NORTH ATLANTIC TREATY
ORGANIZATION

SCIENCE AND TECHNOLOGY
ORGANIZATION

AC/323(MSG-124)TP/825

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-124**

Developing Actionable Data Farming Decision Support for NATO

(Développement d’une aide à la décision
exploitable par la production de
données pour l’OTAN)

Final Report of MSG-124.

Published July 2018

Distribution and Availability on Back Cover

NORTH ATLANTIC TREATY
ORGANIZATION

SCIENCE AND TECHNOLOGY
ORGANIZATION

AC/323(MSG-124)TP/825

www.sto.nato.int

STO TECHNICAL REPORT **TR-MSG-124**

Developing Actionable Data Farming Decision Support for NATO

(Développement d'une aide à la décision
exploitable par la production de
données pour l'OTAN)

Final Report of MSG-124.

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

The content of this publication has been reproduced directly from material supplied by STO or the authors.

Published July 2018

ISBN 978-92-837-2151-2

Table of Contents

List of Figures

List of Tables

List of Abbreviations

BFOR	Blue Forces
BML	Battle Management Language
CAN	Computer Network Attack
CC	Component Commands
CD&E	Concept, Development and Experimentation
CIA	Confidentiality, Integrity, and Availability
CNE	Computer Network Exploitation
COA	Course Of Action
COIN	Counter-Insurgency
CONOPS	Concept of Operations
COPD	Comprehensive Operations Planning Directive
CPG	Commanders Planning Guidance
CPOE	Comprehensive Preparation of the Operational Environment
DACDAM	Data-farmable Agent-based Cyber Defence Assessment Model
DF	Data Farming
DFTOP	Data Farming decision support Tool for Operation Planning.
DOE	Design Of Experiment
DoS	Denial of Service
HPC	High Performance Computing
IT	Information Technology
JHQ	Joint Headquarters
JOPG	Joint Operations Planning Group
M&S	Modelling and Simulation
MOE	Measure of Effectiveness
MSDL	Military Scenario Definition Language
NONB	Nearly Orthogonal, Nearly Balanced
OPD	Operational Planning Directive
OPG	Operational Planning Guidance
OPP	Operations Planning Process
ORBAT	Order of Battle
SA	System Administrator
SDA	Skewed Distribution Analysis
SME	Subject Matter Expert
TRL	Technology Readiness Level

MSG-124 Membership List

CO-CHAIRS

Dr. Gary HORNE*
MCR Global
UNITED STATES
Email: gary.horne@verizon.net

LtCol Stephan SEICHTER*
Bundeswehr Office for Defence Planning
GERMANY
Email: stephanseichter@bundeswehr.org

MEMBERS

Dr. Bernt ÅKESSON*
Finnish Defence Research Agency
FINLAND
Email: bernt.akesson@mil.fi

Mr. Nicolaas DE REUS*
TNO Defence, Security and Safety
NETHERLANDS
Email: nico.dereus@tno.nl

Prof. Dr. Matthias DEHMER
UniBw, UMIT
GERMANY
Email: matthias.dehmer@unibw.de

Mr. Sebastian DÖRING*
Federal Office of Bundeswehr Equipment
GERMANY
Email: sebastian1doering@bundeswehr.org

Mr. Thomas GRUBER*
Airbus Defence & Space GmbH
AUSTRIA
Email: thomas.t.gruber@airbus.com

Dr. Pontus HÖRLING*
Swedish Defence Research Agency (FOI)
SWEDEN
Email: pontus.hoerling@foi.se

Dr. Daniel HUBER*
Fraunhofer IAIS
GERMANY
Email: daniel.huber@iais.fraunhofer.de

Mr. Mario JAEHNERT
EADS Deutschland GmbH/CASSIDIAN
GERMANY
Email: mario.jaehnert@cassidian.com

Mr. Daniel KALLFASS*
EADS Deutschland GmbH/CASSIDIAN
GERMANY
Email: daniel.kallfass@airbus.com

Dr. Esa LAPPI*
PVTT EIOS
FINLAND
Email: esa.lappi@mil.fi

Mr. Sascha MAYER
Federal Office of Defense Technology and
Procurement (BWB)
GERMANY
Email: saschamayer@bundeswehr.org

Assoc Prof. Giacomo MORABITO*
University of Catania
ITALY
Email: giacomo.morabito@dieei.unict.it

Dr. Kevin Yui Ki NG*
DRDC-CORA
CANADA
Email: Kevin.Ng@drdc-rddc.gc.ca

* Contributing Author.

Capt. Niina NISSINEN*
Defence Forces Technical Research Center
FINLAND
Email: niina.nissinen@mil.fi

Dr. Per Johan SCHUBERT*
Swedish Defence Research Agency (FOI)
SWEDEN
Email: johan.schubert@foi.se

Dr. Klaus-Peter SCHWIERZ*
EADS Deutschland Gmbh/CASSIDIAN
GERMANY
Email: Klaus-Peter.Schwierz@cassidian.com

Mr. Martin SOMMER
Airbus Defence & Space GmbH
GERMANY
Email: martin.sommer@airbus.com

Dr. Guro Kristin SVENDSEN*
Norwegian Defence Research
NORWAY
Email: Guro.Svendsen@ffi.no

Maj Burhan ÜREK*
Turkish War College
TURKEY
Email: burek@harpak.edu.tr

Ir. Martin VAN DER KAAIJ
TNO Defence, Security and Safety
NETHERLANDS
Email: martin.vanderkaaij@tno.nl

Mr. Alexander ZIMMERMANN*
Fraunhofer IAIS
GERMANY
Email: alexander.zimmermann@iais.fraunhofer.de

ADDITIONAL AUTHORS

Dr. Santiago BALESTRINI-ROBINSON
Georgia Tech Research Institute
UNITED STATES
Email: sanbales@gatech.edu

Mr. Maxwell BRITTON
Department of Defence
AUSTRALIA
Email: maxwell.britton1@defence.gov.au

Dr. Christopher J. HAZARD
Hazardous Software Inc.
UNITED STATES
Email: cjhazard@hazardoussoftware.com

Dr. Ronnie JOHANSSON
Swedish Defence Research Agency (FOI)
SWEDEN
Email: ronnie.johansson@foi.se

Mr. Peter RINDSTÅL
Swedish Defence Research Agency (FOI)
SWEDEN
Email: peter.rindstal@foi.se

Dr. Patrik THORÉN
Swedish Defence Research Agency (FOI)
SWEDEN
Email: patrik.thoren@foi.se

Cdr Topi TUUKKANEN
Finnish Defence Research Agency
FINLAND
Email: topi.tuukkanen@mil.fi

* Contributing Author.

Developing Actionable Data Farming Decision Support for NATO

(STO-TR-MSG-124)

Executive Summary

Data Farming is a process that has been developed to support decision makers by answering questions that are not currently addressed and uses an inter-disciplinary approach that includes modelling and simulation, high performance computing, and statistical analysis to examine questions of interest with large number of alternatives. Data farming allows for the examination of uncertain events with numerous possible outcomes and provides the capability of executing enough experiments so that both overall and unexpected results may be captured and examined for insights.

The essence of data farming is that it is first and foremost a question-based approach. The basic question repeatedly asked in different forms and in different contexts is: *What if?* Data farming engages an iterative process and enables a refinement of questions as well as obtaining answers and insight into the questions.

The value of applying data farming in an actionable way to provide military benefit has been demonstrated. The core objective of this task group was to apply actionable data farming that could contribute to the development of improved decision making of relevance to NATO forces. Explorations involving two areas of interest to NATO decision makers were undertaken. These areas were operation planning and cyber defence.

The *Operation Planning Syndicate* addressed the question on how to provide actionable support to decision makers in operation planning. We developed the *Data Farming Tool for Operation Planning* (DFTOP) to streamline this support in order to lower the effort needed to prepare analysis and to facilitate for the collaboration between decision makers and analysts. With DFTOP, the possibilities of quantitative simulation-based analysis are made readily available to decision makers and planners at the operational level. DFTOP supports evaluation of operation plans by data farming a broad set of COA. The support is aligned with the NATO planning process, providing support for the planning group.

Initial validation efforts and user acceptance tests have concluded that DFTOP meets the need of the military planner, and successfully brings Data Farming into the actionable decision support domain. This aids decisions based on much broader decision grounds in selecting the best COA to achieve the goal with well-managed risk, adding operational value by increasing the quality of the decisions.

The overall goal of the *Cyber Defence Syndicate* was to leverage the current research, develop a suitable simulation, and explore possible scenarios through data farming that could facilitate the understanding of some aspects of cyber defence. The syndicate members developed the *Data-farmable Agent-based Cyber Defence Assessment Model* (DACDAM) as an extensible proof-of-concept model to test the ideas of data farming and how they may apply it to supporting decision-making. They explored the basic question: "how should organizations invest their resources to maximize their ability to defend themselves against cyber attacks?" The data farming effort using DACDAM concentrated on demonstrating potential analyses that could be performed using the model and data farming techniques. The results were not meant to be predictive in nature, but illustrative of the types of trade-offs that may be studied. The ultimate goal was to provide insight to decision makers as to which protocols, topologies and configurations produce the most secure networks.

The operation planning and cyber defence syndicates both contributed work that led to the many specific results, conclusions, and recommendations described in this report. In summary, the overall conclusion and recommendation to military leaders is that data farming is feasible for NATO and nations, and should be used as a methodology for actionable decision support in operation planning and cyber defence.

Développement d’une aide à la décision exploitable par la production de données pour l’OTAN

(STO-TR-MSG-124)

Synthèse

La *production de données* est un processus élaboré destiné à aider les décideurs en répondant à des questions qui n’ont pas encore été abordées. Elle suit une démarche interdisciplinaire qui inclut la modélisation et la simulation, le calcul de haute performance et l’analyse statistique pour étudier des questions intéressantes ayant un grand nombre d’alternatives. La production de données permet d’examiner des événements incertains ayant de nombreux résultats possibles et offre la capacité de réaliser suffisamment d’expérimentations pour enregistrer à la fois des résultats généraux et des résultats inattendus et en tirer des connaissances.

Par nature, la production de données est d’abord et avant tout une démarche basée sur des questions. La question fondamentale posée sous diverses formes et dans différents contextes est la suivante : *« Et si ? »* La production de données entame un processus itératif et permet d’affiner les questions, d’obtenir des réponses et d’approfondir les sujets.

