their current;

g) *Critical thresholds* - limit values set according to the severity of the impact, disruption or destruction of an infrastructure that determines its identification as ICN / ICE;

h) *Critical Infrastructure Warning Information Network*, hereinafter CIWIN - secure information and communication aimed at assisting national institutions and the Member States to exchange information on vulnerabilities and appropriate measures to reduce their risk mitigation strategies;

i) *Sensitive data* on critical infrastructure protection information on critical infrastructure that could be used, if disclosed, for planning and realization of actions that cause disruption or destruction of critical infrastructure installations;

j) *Essential services* - those services, facilities or activities that are or may be required to provide a minimum standard of living and welfare of society and whose degradation or

interruption of their provision as a result of the disruption or destruction of physical system base would significantly affect the safety or security of the population and functioning state institutions.

The ordinance establishes responsibility for coordination at national level of the activities on the identification, designation and protection of critical infrastructures in the task prime minister who designates for this purpose a state councillor and incorporates the Centre for Coordination of Critical Infrastructure Protection (CCPIC) under the Ministry of Internal Affairs, that is responsible for organizing and conducting activities necessary to implement the Ordinance, namely the establishment of cooperation between the responsible public authorities and non-governmental structures. Also specifies that CCPIC ensure national contact point in relations with other Member States, European Commission, NATO and other international structures and management CIWIN at national level.

By Government Decision no. 1110 3 November 2010 at the Government level, under the coordination of state appointed councillor, shall be set up and functioning a institutional working group for PIC.

The group is active in the meetings held monthly or when the situation requires and has the following main responsibilities:

a) conducts cross-sectorial assessment of vulnerabilities, risks and threats to critical infrastructure;

b) analyses and formulates opinions for draft laws in the field of critical infrastructure protection to be approved / adopted by the Government;

c) reviews quarterly progress made in identifying critical infrastructure and advises the prime minister, through the state appointed councillor in respect with the state and the appropriate measures to improve work in the field;

d) analyses and proposes measures to implement an early warning system in the field of critical infrastructure and to improve it;

e) draws up guidelines / manuals of procedures and best practices;

f) shall promote, as a whole, the policies specific training and scientific research Critical Infrastructure Protection;

g) performs any other tasks, set by the Prime Minister.

II. NATIONAL STRATEGY ON CRITICAL INFRASTRUCTURE PROTECTION

The vulnerabilities, risk factors and threats in the protection of critical infrastructures are established by two regulations at the strategic level or "National Strategy for Critical Infrastructure Protection" approved by Government Decision No 718 of 13 July 2011 and the National Strategy of Defence for the period 2015 - 2019 "A strong Romania in Europe and the world".

II.1. VULNERABILITY, RISK FACTORS AND THREATS ON CRITICAL INFRASTRUCTURE PROTECTION

To properly handle the issue must be accurately defined terms used in the field.

Vulnerabilities represent the status quo, processes and phenomena that reduce the responsiveness of critical infrastructure in existing or potential risks or favour their emergence and development, with consequences in terms of functionality and utility. Ignorance or mismanagement of risk factors can generate vulnerabilities, threats or danger to the state of goals, values, interests and needs are subordinated to national critical infrastructure.

Risk factors designate situations, circumstances, factors, conditions or internal and external circumstances, sometimes doubled by action, causing or favouring a threat to critical infrastructures, according to a vulnerability determined, generating effects of insecurity.

Threats are capabilities, strategies, intentions, plans that enhances a threat to critical infrastructure, evidenced by attitudes, gestures, acts, which creates unbalanced or generates instability and danger and the impact on national security.

The states of concern are situations, events that may jeopardize or threaten the existence or the integrity of critical infrastructures.

Aggressions are attacks, including armed, endangering the existence of balance or integrity of critical infrastructures.

Critical infrastructure can be exposed to various types of risks and threats, depending on their mode of expression. General spectrum of risks and threats include natural events, technical failures, technological and human actions or terrorist attacks, cyber-attacks and other forms of expression which by nature or scale can affect critical infrastructure.

The deteriorating security at a international level and especially regional requires knowledge of the main threats, risks and vulnerabilities facing our country. The capacity of state institutions to assess and mitigate the impact of risks and threats is limited by the

persistence of vulnerabilities in critical infrastructure. The absence of a real multi-annual budgetary planning that entail investment and compliance programs, has negative effects on critical infrastructure protection module.

Inter-institutional reaction in crisis situations is affected by scarcity of resources and inconsistency in the management of various types of risks. This vulnerability is even more important if we consider the interoperability capability of the various state institutions must act in case of asymmetric and hybrid threats.

