NEW APPROACH FOR ENHANCEMENT OF CRITICAL ENTITIES RESILIENCE AGAINST TERRORIST THREATS

Kiril Stoychev

University of National and World Economy
Bulgaria

* Corresponding Author, e-mail: kstoichev@unwe.bg

Abstract: In critical infrastructure security research, multiple solutions are proposed based on different approaches used. An attempt will be made here to present an integrated new approach in cases where organizations take actions to increase the entities resilience. The new approach is mainly based on the existing standardization base that affects the relevant elements of security systems. The main results of the research are the proposed resilience levels that are the main elements of the structure of the business organization. The identification of resilience levels is the basis of the assessment of the degree of trust in the organization which the security systems form in the users of its services, as well as in the society.

Key words: new approach; critical entities; security/resilience levels; information security; integrated security management system.

1. INTRODUCTION

This publication sets one main limitation - a new approach for the security and protection of critical infrastructure against threats caused by human activity will be considered, related to terrorist attacks! Those threats related to the unscrupulous human activity, to accidents caused by technical and technological problems, as well as those related to threats to critical infrastructure, from natural disasters, are not considered in this publication!

At the same time, taking into account the fact that Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 introduces new terminology, in this publication the term "critical entity" will be used instead of "critical infrastructure" [1]. As well as instead of „security and protection of critical infrastructure“ and “security levels”, "resilience of critical entities" and “resilience levels” will be used!

Based on the above limitation, it should be noted that threats caused by human actions to the security of critical entities are primarily the result of terrorist attacks.

In the last two years, the intensity of international terrorism has been "blunted" against the backdrop of regional military conflicts that have arisen in a number of regions around the world, and which are at the basis of a reasonable assumption by all people that there is a real risk of a global crisis in the long term.

And this crisis is present since we cannot ignore the fact that a war has been raging in Ukraine for the third year already, as well as the fact that the crisis between Israel and Palestine forms an international situation unseen during the years of this century! And which situation affects all aspects of public life!

However, regardless of this (that against the array of military conflicts, terrorism "remained in the background"), terrorist threats are a real prerequisite for daily searching for new and new approaches to adequately respond to them.

As a result of all that, in Europe a common ground has been laid in the fields of politics, economics, social, defence and law which aims at consolidation of the military, political, economic, social and other aspects of the security in the different countries and in the community as a whole.

And one of these aspects is strengthening the resilience of critical entities as a fundamental, unavoidable factor in guaranteeing the very existence of the population of the Earth - directly and indirectly.

From this point of view, the approaches of the individual states for identification of the threats and building adequate security and protection systems of the critical entities are various, generally not grounded on internationally accepted requirements which contributes to non-achievement of the desired level of entity resilience – the efforts are directed first of all to the technical and technological parts of these systems.

There are separate cases when the accent is placed also on the organizational part, such as for instance, the development at European level of standardized requirements and procedures for the activity of the operators of security and protection systems, especially in the field of nuclear security. In the present publication we categorically deduce the problem that there is no developed integrated approach for ensuring the resilience of the critical entities to show clearly and accurately the achieved resilience degree of the respective entity?

Just on the basis of the above said it should be noted that the present publication contributes in a significant degree to creation of new, innovative approach for improvement of the struggle against the terrorism by working out a new approach for building and assessment of integrated systems for management of the security of the critical entities.

The publication uses the terms “security levels”, “security layers” and “resilience levels”, which should be considered synonymous as well as “organization” and “entity”.

2. RELATED WORK

In response to the necessity of strengthening the capability of the European community (EC) to prevent terrorist assaults affecting the critical infrastructure as well as to optimize the readiness of the Community to react to them on December 8, 2008, a Directive 2008/114/EO of the EC Council was accepted concerning determination and designation of European critical infrastructures and assessment of the necessity to improve their protection (on November 17, 2005, the European Commission accepted Green book concerning European program for protection of the critical infrastructures).