Il a été démontré que le recours à la production de données actives représentait un avantage militaire. L’objectif central de ce groupe de travail était de mettre en œuvre une production de données actives pouvant contribuer au développement d’un meilleur processus décisionnel pour les forces de l’OTAN. Deux domaines pertinents pour les décideurs de l’OTAN ont été étudiés : la planification des opérations et la cyberdéfense.

L’*Operation Planning Syndicate* (sous-groupe de planification des opérations) s’est penché sur la manière d’apporter aux décideurs un soutien actif pendant la planification des opérations. Nous avons élaboré le DFTOP (*Data Farming Tool for Operation Planning*, outil de production de données pour la planification des opérations) afin de rationaliser ce soutien, dans le but de réduire les préparatifs de l’analyse et de faciliter la collaboration entre les décideurs et les analystes. Avec le DFTOP, les décideurs et les planificateurs ont facilement accès aux possibilités d’analyse quantitative basée sur la simulation, et ce, au niveau opérationnel. Le DFTOP est utile à l’évaluation des plans d’opération en produisant un vaste ensemble de modes d’action. Ce soutien s’aligne sur le processus de planification de l’OTAN et facilite le travail du groupe de planification.

Les premiers travaux de validation et essais d’acceptation par l’utilisateur indiquent que le DFTOP répond au besoin du planificateur militaire et fait entrer la production de données actives dans le domaine de l’aide à la décision. Les décisions reposent sur des considérations beaucoup plus nombreuses. Le meilleur mode d’action est choisi pour atteindre le but avec un risque bien encadré, ce qui renforce la valeur opérationnelle en améliorant la qualité des décisions.

Le but général du *Cyber Defence Syndicate* (sous-groupe de cyberdéfense) était d’exploiter les recherches actuelles, développer une simulation adaptée et étudier, à l’aide de la production de données, les scénarios pouvant faciliter la compréhension de certains aspects de la cyberdéfense. Les membres du sous-groupe ont élaboré le DACDAM (*Data-farmable Agent-based Cyber Defence Assessment Model*, modèle d’évaluation de la cyberdéfense permettant la production de données par un agent), un modèle extensible de validation de principe servant à tester les idées de la production de données et leur utilisation éventuelle dans l’aide à la

décision. Ils ont ensuite étudié la question fondamentale suivante : de quelle façon les organisations devraient-elles investir leurs ressources pour maximiser leur capacité à se défendre contre les cyberattaques ? Les travaux de production de données à l'aide du DACDAM se sont concentrés sur la démonstration d'analyses potentielles pouvant être réalisées à l'aide du modèle et des techniques de production de données. Les résultats n'étaient pas censés être de nature prédictive, mais illustrer les types de compromis pouvant être étudiés. Le but ultime était de fournir aux décideurs un éclairage sur les protocoles, les topologies et les configurations qui produisent les réseaux les plus sûrs.

Le sous-groupe de planification des opérations et celui de cyberdéfense ont tous deux produit des travaux qui ont mené aux nombreux résultats, conclusions et recommandations décrits dans le présent rapport. En résumé, la conclusion générale est que la production de données est possible dans l'OTAN et les pays et il est recommandé aux dirigeants militaires de l'utiliser comme méthodologie d'aide à la décision active pendant la planification des opérations et pour la cyberdéfense.

Chapter 1 − INTRODUCTION

This Report documents work of the NATO Modeling and Simulation Task Group 124 (MSG-124), titled *Developing Actionable Data Farming Decision Support for NATO*. It represents work performed at 12 meetings of the Group during the past four years, some of which were collocated with meetings of the International Data Farming Community, called International What-if Workshops (IWWs) with additional Working Groups (WGs). A great deal of work was also performed between meetings. This Report includes documentation of work done by military, civilian scientists, and subject matter experts from eight countries. Figure 1-1 illustrates the dates and places of the meetings.

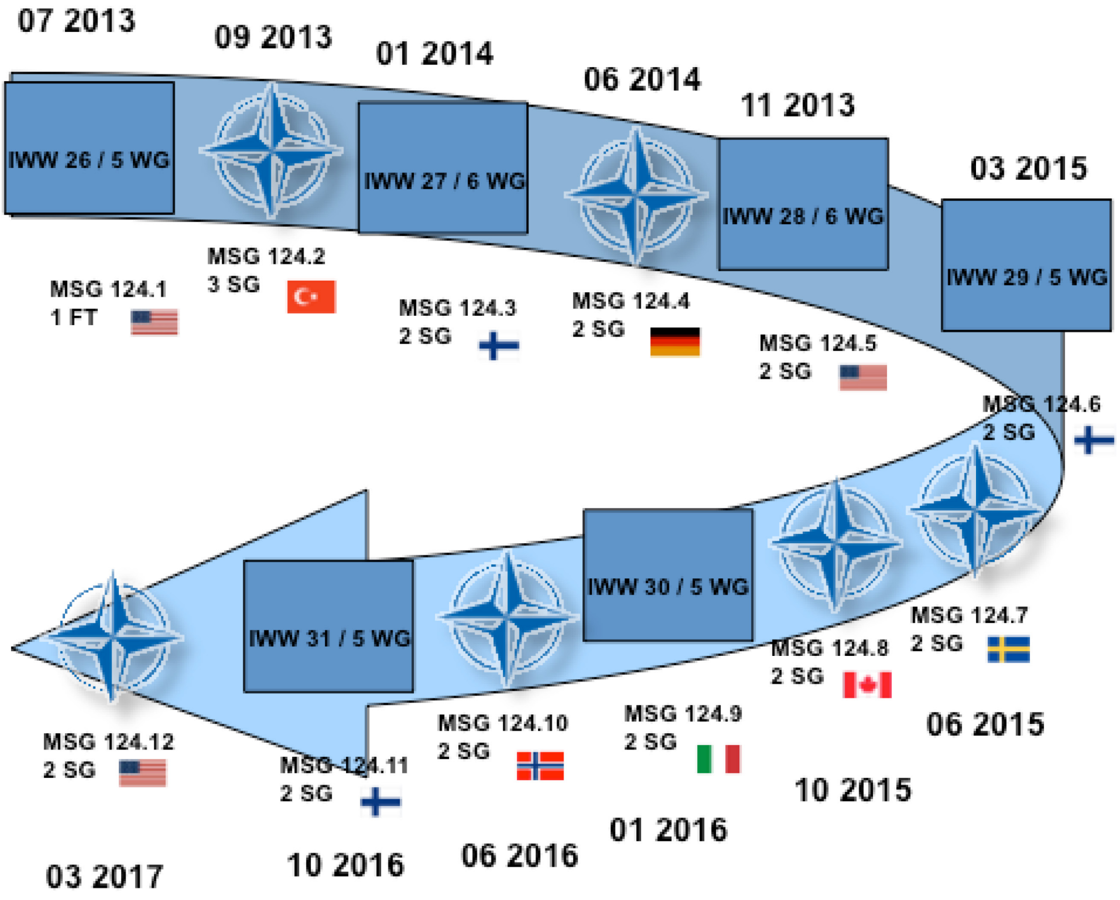


Figure 1-1: MSG-124 Timeline.

The first meeting was held within the full team and the second meeting had 3 syndicate groups. Beginning with the third meeting the Task Group had settled on the two syndicates of operation planning and cyber defence. The main content of MSG-124 is contained in the results of these two syndicates within the task group that will be described in Chapters 4 and 5 of this Report. These chapters are preceded by a summary of data farming in Chapter 3 and also Chapter 2 that provides the key motivation of providing decision support that is actionable. But first, in this chapter, background on data farming will be presented.

Data Farming, introduced by Horne [1], is a process that has been developed in order to support decision-makers in answering questions that are not addressed by traditional modelling and simulation processes. [2] Data farming uses rapid prototyping, simulation modelling, experimental design, high performance computing, and analysis and visualisation to examine questions of interest with large possibility spaces. Using these five domains within a sixth, a collaborative framework, this methodology allows for the examination of whole landscapes of potential outcomes and provides the capability of executing enough experiments so that outliers might be captured and examined for insights. An international community has been conducting common activities for over a decade now around data farming ideas. Workshops have taken place approximately twice a year since 1999 in order to exchange knowledge in the area of data farming and apply data farming to military questions.

The discovery of surprises and potential options are made possible by data farming. But many disciplines are behind these discoveries and their use in the overall data farming process evolved over a period of time. Six realms or domains were incorporated into the data farming methodology from 1997 to 2002: Rapid Scenario Prototyping, Model Development, Design of Experiments, High Performance Computing, Analysis and Visualisation, and Collaborative Processes.

Initial data farming efforts in the 1997 – 98 time frame relied upon the combination of two domains. The first was model development. These models, often called distillations at the time, may not be very close to reality, but could be focused to specifically address the questions at hand. [3] The second was high performance computing as analysts in Quantico gained access to the resources of the Maui High Performance Computing Center. This capability, using high performance computing to execute models many times over varied initial conditions, allowed for improved understanding of the possible outliers, trends, and the distribution of results.

The models need not be agent-based models, but because of the ease with which they can be prototyped, agent-based models were used during this beginning time period. The huge volume of output from the simulations made possible by the high performance computing resulted in a need to develop visualisation tools and methods commensurate with this tremendous amount of data. Thus, visualisation of simulation data and rapid prototyping of scenarios became important to data farming efforts in the 1999 – 2000 time frame.

The simulations that defence analysts use are often large and complex. An evaluation of complete landscapes is extremely time consuming, sometimes not even possible. Also, even the smaller more abstract agent-based distillations referred to above can have many parameters that are potentially significant and that could take on many values. Even with high performance computing and the small models used in data farming, gridded designs, where every value is simulated, are unwieldy. Thus, using efficient experimental designs is essential.

Finally, collaborative processes help to integrate the other five domains of data farming through interdisciplinary work in creating models and data farming infrastructure and during the iterative process of prototyping scenarios and examining output from model runs. Collaboration also takes place between people from different organizations and nations sharing information and perspectives at various points in approaching common questions. With the addition of design of experiments and collaborative processes in 2001-2002 to data farming efforts, much attention then focused on applications.

