Recenzovaný článek

Methodological Framework for Operational Risk Assessment

Metodologický rámec hodnocení operačních rizik

Josef Procházka, Josef Melichar

Abstract: The article brings a "Condition-If-Then" construct as a proven protocol for writing risk statement and its application into assessing risks related to capability gaps identified during the defense planning processAuthors discuss utility of "Common approach" and "Impact averse approach" to risk rank ordering as a tool for ordering risks according to their importance. Using the discussed tools enables the planners to run risk assessment that sets preconditions for prioritizing the Force Development Options (FDOs) and for minimizing the impact of capability gaps on conduct of future operations. The ORAMF and the application of the given protocol for writing risks are some of the building blocks of the defense planning process, offering a toolset for reinforcement of the defense planning of the Czech Republic.

Abstrakt: Článek přináší „Condition-If-Then" konstrukci jako osvědčený protokol pro vyjádření rizika a jeho aplikaci při posuzování rizik souvisejících s nedostatky ve schopnostech identifikovanými v průběhu procesu obranného plánování. Autoři diskutují využitelnost obvyklého přístupu a přístupu založeného na hodnocení dopadu ke stanovení pořadí rizik, jako nástroje ke stanovení tohoto pořadí podle důležitosti rizik. Využití diskutovaných nástrojů pro stanovení pořadí rizik umožní plánovačům realizovat posouzení rizik, které vytvoří podmínky pro prioritizaci variant rozvoje sil (VRS) a pro minimalizaci dopadu nedostatků ve schopnostech na vedení budoucích operací. MRHOR a aplikování uvedeného protokolu pro vyjádření rizika jsou stavebními kameny procesu obranného plánování a nabízejí nástroje pro posílení obranného plánování České republiky.

Keywords: Risk Assessment; Impact; Probability; Impact Area; Risk Identification; Risk Prioritization; Capability Gap.

Klíčová slova: Hodnocení rizik; dopad; pravděpodobnost; oblast dopadu; identifikace rizik; prioritizace rizik, nedostatky ve schopnostech.

INTRODUCTION

Every strategic (long-term) plan is saturated with risks, defined as the effect of uncertainty on objectives. Indeed, there is considerable interest in both defense and non-defense organizations to include risk management in their strategic planning processes.[1]

Risk assessment sets preconditions for prioritizing options for capability development, thus it requires rigorous and complex approach in order to minimize negative impact on conduct of future operations.

Authors propose integrating risk management practices within defense planning, providing a framework for how risk management (as defined in ISO 31000:2009) can be systematically integrated into defense planning processes. This Framework depicts risk assessment procedures as part of risk management process and helps analysts to apply risk assessment in support of capability analysis. The framework reflects the ISO risk management process with specific emphasis on the definition of risk: the effect of uncertainty on the (organization's) objectives.

Furthermore, the ORAMF has been designed from the defense planner's point of view, since it is the defense planner who must ensure that the intellectual effort carried out in support of a planning process and inherent risk assessment is valid, verifiable, consistent, and rigorous. Therefore, the article's ambition is to offer sound methodological framework for defense planners and stakeholders involved in capability development, defense planning and decision-making.

The ORAMF provides effective tools and techniques for determining risks inherent to the defense planning process, for assessing operational risks and for developing propositions for prioritizing capability development options.

The authors offer an innovative methodology for further discussion and best practices for development of a sound risk assessment process and its analytical support.

ORAMF and the application of the given protocol for writing risks have been drafted, based on the need arising from the gaps in the defense planning of the Czech Republic identified by previous research papers[2345]. As the findings show, risk assessment has not been fully implemented yet, which, seen from the other end, presents an opportunity to create value added.

---

1 Analysis Support Guide for Risk-Based Strategic Planning. Scienece and Technology Organisation, Technical Report *STO-TR-SAS-093-Part-I.2017.*

2 MELICHAR, Josef. *Plánování na základě schopností v procesu obranného plánování s využitím prognostických metod v podmínkách rezortu obrany ČR.* Studie. Brno: Univerzita obrany, 2015, 40 s.

3 MELICHAR, Josef; PARGÁČ, Petr; LEŠTINSKÝ, Boris. *Kvalitativní výzkum využívání postupů pro stanovení požadavků na schopnosti a pro plánování rozvoje schopností v resortu MO ČR.* Studie. Brno: 2017, 22 s.

