"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XVIII – 2015 – Issue 1
Published by "Mircea cel Batran" Naval Academy Press, Constanta, Romania // The journal is indexed in:
PROQUEST SciTech Journals, PROQUEST Engineering Journals, PROQUEST Illustrata: Technology, PROQUEST Technology Journals, PROQUEST Military Collection PROQUEST Advanced Technologies & Aerospace

IMPLEMENTATION OF THE OODA-LOOP IDEA ON DESIGN OF OFFSHORE OBJECT SECURITY ZONES

Valentin S. VASILEV[1]
[1] "Nikola Vaptsarov" Naval Academy, Varna, "Vasil Drumev" Str., 73, E-mail: valentin-vasilev@naval-acad.bg

Abstract: *Security zones with temporary dimensions are required for establishing trustworthy protection of an offshore object. Their boundaries are determined according to the threat`s evolution stage. Implementation of the OODA-loop contributes to the optimization of the reaction time.*
Key words: *control, maritime security, offshore industry, OODA-loop, reaction time.*

At the dawn of the twenty-first century the world is in the shade of overhanging inevitable changes that have their projection on maritime security. The processes of transformation of existing economic, energy and military-political relations between maritime states influence the security environment in the region. The Black Sea region dynamically changes its appearance in terms of security. There are a lot of questions asked in new maritime security environment. Is protection adequate to new possible threats in offshore zone or is there sufficient room for the impact on source of threat? There is no doubt it is necessary to meet these challenges where they escalate. This paper represents a cybernetic approach to control process in offshore security environment.

Estimation of the hydrocarbon potential of Western Black Sea Zone shows that these oil and gas fields have got significant economical importance. Most of them have not been appraised yet due to lack of investments and dynamic change of security in the region. All discovered hydrocarbon accumulations in shelves are in water depth less than 100 meters. Nevertheless, there is a trend deepwater areas to be exploited in the near future [3]. For that reason, the Black sea offshore zone inevitably will be the subject of concern.

There are some assumptions made about a realization of threat against an offshore construction. For example, the offshore security environment is an aspect of surroundings in offshore zone. The threat interacts with an environment and it produces some changes in the security environment. The environment also influences the evolution of threat. For that reason there are common "elements", which interacts each other and certain relations could be identified, i.e. there is a peculiar "environment-threat" system. Every offshore installation or structure, positioned in the Economic Exclusive Zone, is considered as a fixed offshore physical object.

Coastal states have got rights given by international low at sea to restrict free navigation within 500-meters safety zones around offshore installations and constructions [6]. Analysis in security aspect point out that such safety zones are insufficient for protecting platforms from deliberate attacks and they are also insufficient for protecting them from security hazards [4].

Security zones are required to create a reliable protection of an offshore facility. There are some challenges in limitation of security zones established around offshore object. Solution of the problem requires a correlation between the time and spatial dimensions of security zones and evolution of threat to be revealed.

The evolution of threat is a composite process consisted of genesis, development and realization sub processes. Genesis is occurrence of phenomenon in offshore environment such as a source of a threat. Development of threat denotes collecting of power and transportation of source of threat toward an offshore facility. Form of realization is performing remote or immediate attack. Despite attack form the aim of process is causing adverse effects.

The impact on the evolution of threat increases in respect of decreasing of distance to the subject. Ones emerged the threat can be influenced to some extent by control and domination of attendees over threat achieved after monitoring of environmental conditions. There are significantly larger number of opportunities to impact the threat during development process and the subsequent realization. Overall, the impact is limited in time aspect and spatial aspects.

There are some disciplining conditions that are derived from fundamental considerations taken into account. So called "scientific considerations" represent the idea of informational superiority in relation with the opposing site or organization, which are source of security risks. There is an assumption that defense should be established as "object oriented". Protection of any offshore construction should be inspirited by modern "smart" approaches. In other words, "zonal oriented" security would consume unduly large amount of resources. The control of security is to be assured relatively autonomously, but the autonomy should be balanced with trustworthy and accurate control management. The security management is to be designed so that the shortcomings of the existing system to be compensated, by providing adequate protection of new constructed offshore platforms, auxiliary vessels and developed supporting logistic system elements in the crucial littoral zone. Another important aspect is revealed by legal considerations. The control of threat`s evolution is to be in compliance with the European, international and maritime legal requirements [8, p.373-374].