Since the incorporation of the above six domains into the data farming process, many articles have captured the fundamental elements of data farming (e.g., Ref. [4]). But the key tenet in the data farming process has been the focus on the questions and since 2002 many application efforts have been documented. For example, over a hundred international work teams have formed around questions at International Data Farming Workshops. These work teams fall into areas, or themes, which include: Joint and Combined Operations (e.g., C4ISR

Operations, Network Centric Warfare, Networked Fires, and Future Combat Missions), Urban Operations, Combat Support (e.g., UAV Operations, Robotics, Logistics, and Combat ID), Peace Support Operations, the Global War on Terrorism, Homeland Defence, Disaster Relief, and others.

In 2010 the NATO Research and Technology Organization (RTO) started a Modelling and Simulation Task Group, denoted MSG-088, to evaluate and further develop the data farming methodology to be used for decision support within the NATO. Proof-of-concept explorations in the form of two case studies involving questions and models of interest to NATO nations were also undertaken. The results of both the assessment and case study explorations indicate the potential high value of data farming to NATO decision-makers and answering their questions. The work of this task group to include the codification of data farming is summarized in Chapter 3 of this Report.

Harnessing the power of data farming to apply it to important NATO question areas is essential to providing support not currently available to NATO decision-makers. Thus, the MSG-088 Report recommended implementing data farming methods as codified in the report in NATO modelling and simulation contexts and undertaking specific efforts to apply data farming to NATO questions.

Thus in applying the codification of data farming in MSG-088, the core objective of MSG-124 was to apply actionable data farming that could contribute to the development of improved decision making of relevance to NATO forces. Explorations involving two areas of interest to NATO decision makers were undertaken. These areas became the subject matter areas of MSG-124. They are operations planning and cyber defence and they will be discussed in Chapters 4 and 5 of this report.

The *Operation Planning Syndicate* work discussed in Chapter 4 addressed the question on how to provide actionable support to decision makers in operation planning. We developed the Data Farming Tool for Operation Planning (DFTOP) to streamline this support in order to lower the effort needed to prepare analysis and to facilitate for the collaboration between decision makers and analysts.

The overall goal of the *Cyber Defence Syndicate* discussed in Chapter 5 was to leverage the current research, develop a suitable simulation, and explore possible scenarios through data farming that could facilitate the understanding of some aspects of cyber defence. The syndicate members developed the Data-farmable Agent-based Cyber Defence Assessment Model (DACDAM) as an extensible proof-of-concept model to tests the ideas of data farming and how they may apply to supporting decision-making.

The operation planning and cyber defence syndicates both contributed work that led to the many specific results, conclusions, and recommendations described in Chapter 6 of this report. In summary, the overall conclusion and recommendation to military leaders is that data farming is feasible for NATO and nations, and should be used as a methodology for actionable decision support in operation planning and cyber defence.

The key motivation behind this task group was to extend data farming beyond the results of MSG-088 that are described in Chapter 3 of this report. Thus, Chapter 2 of this report follows with a description of what actionable data farming might entail regarding decision support in the context of important NATO questions.

1.1 REFERENCES

[1] Horne, G. (1997). Data Farming: A Meta-Technique for Research in the 21st Century, Naval War College. Newport, RI.

[2] Horne, G. and Meyer, T. (2004). Data Farming: Discovering Surprise, in: R. Ingalls, M.D. Rossetti, J.S. Smith, and B. A. Peters, (eds.), *Proceedings of the 2004 Winter Simulation Conference*, pp. 171-180. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

[3] Horne, G. (1999). Maneuver Warfare Distillations: Essence Not Verisimilitude, in: A. Farrington, H.B. Nembhard, D.T. Sturrock, and G.W. Evans, (eds.), *Proceedings of the 1999 Winter Simulation Conference*, pp. 1147-1151. Phoenix, AZ.

[4] Horne, G. and Meyer, T. (2005). Data farming: Discovering Surprise, in: M.E. Kuhl, N.M. Steiger, F.B. Armstrong, and J.A. Joines, (eds.), *Proceedings of the 2005 Winter Simulation Conference*, Orlando, Florida.

Chapter 2 − ACTIONABLE DATA FARMING

The title of MSG-124 is *Developing Actionable Data Farming Decision Support for NATO*. The core objective of MSG-124 is to apply data farming capabilities within NATO, PfP, and Contact countries and agencies that could contribute to the development of improved decision support to NATO forces. The task group examined questions in the areas of operation planning and cyber defence in order to recommend and demonstrate an *actionable* way forward in NATO contexts where M&S methods in concert with data farming are useful in capturing the possibilities inherent in the questions and thus more insight into answers. So, before we describe data farming in Chapter 3 and the results of the operations planning and cyber syndicates in Chapters 4 and 5, here in Chapter 2 we answer the question "why actionable data farming?" which is the natural extension of the question "why data farming?" that we explain first.

2.1 WHY DATA FARMING?

The data farming methodology applies a simulation-based, holistic and iterative approach to analyze complex systems. In general, the challenge of all simulation systems is the fact, that running *one* simulation only provides *one* singular result regarding just the *one* given situation and circumstances. In this case, no conclusions as to different circumstances – including (identification of) best / worst case scenarios – can finally be drawn. A wider description of the underlying system would be most valuable to obtain a deeper insight. And awareness of this fact gave rise to the establishment of data farming, a simulation based analysis process that enables quantitative analysis of complex questions, obtaining robust results, the comparing of results, and "What-if?" analyses [1].

The nucleus of data farming builds on myriad simulation runs, conducted on high-performance supercomputers, with numerous input parameters varied along a deliberately defined plan, measuring the output and finally examining the mutual interrelationships. Within this activity, data farming enables the ability to check assumptions, to gain new insights into relevant relationships and, last but not least, to obtain more robust statements on opportunities and risks of specific mission situations. Briefly, to obtain a more detailed insight into the properties of the examined complex system. This goal is achieved through a deliberate alternation of parameter values of decided input parameters, assuming them to be crucial as regards the measures of effectiveness. Data generated in this way can be of a different nature. Depending on its extent, the analysis can be exploratory or descriptive [1].

2.2 WHY ACTIONABLE DATA FARMING?

Decision makers in NATO are faced with the challenge of making decisions regarding highly complex systems. A large set of uncertain factors makes it difficult to foresee all possible implications of their decisions. This challenge is ideally aligned with the benefits of data farming.

The data farming methodology provides for a better understanding of the many possibilities that decision makers face. In MSG-088 we demonstrated how data farming could be used to analyse a set of questions, e.g., regarding how to best protect a command post. In MSG-124, we push the frontier of data farming further, demonstrating how data farming can be used as an integrated tool for decision-makers. The aim is to allow decision makers to gather insights more quickly and be more confident that the decisions indicated will lead to good results. To provide the insights from data farming in this manner is the extended goal that motivates MSG-124 and that is what we refer to as *Actionable Data Farming*.

Data, information, and insights are not synonymous. There is a hierarchical pyramid with data at the foundation, information in the middle, and insights at the top [2]. In turn, actionable insights sit at the very pinnacle of this pyramid. These are the outputs of data farming that are of the most value to decision-makers. MSG-124 members were motivated to illustrate how these outputs might be achieved using data farming.

Data farming has always been question-based. But an insight that drives action is more valuable than one that simply answers a question, especially an insight that makes you rethink something and pushes you in an innovation direction. Data farming has the advantage of examining a vast number of possibilities through simulation and high performance computing. And these possibilities are simply data until they are analyzed and patterns, trends, or other information is gleaned from them. Iterative exploration of “What-If?” questions reveals the landscape of possibilities inherent in the scenarios and enables the study of any “outliers” that are discovered. This exploration can then produce information that subsequently can be used to synthesize insights that might guide our decision-makers. This step is carried out in collaboration with decision makers, pairing the information from the simulations with the insights, preferences and military expertise of the decision maker. When these insights are developed quickly enough to be aligned with the decision making process and resonate deeply enough they become actionable.

Thus, actionable insight is a term that denotes insight that can be acted upon or results that give enough insight into the future that the actions that should be taken become clear for decision makers [3]. In the context of data farming, actionable insight is the result of simulation and extensive data analysis and visualisation of the simulation data in a process aligned with the needs of the decision makers. And in the context of NATO decision makers, the results are such that they provide enough data, to in turn provide enough information, and to finally then provide enough insight to make an informed decision and act on it.

In pursuing the two topics of operation planning and cyber defence, MSG-124 has developed methods and produced results in ways that can be considered actionable data farming. Chapters 4 and 5 will describe the efforts in these two context areas. But in Chapter 3, the basic methodology of data farming codified in MSG-088 will first be described.

2.3 REFERENCES

[1] Horne, G., *et al.* (2014). MSG-088 Data Farming in Support of NATO, Final Report STO-TR-MSG-088, NATO Science and Technology Office (STO).

[2] https://www.forbes.com/sites/brentdykes/2016/04/26/actionable-insights-the-missing-link-between-data-and-business-value/#5ed88d2451e5, Actionable Insights: the Missing Link between Data and Business Value, accessed March 2017.

[3] https://www.techopedia.com/definition/31721/actionable-insight, Actionable Insight, accessed April 2017.

Chapter 3 − SUMMARY OF DATA FARMING

3.1 OVERVIEW

Data Farming is a process that has been developed to support decision-makers by answering questions that are not currently addressed. Data farming uses an inter-disciplinary approach that includes modelling and simulation, high performance computing, and statistical analysis to examine questions of interest with large number of alternatives. Data farming allows for the examination of uncertain events with numerous possible outcomes and provides the capability of executing enough experiments so that both overall and unexpected results may be captured and examined for insights.

In 2010, the NATO Research and Technology Organization started MSG-088, the three-year Modelling and Simulation Task Group "Data Farming in Support of NATO" to assess and document the data farming methodology to be used for decision support. This chapter includes a summary of the six realms of data farming codified during the course of MSG-088. The first realm, rapid prototyping, works with the second realm, model development, iteratively in an experiment definition loop. A rapidly prototyped model provides a starting point in examining the initial questions and the model development regimen supports the model implementation, defining the resolution, scope, and data requirements. The third realm, design of experiments, enables the execution of a broad input factor space while keeping the computational requirements within feasible limits. High performance computing, realm four, allows for the execution of the many simulation runs that is both a necessity and a major advantage of data farming. The fifth realm, analysis and visualization, involves techniques and tools for examining the large output of data resulting from the data farming experiment. The final realm, collaborative processes, underlies the entire data farming process and these processes will be described in detail in this report.

