ANALYSIS OF PORT SECURITY

Nicolae ZAVERGIU, PhD Candidate [1]
Eugen SITEANU, PhD [2]

Abstract: *The hybrid war in Ukraine has emphasized again the security problem in the Extended Black Sea Area and, obviously, in its ports. Our study aims to analyze port security in the context of the new security environment, in which several EU member states show a desire to move toward the Russian Federation which worries the states in the Extended Black Sea Area. The authors focus on three key concepts: optimum reliability, optimum viability and optimum security.*

Keywords: *port security, analysis, risks, threats and dangers.*

Introduction

In the last years on the global scene there were a series of strategic shifts/changes generated by United States intention to shift its security strategic/effort towards Asia-Pacific area. This is why the Russian Federation is concerned with controlling the Black Sea Region and the Danube Mouths and with turning this Sea into a "Russian Sea" in order to get access to the Mediterranean Sea. These circumstances would allow the Russian Federation to gain military superiority in the Black Sea.

In this respect, we think it is necessary for Romania to strengthen its ports' security. The military protection of Romanian ports must be extended beyond Romanian borders, enforcing the state power at the Danube Mouths and into the Black Sea Area.

[1] Chief Security Officer – Midia, Maritime Ports Administration National Company S.A. Constanta, Telephone: 0730. 019. 398, email: nzavergiu@constantza-port.ro.
[2] Professor, corresponding member of the Academy of Romanian Scientists, adviser of the president of "Alexandru Ioan Cuza" National Association of Reserve and Retired Militaries, vice president of the Association of "Carol I" National Defense University Graduates, member of the Editorial Board and co-editor of the Military Magazine, email: esiteanu@yahoo.com.

Any port can be considered or analyzed as a system within the general theory of systems. During the process of building and developing ports, depending on the requirements that need to be fulfilled and the terms imposed upon them, a gap appears between the time when ports were built or a phase in their development and the one of the current date; the gap is bigger if there is a big time difference between the former and the latter. The gap is a consequence of technology, time and other factors which determine dangerous behaviors of the system (in our case, the port) if disturbing forces act upon it affecting people, equipment, ships, infrastructures and other facilities or materials. These disturbing forces do not act only in real life, but also in the virtual reality that can be found in the cybernetic environment. However, their effects are felt in real life.

Thus, it is necessary to do a special analysis of the systems' (ports') security based on the theory of reliability and viability of systems and some new methods.

In the literature in the field, there are different security concepts: *timely security, sufficient security, total security, minimum security, maximum security, absolute security, durable security or vital security* – as an extension of the concept of sustainable (vital) development – optimum security, minimum security or obligatory security and others.[3]

Port security is both a functional and a social problem because the lack of security can result in various damage and also information theft or data corruption.

It must be understood that the aim of building a port is not about creating a structure in itself, but a structure that ensures the operational capacity of obtaining the technical, economic, social and military projected effects safely. Still, we should always take into account that we cannot ensure a complete security against terrorist activities for a maritime or fluvial port, but we can reduce the effects of the terrorist attacks by using resources reasonably and first and foremost by using financial resources. Identifying the weak/vulnerable points, staying alert all the time and knowing the security measures perfectly can ensure the increase of ports' security level.

[3] Gheorghe Ilie, *Risk and security,* volume I, UTI Press House Publishing, Bucharest, 2015, p. 11.

Nicolae Dolghin, Alexandra Sarchinschi and Mihai Dinu, in the paper called "Risks and threats that can jeopardize Romania's national security. Actuality and perspective", published in 2004, consider that there are three types of risks and threats that can jeopardize our country's south-eastern border: non-military, military, and asymmetric and transnational risks.

The concept of reliability refers to a system's (port's) capacity to fulfill its functions specified in time, if it used in the context which it was built (and modernized) for and if it is maintained and repaired correctly. So, the reliability (R) of a system (port) has two components: safe functioning (S) and maintenance (M); mathematically speaking this is:

$$R = S + M, \tag{1}$$

Reliability is analyzed in terms of the connections, the causes, the factors that influence it, the effects and the behavior of the composing subsystems and the interactions among them.