4 BAXA, Fabian. *Stav plánování schopností v rezortu obrany ČR a jeho příčiny.* Studie. Brno: CBVSS, 2015, 33 s.

5 MELICHAR, Josef; PROCHÁZKA, Josef; PROCHÁZKA, Dalibor; HODICKÝ, Jan. *Ověření návrhu rámce pro plánování schopností, hodnocení rizik a využití válečné hry pro plánování schopností.* 2017, 41 s.

RISKS IN THE PLANNING PROCESS

Capability Based Defense Planning Framework (CBDPF), as shown on the figure bellow, has been developed and accustomed to the Czech Ministry of Defense environment as one of the outputs of the research project STRATAL. The CBDPF consists of 5 phases (1) Political Guidance Review, (2) Determining Capability Requirements, (3) Capability Development Planning, (4) Implementation, (5) Capability Development Review, out of which phase (4) Implementation is not sequential and is implemented permanently in parallel with other four sequential phases.

Phases (1) – (3) and (5) are implemented periodically in a sequence that enables developing capabilities that keep their relevance in future security environment.

Drafting the CBDPF has been based on the outputs of analyses of the approaches to planning, and the experience of the USA[6], Canada[7] Norway[8] and Technical Cooperation Program countries[9], as well as the experience and findings of NATO.[10] NATO Defense Planning Process (NDPP) was the fundamental inspiration for the CBDPF, as the Czech Republic participates in the NDPP and there is a need to run a comprehensive national defense planning process that is complementary to the NDPP and that provides country specific outputs. The 5 phases of the CBDPF relate to the 5 phases of the NDPP that are: (1) Establish Political guidance, (2) Determine Capability Requirements, (3) Apportion requirements, Set targets, (4) Facilitate implementation, (5) Review results. The CBDPF accommodates the need for the risk assessment related to capability gaps, which served as an incentive for designing the ORAMF, which has been designed as an inherent part of the CBDPF.

The need for ORAMF type arises in phase (2) "Determining Capability Requirements" of the CBDPF. I comes into place once comparison of Capability requirements and Current and planned Capabilities has been accomplished and Capability gaps have been identified. Risk Assessment is the next crucial step of phase (2) of the CBDPF after "Comparison." Sound Risk Assessment provides defensible arguments for prioritizing the FDOs.

6 DAVIS, Paul, K. RAND National Defence Research Institute, 2002. *Analytic Architectire for Capabilities-Based Planning, Mission-System Analysis, and Transformation, dostupné na internetu:* http://www.rand.org/pubs/monograph_reports/MR1513.html

7 (Capability Based Planning Handbook, MOD Canada, June 2014, 2014)

8 GLAERUM, Sigurd, Alf Christian Hennum, *Analytical Support to Norwegian Long-Term Defense Planning*, Czech Military Review, Brno, Czech Republic, pp. 82-91, 2016, Extraordinary volume, ISSN 1210-3292.