Figure 3-1 arranges the 6 realms of data farming with the key properties around a question base, in our understanding as a sequential process starting with rapid prototyping and ending with analysis and visualization – historically the 6 realms developed in a different order. All activities started out with modelling and high performance computing support to answer decision-makers questions. Feasibility was the initial driver. From the beginning Collaboration was the key – all work on the realms took place in international collaboration and all working groups were multi-disciplinary and, if possible, international. Result analysis and visualization developed to make the enormous amount of result data understandable. Getting more and more mature, Rapid Scenario Prototyping got the starting point of the process. Finally, the "youngest" realm is Design of Experiments. From a complete cover of the parameter space we went to a statistical cover making Data Farming effective. The combination of six realms to the "process" Data Farming is unique.

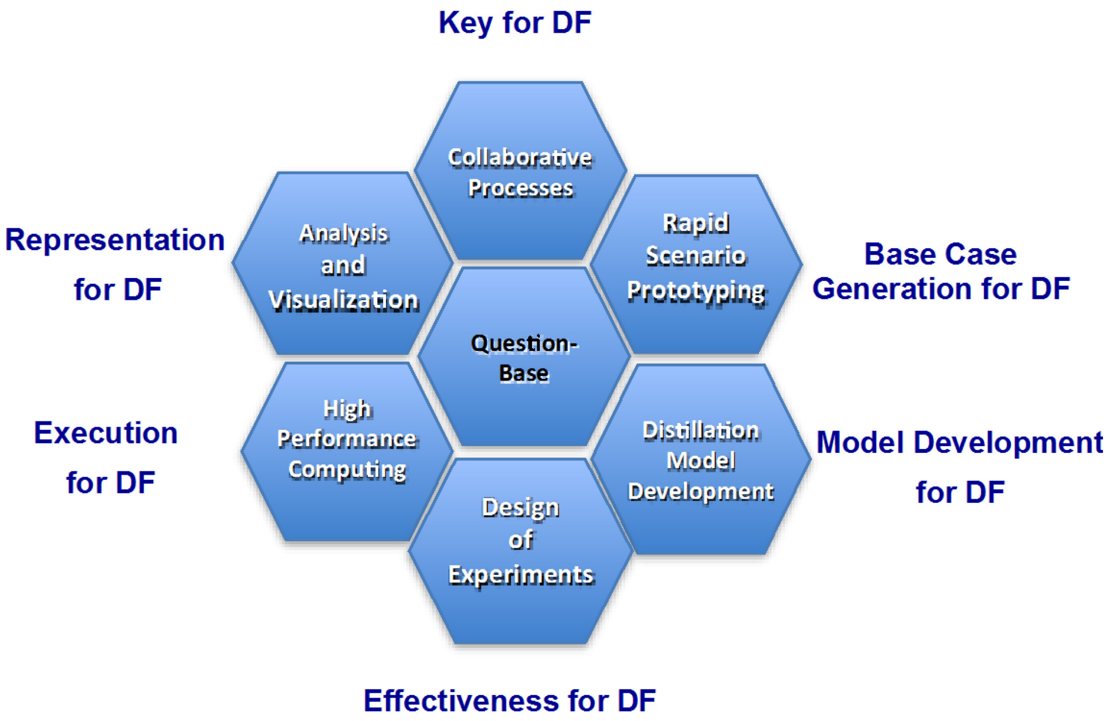


Figure 3-1: The Six Realms of Data Farming Around a Question Base.

In summary, the essence of data farming is that it is first and foremost a question-based approach. The basic question, repeatedly asked in different forms and in different contexts, is: What if? Data farming engages an iterative process and enables a refinement of questions as well as obtaining answers and insight into the questions. Harnessing the power of data farming to apply it to our questions is essential to providing support not currently available to NATO decision-makers. This support is critically needed in answering questions inherent in the scenarios we expect to confront in the future as the challenges our forces face become more complex and uncertain.

3.2 INTRODUCTION

Data Farming is a process that has been developed to support decision-makers by answering questions that are not currently addressed. Data farming uses an inter-disciplinary approach that includes modelling and simulation, high performance computing, and statistical analysis to examine questions of interest with large number of alternatives. Data farming allows for the examination of uncertain events with numerous possible outcomes and provides the capability of executing enough experiments so that both overall and unexpected results may be captured and examined for insights. Harnessing the power of data farming to apply it to our questions is essential to providing support not currently available to NATO decision-makers. This support is critically needed in answering questions inherent in the scenarios we expect to confront in the future as the challenges our forces face become more complex and uncertain.

Data farming is an iterative team process. Figure 3-2 shows the iterative process as a loop of loops with five of the six realms of data farming depicted. The sixth, collaboration, underlies the entire process and emphasizes the importance of the team aspect of data farming.

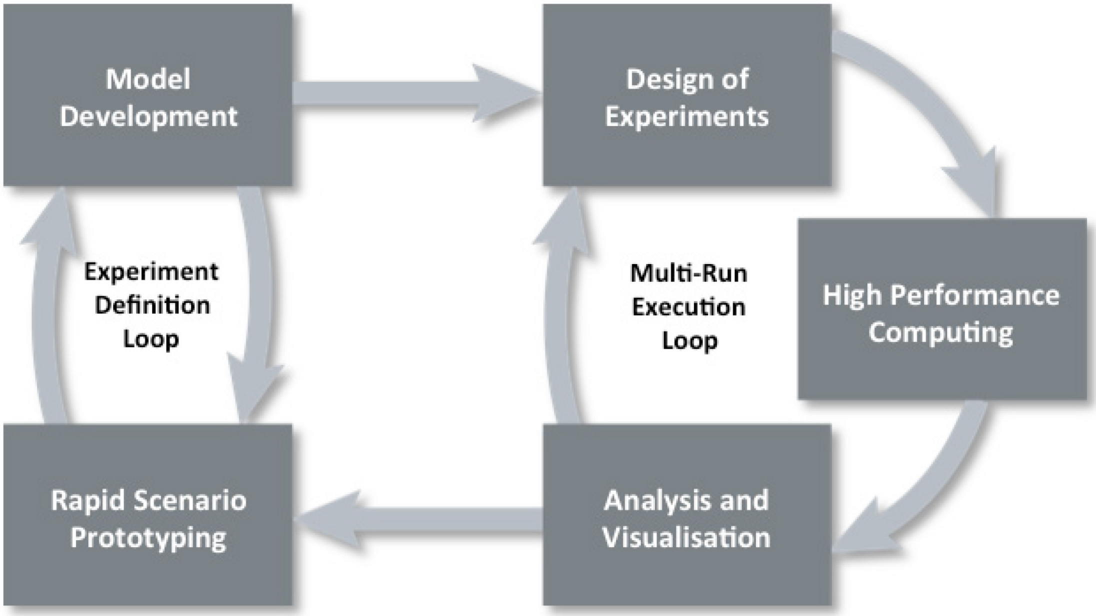

Model Development
Design of Experiments
Experiment Definition Loop
Multi-Run Execution Loop
High Performance Computing
Rapid Scenario Prototyping
Analysis and Visualisation

Figure 3-2: Data Farming "Loop of Loops".

Since the term was coined in 1997 [1], the essence of data farming is that it is first and foremost a question-based approach. The basic question repeatedly asked in different forms and in different contexts is: What if? Data farming enables a refinement of questions as well as obtaining answers and insight into the questions. From 1998 to 2006, data farming developed along with a project funded by the US called Project Albert which quickly grew into an international effort where each member nation funded the national efforts and where the iterative nature of data farming was documented over these years [2], [3], [4], [5]. Development of data farming continued after Project Albert officially ended through sponsored work, again in an international community, using the methods and the Data Farming Community has met for workshops that continue to be held about twice a year (e.g., see the proceedings in Refs. [6] and [7]).

In 2010, the NATO Research and Technology Organization started the three-year Modelling and Simulation Task Group 088 (MSG-088) called "Data Farming in Support of NATO" to assess and document the data farming methodology to be used for decision support [8]. This chapter will continue with a summary of the six realms of data farming in the next six sections using the completed work of MSG-088 as the primary reference [9] as well as case study work such as that found in Ref. [10].

3.3 RAPID SCENARIO PROTOTYPING

The model development and the rapid prototyping realms together make up the experiment definition loop in Figure 3-2. As such, they work hand-in-hand with each other and we could choose either realm to begin our detailed description of data farming – with a narrow margin on rapid scenario prototyping, because here the model is chosen and specified. Thus the rapid scenario prototyping process is a good place to start our discussion.

As with the data farming process in general, the rapid scenario prototyping should always be within the context of the questions to be answered. These questions have to be prepared in such a way that simulation can help to find answers and to get insights. The most important step here is to define measurements to be collected by means of simulation together with required input and output data for the simulation. In most cases this step already requires some rough ideas about the scenario settings. Thus, this realm simply represents the initial formation of the basics of a scenario to be simulated.

The analysis team should make several decisions on the specifics and the resolution of the required simulation model. The analysis team should consider which kind of data is required for the analysis and how to collect these data. Many abstractions and assumptions within the modelling process have to be made and documented. A simulation model then must be chosen and if necessary, adapted to the requirements of the specific analysis. If a suitable simulation model is not available, a new model has to be developed. All of the above is, as shown in Figure 3-3, a prerequisite of the actual rapid scenario prototyping process, which starts with drafting a more detailed description of the scenario settings together with all the assumptions made so far. Once the scenario is drafted, it can be instantiated into a simulation model and the realm of model development is described in the next section [9].