The following relation can be deducted based on the theory of reliability and the General Theory of Systems (GTS):[4]

$$R = \sum_{i=1}^{K} p_i \cdot R_i + R' \tag{2}$$

k – the number of the composing subsystems;
R_i – the reliability of i subsystem;
p_i – the functional share of i subsystem;
R' – a component due to the system's organization

Thus, reliability is a quality characteristic of any system and it depends on the influence of all the composing subsystems, and also on the synergy of the system's organization; the failure of a subsystem can cause the system's failure (a breakdown in functioning or a functional error).

There is an organic connection between the quality and the reliability of the port system because quality means the sum of the necessary properties for the right use of the port, and reliability is its capacity to maintain its quality in time. It results that the best value of reliability

[4] Ibidem, p. 17.

corresponds to the minimum costs intended for preserving Reliability (figure no. 1).

Viability (V) can be defined based on the Reliability of the port system as follows: "Its capacity to preserve its characteristics (functional, operational and relational and informational), in case the variations of its entry values, external or internal disturbances, cause major changes (or similar consequences) of the conditions which it has been projected for".[5]

Major changes refer to the functioning situations (cases) in exceptional conditions (which have as a result breakdowns in functioning, functional errors or exceptions). Exceptions are some diversions from the normal values of the functioning parameters, and these deviations are considered to be errors.

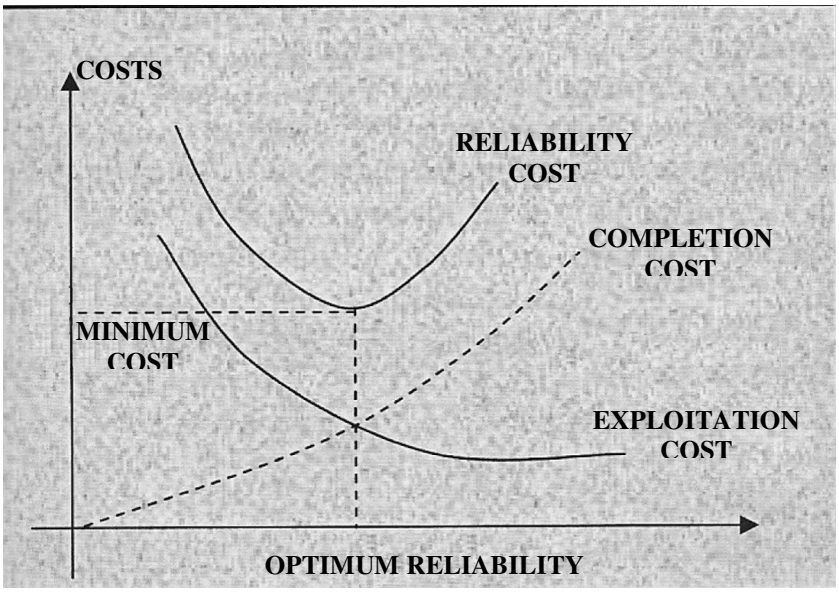

Figure no. 1. Determining optimum reliability
Source: Gheorghe Ilie, Risk and security, articles, communications, lectures, volume 1, Articles published in Alarma magazine, 2005-2011, UTI Press publishing House, Bucharest, 2015.

[5] Ibidem, p. 19.

Viability (V) represents the sum of the reconfiguration/readjustment (Ra) and the functioning reserve (M') which is similar to Maintenance (M) and has the following mathematical expression:

$$V=Ra+M' \quad (3)$$

There is an organic link between viability and reliability, just as there is one between security and viability because security represents the essential qualitative property of systems and organizations.