9 DAVIE, M., Comparative Defense Planning Lessons for New Zealand, Palmerston North, New Zealand, 2013

10 RTO/NATO, *„Handbook on Long Term Defense Planning"*, St. Joseph Print Group Inc., Otawa, 2003. ISBN 92-837-1098-3.

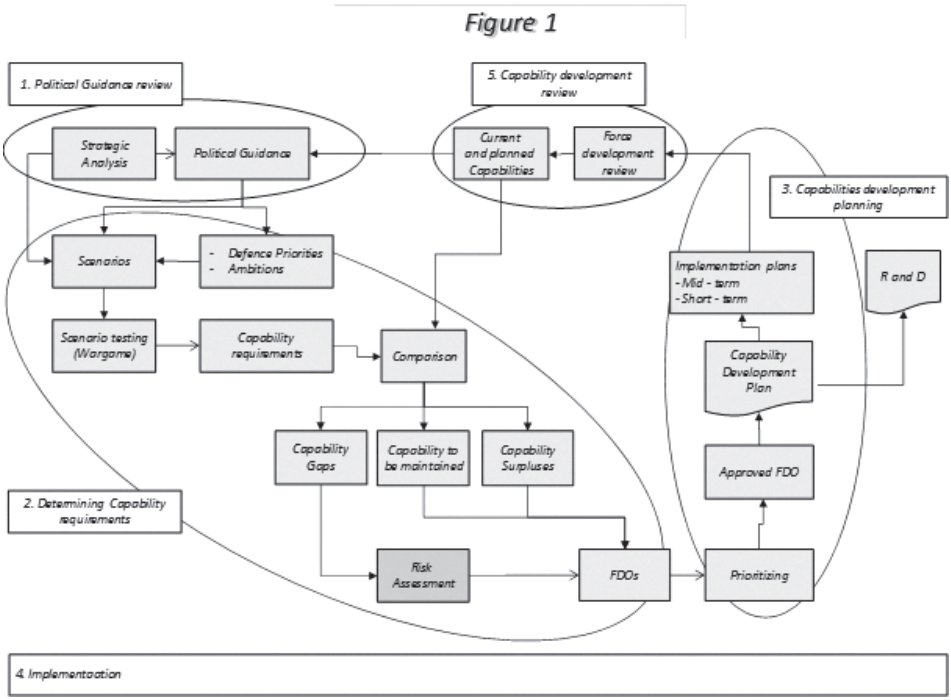


Figure No. 1: Capability Based Defence Planning Framework (CBDPF)

RISK ASSESSMENT IN SCENARIO CONTEXT

Sound risk assessment is based on clear understanding to the term „risk" and on an agreed and well understood risk statement. Risk statement enables the analysts to deliver sound risk assessment and defensible risk prioritization.

„Risk is an event that, if it occurs, adversely affects the ability of a project to achieve its outcome objectives."[11]

Contemporary understanding to the term „Risk" relates this term to a possibility of damage occurrence, loss, destruction or failure.[12]

„Risk is defined as a cumulative effect of the probability of uncertain occurrences that may positively or negatively affect project objectives".[13]

11 GARVEY, Paul, R., Analytical methods for risk management: a system engineering perspective, Chapman and Hall/CRC; 1st edition (1601), Bedford, Massachusets, USA, 2008, ISBN 978-1-58488-637-2

12 SMEJKAL, V., RAIS, K, Řízení rizik ve firmách a jiných organizacích. 4. vydání. Praha: Grada Publishing, 2013, 488 s. Expert. ISBN 978-80-247-4644-9.

13 PITCHARD, Carl, L., Risk Management: Concepts and Guidance, Fifth edition, CRC Press, Taylor & Francis group, USA, 2015, ISBN 978-1-4822-5845-5

From the „risk" definitions there is an understanding to the risk as the level of danger that the threat will materialize, causing undesired result causing a damage (undesired consequence or Impact). The volume of risk is expressed as risk level.

There are two major attributes of risk event stemming from risk definitions. Its occurrence probability and Impact on Impact Area (IA). IAs in context of CBDPF relate to the protected interests (security interests) and to the scenarios that are inherent part of the CBDPF. Scenarios describe situations, in which identified security threats may materialize, causing a damage to the security interests. Scenarios in their normative part[14] describe the objectives that are necessary to be achieved in order to protect the security interests projected into given scenarios. The objectives and key tasks (KT) described in scenarios, together with own force represent the three basic IAs to be considered.

A general expression of risk with these two attributes (probability and impact) is given by the Equation:

Risk = F (Probability, Impact)

IAs in the CBDPF context. The objectives and key tasks might differ in each scenario significantly; own force will differ in type and volume. IAs for scenarios e.g. *„Strategic Assault"* or *„Hybrid Attack"* will typically be *"Freedom of movement for Humanitarian assistance in conflict zone", "Border area x-y of a country ZU secure" (objectives); "Eliminate the adversary forces from the border area" (KT); "own force"* will cover lives and health of own force and own materiel. A *„Cyber Attack"* scenario then might have different IAs: *„Water supply system running smoothly without disturbances"* (objective); *„Eliminate Malicious software causing malfunctions of water purification section", „Clean water distribution network", „Provide sufficient volume of drinking water supply to the town"* (KT). *„People on the water distribution network of respective town (health, lives)"* represent additional IA to own force.

To work sensibly with risks, they should be expressed by agreed and proven protocol. Best practice for writing risks[15] is expressing them in a form of *„Risk Statement".* Risk Statement provides clarity and information about the risk, so that the risk assessment constituting probability of risk occurrence and its impact or consequence is defensible.

A proven protocol for writing a Risk Statement is the *Condition-If-Then* construct. The ***Condition*** reflects what is known today, in the CBDPF context, condition represents identified capability gap that can cause a risk event to occur with certain probability. ***If*** represents a risk event that, if it occurs, it has negative impact (consequences). ***Then*** represents the impact (consequence) event, that means if the risk event occurs, then it impacts on IAs (it has consequences for IAs).