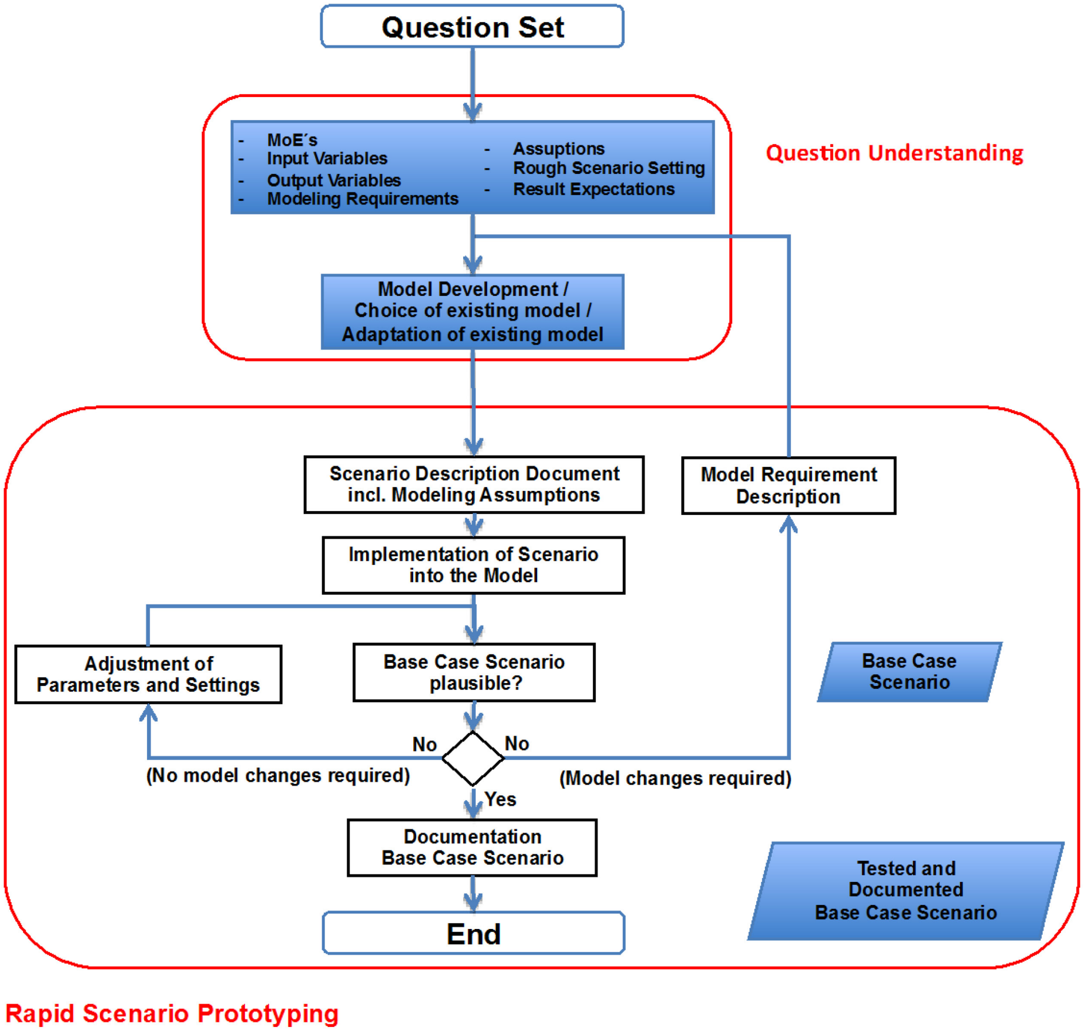

Question Set
- MoE´s
- Input Variables
- Output Variables
- Modeling Requirements
- Assuptions
- Rough Scenario Setting
- Result Expectations
Question Understanding
Model Development / Choice of existing model / Adaptation of existing model
Scenario Description Document incl. Modeling Assumptions
Model Requirement Description
Implementation of Scenario into the Model
Adjustment of Parameters and Settings
Base Case Scenario plausible?
Base Case Scenario
No
No
(No model changes required)
(Model changes required)
Yes
Documentation Base Case Scenario
Tested and Documented Base Case Scenario
End
Rapid Scenario Prototyping

Figure 3-3: Rapid Scenario Prototyping Process [9].

The analysis team faces many challenges during the RSP process that are similar to the challenges found in a code of best practice of simulation based analyses [11]. The following aspects, presented in the following "checklist", need to be considered to help in meeting the challenges in this area. Because each analyst in a multidisciplinary team with highly collaboration efforts has different needs and opinions, which may change depending on the question at hand, the checklist is not necessarily presented in any particular order:

- ***Scenario implementation without analysis question:*** A common problem if analysis team and model experts work separately. Also a common malpractice to build a model, implement a scenario and then to ask: "Which question can we answer now?" This leads to adjustment of questions to the tool and often to answers nobody needs.
- ***Wrong model for the question:*** Common causes for this problem might be that someone ordered to use a specific model or that the analyst is familiar with a certain model and wants to use only this model or that only one model is available for usage. Using a "wrong" model clearly limits the amount and scope of insight we can expect from the analysis. The analysis team has to communicate this to the client (decision-maker). It might be necessary to adjust the questions, to refocus the analysis or to stop the analysis project in order to avoid getting useless results.
- ***Data not available or of bad quality:*** Data problems often lead to additional assumptions. Sometimes during model development data "dummies" are used to test the model and later left in as parameters. If this is not known or forgotten, it can lead to wrong conclusions or recommendations.
- ***Bad or missing model documentation:*** The model documentation should answer the question "How are things modelled?" It is obvious that bad or missing model documentation seriously impedes a useful scenario implementation. Model documentation cannot replace the model expert, but there is no model expert without model documentation. Again a serious threat for the success of the whole analysis project!
- ***SMEs not available:*** This is certainly a kill-criterion for a successful analysis. During RSP, SME knowledge is needed to implement and test the scenario. For the usefulness and acceptance of analysis results the involvement of SMEs is essential.
- ***Model expert not available:*** Even a good model documentation cannot replace an experienced model expert, because model expert means much more than being able to handle the simulation model. Knowing how things are modelled in the model is the crucial part here. The model expert is not only necessary for implementing and testing the scenario, but also later for interpreting simulation results together with analysts and SMEs.
- ***Too much detail in modelling:*** The art of modelling is to get the level of abstraction right. Too much detail in the scenario will make it nearly impossible to extract the relevant information and to come to valid conclusions in the problem area. The analysis team has to withstand the temptation to put more and more details into the model and the scenario. The required level of detail should be determined by the analysis questions only.
- ***Not enough detail in modelling:*** If the model or the scenario is not detailed enough, the analysis will not reveal the kind of insights we hope for. Much thought has to be spent in the starting phase of the analysis to get the right level of abstraction.
- ***Missing possibilities for editing the scenario settings:*** Suitable editors should be available to implement and to adjust scenario settings. This is not only important to save time, but also to better involve SMEs in this process. An example might be an editor to create or change rule sets for agents in the simulation model. Parameters or data hardcoded into the model often create the necessity to construct work-arounds.

- ***Missing equipment or software:*** Effective RSP requires the right tools. Insufficient support in this area leads to more time-consuming and inefficient processes. A common example is the need to generate or manipulate terrain databases for the simulation system.
- ***Question changes during RSP process:*** Whenever an analysis question changes the analysis team has to check the implications on all the aspects of the analysis including model and scenario, otherwise the analysis work might be invalid and the findings useless.
- ***Exaggerated Political Correctness:*** The scenario description within RSP used as basis for scenario implementation should be separated and distinguished from more general scenario context descriptions, which often include many more domains like historical development of the situation. The RSP scenario description should strongly focus on the investigation of the analysis question, otherwise other influences might reduce the usability of the scenario for the analysis.
- ***Model still under development:*** It is not uncommon that a model still under development is chosen for the analysis. In this case it is important to use a specified version of the model ("freeze the model") for the analysis; otherwise simulation output might change due to the influence of new model features without being aware of this cause.
- ***MOE / input data / output data not defined:*** Scenario implementation and testing should take the required simulation input and output data as well as the MOE into account, otherwise the analysis project will re-enter the RSP sooner than expected.
- ***Insufficient time for RSP:*** Rapid is relative. The analysis team should not underestimate the time necessary to implement and test the scenario. Insufficient time can lead to a low quality base case scenario, which will lead to low quality analysis results.
- ***Assumptions not documented:*** Assumptions and development of assumptions can have a large impact on the interpretation of simulation results. Different groups need a common understanding, and if the assumptions are documented there may be less room for error.
- ***Reality not reflected sufficiently in scenario ("Working on the wrong model"):*** The simulation will still produce numbers, which we can analyse and visualize statistical insights. We can even draw conclusions and give recommendations but they might not be applicable or even dangerous. This shows that involvement of SMEs is essential during the whole RSP process.
- ***Simulation produces unwanted effects not present in the real world:*** This aspect might be caused by model errors, work-arounds or modelling errors during scenario implementation. Such effects oftentimes remain undiscovered until the analysis of the data farming results or until the interpretation of these results. These unwanted effects can be dangerous if they are never discovered, because they can lead to wrong conclusions as result of the whole analysis project.

3.4 DISTILLATION MODEL DEVELOPMENT

As stated in the previous section, the model development realm works hand-in-hand with the rapid scenario prototyping realm in the experiment definition loop on the left side of Figure 3-2. The fundamental output of this loop is a scenario instantiated in a working model that captures the essence of a question and that can be sent to the multi-run execution loop of the data farming process. Of course, more insight into the question, refinement of the question, and/or deeper examination of the question may be enabled later through a return to the experiment definition loop later in the process.

The model development subgroup of MSG-088 pursued the task of providing basic characteristics of data farmable simulation systems, such as general technical requirements on simulation systems that are used for data farming. We investigated possible application areas of data farmable simulation systems and studied technical concepts within modelling. The group documented some of the most important system contributions made by each member nation. Figure 3-4 shows a list of mature data farmable models, each applicable for a variety of question bases and which model was developed in which member nation. In addition to these, especially for Data Farming developed, models all agent based model development environments can be used to rapidly develop a model appropriate to the actual question base.

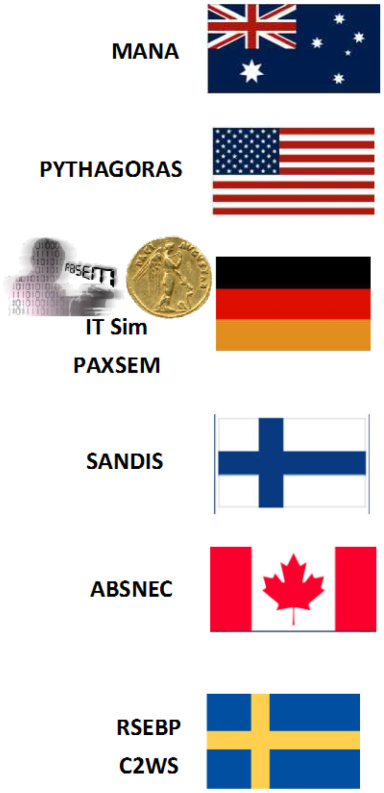


Figure 3-4: Modelling Contributions of the Member Nations.

And in a few words follows a very short description of the models:

- **MANA** (Map Aware Non-uniform Automata) is an agent-based, time-stepped, distillation model developed by the New Zealand Defence Technology Agency (DTA) for the New Zealand Defence Force.