Each running process of genesis, development and realization of a threat to offshore object becomes manageable if it is slowed down to the appropriate level. It is necessary to accomplish promptly proactive or reactive impacts.

Proactive impacts are active effects on the evolution of a threat - the genesis, further development according a specific trajectory and, ultimately, realization. On the one hand, these proactive impacts are executed in advance in order to eliminate the environmental conditions, which appeared as a prerequisite for generation of security threats and impacts during the threat evolution. On the other hand, it has impact on the threat development process in order to reduce the probability of realization of the threat and to decrease its adverse effects. These control actions should anticipate the occurrence of events in the development threat process. Proactive impacts are able to manage the evolution of the threat. The moment of realization, a place of realization and a form of realization would be controllable.

In contrast, reactive impacts should mitigate the inevitable realization of a threat on offshore object. In that case the evolution of a threat is relatively "ahead" in comparison with control activities. In fact, the control is an answer to those aggressive actions. The control, implemented by reactive impacts, does not affect the trajectory of source neither the exact moment nor the form of realization.

The controllability of the threat could be achieved under the following circumstances:

- The process is slowed down by established barriers along a trajectory of evolution. The overcoming of these barriers takes time and thus reduces the advancement of processes.
- In dimensional aspect, boundaries of surveillance and countermeasure processes are set as distant as it is possible from offshore object. These fictional bounding lines around the protected object often are relevant as follows: (1) to the monitoring of the environmental conditions; (2) assessment of revealed threat, based on identification and classification indications; (3) taking a decision for counteraction; and finally, (4) physical impact on the source of threat [1].

The strike against threat, according to time aspect, should be differentiated and focused on selecting the best time for counteracting in order to achieve the desired result of lower "cost" [11]. Actually, the selection criterion for the discretion of impact, in that case, is the moment when the suspected platform or physical source of threat attains observed line.

These boundaries should be calculated by using iteration cycle based on the OODA-loop[1]. Naturally, it is possible cognitive processes, such as observation, orientation, decision and action to be projected in offshore environment. After that, they could be linked with dimensional boundaries around an offshore object. Further, it is necessary thus derived defensive borders to be defined in quantitative and qualitative aspects.

The commencement of threat could be influenced to some extent by the impact on the "environmental" conditions - control of navigation, control of transfer, brokering and transit of dual-use items and by gathering information and taking proactive action against suspicious persons. The impacts on the environmental conditions have a comprehensive character. Different approach would be applicable, if the source of threat has been discovered after its genesis. There are considerable opportunities to produce effects on threat`s evolution. The shortage of resources leads to some restrictions in usage of forces and technical devices. They will be used limitedly in time and in dimensional term.

The evolution process - from genesis and progress till realization against offshore object - is possible to become controllable if it is slowed down to some extent. Then the speed of the process is favorable for adequate proactive countermeasures. Controllability of the process will be reached, if preconditions exist as follows:

- The process is slowed down by established barriers. The result of usage of these barriers projected upon the threat is that completion of attack takes a comparatively long time.
- Boundaries of security zones are established at affording advantage distance from the offshore object. Ergonomic solution of problem connected to establishing boundaries corresponds to implementation of OODA-loop and processes of observation of environment, assessment of indicators, thus identifying and classifying source of threat and making a decision for active or passive countermeasures. Nevertheless, products of the negative factors analysis are a base to state definitely the indicators that set the readiness levels of security system [8, p.374].

As it is shown above, there is a possibility the existence of any threat to be visualized by "environment-threat" system indicators. The non-favorable process could be slowed down via intervention in "environment - threat" system so as to modify a process, elements of the system and internal interconnectors between elements. This is a requirement for establishing a control of interaction between system and offshore object. The threat is developed in environment and its evolution depends on environmental conditions. The possibility of impact on the threat stems from a chance to alter trajectory and behavior of threat in the desired direction. Environmental conditions should be monitored so that situational awareness to be at appropriate level.

