Methods for System Analysis of the Operational Capability of Armed Forces for Defence Including Electronic Warfare

Andrzej Najgebauer
Ul. Gen. S. Kaliskiego 2
00-908 Warsaw
POLAND

andrzej.najgebauer@wat.edu.pl

ABSTRACT

The presentation will present a model for analysing the operational capabilities of the armed forces, including consideration of selected aspects of electronic warfare. The model should identify and prioritize the required capabilities by identifying key objectives :Identification of the future security environment and within it the operational environment, Identification of planning scenarios and requirements for future armed forces including forces to execute EW. Identification of specific tasks in relation to AF missions and tasks, Confirmation of the list of required capabilities in the capabilities catalogue. The idea of identifying required capabilities and identifying gaps is shown in the paper. The key questions/problems posed in the analysis process are: Do the identified capabilities match the missions and operational concepts and threats? What are the metrics for achieving the desired operational capabilities? What might be the cost of providing the Armed Forces with the required capabilities? What is the key approach to the problems? A capability-based approach to planning is used, including the identification of reference (calculation) modules of the Armed Forces, including electronic warfare units. An important problem, is the dimensioning of operational capabilities using formal and simulation methods. As a result, the construction of an optimization model to determine the structure of the Armed Forces, based on reference modules with the desired capabilities, enabling the implementation of the identified operational concepts, taking into account the criteria: operational and cost. The analysis proposes its own simulation models, based on mathematical models of the operation of the Armed Forces. Simulation based on step-by-step analysis with the introduced scenario and possible structure of the opponent and the defined mission. The approach proposed in the work also provides a tool for evaluating the budgetary development of the armed forces.

1.0 INTRODUCTION

The issues of strategic planning in the Armed Forces should not deviate from the essence of strategic planning for any organization, although it is important to emphasize a certain difference, which is to take into account the destructive impact of the adversary causing a partial loss of capabilities of the Armed Forces. Referring to works in the field, it can be put as follows: Strategic planning is a formalized process of long-term planning aimed at determining and realizing the goals of the organization [8]. In the field of strategic planning in the Armed Forces of the Republic of Poland, otherwise defence planning was extremely important formal documents that provide guidance for this planning, which as a result of the strategic defence review and state security reviews may be subject to modification.

The force development planning process, based on the Capability Based Planning (CBP) approach [7], is a relatively new process used in NATO and selected non-NATO countries. A presentation of this approach is presented in a guide [9] and, with consideration of Polish conditions, in a report [6], elements of which are cited and quoted below.

The goal of the CBP process is to transform the armed forces and provide the command with the capabilities necessary to conduct armed combat in the future operational environment. The process has three basic components, which include: defining the capabilities needed to counter future threats, materializing them by acquiring new systems for conducting armed combat, and budgeting. It is directed at conducting analyses and assessments to prioritize designed capabilities and then procure them so that future missions can be conducted effectively.

1.1 Essence of the Capability Acquisition Process

The need to make changes in the process of acquiring operational capabilities forced, on the one hand, by negative operational experiences, and on the other hand, by the emergence of new challenges and threats in recent crises and military conflicts. The current process was formulated based on the following principles [6], [7], [9]:

1) Operational needs should be defined in the context of capabilities, rather than systems assigned to individual types of armed forces, or armies.

   The new approach to planning assumes that the emergence of new threats does not necessarily automatically generate a need for new military equipment. It was intentional to answer the question, what needs to be done? This was concretely reflected in the intention, which can be described by replacing the phrase we need better combat aircraft with the statement we need the ability to overpower the enemy in the airspace. The formulation edited in this way not only clarifies and justifies operational needs, but also allows for creative concepts for new system solutions in terms of how to acquire capabilities and even compete among them.

2) Needs should be identified on the basis of joint concepts for conducting military operations in the future.

   The formulation of operational needs must not be limited to the familiar, traditional ways of operating, but must refer to the conditions of the future operational environment. Operational concepts should describe possible ways of solving, by the armed forces, a broad spectrum of military problems, and not be limited only to classical conflicts.

3) One officer should be responsible for each functional area.

1.2 Planning Scenarios

A scenario is a tool that enables and facilitates the development of operational concepts, as well as the identification in the process of functional analysis of required capabilities and the prioritization of material and non-material solutions for all DOTMLPF functional components.

Threat scenarios (planning scenarios) introduce the context for identifying required capabilities. Considerations from this are used in all three phases of functional analysis, problem area analysis, needs analysis and possible solutions. As a result, the required capabilities are identified on the basis of conceptual analyses, followed by the relevant prerequisites, conditions and standards. It is assessed whether the current armed forces are capable of carrying out tasks, and if not, capability gaps are identified, and eventually ways to fill them through intangible or tangible solutions, so as to reduce the possibility of operational risk.