  The model was built on the idea that overly detailed models are not helpful in finding robust system settings for desired battlefield outcomes, because they are too focused on extraneous issues. MANA, therefore, models only the essential details of a scenario and tries to create a complex adaptive system that mimics real-world factors of combat. The agents are map aware meaning that the map serves as the agent's impression of its environment. This modelling environment has a relatively easy GUI, allows for quicker scenario development, and is capable of data farming.

- **Pythagoras** is a multi-sided Agent-Based Model (ABM) created to support the growth and refinement of the U.S. Marine Corps Warfighting Laboratory's Project Albert.

Anything with a behaviour can be represented as an agent.

The interaction of the agents and their behaviours can lead to unexpected or emerging group behaviours, which is the primary strength of this type of modelling approach.

As Pythagoras has grown in capability, it has been applied to a wide variety of tactical, operational and campaign level topics in conventional and irregular warfare.

- **ITSimBw** is a multi-agent simulation system designed to simulate and analyse military operations in asymmetric warfare. The core abilities are data farming, optimization and analysis. It is designed to adapt to different military scenarios scalable in time, space and functionality. Therefore several so called "Szenarkits" were developed to cover certain question-driven surveys inspired by the German Bundeswehr.

- **PAXSEM** is an agent-based simulation system for sensor-effector simulations (**ABSEM**) on the technical and tactical level that can be used for high performance data farming experimentation. PAXSEM addresses combat-oriented questions as well as questions relevant to peace support operations. For being able to take into account civilians in military scenarios, PAXSEM also contains a psychological model that can be used to model civilians in an adequate way. Civilians in PAXSEM behave according to the current status of certain motives, such as fear, anger, obedience, helpfulness or curiosity (**PAX**). According to the motivational strength of these human factors, the civilian agent will choose and execute certain actions.

- **SANDIS** is a novel military operational analysis tool used by Finnish Defence Forces (F3) for comparative combat analysis from platoon to brigade level.

  In addition, it can be used to study the lethality of indirect fire, since it includes a high-resolution physics-based model for fragmenting ammunition.

  SANDIS has also been used for analyses of medical evacuation and treatment.

  The software is based on Markovian combat modelling and fault logic analysis.

- **ABSNEC** is a simulation system that is able to represent realistic force structures with tiered C2 architectures, as well as human factors such as stress, fear, and other factors towards the analysis of battle outcomes in network operations.

  In addition, the simulation system provides flexibility to users in creating customized algorithms that define network agents in route control and bandwidth capacity assignment in the communication network.

- **RSEBP** is a simulation-based decision support system for evaluation of operational plans for expeditionary operations.

  The system simulates a blue forces operational plan against a scenario of red and green group actors.

  This system uses a special form of data farming based on A*-search a tree of alternative plan actions, where a full plan instance corresponds to one data input point.

- **C2WS** is a command and control simulation system. The system models all levels from combat level up to operational levels. It can be used for planning, procurement, and training/exercises.

  This system does not currently use data farming, it may be extended to include data farming under a data farming wrapper.

Furthermore, we documented existing model practices for data farming obtained from experiments with applications within each nation. In addition the group identified and documented the overall scope of applications and the real world domains that can be addressed using data farming methodology with the existing models. Space constraints prohibit us from discussing all of this work, but here in the remainder of this section we will summarize our recommendations regarding model development in data farming applications.

When developing models, both modelling and subject matter experts should be present. Rapid scenario prototyping provides model requirements for model development. For example, it is important to do one thing well, such as creating aggregated models that combine simple models instead of building single monolithic models, whenever possible. The more independent models are from each other, the better the potential results. Thus, one needs to encourage modularization and clear separation of different models, including development practices for using models of different aggregation level and scope.

Reusability of models is also an important topic. To achieve good reusability, models should be loosely coupled and be interoperable. We need to make models interoperable with other models and easily data farmable. Interoperability is achieved, when input and output variables of a model are properly exposed and documented. Existing standards of the modelling and simulation community should therefore be applied wherever applicable.

Furthermore, model calculations and results should be exactly repeatable. For example, any random number generators in models should have their seed values exposed as input variables, so that simulations can be repeated. Good standards require appropriate validation of models. To be useful they need to reflect reality at the correct level of approximation. In addition, data validation should be properly documented and provided.

User interfaces should be clearly separated from calculation engines. This makes it easier to reuse the models. For example, in high performance computer applications, simulation systems are often used without a graphical interface. Also, model verification should be made as easy as possible. To ensure that the models work properly, they should have an extensive test suite that can be run through. In case of problems, simulation systems should provide transparent state of their inner workings to make investigation and problem fixing easy.

Whenever possible, it is recommended to provide supporting software with the simulation systems. Complex models, especially those dealing with complex input parameters, need supporting software. This supporting software should also be provided with the simulation systems, using similar good software practices. Because even the most accurate and efficient model is useless without information on how to use it, documentation of models and their validation has to be done properly. And, finally, openness should be encouraged, the source code should be provided with the model when possible given other constraints [9].

3.5 DESIGN OF EXPERIMENTS

Design of experiments is one of the three realms of data farming in the multi-run execution loop. Along with the realms of high performance computing and analysis and visualisation, the realm of design of experiments allow us to perform multiple runs to gain simulation results over a wide landscape of possibilities. The full MSG-088 report describes the methodology in design of experiments related to data farming and documents currently available designs in this area, but here we simply give a broad overview of design of experiments.

Simulation models have many inputs or parameters (factors) that can be changed to explore alternatives. A designed experiment is a carefully chosen set of combinations of these inputs, called design points, at which the simulation model will be run.

Changing the factors all at once limits your insights. It will allow you to see whether or not this changes the responses, but you will not be able to tell why the changes occur. For example, if mission effectiveness improves when you equip a squad with better sensors and better weapons, you will not know whether it is the weapon or the sensor that has the most impact.

Changing the factors one at a time also limits your insights. If the squad gets a very small improvement from a better weapon, a very small improvement from a better sensor, but a large improvement from both, you will not be able to identify this interaction (or synergistic effect) if the experimental design does not involve factors for both the weapon and the sensor.

Changing the factors in a brute force way, by looking at all possible combinations, is impractical or impossible, except for extremely simplistic simulations with only a handful of factors. If you have 100 sensors, each of which can be turned on or off, there are 2^{100} possible sensor configurations. Even printing these alternatives would take millions of years on the world's fastest supercomputers.

Design of experiments helps overcome the curse of dimensionality, while letting you achieve a broad variety of insights about your simulation model's performance. It provides smarter ways of setting up the experiment that facilitate follow-on analysis and visualization of results in a reasonable amount of time. The type of design used in an experiment dictates the output data that will be generated and collected in a simulation experiment. It also impacts the analysis and visualization methods that can be used in the analysis of simulation output data [9].

Figure 3-5 shows, in two very simplified representations, on one side the complete cover of the parameter space on the other side the statistical cover of the parameter space.

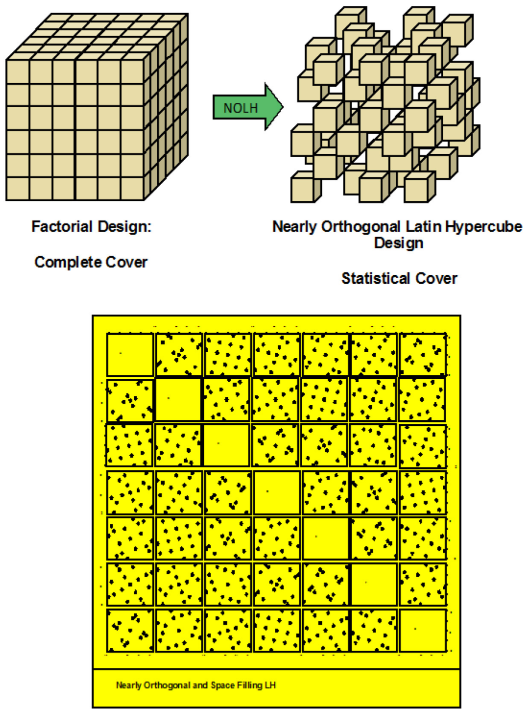

NOLH
Factorial Design:
Complete Cover
Nearly Orthogonal Latin Hypercube Design
Statistical Cover
Nearly Orthogonal and Space Filling LH

Figure 3-5: Complete Cover and Statistical Cover of the Parameter Space (two simplified representations).

3.6 HIGH PERFORMANCE COMPUTING

The main task of the High Performance Computing (HPC) subgroup of MSG-088 was to document best practices and the lessons learned by the member nations in their pursuit of implementing an HPC environment for data farming. In addition, the subgroup documented those individual member nations' environments. This documentation appears in the full MSG-088 report. Here we will summarize the realm of high performance computing within the loop of loops that make up the data farming process.

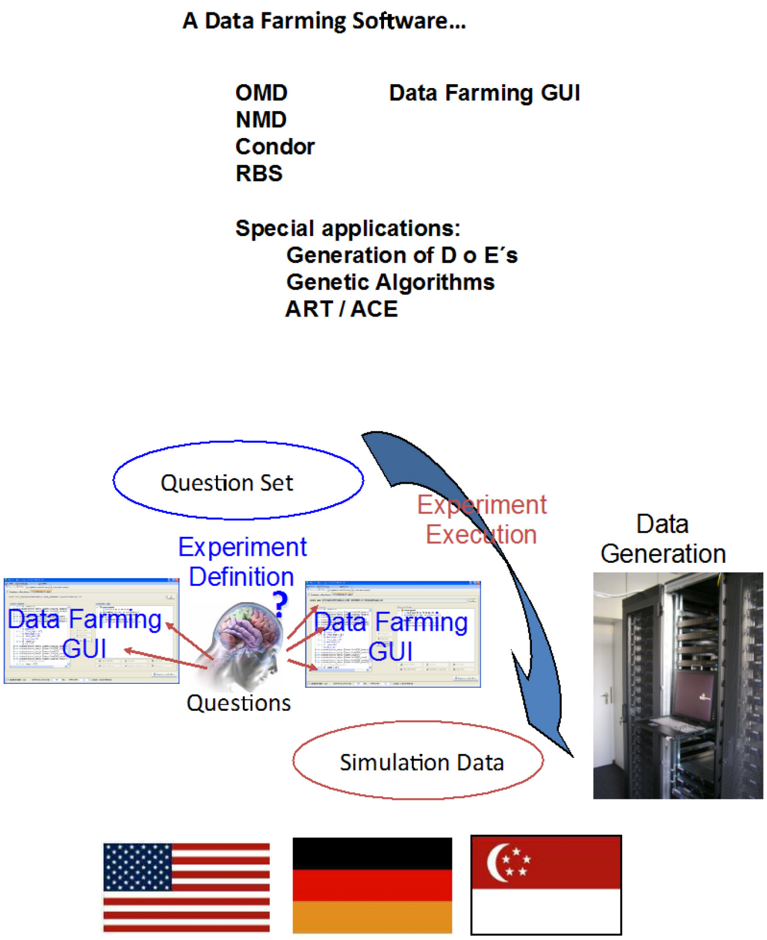
HPC consists of both hardware and software resources. HPC systems can be configured as a single supercomputer with thousands of processors, as a network of clustered computers, or even as a single powerful desktop computer with multi-core processors. The hardware on these systems includes such things as processors, memory, networking hardware, and disk storage. HPC software includes, among other things: the operating system; underlying or supporting software which provide the environment to execute the model; and the data farming software, which enables running instances of the model across the HPC systems' "compute units". By generating and managing each of the model runs over a set of design points or input sets, the data farming software provides the infrastructure "glue" that "sticks together" the model, its set of inputs, the design, and the HPC resources.