The situational awareness is a necessity of decision making process. Management decision set side by side the arisen situation with suitable scenario in order to realize hindering effects against threat. Model "barrier" [7, p. 218-225] incorporates system of elements which are engaged with altering speed and direction of the process. Protective barriers are applicable in offshore environment. Establishment of safety zones around offshore object is a kind of barrier. For example it is the announcement of the exclusion zone, etc [10]. Protective zones could be formed by using physical devices to obstruct passage such as a different type booms and fences.

However, it is possible security to be ensured not only by "physical" barriers but also by barriers made up of procedures. The latter actually are a specific way of acting given by developed scenario. Usually barriers in offshore environment should be promulgated and announced in accordance with norms of international law at sea [10].

There are static and dynamic barriers in accordance with their characteristics in space and time [7, p. 221-222]. For instant there is distinctive buffer zone inside dynamic barrier. The advent of the source of threat in the buffer zone could be registered by identifying indicators of the environment. It is a trigger of the sequence of actions or instructions followed in accomplishing scenario objectives. Usually scenario objectives are focused on timely executed cognitive processes such as orientation and assessment of environment and indicators of presence of source of threat and resolute proactive action. Good example for indicator could be crossing the barrier located at the minimum distance to the object, enough for timely execution of the OODA-loop.

On the one hand **aspect "time"** shows that impacts should be differentiated and focused in particular time intervals when effects on the development of the threat are bold and intensive. A selection criterion for the discretion of impacts in respect of time is entering of source of threat in monitored buffer zone. Boundaries could be determined in quantitative and qualitative term by ultimate limits of the OODA-loop processes.

On the other hand **dimensional aspect** presents a trajectory of threat`s source and condition of boundaries of security zones with reference to distance to offshore object. There is an option the impact to be put in correlation with security zones around the object. In other words, the movement of source is a projection of the aspect "time" upon the dimensional aspect of threat.

The total available time for response shouldn`t be greater than the sum of times of the realization of adverse effect on offshore object. The total response time, needed to reach a state of process controllability, depends on the length of reiteration of a set of cognitive processes after detection of threat, i.e.

$$Tr = \sum_{i=1}^{n} \sum_{j=1}^{m} Tij \qquad (1)$$

Where: Tr - Available time for reaction;
Tij - Time required for finishing a process;
n - Number of processes;
m - Number of threats.

Successful management of adverse impacts on offshore object depends on the availability of enough time to response. It is the sum of time periods of monitoring, assessment, making a decision and finally taking an action against threat. The sequence of executed processes depends on the construction and design of security zones. It is necessary security zones to meet some requirements. The zones should be flexible and versatile due to the nature of possible threat and security environment in general. For that reason their boundaries are not fixed in time and space. They have got specific features and may be distinguished in accordance with their functional characteristics.

The **monitoring security zone** is a part of offshore environment where specific predefined indicators are observed. Monitoring would be performed with some breaches and interruption of continuity because of technical shortages. Boundaries of monitoring zone are determined by a dichotomy between ranges of technical devices and, on the one hand, and on the other hand, the level of ambitions set at national level. Reducing the ambiguity allows to determine the time interval from identifying the source of threat to the beginning of carrying out its assessment, i.e. the observation and identification time Tob. This is the first component of the total time available for reaction Tr. The source of threat is encountered in monitoring security zone. Once revealed the threat should be identified. The latter process incorporate association of physical platform, determination the elements of source movement such as course, speed, characteristics of trajectory and behavior.

[1] The term "OODA Loop" refers to the cognitive cycle of observation, orientation, taking decision and action. It is originally developed by John Boyd. Initially, he outlined the concept to figure out processes inside a combat operation. Now, it also has practical use in various aspects of human activity, such as to understand commercial operations, learning processes or could give an approach to contribute "agility over raw power in dealing with human opponents in any endeavor" [2].

Nearest border of the monitoring area $Dob\min$ in each case is different and it is determined by the distance of detection Dob, reduced by projection on the path traveled by source toward the offshore object $\Delta Sob = Sob\ \cos\alpha$, passing trough time interval $\Delta t\,ob$. This time interval is defined by the time of detection decreased by the time of beginning of classification.

$$Dob\min = Dob - Sob\ \cos\alpha \quad (2)$$

Where: Sob - Absolute meaning of the path, travelled by source during the identification process;

α - Average meaning of the angle between the direction toward an offshore object and course of observed physical platform.