Security is the essential qualitative property of systems and organizations, or, in our case, of ports, their capacity to function safely, to preserve their functioning characteristics against risks, threats, and dangers through avoidance, attenuation or restyling and to readapt themselves functionally.[6]

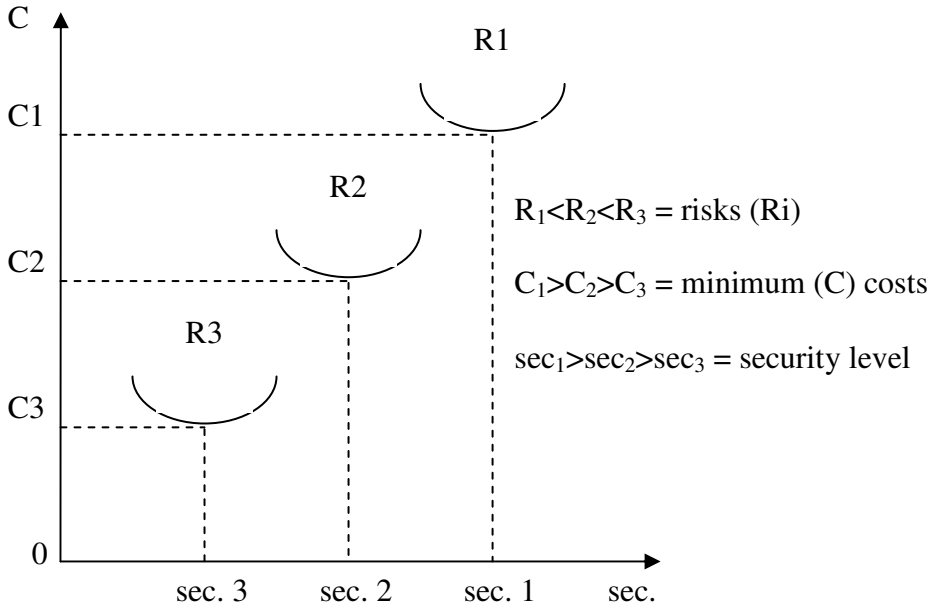

Figure no. 2 Determining optimum security

[6] Gheorghe Ilie, *Risk and security, articles, communications, lectures*, volume 1, Articles published in Alarma magazine, 2005-2011, UTI Press publishing House, Bucharest, 2015, p. 22.

Yet, risks, threats and dangers act both in real life and digital (cybernetic) environment, affecting ports' infrastructures.

In our opinion, ports' security represents the property of the essential quality of port systems (organizations), their capacity to preserve their functional characteristics against risks, threats and dangers by avoidance, attenuation or Restyling (Cv), safe functioning (s) and functional readjustment (Ra) to the new conditions of the security environment.

$$Sec = Cv+Ra+S \tag{4}$$

The smaller the assumed operational risk (Ri) is, the bigger the value of the optimum economic threshold (A) of the security system is and also the value of the security is bigger (R=1-A).

We can also express ports' security as follows[7]:

$$Sec = \sum_{i=1}^{n} m_i \cdot S_i + Sc \tag{5}$$

where:

n = the number of domains that contribute to security (economically, socially, culturally, religiously, politically, militarily, technically, scientifically, nutritionally, energetically, etc.)

S_i = the security of i domain;

m_i = the share of i domain;

Sc = the component resulting from the characteristics of the security system;

If we take into account only those domains that contribute to ports' security, it appears that each domain's (subsystem's) security influences ports' security with a certain share (which is determined by the place that this one occupies in the security system). The exceptions from the normal functioning of the system or errors, irrespective of their nature, can cause failures, deteriorations and malfunctions of the port's system.

[7] Ibidem, p. 23.

Just as in the case of reliability and viability, the value of security depends on costs (expenses for security), determining their optimum value (for the minimum costs), according to costs and risk assumption.

The consequence that results from here is that according to costs and risk assumption, the dynamics of security corresponds to the curves in figure no. 2.

Our analysis of security has shown that the security measures and mechanisms are perishable in time due to the moral consumption or ageing of the used technologies so that if we do not maintain and replace the old technologies periodically, every security mechanism or system can be compromised at a certain moment.

Conclusions

In conclusion, there is a need for new approaches to ensure greater port security at a lower cost by joint completion (production), exploitation (maintenance) and reliability efforts in a time of financial austerity.

BIBLIOGRAPHY

ILIE Ghe., *Risk and security, articles, communications, lectures*, volume 1, Articles published in Alarma magazine, 2005-2011, UTI Press publishing House, Bucharest, 2015.