The main purpose of HPC in the context of data farming is to provide the means to execute a data farming experiment. Other purposes of HPC are for use in analysis and visualization of the output and for generating designs used in future data farming experiments. Given the large number of model runs made in a typical data farming experiment, HPC facilitates conducting the experiment in a timely manner as well as supporting the storage and analysis of huge volumes of output. From a purely computational perspective, there are six elements involved in a data farming experiment:

1) A "data farmable" model (we use the term "model" generically; it can refer to any computational model or simulation).
2) A set of model inputs, generically called the "base case".
3) A specification of your experiment (the set of factors in your design and a mechanism for finding and setting those in the set of model inputs).
4) A set of HPC resources, both software and hardware, needed to execute a model "instance".
5) The data farming software.
6) A set of model outputs.

The first five elements are required to begin execution of the data farming experiment; the final element is the product or the results of the data farming experiment. Basically, the process proceeds as follows: for each "design point" in the design, the data farming software creates and executes a compute "task" or "job", where that task consists of creating a set of model inputs using the base case as a template; executing the model with that modified input set; and collecting and storing the model output for that design point. Other tasks may include collecting and staging the raw output for further analysis and visualization, additional post-processing of the output, or automated analysis of the output [9].

Figure 3-6 refers on top to a Data Farming software in a Data Farming GUI followed by a sketch of the path from the question base to simulation results and the here contributing nations.



A Data Farming Software…

OMD Data Farming GUI
NMD
Condor
RBS

Special applications:
Generation of D o E´s
Genetic Algorithms
ART / ACE

Figure 3-6: Data Farming Software, the Experiment Execution Loop and the Contributing Nations.

3.7 ANALYSIS AND VISUALISATION

We define analysis as the process of examining data that is produced by data farming processes using statistical, summarization and presentation techniques to highlight useful information, extract conclusions, and support decision-making. Visualisation is a collection of graphical and visual analysis techniques used to optimize and speed the process of exploring data, conveying understanding, and presenting in data farming processes. Much of the current usage of analysis and visualization in the data farming process has been the analytic examination of multiple replicate and excursion model output and we describe this usage in the full report. Here we will give some of the high level conclusions regarding the realm of analysis and visualisation from MSG-088.

In order to exploit the potentially huge data output from the high performance computing execution of the design of experiments, highly effective analysis techniques must be employed. Statistical analysis and visualisation can be used to discern whether data may has useful meaningful value and aid in the translation of data into information useful in making progress in understanding possible answers to the questions at hand. Figure 3-7 shows the Analysis and Visualization Architecture for the three types of stakeholders:

1) Decision makers;
2) Modellers; and
3) Analysts for any level of decision making.

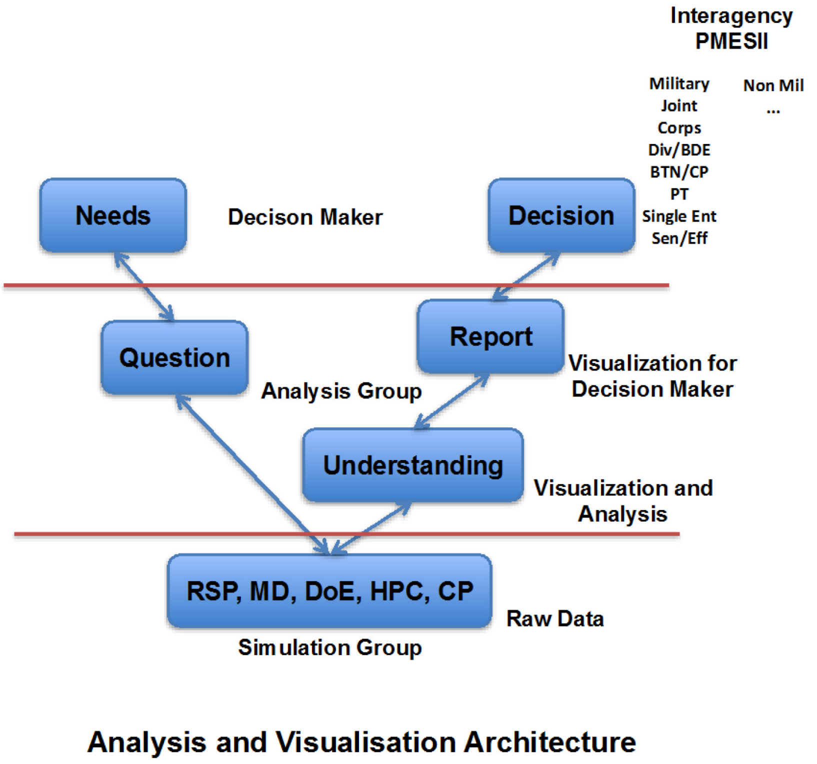


Figure 3-7: Three Types of Stakeholders for Analysis and Visualisation – Decision Makers, Modellers, Analysts.

Every stakeholder has his own needs in analysis and visualization and finally representation of the data output.

Visualisation consists of analysing the simulation output data using appropriate techniques as well as presenting the results to the decision-making authorities. Even with a smart design of experiments, simulation experiments can create huge volumes of multi-dimensional data that require sophisticated data analysis and visualisation techniques.

The ability to use multiple techniques gives us the ability to explore, investigate, and answer the questions posed. Every technique has strengths and limitations, therefore, especially for highly-dimensional datasets, use of a family of techniques is preferable to use of a single technique. The key here is the understanding of the data.

As stated earlier, data farming gives us the ability to map the landscape of possibilities and in the process discover outliers. These outliers should always be considered and only be eliminated for appropriate reasons. Using various analysis and visualisation techniques these outliers can also be investigated as a separate cohort of the data. The full MSG-088 report describes analysis and visualisation techniques and technologies that have been used in this pursuit of both examination of the full landscape of possibilities as well as discovering the surprises that can often lead to important additional support to decision makers [9]. The report provides in addition a basic strategy for the analysis and visualization of HPC experimental outputs by asking the following top ten questions (to ask to the experiment results) and delivers multiple techniques with complementary capabilities to answer these questions:

- Q1: What was the *spread* of the responses over the entire experiment?
- Q2: How much random variation was observed *just over the random replications?*
- Q3: Were there any *outliers?*
- Q4: Were the responses *correlated?*
- Q5: Which factors were most *influential?*
- Q6: Were there any significant *interactions?*
- Q7: What were the interesting *regions* and *threshold values?*
- Q8: Are any of your results *counter-intuitive?*
- Q9: Which configurations were most *robust?*
- Q10: Are there any configurations which satisfy *multiple objectives?*

3.8 COLLABORATION

The spirit of collaboration is the key tenet of data farming. It underlies the loop of loops in Figure 3-2 and holds within it much of the power of data farming. Throughout the development of data farming and the formation of the data farming community, people from all attending nations have openly shared experiences and expertise. One focus for collaborative efforts has been and continues to be the international workshops. The first international workshop took place in 1999 at the Maui High Performance Computing Center. The first 4 workshops were methodology driven, dealing with complex adaptive systems modelling and agent based representation, with statistical experiment design and experiment evaluation. The subsequent workshops were application driven, contributions to the overall advancement of data farming takes place in the development of simulation models, scenarios within the models, and computer clusters to run the models audacious numbers of times.

The real work is in making progress on important questions and the real secret is the combination of military subject matter experts and highly knowledgeable and multi-disciplinary scientists. This special mix of personnel has been the hallmark of the international workshops and this mix has promoted much networking opportunity. It has been a dynamic combination to have data farming work teams headed up by a person who really knows and cares about the question (e.g., a military officer who knows that the answers may have an impact on both mission success and lowering casualties) and supported by men and women with technical prowess who can leverage the tools available.

The collaboration subgroup of MSG-088 documented the following aspects of the collaborative processes in data farming: defining the characteristics and dimensions of collaboration in data farming, collaboration within and between the realms in data farming, collaboration of the people, collaboration of the data farming results, application of collaboration tools. This information can be found in the full report as well as information on the current status of data farming in the attending nations and ideas about the future development of data farming [9].

3.9 REFERENCES

[1] Horne, G. (1997). Data Farming: A Meta-Technique for Research in the 21st Century, Naval War College. Newport, RI.

[2] Horne, G. (1999). Maneuver Warfare Distillations: Essence Not Verisimilitude, in: A. Farrington, H.B. Nembhard, D.T. Sturrock, and G.W. Evans, (eds.), *Proceedings of the 1999 Winter Simulation Conference*, pp. 1147–1151. Phoenix, AZ.

[3] Horne, G. and Leonardi, M., editors (2001). *Maneuver Warfare Science 2001*. Marine Corps Combat Development Command, Quantico, Virginia, USA. ISBN 0-9711487-1-6.

[4] Horne, G. and Meyer, T. (2004). Data Farming: Discovering Surprise, in: R. Ingalls, M.D. Rossetti, J.S. Smith, and B.A. Peters, (eds.), *Proceedings of the 2004 Winter Simulation Conference*, pp. 171-180. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, Inc.