Time for observation in fact is the time required for identifying the source of the threat Tob and it will depend on the path Sob and speed of movement v of the source. If equation (2) is considered the time will be inversely connected with projection of speed of source on direction toward object:

$$Tob = \frac{Sob}{v} = \frac{Dob - Dob\min}{v\cos\alpha} \quad (3)$$

The **assessment security zone** is determined by the distant boundary coinciding with the nearest boundary of the surveillance zone, i.e. $Do\max = Dob\min$

When physical source of threat is in the zone, and normally classification and assessment processes begin to flow. Classification process includes determining the type of the physical platform. It is possible by analysis of physical dimensions relative to the effective reflective surface and further to be estimated displacement or supposedly load capabilities, etc. Standard operations are carried out and course, speed and character of the physical platform are analyzed. Assessment of the threat produces arguments for determination of security level of offshore object[2].

Nearest border of the assessment security zone $Do\min$ could be calculated when minimal distance of observation $Dob\min$ is reduced with the projection of the path of source toward offshore object So. The distance So is covered in time interval Δto, that is to say:

$$\Delta So = So\ \cos\alpha \quad (4)$$

The time for orientation To in fact is the mentioned above time interval of classification and assessment Δto. After taking in mind the expression (4), the time

$$To = \Delta to = \frac{So}{v} = \frac{\Delta So}{v\cos\alpha} \quad (5)$$

The **decision security zone** is designed in order to facilitate proactive actions against possible threat. It is a buffer security zone and is limited by far border coinciding with the nearest boundary of the area of assessment, i.e.

$$Dd\max = Do\min$$

The distance $D < Dd\max$ from the source of threat to the offshore object is a criterion for triggering a process of selection of the most appropriate scenario for proactive impact[3]. Scenarios according to the nature of the ongoing impacts and the desired effects could be divided into proactive and reactive. It is necessary these scenarios to be independent each other. Different sequence of activation during monitoring of the environment and in relation with the evolution of threat should be activated simultaneously or in a different sequence.

Closely border of decision security zone $Dd\min$ related to an object is determined by the distance $Do\min$, decreased by projection of the path of source of threat in the same zone upon the direction toward the object.

$$\Delta Sd = Sd\cos\alpha \quad (6)$$

The continuous curve that connects initial and end position of a source during decision process Sd is made inside a time interval Δtd, equal to the time for decision making Td.

$$Td = \Delta td = \frac{Sd}{v} = \frac{\Delta Sd}{v\cos\alpha} \quad (7)$$

Traditionally, the **action security zone** is established around the object and covers area from protected object to the distance of 500 meters given by legal framework of low at sea. Definitely the zone is crucial for trustworthy protection of any abject [4, 10]. It should be adequately designed so that a sufficient room for the impact on the source of threat to be ensured.

Actually, the design of action security zone is a challenge to control process. The far border $Da\max$ could be established so that the effective distance of active countermeasures $Da\,ef$ to be not greater than above mentioned distance. It is a disciplining condition in the same time, i.e. $Da\max \geq Da\,ef$. The near border should be set so that the threat to be neutralized prior its realization toward offshore object. There are some legal challenges worldwide, related with rules of engagement and "prohibited" zones around offshore constructions [10].

The distance $Da\max$ should cover available range of active countermeasures in accordance with an assessment of threat and an appropriate security level of security of offshore object [9]. The effective distance for action is linked with actual capabilities for maintaining auxiliary vessels and ships, on the one hand, and on the other hand, capabilities depend on the developed and trained techniques, tactics and procedures for active countermeasure against threat.

The time of proactive countermeasure Ta is defined in the following equation:

$$Ta = \frac{Da\,ef - Da\min}{v\cos\alpha} \quad (8)$$

The distance $Da\min$ is to be considered as the shortest distance appropriate for effective countermeasures against the physical source of threat.

The total time for reaction is a sum of time intervals when the source is consecutively in the security zones designed around offshore object. It starts with the moment of revealing the source and finishing with initiation of proactive action. It corresponds with movement of source trough the security zones.

