THE ANALYSIS OF BENCHMARKING APPLICATION IN CYBER SECURITY

Cătălin CIOACĂ, Alexandru BRATU, Daniel ȘTEFĂNESCU

"Henri Coandă" Air Force Academy, Braşov, Romania (catalin.cioaca@afahc.ro)

DOI: 10.19062/2247-3173.2017.19.2.8

Abstract: *Cyber security is a sensitive issue that derives from recognizing the existence of some vulnerabilities within the system. The current study analyzes a number of five national cyber security strategies, with particular emphasis on the specific features, in order to identify possible future directions. To identify the areas that need cyber defense improvement, based on the results of a benchmarking process, a simplified model is used, using cyber threats/ cyberattacks (CA) and information security (IS) as variables. By comparing national security strategies, it is desirable to disseminate best practices and integrate them on a global scale.*

Keywords: *cybersecurity, benchmarking, maturity indicator levels, Data Envelopment Analysis*

1. INTRODUCTION

The information environment is in a continuous dynamic, and with it the threats. Ensuring the availability, integrity and confidentiality of information has become one of the greatest concerns of modern society, in the context of integrating information technologies at all organizational levels as an essential condition for progress.

According to technological determinism, the most important factor in achieving success for an organization is technology [1]. "Technology push" investment programs in the military field have removed the fear of being "left behind" (low confidence in existing capabilities).

There is currently no generally accepted definition of "cyber security", which leads to different approaches (between states, between the public and private sectors, between different fields of activity), in the context where the need for cooperation in this field is unanimously recognized [2].

21 of the 28 NATO member states adopted a range of cyber security documents in 2010-2014: national security and defense strategy, national security information strategy, action plan, white carta.

The European Network and Information Security Agency (ENISA) is concerned about increasing the resilience of critical infrastructures against cyber threats, identifying in this regard a series of concrete actions that each strategy should include on the basis of the answers to the following questions: *What are the security requirements? What are the threats? To whom does this address? What are the vulnerabilities? Who is responsible for the prevention and response? What are the ways of cooperation and with whom?*

The International Telecommunication Union (ITU), an information security and networking agency, in partnership with ABI Research, has developed a Global Cyber Security Indicator (GCI) that assesses the cybernetic security level of each state from the perspective of five areas of interest: legislative, technical, organizational, action and cooperation [3,4].

By adopting the Cyber Security Strategy and the National Action Plan in 2013, Romania recognizes the existence of such threats and is concerned with maintaining a secure and resilient virtual environment that is an important pillar of national security and good governance [5].

2. BENCHMARKING. DESIGNING PERFORMANCE INDICATORS

The specialized literature offers a multitude of approaches to assessing and comparing the performance of organizations in different areas of activity. Such an approach in the field of cyber security must address a number of issues, such as: data collection (in an environment characterized by frequent changes), the quality of information (under explicitly uncertain conditions), the quantification of performance qualitative parameters or intangible results (e.g. innovation and adaptation capacity), the inclusion of sensitive data (ethical and legal barriers).

The military organization is subject to significant uncertainties in the connections between strategic units and functional cells. On the one hand, there is the influence of the external environment (dynamic security context, technological progress, budget constraints, operational capability requirements), and the impact on strategic units and cells on the other hand.

Defining performance indicators and identifying the best practices in the field does not fully solve this complex issue, as a series of challenges arise from the analysis of the data of potential evaluation partners:

- increasing expenditure (operational - against the background of system reliability requirements, training - ensuring the necessary staff training to avoid problems of inactivity, expanding and upgrading operational capabilities - infrastructure);
- the limited absorption capacity of investment funds in the national defense industry;
- overcoming institutional resistance to change (technical, operational or cultural).

The development of a model that incorporates the institutional benchmarking process becomes extremely useful in the decision making process in the context of the trend of updating the technologies with the existing challenges.

Performance indicators provide information about both the cyber security strategy as a whole and some specific activities. Table 1 presents the main (quantitative and qualitative) indicators on the basis of which a benchmarking study on cyber security can be carried out. The grouping of parameters is based on the set objectives, as follows: strategy and priorities; cyber security risk management at a national level; policies and regulations; assessing the responsible governance structure; involved parties; information transfer mechanisms; response capability from emergency plan views; organizing exercises; establishing the basic requirements [2].

The list of parameters and domains is not an exhaustive one. For enhancing cyber security capabilities at the organizational level; evaluation could include IT assets (traditional and emerging) or specific operations technologies (e.g. process control systems, control systems, and data acquisition).

The partial performance indicators method is very popular due to the low complexity of the calculations, but the results obtained provide a truncated image of the cyber security performance. For the interpretation of the results, additional data linked to specific conditions are required.