---

14 MELICHAR, Josef. Scénáře – tvorba, vnitřní struktura, scénáře a bezpečnostní hrozby. *Vojenské rozhledy.* 2017, 26 (2), 18-32. DOI: 10.3849/2336- 2995.26.2017.02.018-032. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz

15 GARVEY, Paul, R., Analytical methods for risk management: a system engineering perspective, Chapman and Hall/CRC; 1st edition (1601), Bedford, Massachusets, USA, 2008, ISBN 978-1-58488-637-2

To illustrate the protocol, suppose there is a Condition (Capability Gap) 1 and If (the risk event) 11. Numbering here serves to show the link from Capability Gap to the Risk event and to the Consequence/Impact events.
The scenario for this illustrative example – Random Cyber-attack (Cyber-Attack on Water supply system of a medium sized town)

IAs:

IA 1 - Objective: „Water supply system running smoothly without disturbances"
IA 2 – Key Task: „Eliminate Malicious software causing malfunctions of water purification section"
IA 3 – People: „People dependent on the water distribution network of respective town (health, lives)"

Condition (Capability Gap) A – Xth generation firewall that represents Computer Network Operations Capability (specifically Computer Network Operations defense capability).

If (the risk event) AA – Malicious virus penetrates computers in a control system and interferes with computer operations. Specifically, computer that controls the processes for water purification and distribution to the companies and households of a medium size town has been penetrated by malicious software. Malicious software is developed to interfere with computer operations necessary for purifying water and for seamless water distribution throughout the town.

Then (the Impact/Consequence event):

111 Water purification section malfunctioning.
112 Water distribution network polluted by contaminated water
113 Health problems and diseases.

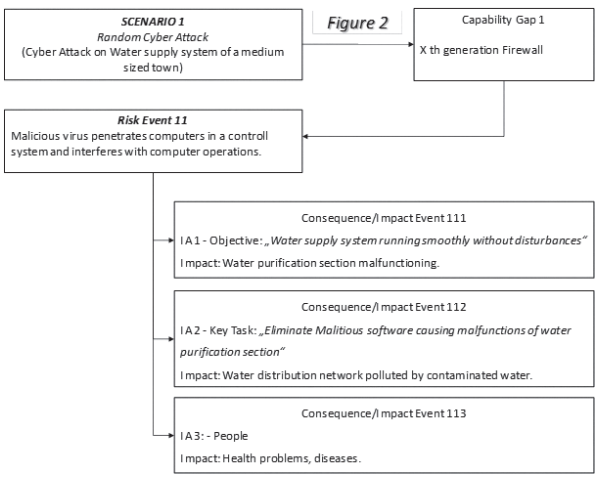


Figure No. 2: Illustrative example of Condition-If-Then construct of a risk statement

The Condition-If part of the risk statement reflects probability of risk event to occur if the Capability gap exists. The Then part of the risk statement contains additional information describing the risk event's consequences (Impact on IAs). Impact of risk events is assessed against the IAs in each scenario. An illustrative example of a risk statement in Cyber attack scenario context is shown in the Figure bellow.

ESTABLISHING THE PROCESS

The ORAMF is based on a process consisting of following steps: (1) Impact Areas (IA) review; (2) Risk identification; (3) Probability assessment; (4) Impact assessment; (5) Risk prioritization; (6) Risk mitigation.
The ORAMF provides answers to the following questions:
What areas of interest (Impact Areas) will be impacted?
What are the risks to IAs in each scenario?
What is the probability of risk occurrence?
What is the impact (consequence) of a risk event, if it occurs?
What is the risk priority order?
How to mitigate the impact of identified risks?[16]

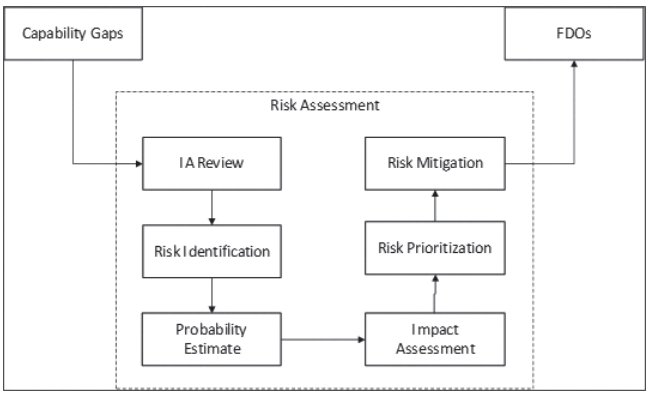


Figure No. 3: Risk Assessment Framework

IMPACT AREAS REVIEW

IA review is the initial step of the ORAMF, during this step the risk assessment team should review IAs that stem from the security interests stated in The Security Strategy of the Czech Republic and from each considered Scenario that has been tested and analyzed through steps of operations planning process. IAs may change based on the out-