If there is only one projected threat, the equation (1) will be transformed in following expression:

$$Tr = Tob + To + Td + Ta \quad (9)$$

Time for reaction against an offshore threat has got all the components that are the OODA-loop expression. The following result is obtained after substitution of time intervals of cognitive processes monitoring and revealing a dormant threat (3), assessment (5), making of decision for action (7) and last, but not least important time for action (8) in equation (9):

$$Tr = \frac{Dob + \Delta So + \Delta Sd + Da\,ef - (Dob\min + Da\min)}{v\cos\alpha} \quad (10)$$

Available time for reaction is increased by increasing the distance of observation Dob and tracking the physical source inside buffer security zone of assessment and making a decision for proactive countermeasures. Furthermore it corresponds with the effective distance of active

[2] Security levels are given in accordance with requirements of the ISPS Code.

[3] Scenarios for impact upon the threat should be prepared and simulated in advance in accordance with the security plan of the offshore object and in the interaction of all the relevant state departments.

countermeasures. Available time will be decreased when the distance of the nearest border of the monitoring area is reduced for one reason or another. Naturally, the time will be reduced if projection of speed upon direction toward an offshore object is growing up.

Furthermore, it is possible movement of the source of a threat also to be bound not only to the available time for reaction but also to the dimensional aspect of offshore environment. It holds out opportunities to design a security zones around an object. Adapting the Boyd`s concept [2] to the risks and challenges to the security of the offshore industry in the Black Sea contributes to building security zones around a relatively immobile offshore object. These security zones are variable in respect of a nature of threat, physical foundations of adverse impact and its source, as well as temporal state of capabilities for active countermeasures.

In fact, the latter mentioned lasting for a relatively short moment state of capabilities could be figure out in two aspects. On the one hand, it corresponds with abilities to execute monitoring of environment and technical devices for active countermeasures. Implemented techniques, tactics and followed procedures conduce to reducing the effects of threat realization. Moreover, applied standards of proficiency to personnel are of great significance [8].

On the other hand capabilities depend on the stage of the threat`s evolution. It means that applied intensity of efforts to reduce impact would be increased over time, i.e. the more the distance decreases, the more efforts are needed.

Implementation of basic OODA-loop principles entirely conforms to safety and security demands of any offshore environment. It contributes to the design of offshore security zones and ultimately it optimizes the time available for reaction.

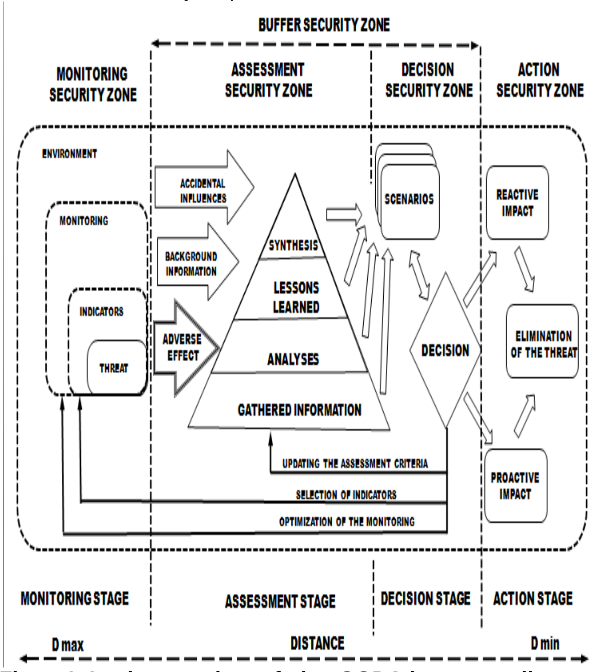

Figure1: Implementation of the OODA-loop contributes optimization of the reaction time. Security zones with their boundaries are determined in accordance with the threat evolution stage.

The threat of offshore object is originated in maritime environment (figure 1). Generally, there are located numerous interacting physical objects. The aim of monitoring is to reveal any suspicious or potentially hazardous influences as soon as possible. This is an opportunity, the physical source of threat to be differentiated. The earlier detection of threat is possible to be achieved by observation of environmental conditions and keeping in touch with the situation. It is reasonable indicators to be used for increasing the efficiency of monitoring. Unceasingly control made at regular and frequent intervals gives appropriate chance adequate criteria for comparison of indicators to be implemented. Further, thus obtained information is delivered for assessment and analyses. Monitoring of environmental conditions usually provides piece of data, gathered by observing signs of existence of distinctive physical objects. In fact, the system “environment-source of threat” is requiring no great efforts to be tracked because signs of interaction of the source of threat with the environment are more apparent than the threat itself.