In 2019, the EC Council evaluated this directive and found, that due to the increasingly interconnected and cross-border nature of activities using critical infrastructures, security measures are not sufficient to prevent threats of any nature [1].

In this regard on 14 December 2022 was approved Directive (EU) 2022/2557 of the European parliament and the Council on the resilience of the critical entities and repealing Council Directive 2008/114/EC (unfortunately, the European Commission on November 28, 2024 called on Bulgaria and 23 other Member States to implement the Directive in these countries).

By accepting the Directive, the bases are laid for systematization of the efforts of EC member countries in response to their will to increase to the required volume the resilience of the critical entities in the fields of "energetics", "transport", "banking", "financial market infrastructure", "healthcare", "drinking water", "wastewater", "digital infrastructure", "public administration", "Space" and "food production and processing".

But the above said requirements present only the frame of the EC policy in this field. It gives only and solely the directions while the national governments should develop in detail the requirements and make them workable for their concrete infrastructures. In support of the latter, Para (6) of Directive (EU) 2022/2557 recognises, that „some Member States have less stringent security requirements on those entities not only leads to various levels of resilience but also risks negatively impacting the maintenance of vital societal functions or economic activities across the Union …..".

It is precisely these different security requirements, which the relevant authorized bodies in the Member States determine, that require a unification of the approach to building this security and its assessment, in order to achieve the planned resilience of critical entities.

On the base of the above said it is necessary to note that for security levels or security degrees in the scientific community in Bulgaria and around the world there are many developments. Thus, for instance, next five security levels are specified in [2]:

- The first level is security of the individual (security of the single person, security of the personality), called differently – „individual", „personal", „human", etc.;
- The second level is security of the Group of individuals or group security;
- The third level is security of the State;
- The fourth level is security of the Community of states - i.e. collective, community, alliance, coalition security;
- The fifth level is security of the World (the planet) - i.e. global, common, cooperative, comprehensive security.

In addition, individual security, group security, state security, regional security, global security, national and international security are formalized in [3].

The law enforcement authorities in the individual states determine different threat degrees or the so called by them „security levels", whose purpose is first of all the struggle against the primary source of terrorist threats.

As seen from the above said the differentiation of the security in degrees and levels is applied to achieve various aims in the considered area but not for ensuring the resilience of the critical entities.

On the other hand, if we say that there are no theoretical developments or realized in practice integrated systems for resilience of the critical entities will be incorrect to our colleagues in this field. But in one or other degree they present different in complexity models that would hardly answer adequately the question „How sure are we that we have ensured 100% security and protection of the respective object?". In the structure of these models and used approaches single components of the business organization management system are included but the practice has shown that these are not all management subsystems. Thus, for instance, the scientists from the University of Applied Sciences, Brandenburg, Germany, treat the integrated security and protection system as combination of only the subsystems: for quality securing and control in compliance with standard ISO 9001;

environmental protection in compliance with ISO 14001; information security in compliance with ISO 27001 and security of supplies in compliance with ISO 28001 [4].

That is why it is necessary to cover in an integrated approach for use in practice all of the elements of management subsystems in the business organization that are relevant to their resilience.

3. DESCRIPTION OF THE PROBLEM AND PROPOSED SOLUTION

3.1. General conditions

But whether the actions taken by the various bodies and organizations in the field of ensuring the security of the critical entities are sufficient to achieve the necessary level of resilience, taking into account the dynamics in the international situation? The latter is saturated with all possible crisis situations, predisposing the environment to increase the risks to the critical infrastructure!

On the other hand, in Para. (36) of Directive (EU) 2022/2557, the Commission organises an advisory mission to assess the resilience measures put in place by the critical entity concerned. And in Para. (37) of the Directive, the Commission established a Critical Entities Resilience Group as a Commission expert group. But neither for the expert group nor for the advisory mission does the Directive provide a unified, systematized and comprehensive basis whereby the results obtained from the group's activities and the conduct of the mission would be objective and correspond to reality.