16 FDOs – Force Development Options

comes of the scenario review, reflecting the changes in the security environment and specific changes in the scenario objectives and key tasks. Up to date set of IAs provides a firm foundation for risk assessment criteria. Set of IAs in generic terms, as mentioned earlier, will typically include scenario objectives, key tasks and own force. IAs in each scenario will differ based on scenario characteristic, e.g. *Strategic assault* scenario will embrace different objectives, different key tasks and will require different force package then e.g. *Cyber defense scenario.* Clearly described set of IAs makes risk identification focused and creates conditions for thorough risk identification.

RISK IDENTIFICATION

Risk identification is a critical step of risk assessment process. The objective of this step is an early and continuous identification of operational risks stemming from capability gaps to ensure that all the potential operational risks could be managed proactively instead of reacting on a risk event on its occurrence in operations. Risks related to capability gaps have to be identified for each scenario and clearly described. Failure to identify risks relevant to the respective scenario and to identified IAs may cause undesired consequences. Perhaps the key failing that appears over time is a description of a risk event.

For rigorous risk identification it is necessary to elaborate scenarios into appropriate level of detail that means specific scenarios should be used for this purpose. Specific scenarios provide sufficient information and details so that the risk identification can proceed with required level of granularity. Risks are then identified during applied use of operations planning process and war gaming techniques.

PROBABILITY ESTIMATE

Once the risk events have been identified, it is necessary to estimate probability of occurrence of each risk event. The risk events are events that may or may not occur with probability „P“ faling into interval 0 – 1. In context of CBDPF the probability of risk occurrence will depend on number of factors: objectives of the source of threat/potential opponent, willingness of the potential opponent to seize the opportunity given by capability gaps, rapid changes in nature or unforeseen technological advances, to name just a few. These are some factors that make difficult to establish specific and exact level of probability, it will typically be a qualified and informed estimate at best. Probability interval 0 - 1 should be scaled (3 to 5 levels of probability with set boundaries for each probability level). A probability can be expressed as percentage (e.g. 60%), as a value statement (e.g. extremely likely), as a comparison (e.g. D1 highway congested at rush hours), or as a frequency level (e.g. in at least four or five instances per week). Probability boundaries can be set as follows: 1 – 30% - low probability with the threshold 30% for maximum value accepted for a low probability, 31 – 60% - medium probability with

the threshold 60% for maximum value accepted for medium probability etc. Risk events with probability estimated as 0 – 1% should not be taken out of further assessment only for extremely low probability, as some risk events may have catastrophic impact (consequences) if they occur, and it is not possible to say with certainty that these risk events will not occur in the future.

IMPACT ASSESSMENT

Impact Assessment is related to IAs, which means it is necessary to have a clear list of IAs identified and up to date for each scenario. The IAs considered within ORAMF consist generally of three broad areas, own force (own human assets, own non-human assets), scenario objectives and key tasks, against which the impact is assessed. Risk event may have different impact on achieving the objectives, on key tasks, on human assets (casualties), or on non-human assets (weapon systems, equipment, etc. damages or losses). Impact can be expressed in numbers (e.g. number of casualties, number of destroyed weapon systems, etc.), or described qualitatively when numbers are not relevant (e.g. achieving the objectives delayed, objective not achieved, etc.). For rigorous Impact Assessment it is recommended to combine qualitative and quantitative approach and assess the impact of each risk event in context of the overall scenario end-state. Furthermore, the team conducting the impact assessment will add a weight to each impact event as additional attribute that will be considered during Risk Prioritization.

RISK PRIORITIZATION

Risk events are analyzed in terms of their occurrence probability and potential impact on given scenario IAs (objectives, key tasks and own forces). Risks are prioritized in terms of establishing risk importance ranking from most to least critical, using common approach with ordinal scale. This approach is based on grouping the risk events into probability and impact categories. That requires developing ordinal scales that are measurement scales in which attributes are assigned a number representing order. The ordinal risk matrix is widely used approach for ordering risks into priority or criticality categories. Figure bellow represents an illustrative example 3 x 3 ordinal risk matrix.