1.3 Threat Analysis for the Development of Planning Scenarios

It should be noted that Poland's strategic documents, as well as those of the EU and NATO, prioritize five categories of threats, with variations (using different types of weapons, different scales, different locations) [12]:

- Terrorism/terrorist attack;

  The probability of this threat occurring both inside and outside the EU, NATO countries is assessed as high. In Poland, it is slightly lower, although the growing likelihood of retaliatory actions, associated with the participation of the Polish Armed Forces in foreign missions, is noted.

- Proliferation of weapons of mass destruction and their means of delivery;

  The probability can be assessed as medium, with an increasing trend. For Poland, this threat is primarily external.

- Threatened security of supply: energy, information, other types of goods (related to attack on critical infrastructure, transport and communication routes, cyber-attack, etc.). The probability is high, the occurrence of such a situation, however, does not necessarily lead to the use of the Armed Forces. Threats can have internal and external sources, can be political, economic, military.
- Hybrid threats;
- Threats of large-scale conflict.

Regardless of the threat assessment contained in the strategic documents, the created scenarios for the use of the Armed Forces should take into account the fact that depending on the type and scale of the threat, their tasks and role will differ. When working on scenarios, the following factors should be taken into account:

- The location of the threat: inside the country, outside the country but within the EU and NATO territory, outside the EU and NATO territory;
- The source of the threat (state/non-state actor, individual/group/organization, nature);
- Nature of the incident: terrorist attack/aggression/disaster;
- Nature of weapon used: attack with conventional/non-conventional weapons;
- Space: land, water, air, cyberspace, (and/or cyber-electromagnetic space);
- Scale and impact: city/region, country, group of countries, number of casualties.

The number of possible scenarios for the development of the situation is in practice infinite. Therefore, when developing a catalogue of such scenarios, it is necessary to make some division and assumptions related to:

- The entrenchment of AF in the legal system, regulations related to states of emergency, crisis management;
- Probability of occurrence of threats;
- Assessment of the significance/importance of threats;
- The area of operation of the Polish Armed Forces.

The following framework division of scenarios is proposed, according to the statutorily defined tasks and role of the Armed Forces:

- Missions and operations of the Armed Forces outside the country (Law on the principles of use or stay of the Armed Forces outside the country, relevant provisions of the President of the Republic of Poland, North Atlantic Treaty);
- Emergencies within the country; (Constitution, Crisis Management Act, emergency laws, but also EU regulations, e.g., on cooperation in the protection of critical infrastructure);
- Participation in conflict/repulsion of aggression (territorial defence),(Constitution, Law on general duty of defence, laws on states of emergency, etc.).

1.4 Concept of Operations

Concept of operations (CONOPS) are the basis for the capability identification process, and are required for future operations [5], [6]. A concept is an idea, a general plan that can be transferred into an operational context. Thus, concepts illustrate how armed forces conduct operations (will conduct operations). They describe what capabilities are needed to conduct the full spectrum of missions and to counter potential adversaries, in the expected operational environment. They explain how the commander, using operational art and possessed capabilities, achieves the intended effects and strategic objectives.

The development of a new concept is required when it becomes apparent that a particular military problem cannot be solved. In addition, a new concept is desired when a potential solution cannot be achieved by changing the functional components of the DOTMLPF. This can occur in the following cases:

1) Lessons from operations conducted by the armed forces of various countries show that the existing force doctrine is ineffective, and that the armed forces of other countries are creatively integrating capabilities or successfully applying new capabilities;
2) New capabilities have emerged that are available to potential opponents;
3) Major changes in the operational environment are anticipated;
4) A new Politico-Strategic Defence Directive, National Security Strategy or Defence Strategy has been implemented;
5) New, breakthrough technologies have become available, both for own troops and potential opponents.

2.0 MODELLING THE FUNCTIONING OF THE ARMED FORCES OF THE REPUBLIC OF POLAND

The formal model of the armed forces and the algorithms of functioning are the basis for the development of IT services, supporting the planning and programming of the development of the armed forces. The scope of these services includes dimensioning the capabilities of abstract and physical capability carriers, dimensioning the capabilities of calculation modules and physical modules, and finally dimensioning the physical capabilities of the entire armed forces. Using functionalization algorithms, optimization algorithms can be built to determine the amount of capabilities required and simulation verification of the concept of acquiring missing capabilities. The model takes into account the division into functional systems, the so-called capability areas (command, reconnaissance, missile, troop survival and protection, logistical security of operations).