From this point of view, the development and implementation of a generally accepted approach for the creation of minimum and mandatory requirements for the creation of an adequate security system of the critical entities to counter potential terrorist threats, should become the next step in the implementation of Directive (EU) 2022/2557. In this way we shall succeed to contribute to the development of integrated approach in this field which can be a base of comprehensive approach (Para. (13) of the Directive) for the successful application of the strategy for enhancing the resilience of critical entities.

In the same time there are numerous international and national requirements providing physical and informational security of the critical entities and guaranteeing their continuous operation as well as ensuring financial security, environment protection, health and labour safety, human resources management, corporative social responsibility and many others. All they are directly or indirectly connected with the providing of the security and protection of the corresponding object of critical infrastructure. Large part is unified by integrated methodologies but between the individual requirements to the respective systems, in most of the cases, there is no interconnection.

So, how we can assess to what degree the resilience of an entity is ensured so that we can be confident that its continuous functioning will be ensured even after a terrorist attack? This is of utmost importance and in most of the cases it is vitally determinative for the health and life of the workers and employees in the organization and the society. For the purposes of applying an integrated approach it is necessary to determine the frame of resilience levels of critical entities, to determine and systematize their requirements.

The main problem identified in the process of numerous examinations of the available information is the absence of approved theory and generally accepted practice in relation to the resilience of critical entities as a guarantee for the health and life of the population and the completeness of the material valuables at national, regional and international level as well as clear, standardized and/or norm-specified criteria for determination of the resilience degree of the entities and for their objective assessment.

Main purpose of the present publication is to provide contribution in the progress of the theory and practice for improvement of the resilience of the critical entities through creation of a new comprehensive approach and determination of requirements frame for the building and assessment of integrated security systems in support of the implementation of Directive (EU) 2022/2557, but not only.

3.2. Nature of the New Approach

As already noted, the above said is only one of the many examples where incomplete integrity is observed of all related to the resilience of the critical entities components of the business organization's management system.

Therefore, here we shall try to outline the structure of the new comprehensive approach for development of integrated security and protection of these organizations, leading to an increased level of resilience of critical entities.

When we talk about integrity, it is necessary to define the connecting link between the individual elements of the security system. For ensuring the resilience of critical entities, the role of such a solder is proposed to be played by Business Continuity Management.

On this basis we offer structure and content of resilience levels the building of which determines the succession of activities that regulate the realization of the approach for creation of integrated security management system.

In the same time, it is necessary to specify in what manner the requirements to these resilience levels should be formalized.

These levels of resilience, their content, procedures for construction and assessment can be adopted and implemented by using the available standardization base, but not only! The proposed approach can be described in a separate standardization document or procedure adopted by the Commission or Commission expert group for implementation in practices of the Member States (Article 16 of the Directive 2022/2557).

Or even more clearly, by building levels of resilience of the critical entity against terrorist threats, an integrated security management system is created, leading to the full satisfaction of the entity's needs to guarantee the reliability and continuity of its activities.

The various aspects of building security management systems are regulated by numbers of departmental, national, regional or international normative documents or those in the field of standardization. The main ones that determine the frame of requirements are developed and accepted by International Standardization Organization in the fields as (without guarantees of completeness): information security; business continuity management; security management; risk assessment, etc. [5].

All they define detailed requirements to the various aspects of the organization resilience process and contribute in a significant degree to enhancement of its security in general.

However, at the same time, there are two basic objective facts that do not allow these and related to them other documents to ensure the so necessary efficiency of the efforts in direction of building the required resilience level for the corresponding critical entity:

- They are deficient in unified structure and general terms and basic definitions. Not until 2011 the International Standardization Organization laid the beginning of a new approach for determination of the requirements to the management of the

organization (the entity) – creation of integrated ISO Management System Standards;
- There is no generally accepted methodology or approach for binding them in a unified system.

At the same time, various methods are introduced to determine the relevant safety levels (especially in nuclear energy and not only).

The valid European standards define four levels of safety. The highest is the reliability of Fourth level and the lowest one is a First level.