There are specifics in monitoring of the environment in the offshore zone. First of all, the information is gathered and it contains discrete environmental data over the time. Other restrictions are related to the limited number of indicators, the values of which are monitored. Therefore, objective indications of existence in time and space of the "environment - threat" system will be disclosed in a priority sequence manner. Threats which cause distinguished change of the indicator values are normally to be discovered first.

The elimination of revealed threats trigger consecutive iteration process of monitoring and gathering information, analyses and synthesis and implementation of lessons learned. The conclusion of former iteration loop allows other dormant threat to be revealed [6, p. 113-119].

The assessment process corresponds to the Boyd`s orientation in conflict situation. It consists of analysis of the incoming information, implementation of experience and synthesis. It normally occurs during the assessment stage. The separation of any piece of information into its component data elements allows for an adverse to be separated from those who have no influence. That information along with the extracted by monitoring of the indicators and observation of an accidental influences is converted into useful information for management of security. Lessons learned are entangled in that useful information. Lessons learned comprise the practical experience of the management system, conclusions and implications collected after assessment of comparable security incidents worldwide [9]. Synthesis is an important element of the assessment stage. There a picture compilation is figured out. The decision maker becomes more familiar with the situation, i.e. thus the level of situational awareness should be increased.

The decision stage corresponds to the presence of a source of threat in the decision security zone. The decision making process of performing an influence against the evolution of threat is supported by the set of planning scenarios. The scenarios are selected in correlation with the results of the former assessment stage. It is peculiar that the assessment and decision security zones are fundament of the buffer zone related with the available time for reaction. There are some feed backs in the decision stage. The decision process should be flexible, so that it is necessary an assessment criteria to be updated constantly. The selection of indicators and optimization of monitoring are also important feedback between the decision stage and monitoring and assessment stages.

The result of the decision is a proactive or reactive. Such types of actions are the essence of the action stage. The physical source of threat during the action stage is situated in the action security zone. It is a matter of great significance the physical source of threat to be eliminated prior the moment of attack. The nature of taken action depends on collaboration between the assessment process and the available set of scenarios [6, p. 90-101].

The content of included scenarios develops details of threat effects on offshore object, linked with the offshore object level of security and also environmental conditions (figure 2).

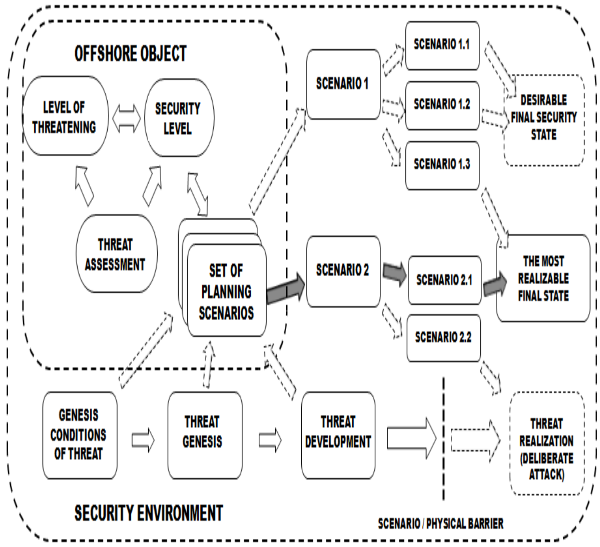

Figure 2: Options for reaching the final state are schematically represented by choice of scenarios for implementation of control management.