Regarding threats and assessments of the current security environment we have highlighted the main types of such events that may occur in the national territory:

a) **Organized crime**, especially cross-border, of which escalation may be enhanced by Romania's increasing role in supporting international policies to counter this phenomenon;

b) **Cyber threats** launched by hostile entity, state or non-state, the information infrastructure of strategic interest of public institutions and companies, cyber attacks carried out by groups of cyber crime or extremist cyber attacks launched by groups of hackers directly affect critical infrastructure.

c) **Terrorism** is a persistent threat, with manifestations difficult to anticipate and counteract

d) **Natural hazard** caused by natural phenomena;

e) **Technical failure**, interruptions in the operation of systems / equipment, in particular as a result of higher seniority in service and insufficient maintenance activities;

f) **Errors/human actions**, poor exploitation / unauthorized *intrusion*

II.2 PURPOSE AND STRATEGIC OBJECTIVES

The aim of the strategy is to provide the framework for the protection of critical infrastructures in order to promote national interests and the achievement made under alliances to which Romania is a party.

The strategy aims to:

a) establish benchmarks for the continuous development of national capacities for the protection of critical infrastructure;

b) harmonization of domestic legislation with the European Union and NATO in the field;

c) the involvement of all national authorities in the field, as well as private sector partners in formulating and implementing structural assembly and procedural measures to ensure a coordinated action at national level for identification, designation and protection of critical infrastructures.

The strategic objectives set at national level for critical infrastructure protection are:

a) Ensuring the unitary character of the identification, designation and protection of critical infrastructures national and European

b) harmonization of domestic legislation with the European Union and NATO in the field;

c) the involvement of all national authorities in the field, as well as private sector partners in formulating and implementing structural assembly and procedural measures to ensure a coordinated action at national level for identification, designation and protection of critical infrastructures.

The strategic objectives set at national level for critical infrastructure protection are:

a) Ensuring the unitary character of the identification, designation and protection of critical infrastructures national and European

b) Set up and operationalization of the national early warning networks by integrating all existing organizational and informational capabilities;

c) The correct evaluation of the level of vulnerability of critical infrastructures and identifying the measures required for preventive intervention and its reduction;

d) Develop the cooperation at the national, regional and international level in the field of critical infrastructure.

In order to achieve strategic objectives, all entities involved should consider:

a) highlight all existing or foreseeable risks, while identifying critical elements and processes;

b) eliminating malfunctions that may affect the stability and optimal functioning with the support of essential services critical infrastructure by implementing proactive measures in an effective risk management system;

c) increasing the expertise and updating risk analyses, including benchmarking with specific situations manifested in other states with translating these results into national standards;

d) compliance with data privacy and unauthorized dissemination of information which may affect the protection of critical infrastructure systems, under national legislation in force.

II.3 THE PRINCIPLES OF ACHIEVING THE CRITICAL INFRASTRUCTURE PROTECTION

The strategy is based on the following principles:

a) The principle of legality - the activities are carried out in the law and in accordance with it;

b) The principle of subsidiarity - ensuring decisions as close to the citizen, in parallel with the ongoing assessment of the need for action at national level with the existing regional or local existing plan;

c) The principle of complementarity - establishing a legal framework enabling the adoption of flexible ways and means connected to the specific current situation with harnessing and, where appropriate, adapt / develop mechanisms and measures to ensure the security of critical infrastructure already in place;

d) The principle of confidentiality - dissemination of information on critical infrastructure protection will be achieved within a framework that ensures the protection of those specific information whose disclosure could cause security vulnerabilities at those facilities. Information will be classified and access to them must be compliance with the principle of "need to know". Management and access to classified information shall be carried out according to the law, by the people who hold security clearance or authorization for access, valid for their secrecy level;

e) The principle of proportionality - protection measures will be proportionate to the level of risk accepted. By applying management techniques of risks, attention will be focused on areas with the potential highest risk, taking into account the threat, criticality probability of the risk, cost-effectiveness, the level of security and protection necessary the effectiveness of strategies available. The vulnerabilities of critical infrastructure will be classified according to the properties and potential effects in "acceptable" - which call for monitoring of the evolution and "critical" - involving active steps to limit / removal;

f) The principle of cooperation between holders - all critical infrastructure owners, operators and managers, including business and industry associations or standardization bodies, play a role in critical infrastructure protection. All holders should cooperate and contribute to the development and implementation of critical infrastructure protection according to their specific roles and responsibilities. Responsible public authorities should ensure the coordination of the development and implementation of policies and measures to

protect critical infrastructure in the fields of its competence. Owners, operators and managers of critical infrastructure will be involved at national and European level;

g) The principle of securing vital functions - priority in adopting and implementing protection measures will be those services, facilities or activities that are or may be required to maintain vital functions of society, health, safety, security, welfare or economic people and the disruption or destruction would have a significant impact nationally.

II.4 FINANCIAL IMPLICATIONS

Critical infrastructure protection activities require a combined effort and multidisciplinary in terms of human and material resources to be allocated according to skills in the field of responsible public authorities and owners, managers and / or operators of critical infrastructures.

The optimization of the resource management system for critical infrastructure protection could involve an increase in the share component information generated by the increase of their relevance in all areas of society, and as a result of diversification of threats targeting this area.

In this area several ministries have taken steps to allocate budgetary funds significant to ensure a high protection of critical infrastructure especially in the field of air transport (securing airports), the dams and power equipment (hydro, thermal power stations, transformer). The Ministry of Defence develops a major program of investment to develop and implement an integrated security system for defence area (military objectives) called SISOM.