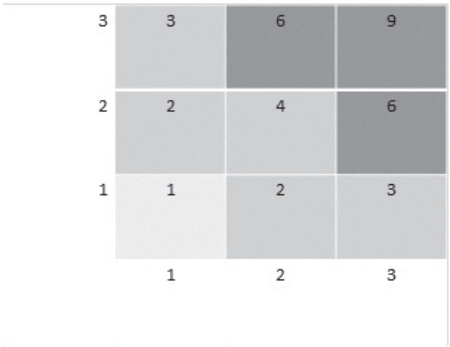
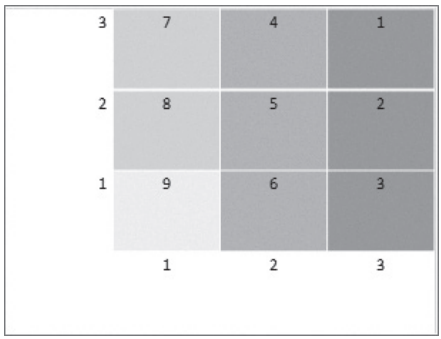


Figure No. 4: 3×3 ordinal risk matrix – Common approach

Two ordinal scales define this matrix. Scale for probability level is distributed along the vertical side of the matrix and for the impact (consequence) level along its horizontal side. The probability level 3 represents the highest likelihood of the risk event occurrence, the probability level 1 represents the lowest likelihood of the risk event occurrence, probability level 3 represents the highest level of the risk event occurrence. This rule is valid likewise for the impact levels.

Common approach to prioritizing risk events distributed across the risk matrix means multiplying the impact and probability levels attributed to each square and use the results to define each square's score. The square's score defines the risk event priority order. The higher the score, the higher the priority. Problem with this approach is that arithmetical operations with ordinal numbers are not permissible.[17] This results in squares with different probability and impact value having the same score. That requires additional assessment of risk events and adding additional attribute to them in order to prioritize events with the same score. Adding weight to the impact provides more granularity to common approach.



Common approach can be also modified to eliminate the „equal scores" trap. A possible modification is to apply risk rank ordering by the level of impact. That implies the highest priority to be assigned to all the risk events within the highest impact column, and priority ordering within that column to be based on the level of probability. This approach is called Impact Averse approach as the risks are prioritized strictly by the level of Impact.

Figure No. 5: 3×3 ordinal matrix Impact averse approach

As the figure above shows, the risk events priority ordering here is different from priority ordering in common approach. Probability receives a supporting role; while the impact is a driving factor when assigning priority order to the risk events. Assigning priority order to the risk events is implemented in several iterations in order to deliver consolidated results. To support decision making when selecting a capability development option for implementation, an agreed threshold for acceptable risk level for each capability gap should be determined. That means necessity to assess the risk acceptability for each risk event related to the respective capability gap individually and based on the results, group the risk events into risk priority groups. (Group 1 – unacceptable risks, Group 2 – conditionally acceptable risks, Group 3 – acceptable risks).

17 GARVEY, Paul, R., Analytical methods for risk management: a system engineering perspective, Chapman and Hall/CRC; 1st edition (1601), Bedford, Massachusets, USA, 2008, ISBN 978-1-58488-637-2

RISK MITIGATION

At this stage of the ORAMF, risk mitigation means identifying options to fill the capability gaps based on risk prioritization results that show their criticality. Capability gaps with unacceptable risks are included into the prioritized options for capability development. Capability gaps with associated conditionally acceptable risks require careful assessment of the conditions that have to exist in order to accept the risks. Capability gaps with associated acceptable risks are not taken into further considerations.

There are different options for proceeding with Risk Mitigation. Firstly, adding a new capability to the existing or planned forces (modernization). Secondly, acquiring the assets that will deliver required capability through the acquisition process (new system). Thirdly, mitigating capability gap via capability sharing based on multinational arrangements e.g. Pooling and Sharing, Smart Defense etc. or via outsourcing (private sector). Risk assessment may also result in a proposition to lower the Level of Ambitions as a risk mitigation measure, if the set objectives are unattainable within specific timeframe, budget or due to technical immaturity.

Risk mitigation measures materialize in prioritized set of FDOs. Once the preferred FDO has been approved for implementation, it represents risk mitigation measures to the identified capability gaps.