On the other hand, in determination of the information security the following three architectural levels are used: Strategic; Logic; Technologic (frequently called realization level).

In continuation of the above, Gartner Inc. proposes the Cybersecurity Mesh Architecture Approach to include the following layers [6]:

- ✓ Identity fabric layer enable;
- ✓ Security analytics and intelligence layer;
- ✓ Consolidated policy management layer;
- ✓ Consolidated dashboard layer.

All this brings to the fore the need to formulate certain levels to ensure the maximum resilience of critical entities.

In order to overcome these problems (deficiency of sufficiently clear, systematized and in-depth approaches to build the organization's security systems - to be understood absence of assessment criteria for resilience level), it is necessary the maximum use of available standardization, regulatory and institutional tools to create high levels of resilience and it is necessary to rely on the already accumulated vast experience from the implementation of some of them. For example, these documents and approaches can be used in the field of information security or ensuring internal security, and the scientific community and practicing professionals can unite around unified approaches for their complex use in order to increase the level of resilience of the entity.

Bearing in mind the above, it is necessary to note that the management system of any organization/entity consists of multiple subsystems, the collective functioning of which determines its function, in one direction or another, depending on the "maturity" of each subsystem. **If these subsystems are designed with the resilience of the organization in mind**, then the resilience elements/levels of integrated security system can be defined as follows:

- Risk Assessment;
- Business Continuity Management;
- Safety;
- Quality Assurance;
- Information Security;
- Financial Security;
- Human Resources;
- Corporate Social Responsibility;
- Environmental Security;
- Internal Security;
- External Security.

4. PRESENTATION OF THE RESULTS AND DISCUSSIONS

Above all, there are two main elements in the organization's management system - analysis and assessment of risk (Risk Assessment) and Business Continuity Management (BCM).

Risk Assessment is the basis of the development of modern management systems. The formation of each of the subsystems of the organization's management system requires the presence of a risk analysis. By themselves, risk analysis and assessment cannot be an independent subsystem/level in the organization's management. It is a process on which the expected functioning of each subsystem depends. Analysing and evaluating not only the external, but also the internal environment in which the organization functions, results are obtained, which are used as input information for the successful operation of each subsystem! In this case, the analysis and assessment of the security environment enables the assessment of the resilience threats in each subsystem or level of resilience proposed below in the publication.

Another basic element of an organization's management system is business continuity management. Unlike analysis and risk assessment, which as a process stand at the very beginning of the "chain" of actions accompanying the construction of a complete management system of the organization, BCM stands at the end of this "chain"! The development of each subsystem of the management system must consider the need to comply with BCM issues, i.e., include elements that guarantee its uptime and reliability. At the same time, BCM is also an independent subsystem that interacts with all others and ensures the continuity of operation of the entire management system of the organization.

Considering the above, we can formulate the following levels of resilience for critical entities, forming an integrated security management system:

First level RA, IS (Risk Assessment and Internal Security);

Second level RA, IS, ES (External Security);

Third level RA, IS, ES, QA (Quality Assurance), Safety;

Fourth level RA, IS, ES, QA, Safety, Information Security (ITSEC), Human Resources, Financial Security (FINSEC);

Fifth level RA, IS, ES, QA, Safety, ITSEC, Human Resources, FINSEC, Environmental Security and Corporate Social Responsibility.

Sixth level RA, IS, ES, QA, Safety, ITSEC, Human Resources, FINSEC, Environmental Security, Corporate Social Responsibility, Business Continuity Management.

On Fig. 1 is presented the structure of the proposed integrated security management system with the resilience levels in it.

The subject is debatable and therefore we will note here only the main grounds that determine the structure and content of the levels.

It is suggested the *First level* to comprise Risk Assessment (RA) and Internal Security (IS). This is the lowest security level which a respecting itself organization (still more if this is a critical entity) has to create. There is no case when a critical entity has not internal security system. And here is the place to note that RA is accepted not as subsystem or system but as process that lies at the base of any of the presented here subsystems. Conversely, if RA is perceived as a system this means that it will „usurp“ all the rest and then we will not talk about multitude of subsystems or systems but about only one – RA. RA is an umbrella on all elements of the integrated security management system. But in any case, if we want to build functioning access control system this combination of RA and IS should be present.