The desired end state of security is achieved by carrying out required number iterations. Detected threats are neutralized in result of each iteration loop.
Indicators rebound environmental changes caused by presence of the physical source of threat. Some threats produced stronger effects on the environment than others. Their influences are more distinctive and could be registered at considerable distance. Therefore the act of registering is easier but it is a precondition for existence of dormant threats. The desired end state of security it is possible to be reached by the consecutive iteration process of threat elimination. The tendency is usually from strongest hazardous influences to dormant threats with lack of strength or intensity.
Any deviation from the desired trajectory of process development requires the application of well-timed control action. Furthermore, these control actions direct the flow of the process of threat`s evolution and thus facilitating entry from one scenario to another. Each immediately following in time scenario is necessary to be more favourable to the offshore object security, i.e. it is a precondition for lowering the level of vulnerability of the object.

The exerted influence on the "environment-threat" system should be discreet in time and space in order to achieve a balance between efficient and effective use of available resources. Definitely, the functioning of offshore protective system depends on availability of resources. The prerequisite for stopping the process is the lack of the "environment-threat" system, i.e. there are no more physical sources of threat revealed during surveillance.
In summary, it should be said that security zones with variable dimensions are appropriate countermeasure not only against deliberate attack, but also contrary to any safety and security hazard in offshore and littoral zone too. Trustworthy protection of any threatened offshore object is established by the available time for reaction managing. Implementations of the OODA-loop hold out opportunities for optimization of the reaction time. Besides, the boundaries of these security zones are determined according to the threat`s evolution stage.
The following conclusions relevant to the implementation of OODA-loop idea on design of security zones could be made:

- An effective approach for optimization of OODA-processes is to optimize every single incorporated cognitive process. It is necessary relationship between these processes to be modified so that the maximum efficiency in countermeasures against offshore threat to be achieved.
- Existence indications of the "environment-threat" system are revealed so as the most hazardous is a priority.
- The adverse impact could be minimized by slowing down of processes using the "barrier" method.
- The decision making process to counter an adverse impact could be supported by developed in advance set of planning scenarios.
- The observed deviation from the initial trajectory of the threat`s development process or decreasing of the speed of adverse process is an impartial criterion for the successful implementation of control action.
- Options for reaching the desired final state of security could be represented by choice of scenarios for implementation of control management.
- The implementation of the OODA-loop idea, linked with the offshore object security management, discloses a new perspective on design of "special-purpose" zones. Monitoring, assessment, decision and action zones around an offshore object correspond with the OODA-loop. The "buffer" security zone is distinctive, based on assessment and decision zones.
- The implementation of the OODA-loop in offshore environment contributes optimization of the available reaction time.

Bibliography

[1] Boyd, John R., Destruction and Creation, U.S. Army Command and General Staff College. Centre for Army Tactics, 1987, 12 p.
[2] Brehmer, Berndt, The Dynamic OODA-loop: Amalgamating Boyd's OODA-loop and the Cybernetic Approach to Command and Control - Assessment, Tools and Metrics//10th International Command and Control Research and Technology Symposium the Future of C2, Conference Paper, 2005.
[3] Georgiev, Georgi. Prospects and Challenges for Oil and Gas Exploration in western Black Sea // Plenary reports by International Scientific-Applied Conference "New Technologies in the Offshore Industry", Varna, 2013, p. 13-25.
[4] Harel, Assaf. Preventing Terrorist Attacks on Offshore Platforms: Do States Have Sufficient Legal Tools? // Harvard National Security Journal, Vol. 4, 2012, p.131-184.
[5] International Ship and Port Facility Security Code (ISPS Code), International Maritime Organization (IMO), London, 2003.
[6] Kolev**,** Kiril. Management of maritime security. Varna, 2014, ISBN 978-954-449-756-9.
[7] Kolev**,** Kiril. Upravlenie na bezopasnostta na morskia transport. Varna, 2012, ISBN 978-954-449-601-2.
[8] Mednikarov, B., Kalinov, K., Stoyanov, N. Case Study From Bulgaria – Building A Conceptual Model For Simulation Architecture In Support For Education And Training (Bulgarian Standpoint) // Military Modeling & Simulation, Singapore, 2008.
[9] Offshore Oil and Gas Resources Sector Security Inquiry. Office of the Inspector of Transport Security, Commonwealth of Australia, 2012, ISBN: 978-1-921769-72-6.
[10] United Nations Convention on the Law of the Sea (UNCLOS-1982)., 1982, p.40-166.
[11] U.S. Joint Publication 3-0. Joint Operations. 2006, Incorporating Change 2, March 2010.