Table 1. The main areas under benchmarking

<table>
<tr>
<td>Strategy, objectives, priority
- the number of tasks completed according to the Action Plan
- the level of public trust
- existence of a national cybersecurity
- reports of improving resilience</td>
<td>Risk management
- the number of incidents during a period of time
- the impact incidents
- the number of critical infrastructures identified</td>
</tr>
<tr>
<td>Policy and regulations
- the complexity of procedures
- the number response capabilities
- the number of documents adopted after the promulgation strategy</td>
<td rowspan="3">Evaluation of responsible governance structure
- the number of shares executed and state actions;
- the number of tasks/ responsibilities unassigned
- type response chain of command
- the number of cooperation mechanisms, procedures and communication channels that do not work</td>
</tr>
<tr>
<td>Stakeholders
- the number of stakeholders
- the number of existing working groups</td>
</tr>
<tr>
<td>Information transfer mechanisms
- indicate the use of information exchange platform
- the number of measures/ actions taken as a result of analysis of the data;
- the number of parties involved;
- the number of newly identifield threats and vulnerabilities</td>
</tr>
<tr>
<td>Organizing exercises
- the number of exercises performed;
- the status evaluation reports;
- the number of sectors involved;
- the number of persons involved;
- the involvement of the public sector;
- the numbers of plans/ procedures tested</td>
<td>Responsiveness in terms of emergency plans
- the number of activities in the national plan completed on time;
- the number of sectors and stakeholders in the development plan;
- the number of exercises conducted to test the plan;
- the level of trening in response to a cyberattack on different scenarios;
- the existence of crisis management facilities</td>
</tr>
</table>

The Stochastic Frontier Analysis (SFA) method is an extension of the simple regression method, aiming at estimating a border of the security function with different intermediate levels of efficiency.

The Data Envelopment Analysis (DEA) method is a method of calculating the relative efficiency by referring to the best examples of good practice in the reporting group. It involves the use of mathematical programming methods to determine a boundary of good practice, the efficiency being calculated by reference to this limit.

In order to quantify the qualitative parameters the maturity level indicator is used [6]. This tool allows, in a relatively short time and with a flexible approach, the assessment of cyber security capacity, the identification of improvement solutions and the prioritization of investment actions in the field. Examples of risk management are the design of the maturity indicator level (MIL) as follows:

MIL 1 - cyber risks are identified;

- the identified risks are managed (e.g. accepted, tolerated, transferred).

MIL 2 - risks are evaluated according to the management strategy;

- identified risks are authenticated;
- response actions are prioritized;
- the risks are monitored;

- risk analysis is carried out on IT architecture.

MIL 3 - policies and procedures for implementing the risk management strategy are different from the risk management program.

3. USING THE DATA ENVELOPMENT ANALYSIS METHOD

The Data Envelopment Analysis method (DEA) is considered one of the most successful methods for assessing effectiveness. DEA is a method of calculating relative efficiency by referring to best practice models in the reporting group.

In order to determine a boundary of good practice, mathematical programming techniques are used. The limit of good practice is nonparametric and entries may be variable or fixed. The method has the advantage of being able to work with a large number of variables and their restrictions.

To illustrate the relative efficiency assessment mode based on the DEA method, there is a simple example of comparative analysis of five national cyber security strategies (corresponding to Romania, Spain, Great Britain, Poland and Latvia) aiming at establishing and implementing the legislative framework [7,8,9,10,11]. They produce a single output variable, ***the development of cyber defense capabilities***, using two input variables: ***cyber threats/ cyberattacks prevention*** and ***information security*** (IS).

For each of the two input variables the are defined the Maturity Indicators Levels of Strategy (MILS). The levels, which are not cumulative, are highlighted in Table 2.

Table 2. Defining the maturity indicator levels for strategies

<table>
<tr><td colspan="3">Preventing threats/ cyberattacks</td></tr>
<tr><td>MILS 1</td><td>- one activity</td><td rowspan="4">- legislative measures;
- stimulating and funding initiatives to develop secure systems;
- participation in regional and international cooperation;
- increased capacity of law enforcement;
- warning systems and reporting.</td></tr>
<tr><td>MILS 2</td><td>- two activities</td></tr>
<tr><td>MILS 3</td><td>- three or four activities</td></tr>
<tr><td>MILS 4</td><td>- five activities</td></tr>
<tr><td colspan="3">Information Security</td></tr>
<tr><td>MILS 1</td><td>- one activity</td><td rowspan="4">- coordination between (public-private) involved;
- ensuring the confidentiality, integrity and accessibility of information and services;
- reducing or eliminating disruptions in vital services company;
- increasing the capacity of critical information infrastructure protection;
- secure and reliable cyberspace.</td></tr>
<tr><td>MILS 2</td><td>- two activities</td></tr>
<tr><td>MILS 3</td><td>- three or four activities</td></tr>
<tr><td>MILS 4</td><td>- five activities</td></tr>
</table>

Significant differences between entry and exit data of the security strategies of the countries in this example allow for an immediate comparison of efficiency. Because these reports mean inputs/ outputs, a strategy is all the more effective as these reports, meaning the points in Figure 1, are closer to the origin of the axle system.