Using the developed formal model, algorithms were developed for the implementation of selected tasks performed by individual types of armed forces and types of troops, taking into account the division into capability areas defined in standardising documents. The prepared models and algorithms achieve two goals:

- To dimension, that is, quantitatively assess both the required and possessed capabilities of the armed forces;
- Develop procedures for simulating the performance of types of armed forces and types of troops during the implementation of a selected set of tasks.

It was assumed that dimensioning would be carried out for different needs and at different levels of detail. Due to the needs of dimensioning, the following cases were distinguished [12]:

- Dimensioning for simulation needs – a very detailed model, taking into account the influence of environmental conditions, the category and class of the capability carrier and the target, the degree of training of the capability operator;
- Dimensioning for capability planning – measures used in the process of assessing required capabilities;
- Dimensioning for capability cataloguing – measures of capability evaluation are averaged due to selected environmental conditions;

The capability dimensioning method uses the concept of a capability carrier. We will call a capability carrier an abstract object that corresponds to a single piece of military equipment (tank, armoured personnel carrier) or a group of such equipment forming a system (radio communication system, rocket launcher battery). In order to dimension the capability of a calculation module, and in the next sequence of the SZ, the capability of a single carrier will be dimensioned at first.

In terms of the area of command capabilities, the capabilities of the command post system and ICT infrastructure are distinguished. With regard to the command post system, the operation of command posts at the operational and tactical levels was modelled and algorithmized in detail, including:

- Development of essential and backup command posts and their attachment to the ICT infrastructure;
- Times of developing combat documents;
- Movement of command posts during the execution of operations;
- Fire and electronic impact on command posts during stationary operation and relocation;
- Restoration of destroyed command posts.

With regard to the ICT infrastructure and services of the command system, the functioning of the command system was modelled and algorithmized in detail:

- Radio communications - mobile battlefield radio networks;
- Non-horizontal radio communications;
- Horizontal radio communications;
- Satellite communications;
- Extensive tactical and operational networks (radio line-wire and tropospheric);
- Radio line-wire communications;
- Tropospheric communications.

The developed models make it possible to assess the coherence of the command system (the possibility of obtaining a connection between any nodes of the command system), as well as the throughput and latency of the transmission of combat documents. The sensitivity of the ICT infrastructure to electronic impact and fire flare is taken into account.

In the area of strike capabilities, measures and simulation algorithms have been developed for such capabilities as:

- Kinetic strike of land targets of a certain type under certain conditions (expected number of destroyed targets in a fixed unit of time without taking into account the impact of the adversary);
- Kinetic attack on air targets of a specified type under specified conditions (expected number of destroyed targets in a fixed unit of time without taking into account the impact of the adversary);
- Kinetic damage to naval targets of a certain type under certain conditions (expected number of destroyed targets in a fixed unit of time without taking into account the impact of the opponent).

In addition, models and algorithms have been developed for the operation of the following calculation modules, the main capability of which is the ability to strike the enemy. These are:

- Armoured battalion;
- Mechanized and motorized infantry battalion;
- A division of barrel artillery;

- Rocket artillery division;
- Anti-tank artillery squadron;
- A squadron of fighter-bomber aircraft;
- A squadron of helicopters.

Tasks of reconnaissance and electronic jamming of air command and air defence communication systems, as well as on-board radionavigation and radiolocation stations and systems are performed by units (reference modules) of the type radio-electronic centre of complex structure or radio-electronic battalions. The models and algorithms have been developed for the operation of the following reference modules, the main capability of which is the ability to jamming (electronic attack).

Within the area of logistic security, detailed modelling and algorithmizing were subjected to:

- Movement of forces and resources (movement capacity, loading/unloading/reloading capacity);
- Continuity of supply of the Armed Forces of the Republic of Poland (ability to supply/supply/carry, store/storage);
- Material service capability (capability for: containerization, collection and maintenance of means of supply, transportation, storage);
- Weapon exploitation security (capacity for land transport of battalion module equipoise, see resupply/shifting capacity);
- Medical security (capacity for medical evacuation by land, sea, air).

Within the area of military protection and survival, detailed modelling and algorithmizing were subject to:

- Fortification expansion (models and algorithms depending on the degree of expansion);
- Minesweeping and demining (clearing) of the area (different ways of minesweeping/ demining, different types of mines);
- Construction and maintenance of crossings (ferry crossings, pontoon crossings);
- WMD defence (under contamination reconnaissance: routes to reconnaissance, area to reconnaissance, sample collection, sample transport; under decontamination: people and equipment, area to decontamination, routes to decontamination).

Within the reconnaissance capability area, measures and simulation algo-rhythms have been developed for the following capabilities:

- All-military, patrol and long-range reconnaissance, including: the ability to uncover enemy facilities, identify approach routes, manoeuvre corridors, guidance of means of destruction;
- Electronic reconnaissance, including: reconnaissance of radio communication systems, reconnaissance of radiolocation systems, tracking of emission sources (radio and radiolocation systems);
- Reconnaissance of military types, including: artillery reconnaissance (including imagery, sound, radiolocation, on flying platforms), engineering reconnaissance.