But it is not a panacea, as described in all leading documents in the field of resilience of critical entities. It is the basis of all security plans, but for the purposes of its effectiveness in implementation it is appropriate that it be the leading process, but not everything that is required of critical entities.

6th level – 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
5th level – 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
4th level – 1, 2, 3, 4, 5, 6, 7, 8
3rd level – 1, 2, 3, 4, 5
2nd level – 1, 2, 3
1st level – 1, 2

Figure 1. Integrated security management system with the resilience levels

The Second level are proposed the subsystems RA, IS and the External Security (ES). There are numerous cases when the organizations build access control systems but there is a very small number of those that have also built an external security system. That is related in almost all cases to objects located in populated regions or organizations which share one building with other organizations. But even then, it is possible to build an external security system. It depends to a great degree on the system designer who can build the external security system using both his own sources of information and such in possession of other organizations (for instance in the shared building).

The First and Second levels of resilience are inherent to small and medium-sized enterprises. Building these levels of sustainability does not require highly qualified personnel, given the fact that there are a number of high-tech companies on the market that can form the requirements for the levels themselves and fulfil them.

The Third level may include *RA, IS, ES, QA and Safety.*

The content of this level is as follows: Quality Assurance and Safety. Not all organizations, particularly the critical entities, possess QA systems and still further for Safety. Certainly, components of these systems have been developed in the critical entities but in most of the cases the management does not realize the truth that the international standards that introduce requirements for these systems could help both for management improvement of the objects and for enhancement of their security. The practice has many time proved the logics and truth of the last. The development of clear rules of effective organizations management for the first time is laid in the standard of ISO 9000 series (it is not accidentally that in 2012 the standard structure is accepted as reference in the development of standardization documents which regulate the requirements for the management subsystems), which we think is in the basis of the good organization of ensuring the resilience of the critical entities.

As far as the Safety is concerned here, we do not mean only safety that will guarantee the health and life of the organizations employees, but the accent is also placed on the safety and life of the citizens in vicinity to the critical entity and the community as a whole.

Therefore, the third higher degree comprises these two additional subsystems (which should operate together) with the idea to become an object of discussion and at last to enter the frame of tools which the organization management has to use for their resilience.

The construction of the proposed two subsystems requires highly qualified personnel in the critical entities as well as it requires mandatory knowledge of RA and the presence of built IS and ES.

The subsystems RA, IS, ES, QA, Safety, Information security, Human Resources and the Financial security form *the Fourth level.*

Additional levels are: Information security, Human Resources and Financial security. The key organization management system subsystems are those ensuring the information security - ITSEC. It is not suggested in the above levels because:

1. Not all critical infrastructures possess information systems (for example, some ammunition storehouses);
2. Require serious investments for their building;
3. They are applicable in organizations where the information systems are the basis of the functioning of the same. In spite of this, if the respective organization wishes to pass at higher security level it has to create such a subsystem.

Such a management subsystem is being built in large, complex critical entities in the fields of energy, transport, banking, etc. It is being built in large, complex critical entities in the fields of energy, transport, banking, etc. It necessarily includes the above-mentioned management subsystems, for understandable reasons. The construction of this subsystem needs to follow the requirements of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, which sets out the baseline for cybersecurity risk-management measures and reporting obligations across the sectors that fall within its scope, in order to avoid the fragmentation of cybersecurity provisions of Union legal acts [7]. In confirmation of the logic set out in this publication, regarding the use of the standardization base and that the proposed new approach can become good practice, is what is stated in Para. (59) of Directive 2022/2555, namely "… Member States should continue to foster alignments with international standards and existing industry best practices in the area of cyber security risk management…".