II.5 THE MECHANISMS FOR IMPLEMENTING, MONITORING AND EVALUATION

In adopting procedures for implementation, monitoring and evaluation are considered the following coordinates:

a) legislative - updating / completing specific regulatory framework in relation to boundaries, powers and the powers of the institutions involved acting in protection of critical infrastructure;

b) institutional - developing the capacity to develop, implement, monitor and coordinate the implementation of goals;

c) human - development and training through: 1. professionalization of human resources involved in the identification and protection of critical infrastructure; 2. establishing "niches" band to create opportunities for specialization in Europe, which could put Romania in a position of training provider in the field;

d) cooperation between the public and private - to harmonize national measures, exchange of expertise and innovation in the field of research and development.

In the evaluation process are considered national criteria and assessment techniques established in all Member States of the European Union. Implementation at national level a mechanism for adequate communication between the responsible national authorities and liaison officers for security or their equivalents, in order to achieve the exchange of relevant information on risks and threats identified in the critical infrastructure in question is essential for monitoring and effective coordination of critical infrastructure protection activities short and medium term.

CONCLUSIONS

After analyzing legislation (national and European) have observed that the definition of critical infrastructure and ways to address their protection varies from one country to another, from one organization to another, but can identify common structural elements, measures taken to date , compatible functions and responsibilities.

A whole range of facilities or infrastructure can be considered critical because:

- Unique condition, and complementarity, within a system or process infrastructure;

- The vital importance they have as material support or virtual (network), in the operation and conduct of the economic, social, political, informational, military, etc .;

- The important role they fulfill in stability, reliability, security, functionality and, in particular, the security of the systems;

- Increased vulnerability to direct threats, as well as the targeting systems they belong.

Critical infrastructure helps support key strategic component of national security and require adequate protection.

Establishing security measures must cover both the organizational (internal security policies and strategies, which include instruction in an organized and security personnel) and physical and computer security systems that form critical infrastructure itself. The framework is necessary to ensure optimum and effective "early warning" and preventive intervention against risks that can affect the integrity and functionality of the systems infrastructure. Reliable, accurate and timely - mainly with proactive / predictive - is warning Instrument authorities to adopt appropriate countermeasures and crisis times to avoid "strategic surprises". Also revealing, in no time, actual developments in crises and potential effects help to optimize their management.

In my view an item imperative of protecting critical systems is to promote safety culture in the field, by working owner, operator, user and expert, based on information, education and regular training of the population, conducting simulation exercises to major incidents, from which to study how to coordinate the services provided by both the private sector and state authorities in these tasks.

Underfunding is one of the major causes that prevent application of protection measures for critical infrastructure viable and failure strategic objective no. 1

REFERENCES

[1] Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European Critical Infrastructure and the assessment of the need for improving their protection;

[2] M. Rizea - Critical infrastructure protection in the Euro-Atlantic area, Bucharest 2008;

[3] Order no. 660 of 22 November 2005 approving the "Guidelines for identification of critical infrastructure in the economy" published in Official Gazette no. 1099 of 6 December 2005.

[4] The Romanian Government Emergency Ordinance No. 98 on the identification, designation and protection of critical infrastructures published in the Official Gazette no. 757 of 12 November 2010.

[5] Law no. 18 of 11 March 2011 approving Government Emergency Ordinance no. 98/2010 regarding the identification, designation and protection of critical infrastructures published in the Official Gazette no. 183 of 16 March 2011.

[6] Government Decision no. 1110 3 November 2010 on the composition, powers and organization of inter-institutional working group Critical Infrastructure Protection published in Official Gazette no. 757 of 12 November 2010

[7] Government Decision no. 718 of 13 July 2011 National Strategy for Critical Infrastructure Protection published in Official Gazette no. 555 of August 4, 2011

[8] National Strategy for the period 2015-2019 Defense, a strong Romania in Europe and the world, the Presidential Administration, Bucharest, 2015

[9] Filofteia REPEZ - Publisher Critical infrastructure protection - needs this. Case study: The impact of the March 11, 2011 Tohoku Tsunami on the defensive elements of the critical infrastructure of Japan's - National Defense University "Carol I" Center for Strategic Studies of Defense and Security Strategic Colloquium no. 3, 2012

[10] Government Decision no. 585/2002 for approving the national standards for the protection of classified information in Romania, Official Gazette no. 485 of July 5, 2002

[11] Government Decision no. 1.154 / 2011 approving critical thresholds related cross-sector criteria to identify potential underlying national critical infrastructures and approving the Methodology for applying criteria related to cutting and critical thresholds determining the level of criticality, the Official Gazette no. 849/2011.

[12] Government Decision no. 271/2013 for the approval of Romania's cyber security strategy and national action plan on implementation of the national cyber security, Official Gazette, Part I no. 296 of 05/23/2013.

[13] Dr. Grigore ALEXANDRESCU, Dr. George VĂDUVA - Critical infrastructure. dangers, threats to their security systems - Publisher National Defence University "Carol I" Bucharest, 2006.

[14] Executive Order nr. 13010 - William J. Clinton for Critical Infrastructure Protection Federal Register page and date: 61 FR 37347; July 17, 1996