The entire formal model and developed algorithms for the operation of the armed forces are presented in a report [10] prepared by the Military University of Technology. The development of the basis and terminology for the formal model of the armed forces and the algorithms of operation was based on the report [3] prepared by the National Defence Academy.

2.1 Reference Modules and Their Combat Potential and Cost

We should consider organization and military equipment and armament of the reference module in order to evaluate its relative combat power and cost of exploitation.

The mathematical model of a reference module is represented as follows [12]: $RMd_{F(E)}(i) = \left(\overline{n}_{F(E)}(i) = (n^{w}_{F(E)}(i))_{w\in W_{WS}}, \overline{MCP}_{F(E)}(i), AMC_{F(E)}(i)\right)_{i=1,..,N^{F(E)}_{RMd}}$, where $N^{F(E)}_{RMd}$ - number of types of reference modules for side F – the friendly forces (for side E – the enemy forces) and

- $\overline{MCP}_{F(E)}(i)$ - vector of combat potential general and different categories of the reference module type i of side F(E);
- $AMC_{F(E)}(i)$ - annual cost of the reference module type i of side F(E).

Each weapon system could be evaluated by its individual combat power index cpi_w. There is no universal methodology for weapon systems combat power evaluation. Different methodologies are used in different countries. Always some parameters of weapon are taking into account, in order to evaluate its combat power index.

Let us define the following denotations:

- $W_{WS} = \{1,..,N_W\}$, W_{WS} - the set of number of types of weapon system, N_W - number of weapon system types (for all potential members of analyzed conflict).
- $cpi_w, w = 1,..,W$ - where cpi_w is a combat power index for weapon system w.

In order to formulate some success conditions of military operation, we define category of weapon systems as follows: tanks - W_T, infantry fighting vehicle (BMP) - W_{AV}, long-range anti-armour weapon (LR) - W_{LR}, short-range anti-armour weapon (SR) - , W_{SR} .short-range artillery - W_{SArt}, multiple launch rocket system - W_{MLRS}, tactical ballistic missiles - W_{TBM}, infantry weapon (mortars, small arms) - W_{inf}, attack helicopters - W_H, air defence weapons - W_{AD}.

We assume that:

$$W_{WS} = \bigcup_{n\in WC} W_n$$
$$WC = \{T, AV, BMP, LR, SR, SArt, MLRS, TBM, inf, H, AD\}$$
$$\forall n_1 \neq n_2 : W_{n_1} \cap W_{n_2} = \varnothing$$

Now, we can define vector of combat power: $\overline{MCP}_{F(E)}(i) = \left(MCP_{F(E)}(i), (MCP^{n}_{F(E)}(i))_{n\in WC}\right)$, where:

- $MCP_{F(E)}(i) = \sum_{w=1}^{W} cpi_w \cdot n^{w}_{F(E)}(i)$ - the general relative combat power of the reference module type i of side F(E) is calculated as follows;
- $MCP^{n}_{F(E)}(i) = \sum_{w\in W_n} cpi_w \cdot n^{w}_{F(E)}(i), n \in WC$ - the relative combat potential of weapons category $n \in WC$

where $n^{w}_{A(B)}(i)$ is a number of weapon system type w in the reference module type i of side F(E).

Relative combat power of reference modules (general and for each weapon category) should be modified considering terrain conditions and type of combat. There are defined five type of terrain: OPEN, MIXED, ROUGH, URBAN and MOUNT [16], [17]. The main idea of Capability Based Planning is presented as complex process: planning scenario – description of military reaction – estimation of required capabilities – assessment of lacking capabilities – simulation assessment of options for obtaining capabilities – model of armed forces (structure and equipment) (Figure 1).