Human resources, first of all they are considered a basic component of the entity providing qualified personnel for all aspects of the activity. Precisely this is its main role in ensuring the resilience of the critical entity. The risk of employees of critical entities, through their access rights within the critical entity's organisation to harm and cause damage is more and more likely [1]. This subsystem is offered at this level of resilience because only large entities can afford such a complex human resources organization that is competent in selecting employees not only for the information and financial spheres, but especially for security.

The Financial Security systems on the one hand could be considered as an ITSEC component and on the other hand at first glance they are not inherent to some of the critical entities. In the first case the information systems which are used for the organization's financial ensuring are considered. But here the word goes not so much about them but for the organization capability and wish to finance timely and adequately the necessary activities for ensuring its resilience, i.e., we speak about its financial stability and understanding on the side of the management. In the second case only at first glance comes the perception that this subsystem is not valid for some of the critical entities. But if we apply some of the reasoning above us shall see that it is not so at all. Certainly, only the organization capabilities and the management wish are not sufficient to say that there is FINSEC subsystem. The subsystem itself has to be systematized in harmonious documentary frame which comprises (but not only) explicit policy, strategy, plans and procedures for providing financial security as essential component of the resilience of the critical entity.

In the Fifth level are included: RA, IS, ES, QA, Safety, Information security, Human Resources and Financial security, Environmental Security and Corporate Social Responsibility. Here the new ones are: Environmental Security and Corporate Social Responsibility. The last subsystems are to some degree „extraneous“ for the critical infrastructure from the view point that their main purpose is different than to protect environment for which the resilience is developed. But this is only at first glance. Thus, for example, the ensuring of Environmental Resilience is closely connected with the organization Safety, and we have noted above that here the safety of the citizens outside the object and of the society as a whole are considered, especially in the case of terrorist attack.

The Corporate Social Responsibility is a comparatively new area which is yet coming at high rates into practice. In the concrete case it is important for the motivation of the personnel and particularly of the employees responsible for the entity resilience. If the engagement of the management is clearly and accurately written down and a system built which guarantees its fulfilment that in case of realized terrorist threat not only the employees will be compensated but also their families, then the fulfilment of the official duties would be at incomparably higher level. The case of Cantor Fitzgerald is indicative [8]. The Cantor Fitzgerald financial institution lost all of its employees in one of the buildings during the attack on the World Trade Centre Towers on September 11, 2001. On September 19, 2001, Cantor Fitzgerald committed to provide 25% of the company's profits over the next five years for benefits, and within the next ten years to pay health insurance to the families of its 658 former employees who died. In 2006, the company followed through on its promise, paying more than $180 million to the families of its former employees.

At this moment, the CEO who survived September 11, 2001, is Donald Trump's nominee for Secretary of Commerce! Without his social responsibility policy, directly related to the company's resilience, the latter would not have overcome the collapse, and he would not have been nominated for this position.

And finally, the basic component of *Sixth level* is the Business Continuity Management system (including the above mentioned subsystems). Once again it should be noted that it is the connection unit between all the rest subsystems presented in the present section and is at the same time it is a subsystem in the organization management system. In relation to security it is unique not only with the Business Impact Analysis, but most of all with the plans of system functioning. Here is the place to note that the BCM is a part and continuation of the Risk Assessment. The building of such subsystem is the end, the final stage of the creation of organization integrated security management system**.** In this way, the inextricable link between RA and BCM which are at the beginning and end of the "chain" of activities and related subsystems of the integrated critical infrastructure security system, is confirmed.

This sequence of arranging and combining the relevant subsystems of the integrated security management system for enhancement the resilience of the critical entities is an exemplary approach and can be used by the respective managements extremely creatively, taking into account the specific specifics of the organizations! In some of the cases, emphasis may be placed on separate, different from the shown logic of arrangement in the series resilience levels of subsystems, but in the majority of these objects this approach will prove its relevance and logic!