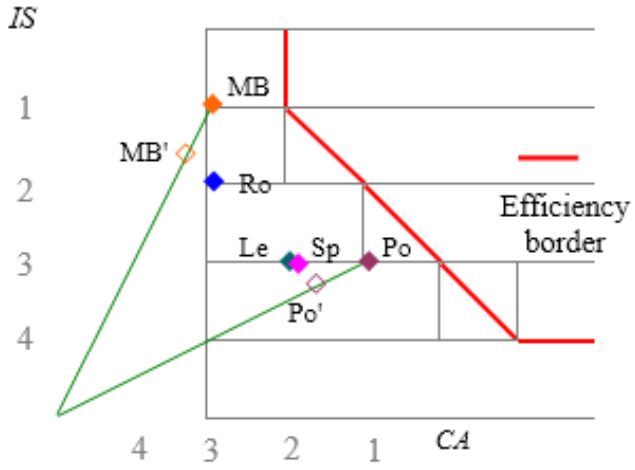

FIG. 1. The representation of the efficiency calculation using DEA

Significant differences between entry and exit data of the security strategies of the countries in this example allow for an immediate comparison of efficiency. Because these reports mean inputs/ outputs, a strategy is all the more effective as these reports, meaning the points in Figure 1, are closer to the origin of the axle system.

The linear Ro-Le curve represents the limit of good practice, the points on it being considered as having a 100% efficiency. So, in the case considered, national cyber security strategies in Romania, Spain and Latvia have an efficiency ratio of 1,0. The Ro-Le curve, also referred to as the unit of isolation (meaning the set of input pairs generating a unit output), allows the measurement of the inefficiency of the strategies that are not located on it. Thus, strategies above the efficiency limit are considered ineffective, consuming larger quantities of inputs to produce a single output unit. To become effective, strategies in the UK and Poland need to reach the MB' or Po' points on the efficiency limit. Their efficiency is given by the ratio between the distance from the origin to the projection of the efficiency limit point and the distance between point and origin.

Another important feature of DEA is predicted in the context of benchmarking. Analyzing the case of the Po strategy, it is clear from the figure that it tends to produce the same results as the Sp and Le strategies belonging to the maximum efficiency curve. However, the strategy to which it relates to establishing relative efficiency is Po', a virtual point on the edge of good practice. The Po' virtual strategy is a combination of the characteristics of the Sp and Le strategies. Therefore, DEA can identify the corresponding pairs with which inefficient strategies can be compared to improve efficiency. Representations in the entry / entry space, as in the example above, are also input-oriented measures.

The study is easy to be graphically represented and interpreted, but if more input and output variables are considered, DEA can no longer be graphically illustrated. In such cases, it is necessary to use linear programming methods for determining the efficiency coefficients and the optimization potential for each of the national cyber security strategies compared.

4. CONCLUSIONS

Ensuring cyber security is more than just a national issue, with the increasing number of threats/ cyberattacks with serious consequences on critical structures, but also on organizations in all areas of activity.

From a security point of view, the IT field experiences a "bipolar cold war": attacked and attacker. The latent, scalable, and accurate detection of threats are features of cyber security tools.

At an European level, ENISA has initiated an assessment of national cyber security strategies without attempting to compare, but rather to explore the state of implementation of these.

Awareness of cyber security risks and motivation to step up national actions in this area can initiate a cybersecurity benchmarking process at international level (including Euro and/ or non-Euro countries).

REFERENCES

[1] D. Chandler, Technological or Media Determinism, 2000. [Online] Available on: http://www.aber.ac.uk/media/Documents/tecdet/tdet01.html;

[2] European Network and Information Security Agency (ENISA), *National Cyber Security Strategies. Practical Guide on Development and Execution.* December 2012. Available on: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport;

[3] ABI Research and International Telecommunication Union (ITU), *Global Cybersecurity Index and Cyberwellness profiles Report.* WSIS Forum'15 Geneva, 2015. Available on: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf.

[4] International Telecomunication Union (ITU), *Global Cybersecurity Index & Cyberwellness Profiles. Report*. ABI Research, 2015. Available on: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf;

[5] *** Government Decision no. 271/2013 for the approval of the Romanian Cyber Security Strategy and the National Action Plan on the Implementation of the National Cyber Security System, published in the Official Monitor, Part I no. 296, 2013;

[6] US Department of Homeland Security (USDHS), Department of Energy, *Cyber security Capability Maturity Model (C2M2),* Version 1.1, February 2014. Available on: http://energy.gov/oe/services/ cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/ cybersecurity;

[7] Ministry of Defence, Government of Estonia, Cyber Security Strategy. Tallinn, 2008. As of 5 May, 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf

[8] Ministry of Administration and Digitation, Internal Security Agency, Republic of Poland, *Cyberspace Protection Policy of the Republic of Poland.* Warsaw. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ copy_of_PO_NCSS.pdf;

[9] Romanian Government, National Cybersecurity Strategy, 2013. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ StrategiaDeSecuritateCiberneticaARomaniei.pdf;

[10] Federal Republic of Germany, *Cyber Security Strategy for Germany*, 2011. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Germancybersecuritystrategy20111.pdf;

[11] Cabinet Office, United Kingdom. *The UK cyber Security Strategy: Protecting and promoting the UK in a digital world*, 2011. As of 5 May 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/UK_NCSS.pdf.