Capability Gaps Identification and Risk Assessment – Case Study

„EPIDEMIE“ case study scenario embraces one of the potential planning situation with which the Armed Forces of the Czech Republic (CZAF) might be confronted today and also in the future. It is the supporting task of the CZAF to assist Integrated Rescue System in non-military kind of crisis situations. This scenario was elaborated in order to identify required capabilities of medical service of the CZAF in long-term time span (till 2025 and beyond). Following process was applied:

1. Scenario development and mission-to-task decomposition

In order to identify required capability, the mission-to-task decomposition was conducted, embracing definition of political end state, strategic end state, strategic objectives and effects, operational objectives and effects and key military tasks. In fact, the mission statement was analyzed by planners, using operations planning procedures. Several key tasks have been identified as an outcome of this process. Each key task constituted a capability, the medical services require for successful fulfillment of this operation (scenario).

2. Capability assessment and capability mismatch analysis

Furthermore, the required capabilities were compared to the existing and planned ones of the Medical service of the CZAF. For more structured way the, capability assessment was conducted with the assistance of DOTMLPFI methodology (functional areas) which was applied for each key military task separately. Functional areas embraces: (1) Doctrines; (2) Organization; (3) Training; (4) Material; (5) Leadership; (6) Personnel; (7) Facilities ; and (8) Interoperability.[18] There are conditions that have to exist in each functional area, that allow the capability to function. For example the capability "Mechanized battalion" requires following inputs structured as above mentioned functional areas: Doctrines (SOP[19]s, TTP[20]s) that regulate employment of the battalion, Organization (specific organizational structure) that allows the battalion to function, Training (the unit needs to achieve and maintain required level of skills), Materiel (weapons, equipment,…), Leadership (leaders need to achieve the required level of leadership skills), Personnel (to fill in positions in the organizational structure), Facilities (military barracks, military training areas, etc.). Interoperability enables the capability to operate as a part of larger international organizational structure using different systems and different platforms. Fulfilling required conditions in each functional area allows each capability to exist and to function. Using functional areas allows for structured description of the status of each capability and offers possibility to assess capability development comprehensively.

3. Risk Assessment

Identified capability mismatches were subject to risk assessment, which was conducted with support of subject matter experts in this area.

It was implemented in following steps:

- Firstly, three impact areas were identified: (1) successful objectives implementation, (2) potential human casualties and (3) material loses.
- Secondly: three levels of risk were defined: (1) Unacceptable (red); (2) Conditionally Acceptable (yellow); (3) Acceptable (green)
- Thirdly, risk assessment was conducted by answering following questions:
    a) What is the probability that any particular capability gap will affect successful objective fulfillment and lead to casualties and material losses?
    b) What is the impact on successful objective achievement caused by risk events occurring due to particular capability gap? Following criteria were employed (the objectives will not be achieved; achievement of the objec-

18 Ministr of Defence Directive 66/2012, Activity Planning and Development of Ministry of Defence

19 Standard Operating Procedure

20 Tactics, Techiques, Procedures

tives will be significantly affected, e.g. the objectives will be significantly delayed; achievement of the objectives will be partially affected).

c) What is the potential impact on own force (volume of casualties during execution of the operation/scenario) related to this particular capability gap? Following scaling was used: 1 - significant number of casualties, 2 - moderate number of casualties, 3 - no casualties foreseen.
d) What is the potential impact on own force (volume of materiel losses or damages during execution of the operation/scenario) related to this particular capability gap? Following scaling was used: 1 - significant number of equipment will be lost, 2 - moderate number of equipment will be lost, 3 - no equipment losses are expected.

Remarks: this scaling might be subject to reconsideration, different criteria might be used and quantitative as well as qualitative assessment might be introduced.

- Next step was to identify combined level of risk and establish level of urgency of each capability gap. It means that prioritizing capability gaps reflected the identified impact related to each capability gap. Each capability gap received the urgency number 1, 2 or 3.
- Finally, recommendations for capability gap mitigation were proposed and action plan was developed accordingly.

Figure 6 demonstrates the outcome of the case study in generic way. Key military tasks (KT) have been assessed in a structured way, using functional areas (DOTMLPFI) methodology. Each KT was subject to capability assessment. In this process, the existing as well as planned capabilities have been assessed against the KT with the aim to identify shortfalls in each functional area. These shortfalls create conditions for potential risks to the fulfillment of KT. In general terms, it impacts on the successful achievement of the overall scenario objective (the end state). The level of impact is color-coded. Green color of capability gap means, that the impact on mission success is low and risk mitigation is not urgent. Yellow color means that the impact on mission execution is significant and might cause casualties and loses on equipment. Risk mitigation is urgent. Third level of capability gap constitutes unacceptable level of risk (red color) to mission success. Without such a capability it is impossible to achieve expected outcomes and significant number of casualties and losses on material must be taken into consideration. Such requirement is of utmost importance and the risk mitigation has the highest priority. For more details, refer to reference 13.