5. CONCLUSION

The new approach presented in this publication is not a panacea! But it can be used with success by many managements of organizations of different nature and character and contribute significantly to achieving this goal! It could become a good practice in the area under consideration and assist the efforts of the authorities involved in combating terrorism in the Member States. For example, it can be used by the Commission expert group, described at Directive 2022/2557. As a first step in its formation, the elements of the proposed integrated security management system can be applied, depending on the specifics of the relevant critical entity, using the "tailoring" method applied in the existing European and International standards! That is, using and combining those elements of the system which best define and are in tune with the specifics of the relevant critical entity.

The next step could be the development of a comprehensive European standard, the creation of which requires a longer period of time, but which will cover all related issues and take into account the experience of a maximum number of specialists from many fields.

What do we think are the advantages of using the proposed approach?

It is "open" to upgrade with new organizational methods and mechanisms that can improve and develop the positive effects of their application!

The detailing of the elements/levels of the system presented in this publication aims first of all to create common approach for increasing the resilience of the critical entities. The latter can be realized by different ways, the main of which, according to some specialists, is the improvement of the techniques and technologies used. But the technology alone is incapable of doing anything if it is not managed. And this is the greatest confirmation of the statement that security is provided by the joint use of technologies and organizational procedures for their management, both taken together and united by individual elements or integrated security management system.

The identification of resilience levels is the basis of the assessment of the degree of trust in the organization, which the security systems form in the users of its services, as well as in the society.

But before getting there, it is necessary to develop detailed requirements for each of the above-mentioned resilience levels, which forms the basis of the future international standardization documents created for that purpose. The development of techniques and technologies, separately for the respective subsystems, is not enough to ensure our security. Therefore, a skilful combination of both of them, with best management practices, can create a flexible, reliable environment for using different combinations of means and obtaining a synergistic effect from their usage to ensure the required levels of security for our organization.

As a next step, a future task, for the development of the proposed approach, it is necessary to be created a methodology for the evaluation of integrated security management systems of the critical entities, which can have three main elements:

1. Key requirements, which we can define as key evaluation criteria. These are the identified eleven subsystems of the integrated security management system of the entity;
2. Evaluation criteria – sub-criteria. Represent the activities and the documentary basis of the elements of each subsystem/key requirement and form the content of the integrated security management system;
3. Assessment categories that apply to each key requirement and each assessment criterion.

The methodology for the evaluation of integrated security management systems of the critical entities should be used with the proposed new approach to obtain a comprehensive, useful tool for use by professionals to increase the resilience of critical entities against terrorist threats.

REFERENCES

[1] *Directive (EU) 2022/2557* of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[2] Slatinski N., The five security levels – approaches and aspects. *International relation*, No. 2, 2009, and No. 3, pp. 49-78 (In Bulgarian).

[3] Yonchev D., *Security levels*, Published by New Bulgarian University, ISBN 9789545355134, 2008 г., pp. 83-233 (In Bulgarian).

[4] Guido Gluschke, NS23 Nuclear Security Management", NS23.5 Protecting Assets, International Seminar "Human Resources Development in Nuclear Security, 01-03 October 2015, UNWE.

[5] Stoichev K., *Critical Infraastructure Integrated Security and Protection*, ISBN 978-619-90310-8-7, February 2018, Sofia, pp. 71-106.

[6] *Planning Guide for Identity and Access Management*, 2022 (4-5 pp.), URL: https://www.gartner.com/en/conferences/hub/identity-access-management-conferences/insights/planning-guide-iam (Visited on 09.10.2024)

[7] *Directive (EU) 2022/2555* of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, Para 22.

[8] ECP – 601: Effective Business Continuity Management, Institute for Business Continuity Training, US, p. 176.

Information about the author:

Kiril Petrov Stoychev is Professor DSc., researcher R3 of Scientific Group 3.2.1. Integrated intelligent management systems for strategic program security, project: "BG-RRP-2.013-0001-C01, financed by the European Union-Next Generation EU, through the National Recovery and Resilience Plan of the Republic of Bulgaria".

Manuscript received on 02 December 2024