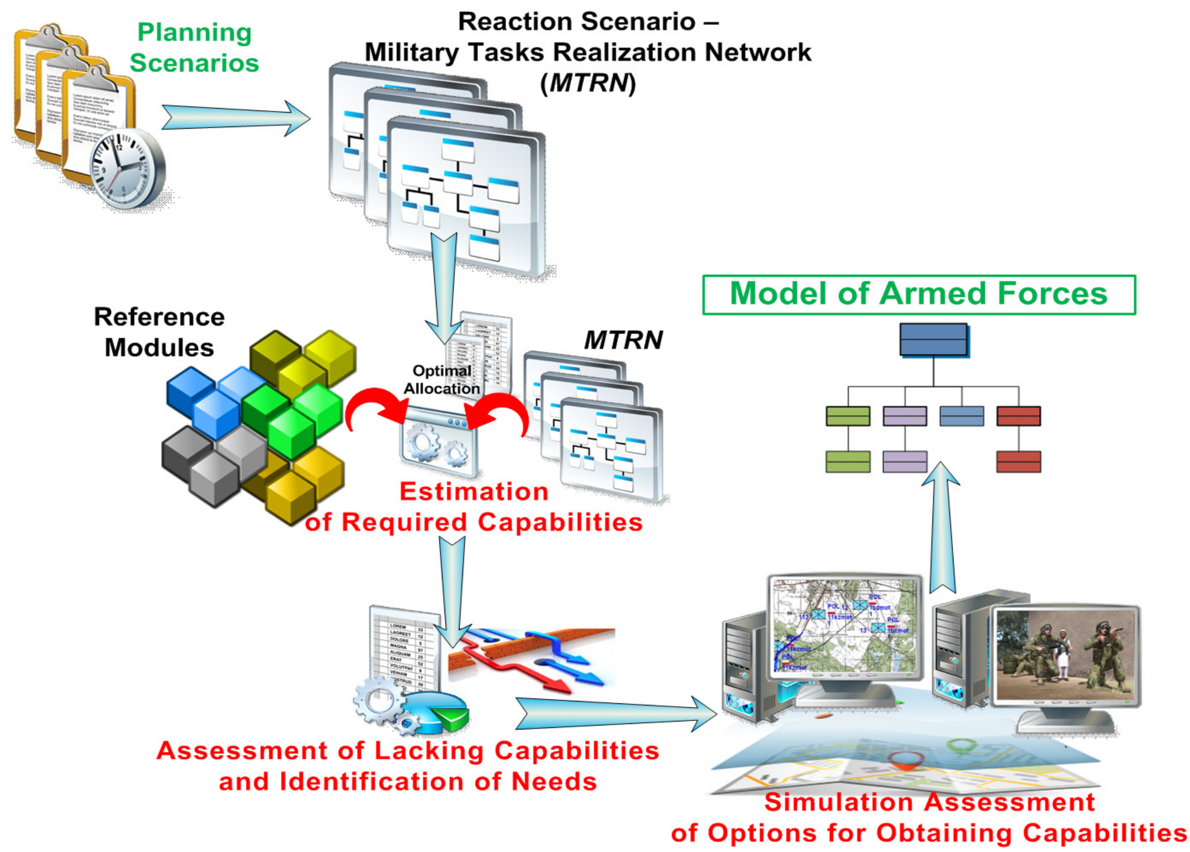

Figure 1: Scheme of Capability Based Planning [12].

The annual maintenance cost of a type *i* reference module shall be defined by annual staff cost of type module *i* , annual cost of warfare, cost of warfare acquisition of type *i* module. The task of optimising the structure of the AF for specific scenarios of state risks was formulated in [16]. We assume knowledge of the structure of the opponent's forces in the form of: $\bar{X}_E = \left(x_E(i)\right)_{i=1,..N^E_{RMd}}$ where $x_E(i)$ – number of reference modules of type *i* and opponent forces:

$$x_E(i) \in \{0,1,...,I\}, i == 1,..N^E_{RMd}, I - \text{max number of modules}$$

Commander decision:

$$\bar{X}_F = \left(x_F(i)\right)_{i=1,..N^F_{RMd}} \tag{1}$$

- The structure of the AF of side F;

where: $x_F(i)$ – number of reference modules of type i for own forces.

Criteria functions:

$$F_1(\overline{X}_F) = \sum_{i=1}^{N_{RMd}^F} AMC_F(i) \cdot x_F(i) \tag{2}$$

- Annual maintenance cost of all reference modules,

$$F_2(\overline{X}_F) = \sum_{i=1}^{N_{RMd}^F} CWA_F(i) \cdot x_F(i) \tag{3}$$

- Cost of acquisition of all reference modules

$$F_3(\overline{X}_F) \tag{4}$$

- Personal losses,

$fr_{F/E}(\overline{X}_F, \overline{X}_E) = \dfrac{CP_F(\overline{X}_F)}{CP_E(\overline{X}_E)}$ - the ratio of the potential of own and opponent's forces,

$CP_{F(E)}(\overline{X}_{F(E)})$ – overall potential of own or opponent's forces, $CP_{F(E)}^n(\overline{X}_{F(E)})$ – the potential of own or opponent's n-th category armament system

$Fl_{F(E)}(\ )$ – the function of percentage losses of the F(E) side depending on the ratio of potentials, type of terrain, type of combat, side of the conflict, whose parameters we can estimate on the basis of historical conflicts data (after Second World War) [16], [18], [19]:

$$\begin{aligned} Fl_F(\overline{X}_F, \overline{X}_E) &= 0{,}2511(CP_F(\overline{X}_F)/CP_E(\overline{X}_E))^{-0{,}762} \\ Fl_E(\overline{X}_F, \overline{X}_E) &= 0{,}2225(CP_F(\overline{X}_F)/CP_E(\overline{X}_E))^{0{,}6556} \end{aligned} \tag{5}$$

The payoff function of player 3 (enemy forces) can be defined in the same way lake for player 1.

The three-criteria task formulated for the compromise method with weighting factors k_1, k_2, k_3:

$$\begin{aligned} &\min_{\overline{X}_F}(k_1 F_1(\overline{X}_F) + k_2\ F_2(\overline{X}_F) + k_3\ F_3(\overline{X}_F)); \\ &k_1 + k_2 + k_3 = 1 \wedge k_1 > 0 \wedge k_2 > 0 \wedge k_3 > 0 \end{aligned} \tag{6}$$

with restrictions:

- Own losses may not exceed the limit d_F :
- The losses of the opponent must not be less than the limit value d_E :
- The ratio of the own power potential and the opponent's power must not be less than the limit value,
- The ratio of the sum of the potentials of own forces (tanks of medium and long-range anti-tank means) to the sum of the potentials of tanks, armoured transporters and combat vehicles of enemy infantry forces must not be less than the limit value,
- The ratio of the potential to arm the enemy's own air defence forces to the potential of the enemy assault helicopters must not be less than the limit value,

  $x_{F(E)}(i) \in \{0, 1, \ldots, M\}$, total number of *i*-type modules, where M - is a large integer.

The presented task was solved several times for different scenarios of attack by the E side. A special computational environment was created in our team for generating the grouping of the armed forces of the home (F) side. The computational environment uses various optimization algorithms mostly of an evolutionary nature, including genetic and ant algorithms, as well as a particle swarm algorithm.

3.0 MODEL OF RADIO-ELECTRONIC WARFARE

The evaluation of the impact of radio-electronic warfare (EW) means is a difficult, but at the same time very important problem from the point of view of planning the disruption of radio-electronic devices of airborne attack means. The problem of electronic warfare planning and evaluation was at one time an important research area for the author of the paper and resulted in publications [13], [14]. The difficulty of analysing and evaluating the impact of radio-electronic warfare measures is established in the random nature of the phenomena occurring during a raid. As a result of the research, a certain way of solving this problem has been determined.

Let's assume that:

- Area with objects of military significance (along with their characteristics) is defined;
- Radio-electronic warfare means are deployed around these facilities;
- Groups of aerial attack measures (AAM) can carry out raids on covered facilities;
- Aircraft, which are part of AAM groups, are equipped with various types of navigation, target detection and guidance systems for attacking them, and these devices and command posts (both land and air) are linked to each other through a hierarchical communication network;
- Application of EW measures can introduce perturbations in the operation of this network.

As a measure of the quality of the impact of EW measures, we take the time that elapses between the moment a group of AAM enters the zone protected by the air defence system and the moment the bombers start bombing or firing air-to-ground missiles toward our facilities. This time is the resultant of the execution times associated with recognizing the target, processing the data obtained about the object and its surroundings, and deciding whether to fire at the target. We assume that each of the task execution times is a random variable. Using jamming, it is possible to influence the extension of these times in terms of selected probabilistic characteristics (e.g., the expected value of time, quantiles of different orders of this random variable) and to make it more difficult for a group of AAMs to detect and destroy a ground target. The increment of this time to the first firing or bombing is the basis for comparing different interference plans (different allocations). Several stages can be distinguished in the engagement of elements of the AAM group during the execution of a raid. The evolution of engagement is shown in Figure 2.

The mission of an AAM group is to seek out and fight high-value targets (airfields, command posts, missile launchers, etc.). On the other hand, the purpose of planning the impact of radio-electronic warfare means is to control the **build-up** of engagement of the attacking AAM group during the execution of the raid. In other words, the goal of the **EW** is to make it difficult or impossible for elements of the AAM group to perform certain actions in the process of reconnaissance and target guidance before executing the final attack (dropping bombs or launching missiles). We assume that our reconnaissance services gather information about the characteristics of signals and their processing by the enemy's radio-electronic means. Electronic Countermeasures (ECM) involves the use of jamming and other techniques to disrupt or disable enemy communication and sensor systems. For example, ECM systems can use high-powered RF signals to overwhelm enemy radar, making it difficult for them to detect and track friendly aircraft. Using a variety of interference techniques, EW means can cause the following effects in the operation of radars, communication channels and data transmission lines [13], [14], [15]:

- Slowing down the performance of target recognition and information transmission tasks;
- Reduction in the scope of recognition;

- Confusing aircraft pilots;
- To prevent the reception of data transmissions to elements of the AAM group carrying out a raid from the airborne command centre;
- The need to use two or more beacons (or other types of reconnaissance equipment) at the same time, to detect and identify attack objects.

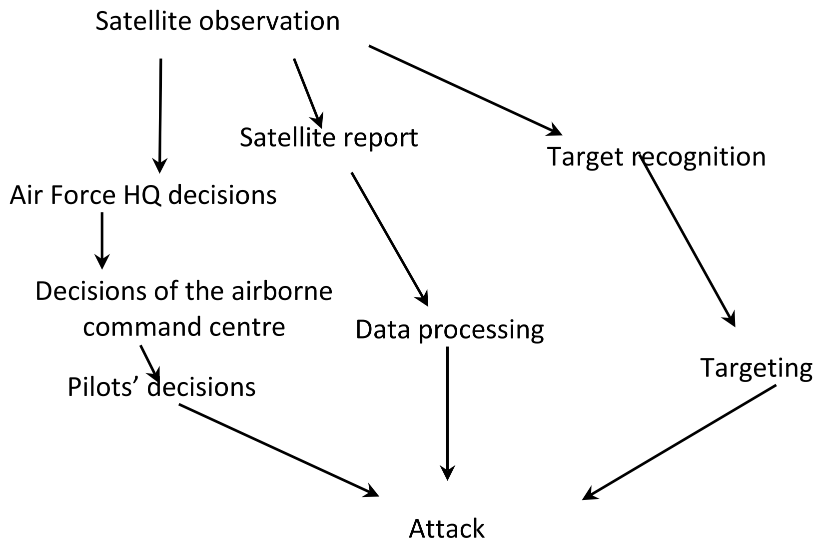

Figure 2: Illustration of the increasing involvement of air force elements performing air-to-ground attack [14].

A model was constructed to support the impact of EW measures operating in the defence system. The model is based on a stochastic network with arcs of random length. A similar model was presented in [14] to show how to determine integrated air defence system (IADS) quality measures. Elements of the model presented in [14] were used to solve radio battle planning tasks. The use of an extended, stochastic, activity network as a model of the functioning of the raiding party proved to be effective from the point of view of determining the characteristics of the radio-electronic warfare system.

The presented combat models illustrate the great complexity of the issues considered. The results obtained in this way can give estimates of selected characteristics of the battlefield, in the introduction it was mentioned that it would be possible to show the influence of other defence elements on the outcome of the battle such as the activity of radio-electronic warfare means.

Due to the lack of physical destruction of combat means during radio-electronic warfare, the problem of assessing the effects of active and passive interference against the electronic devices of these means should be approached quite differently from the assessment of the performance of missile troops, aviation and other fire means.

It seems reasonable to relate the effects of EW directly to the effects of an attack by a single combat unit against shielded or defending objects. A formula should be found to describe the reduction in the effectiveness of fire means when firing or bombarding covered or defending facilities. Two slightly different approaches can be proposed, one presented in the dissertation [13] and the other in the article [14]. In the first approach, the essence is to take into account the deviation of AAM trajectory and faulty guidance by navigation and bombing means depending on the intensity of jamming emitted by the jamming stations affecting this target, resulting in correspondingly lower losses of the bombed object. A characterization under the name of the probability of not destroying a ground object using directed radar interference is given there.

In the second approach, a raid model is considered in the form of a network with arcs, which are assigned random variables describing the durations of the activities performed by the electronic devices of the AAM group. The effect of interference is to change the duration of activities in the sense of the distribution of random variables, and only those activities that are on the critical path that is, ultimately, the time to the first firing (bombing), performed by the AAM group, which is a measure of the quality of the interference.

A very important parameter of the defending system is the time to the first firing of the attacking means, allowing to determine the time of lossless movement of the group of attacking means. To determine this characteristic, with some simplifying assumptions, a similar model and method can be used as in the case of evaluating the effectiveness of interference [14].

4.0 SUMMARY

Analysis of the country's future security environment, and in particular of future threats, requires the use of expert qualitative methods. These can be enhanced by using data mining methods that allow automating the search for hidden patterns, associations and trends in data collected in databases on security issues. Assessment of the possibility of specific threats within a certain time horizon, should be enhanced by the use of forecasting and simulation tools, implemented in the form of IT applications. The paper presents the idea of acquiring the capabilities of the armed forces, including in the selected area of electronic warfare capabilities. It provides a contribution to conducting analysis of military operations in a multi-domain environment. What is required is a good characterization of military operations in a multi-domain environment, taking into account current technologies in combat systems. In addition, the current problem is to develop a method for studying the impact of emerging and disruptive technologies (EDTs) on specific AF capabilities, and this includes developing a method for mapping emerging and disruptive technologies to capabilities in strike (jamming), command, battlefield protection, reconnaissance and logistics by functional capability component. From this emerges the need to identify specific operational capabilities and combat domains in which EDTs will be relevant, a description of methods for dimensioning operational capabilities according to their functional components - a description of metrics and methods for their determination in order to assess the impact of EDTs on these capabilities.