	D	O	T	M	L	P	F	I
KT1								
KT2		GAP3	GAP3					
KT3							GAP2	
KT4				GAP1			GAP2	
KT5						GAP3		
KT6				GAP1		GAP2	GAP2	
KT7				GAP2		GAP2		

Figure No. 6: Capability gap operational risk and priority assessment

CONCLUSIONS

The Operational Risk Analytical Framework for Defense Planning was developed with the aim to provide defense planners with a way to integrate risk management systematically and explicitly into the analytical support provided to defense planning. The resulting framework uses the ISO 31000:2009 standard as the basis to describe the risk assessment process. It provides a way for integrating risk assessment systematically into the defense planning process. It offers a way to verify the outputs stemming from capability assessment and capability gap analysis.

The ORAMF offers a process consisting of 6 sequential steps that lead the planners from identified capability gaps to Force Development Options accompanied by list of prioritized risks related to capability gaps and proposed risk mitigation measures. The process begins with the review of Impact Areas that might be affected, should capability gaps remain unresolved. It continues then with identifying risks (identifying risk events that may occur due to the existing capability gap). Risk identification is followed by estimating probability of risk occurrence. Impact of risk event on IAs is then assessed in order to get a picture of potential consequences of unresolved capability gaps.

Based on the results of impact assessment and probability estimate, risks are prioritized and subsequently risk mitigation measures drafted. The recommended approach for prioritizing risks, as discussed in the article, is the Impact averse approach that prevents pitfall of arriving at the same score for different risks with different impact on IAs.

Implementing the ORAMF, the "Condition-If-Then" protocol for writing risk statement, and using the Impact averse approach to risk assessment can significantly reinforce the ability to draft well informed and evidence based FDOs and to provide defensible arguments to the decision makers for justification of future military needs.

The described methodological framework has been developed and adapted to support decision-making process within the Czech Ministry of Defense with evidence-based and defensible arguments and solid framework for justification of future military needs.

The ORAMF is one of the outputs of the Centre for Security and Military Strategic Studies of University of Defense in Brno institutional research project "STRATAL" – Strategic

Alternatives for the Development of the Czech Armed Forces, that has been conducted by the Centre for Security and Military Strategic Studies of University of Defense in Brno since 2016.

Authors: ***Col. Ing. Josef Melichar,*** *born 1962. A graduate of the Military Academy Brno (1980–1985). He is also a graduate of Fort Lee (USA) and several courses in Oberammergau (Germany). He worked in the field of logistics in management and staff positions. He has participated in military operations in the territory of Bosnia and Herzegovina, Kosovo, Afghanistan, the Republic of Chad and the Central African Republic. He worked as a national representative at AFNORTH (Brunssum, the Netherlands) and in 2009–2012 as a specialist for psychological operations and evaluation of operations at JFC Brunssum. He is currently working at the CBVSS UO in Brno, where he dealt with the theory and practice of strategic management.*

Josef Procházka, Ph.D., *born in 1966. He is graduate of the Military Academy Brno (VAAZ), 1990–1996 he served with the troops in the field of technological and automobile support; 1996–1999 staff functions at the General Staff and the Ministry of Defence, line of work logistics and acquisition; 2000-2007 Institute for Strategic Studies (ÚSS) Brno; 2007-2011 Department of Defence Policy and Strategy, Ministry of Defence. From the year 2011, defence advisor to the Czech Permanent Delegation to NATO – sources and armaments. His military career was finished in 2007. Doctoral study programme management of state defence, he graduated from the University of Defence Brno in 2005. From 1999 till a 2004 he served in SFOR and EUFOR missions, at the region of Bosnia and Herzegovina; in 1995, 2002 and 2008 he was abroad, on short-term attachments on logistics, management sources, security policy. In 2005, General Staff Course, Brno. He an author dealing with managements sources, defence planning, logistics and armaments.*

How to cite: MELICHAR, Josef and PROCHÁZKA, Josef. Methodological Framework for Operational Risk Assessment. *Vojenské rozhledy*. 2017, 26 (4), 19-34. DOI: 10.3849/2336-2995.26.2017.04.019-034. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz