Team 04: NATO MSG-088
"Data Farming In Support Of NATO"
Case Study "Force Protection"

TEAM 04 MEMBERS

GEIGER, André – Team Leader
BWB, Germany

CAPPELINI, Ronald
JORDAN, John
SANCHEZ, Paul
NPS, USA

VIEIRA, Helcio
NPS, Brazil

HENNE, Oliver
NPS, Germany

WAN, Szu Ching
DSO-ORL, Singapore

EE CHONG, Ng
MINDEF, Singapore

LINDBERG, Lars
SCHUBERT, Johan
FOI, Sweden

SEICHTER, Stephan
ZTransfBw, Germany

KALLFASS, Daniel
MALY, Andreas
WAGNER, Gudrun
CASSIDIAN, Germany

BUENAVIDA, Henri
TARD, Laurent
Defence Agency, France

INTRODUCTION

In 2010, the NATO Modeling and Simulation Task Group "Data Farming in Support of NATO" (MSG-088) has been created with the goal of assessing the data farming capabilities NATO, PfP, and Contact Countries, schools, and agencies have and to find out in which way these capabilities can contribute to the development of improved decision support to NATO forces.

As part of the "Program of Work" of MSG-088, proof-of-concept explorations regarding questions and models of interest to NATO nations are to be conducted, with the objective of illustrating the power of data farming for decision support. In order to realize this MSG-088 objective, the task group has planned to set up two case studies. One of those is taking place in the area of "Humanitarian Assistance and Disaster Relief (HA/DR)", whereas the second case study will handle the topic "Force Protection".

For the two mentioned case studies, two NATO working groups have been created, which took part as workshop teams in IDFW22. Team 03 covered the topic of "HA/DR", whereas Team 04 concentrated on the "Force Protection" topic.

The proposed scenario topic for the "Force Protection" study deals with the effective protection of a combat outpost (COP), possibly with the support of joint fire assets, in an Afghan mission setting against strong and coordinated insurgent forces.

GOALS OF TEAM 04

The main goal of Team 04 was to take first steps in developing a Data Farming Experiment (DFE) and therefore to create a scenario that is to be used within the case study "Force Protection" as well as to gather ideas on how to conduct data farming with this scenario. The next steps in developing the DFE, like scenario implementation, review, conduction of data farming experiments and the analysis of those, are scheduled for being completed until the end of 2011.

As different steps towards the overall goal within this workshop, the following subgoals had been defined for the workgroup:

- Defining a question to analyze within the DFE, and from that deriving more detailed questions to answer
- Definition of scenario elements like terrain or model elements to be represented in the scenario (e.g. which joint fire assets to use or which sensors to deploy within the COP)
- Selection of an appropriate model which allows for investigation of the formerly defined question or question sets
- Definition of an appropriate experimental tdesign, based on chosen input parameters and MOEs

The workgroup consisted of various members which were knowledgeable in very different fields, ranging from military experts with field experience in Afghanistan, to simulation and model experts, to experts in experimental designs. The overall mixture of staff inside the group provided an enriching work environment, which was a good basis for endeavoring these goals.

RESULTS

This section presents the results that were gathered from the long rounds of discussion. The results are split up into different sections that constitute the building blocks for afterwards defining a DFE from them.

Which questions to ask?

As mentioned before, the overall topic of the "Force Protection" scenario was the simulation of a COP in an Afghan mission and how to best protect the blue forces within that outpost against insurgents.

The overall question, that has been agreed upon to investigate in this context is the following:
"Which tactics or which equipment are/is most robust against different kings of threats?"

This question can further be split up into sub-questions which depict in a more detailed manner what is to be investigated. The defined sub-questions are:

- How can available sensor and weapon systems be most effectively used?
- What are the most effective tactics that shall be applied?
- Which sensor combination allows best COP protection?
- How does intelligence affect the successful protection? (not further considered for the time being)

The initially stated general question also contains the investigation of the chosen solution's robustness. To also incorporate this aspect, the approach agreed upon was to run the different COP setups or strategies, that are to be tested according to the questions above, against different kinds of insurgent threats and from these results compute the average performance of a specific COP setup.

Which MOEs to look at?

Which MOEs (Measures of Effectiveness) can be used within the scenario to actually identify the performance of the course of action in terms of the formerly formulated questions? The following MOEs have been identified as being suitable for answering the respective questions:

What does effective use of available equipment mean?

- No blue casualties
  ➔ **MOE:** percentage of blue losses
- No collateral damages
  ➔ **MOE:** number of civilian losses
  (skipped for now)

How to define successful protection of COP?

- No insurgents within small arms fire distance
  ➔ **MOE:** count the number of INS within given environment
- How long can the COP hold out until reinforcement / joint fire support arrives?
  ➔ **MOE:** count number of blue casualties within certain period of time

➔ **MOE:** ammunition spent

How to measure robustness?

- Steady success against varying strength / capabilities / tactics of INS
- Maybe specify a target function considering weighed MOEs

Which general scenario assumptions to make?

In defining the rough outline of the scenario, a few assumptions had to be made regarding the scenario in order to keep the investigation focused on the formerly defined questions. These assumptions include:

- The COP in question is generally meant to be a small, platoon-size COP, as attacks on large, heavily fortified COPs are highly unlikely.
- Though generally regarded as an important factor in such missions, no explicit modeling of communication between the different entities of the blue forces will be done.
- Intelligence processes won't be modeled, but the presence of intelligence results will be considered in the initial scenario setup.
- In the first step, no civilians will be modeled, as the involvement of these would make the scenario too complicated.
- The COP will be set up in the terrain next to a village. This implies that the COP can not attack the insurgents as soon as they retreat to the village (prevention of collateral damage).
- The COP's objectives have been defined as "Observe the surrounding" and "Show presence". None of the more complex tasks that are usually assigned to COPs, like setting up road checkpoints or building a relationship with the civilian population, are depicted in the scenario.

Which scenario and which course of action to depict?

The general scenario setup can be described as follows:

A COP is set up next to an Afghan village. It is equipped with various sensor and weapon systems, which help to identify enemies and to protect itself. The sensors as well as the effectors are placed inside and outside of the COP.

Sensors inside the COP may be positioned e.g. on set-up watchtowers or placed on vehicles, whereas an external sensor could be positioned at a nearby hill to get a better overview over the area. Additionally, the COP has access to UAVs, which can be used to scan the area, and also sends out patrols, which provide the possibility to identify enemies before they attack the COP.

In terms of effectors, the COP on the one hand has access to weapon systems stationed inside the COP, like the soldiers' rifles, mortars and effectors placed on the vehicles stationed inside the COP. From outside the COP, joint fire support in form of helicopters, fixed wing aircrafts or artillery can be called in, once a suitable target has been identified.

The red forces on the other hand apply two kinds of tactics to attack the COP. They either attack in the form of homogenous long distance attacks with the help of mortars or sniper rifles, or they approach the COP in the form of a force-on-force attack, seeking direct confrontation.

The course of action in this scenario is that the soldiers inside the COP try to have a good overview over the area around them, and try to reconnoiter enemies either through patrols, UAVs or stationary sensors placed in and around the COP. The insurgents on the other hand try to attack the COP with different tactics. As soon as the attackers have been reconnoitered by the soldiers, countermeasures can be applied, like sending out a Quick Reaction Force, defending themselves from inside the COP with help of rifles, mortars or other effectors, or by calling in joint fire support.

Which input parameters to look at?

For the described scenario, various input parameters have been defined that are deemed likely to have an influence on the course of the scenario and the outcome in terms of the formerly defined MOEs.

On the blue side, the parameters to vary can be summarized as follows:

- The number of sensors, effectors and vehicles at the COP's disposal
- The number of patrols that are being sent out by the COP

- Number, availability, latency and effector parameters of helicopters, fixed wings and artillery that can be used as joint fire support
- The number, type and tactics of UAVs working for the COP
- The number and type of stationary sensors inside and outside the COP
- The blue force's tactics in case they are under attack
- The proficiency of the soldiers inside the COP
- Availability of intelligence reports

On the red side, the parameters to vary are the following:

- Change between long distance and force-on-force attacks
- In case of long distance attacks, the number of attackers and their likelihood after firing to stay in their position or to change it
- In case of force-on-force attacks, the constellation of the attacking force, whether it is more small groups attacking or one large group of insurgents
- Effectors used by the attackers
- The insurgents' strength and proficiency

Which model to take?

After all the above decisions had been made, it was considered which available model would be most suitable to depict such a scenario.

Concerning the scenario's strong focus on elements like simulation of effector and sensor systems, the simulation model PAXSEM by Cassidian was deemed the right tool for the task at hand. Therefore it was decided that the case study "Force Protection" will be conducted with the use of this model.

Which experimental design to apply?

After all input parameter had been defined, it has been discussed which experimental design would be most suited to conduct the experiment with. With the help of experts from NPS, different alternatives were pondered. Finally it was decided, that due to the mixture and combination of the chosen input parameters, of which some are numerical and others categorical, the design fitting best is the so called "Nearly Balanced Nearly Orthogonal Mixed Design". With this design it will be possible to reduce the initially calculated number of $9 * 10^{27}$ design points to a number of 5610 design points.

SUMMARY AND FURTHER STEPS

Summarizing it can be said that we made very good progress during this week of collaborative work and took a few important steps towards conducting the case study "Force Protection". Due to all the valuable inputs from experts in the military, DoE and M&S fields, it has been possible to define the cornerstones of a scenario that on the one hand is likely to be able to really show the advantages of data farming and on the other hand treats an up-to-date military topic.

In the aftermath of this workshop, the above mentioned design will be created, tailored to the input parameters and ranges defined during this week. Furthermore a first version of the defined scenario will be created inside the model PAXSEM.

Currently, the further plans for the "Force Protection" case study include a common review of the implemented scenario during the NMSG-088 meeting 3, taking place in Istanbul, Turkey in July 2011. Afterwards, data farming experiments with the created scenario as well as with the defined DoE will be conducted and the results of these experiments will be presented for analysis at IDFW23 / NMSG-088 Meeting 4 in Finland in September 2011.

REFERENCES

[1] Data Farming in Support of NATO, RTG, March 2010

[2] Data Farming in Support of NATO, Program of Work, 2010

[3] IDFW 22 Team Abstracts, 2011, SEED Center for Data Farming