5.0 REFERENCES

[1] Najgebauer A. et al, System of IT support for capability development and identification of operational needs of the Polish Armed Forces. Appendix 1 to the final report on the implementation of the project for national defence and security. Substantive report on scientific research performed. MUT, Warsaw 2016.

[2] Janczak J., Pilarski G., System of IT support for capability development and identification of operational needs of the Polish Armed Forces. Development of a methodology for planning, budgeting and forecasting the development of capabilities of the Armed Forces of the Republic of Poland. Dictionary of Defence Planning Concepts in the Context of Capabilities of the Armed Forces of the Republic of Poland, Part II, AON, Warsaw 2014.

[3] System of IT support for capability development and identification of operational needs of the AF RP. Report on the realization of research task II.1 Development of a model and algorithms for the functioning of the SZ RP taking into account the current defence strategy of the Republic of Poland, part II, AON, Warsaw 2013

[4] System of IT support for capability development and identification of operational needs of the AF RP. Report on the implementation of research task IV.2. Design and implementation and testing of the prototype of the planning, programming and budgeting system, part II, Asseco, Warsaw 2015.

[5] System of IT support for capability development and identification of operational needs of the AF RP. Report on the implementation of research task II.3 Development of a model and algorithms for the functioning of the AF RP taking into account the current defence strategy of the Republic of Poland, Asseco, Warsaw 2013.

[6] Banasik M., System of IT support for capability development and identification of operational needs of the Polish Armed Forces. Report on the implementation of research task V.3 Subtask 14.3.1 Description of the process of planning and programming the development of the Polish Armed Forces based on capabilities, AON, Warsaw 2013.

[7] Davis P.K., Analytic Architecture for Capabilities-based Planning, Mission_System Analysis and Transformation. RAND Corporation Publication MR 1513, 2002.

[8] Stoner J., Wankel C. Directing, PWE, 1992.

[9] Capabilities-Based Assessment (CBA) Guide Version 3.1. 10 May 2010. TRADOC.

[10] Najgebauer A. et al, System of IT support for capability development and identification of operational needs of the SZ RP. Report on the implementation of research task II.1 Development of a model and algorithms for the functioning of the SZ RP taking into account the current defence strategy of the RP, MUT, Warsaw 2013.

[11] Najgebauer A. et al, System of IT support for capability development and identification of operational needs of the SZRP. Report on the implementation of research task IV.1. Design and implementation and testing of the prototype of the planning, programming and budgeting system, MUT, Warsaw 2015

[12] Najgebauer A., Antkiewicz R., Methods of IT support for the assessment of strike and cyber capabilities of the Polish Armed Forces. Chapter of the monograph Information systems for the needs of state security and national economy: applications, Z. Tarapata, Editor, Warsaw: Military University of Technology, 2019.

[13] Najgebauer A. Computer support for directing the radio-electronic jamming of airborne radiolocation devices of airborne attack means. Doctoral dissertation, Military University of Technology. Warsaw 1988.

[14] Najgebauer A., A Stochastic Network Model for Evaluating of Electronic Countermeasures Effectiveness in Air-Land Battle. Systems Analysis Modelling Simulation, 1996, Vol.24, pp.81-95. Amsterdam B.V. The Netherlands under license by Gordon and Breach Science Publishers.

[15] Adamy, D. EW 105: Space Electronic Warfare, Artech, 2021

[16] Najgebauer A, Antkiewicz R, Pierzchała D. and Rulka J., The Computational Intelligence Methods for the Armed Forces Capabilities Allocation Problem, 2018 IEEE Symposium Series on Computational Intelligence (SSCI), Bangalore, India, 2018, pp. 1723-1730, doi: 10.1109/SSCI.2018.8628787.

[17] Najgebauer A, War Games, Simulation and CI Tools for Strategic Planning, © 2020 EUROSIS-ETI Publication, ISBN: 978-9492859-12-9, EAN: 9789492859129.

[18] Student text 100-3, Battle book, U.S. Army Command and General Staff College Fort Leavenworth, Kansas ACADEMIC YEAR 2007/08

[19] Zanella J.A., Combat Power Analysis is Combat Power Density, School for Advanced Military Studies (SAMS), 201 Reynolds Avenue Fort Leavenworth, Kansas, USA, 2012.