[5] Horne, G. and Meyer, T. (2005). Data farming: Discovering Surprise, in: M.E. Kuhl, N.M. Steiger, F.B. Armstrong, and J.A. Joines, (eds.), *Proceedings of the 2005 Winter Simulation Conference*, Orlando, Florida.

[6] Meyer, T. and Horne, G. editors (January 2007). *Scythe*, Proceedings and Bulletin of the International Data Farming Community, Issue 1, Workshop 13, The Hague, Netherlands.

[7] Meyer, T. and Horne, G. editors (June 2013). *Scythe*, Proceedings and Bulletin of the International Data Farming Community, Issue 12, Workshop 25, Istanbul, Turkey.

[8] Horne, G. (2010). MSG-088 Data Farming in Support of NATO, MSG-088 Program of Work, NATO Research and Technology Organisation (RTO).

[9] Horne, G., Seichter, S., *et al*. (2014). MSG-088 Data Farming in Support of NATO, Final Report, NATO Science and Technology Organization (STO).

[10] Seichter S., *et al*. (2014). MSG-088 Data Farming in Support of NATO: Case Study Force Protection, MSG-111 Symposium Paper Number 17, Sydney, Australia.

[11] ITIS (2011). Leitfaden simulationsgestützte Analysen in der Bundeswehr, Code of best practice of simulation based analyses in the German Armed Forces, non-technical study issued by the Center of Transformation of the Bundeswehr, Munich.

Chapter 4 − DATA FARMING DECISION SUPPORT IN OPERATION PLANNING

4.1 INTRODUCTION

Over the last decade the evolving and maturing methods and technologies in the context of Modelling and Simulation (M&S) have successfully been applied for analysis in operational studies as well as for procurement support in the defence domain. Thus, M&S methods and tools have been established and accepted in these fields of application. One area where there is a great potential for use is within direct support of military commanders and staffs for concrete operation planning.

In order to apply M&S for decision support in direct support of military commanders and staffs, it is important to align the support with the existing processes. The crisis response planning process in NATO is described in the Comprehensive Operations Planning Directive (COPD, Version 2.0, NATO 2013), for different command levels in several phases. In assessing the COPD at the Joint Head Quarter (JHQ) level to identify the best suited phases for application of Data Farming for decision support, the process steps in Phase 3b to develop, analyse, compare and refine Courses Of Action (COA) will clearly benefit from the characteristics of the Data Farming method.

Data farming provides an unprecedented possibility of mapping the possible consequences of decisions. With this approach analysis of many different situations can be aggregated enabling ready-to-use decision support. Simulation-based decision support complements operational experience with an objective, reproducible and transparent analysis. This opens up new possibilities by examining thousands of alternative COA revealing factors of importance concerning operational outcomes. This allows the staff to prepare the grounds for the decision-making of the Commander based on quantitative data.

The goal of this work is to develop a decision support tool based on Data Farming and adapted to the COPD with focus on analysis and visualisation, and to implement a prototype to demonstrate its functionality. The tool supports the JOPG in conducting operation planning along the COPD guidelines. The software tool is named *Data Farming decision support Tool for Operation Planning* (DFTOP). DFTOP is an integrated multirole tool providing tailored views applicable to different roles of the JOPG, i.e., operational analysts, planners and decision makers.

To provide decision support for a commander's specific questions in operation planning, we perform a sequence of process steps, implemented as workflows in DFTOP. From a top-level perspective, we begin with traditional Data Farming. We then go beyond the traditional approach with the analysis and visualisation part automated and tailored to directly support the decision-making process.

We divide the decision support process into three easy sub-processes:

- The Analyst View process, which is automating the traditional statistical analysis usually performed in Data Farming.
- The Commander's Overall Operational Questions process, which is focused on the big picture of how to win in military combat.
- The Commander's Specific Operational Questions process, focusing on more specific questions of when we will win in different specific situations.

Here the purpose of the analyst view is to set-up the decision support tool to be ready to answer that Commander's Overall Operational questions. This is a number of pre-prepared analyses questions that aim at giving the Commander a decision brief pointing out the crucial elements of the operation, and recommending a COA. In developing the decision brief, the JOPG may analyse Commander's Specific Questions aiming at providing answers to all possible specific and detailed questions.

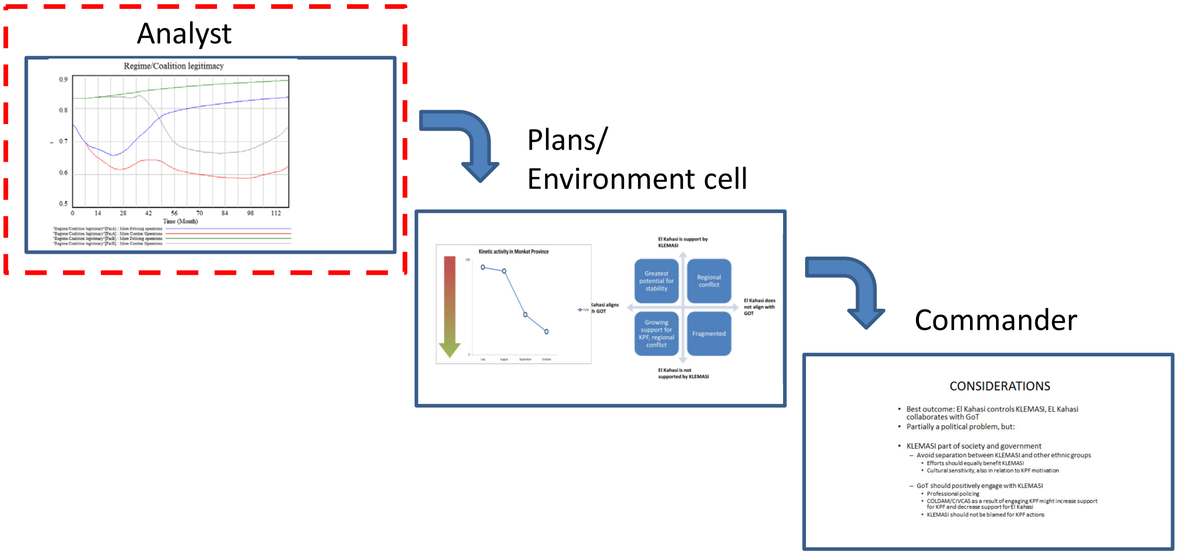
To demonstrate our concept we use the *Bogaland* scenario. This is a large scale symmetric scenario, where the country Bogaland is attacked by another country. The JHQ's task is to develop operation plans to defend Bogaland by the means of Bogaland's forces and combined operations including NATO forces. The scenario represents a realistic situation for potential planning tasks for a JHQ. It describes potential offensive COA of a fictitious aggressor state and the general outline and available forces for the defence by NATO. It also considers the joint aspects of the planning by including air and land forces.

4.2 RELATED WORK

The approach to simulation support of the Military planning process may be divided into statistical or case-based [1]. A clear distinction should be kept as these approaches have different objectives and areas of validity. In Data Farming, the statistical approach is used. The objective is to find statistically significant answers to a set of questions, e.g., regarding the most likely outcome. The statistical nature of data farming enables the possibility to provide objective answers and probabilities regarding possible outcomes. This yields a toolbox for the decision maker, enabling more well-informed decisions. Case-based simulation support may provide detailed analysis on possible outcomes on a few cases. The objective of the analysis is to provide a deep understanding of the underlying principles. It is typically used to train the cognitive abilities of the decision makers, e.g., by observing and interacting with the simulation during run-time. Transparency and representativeness of the chosen cases is therefore important in such simulations. The French simulation system *Aide à la Planification d'Engagement Tactiques* (APLET) is an example of a case-based simulation, developed to support the planning process of the French brigade [2].

One domain of the statistical approach is the method effects-based planning. An approach to this is described by FOI in Ref. [3], with simulation-based decision support techniques for evaluation of operational plans. Using a decision support tool, thousands of alternative plans can be evaluated against possible courses of events and decision can be made regarding which of these plans are capable of achieving a desired end state. The objective is to help operational analysts understand the consequences of numerous alternative plans through simulation and evaluation. A representation was used where a plan consists of several actions that should be performed. Each action may be performed in one of several different alternative ways. These action alternatives make up all possible plan instances that may be searched for the most effective sequence of actions. A test use case was an expeditionary operation with a plan of 43 actions and several alternatives for these actions, as well as a scenario of 40 group actors. Decision makers can use the tool to determine the boundaries of an operation that it must not move beyond without risk of drastic failure. This approach uses a PMESII model (Political, Military, Economic, Social, Infrastructure, Information (sometimes referred to as the physical, information and human landscapes)).

Related work is also carried out at TNO [4], [5]. That work is directed to supporting the Commander in the JOPG in other process steps at JHQ level as defined in COPD, namely the steps that involve the situational awareness and analysis of the mission area (in step 3a). The types of models required for this are PMESII models. The interventions that organisations can apply are usually summarized under the acronym DIME (Diplomacy, Information, Military, Economic). Since these types of models involve human behaviour, they are usually associated with a lot of uncertainty. An approach called *Exploratory Modelling and Simulation* (EMA) takes these uncertainties into account by simulating many plausible (possibly parametrized) models generating many plausible futures. The types of models used were so-called System Dynamics models. These models were built with the Vensim System Dynamics simulation package [6]. The data that is farmed in this way can be analysed to find robust interventions taking into account uncertainty. The statistical tool JMP [7] was used to do the analysis. Process steps for the analyst, the planner and the decision maker are visualised below in Figure 4-1.


Analyst
Regime/Coalition legitimacy
0.9
0.8
0.7
0.6
0.5
0
14
28
42
56
70
84
98
112
Time (Month)
"Regime/Coalition legitimacy"[FacA] : More Policing operations
"Regime/Coalition legitimacy"[FacA] : More Combat Operations
"Regime/Coalition legitimacy"[FacB] : More Policing operations
"Regime/Coalition legitimacy"[FacB] : More Combat Operations
Plans/
Environment cell
Kinetic activity in Monkat Province
100
0
July
August
September
October
Total
El Kahasi is support by KLEMASI
Greatest potential for stability
Regional conflict
Growing support for KPF, regional conflict
Fragmented
Kahasi aligns th GOT
El Kahasi does not align with GOT
El Kahasi is not supported by KLEMASI
Commander

CONSIDERATIONS

- Best outcome: El Kahasi controls KLEMASI, EL Kahasi collaborates with GoT
- Partially a political problem, but:
- KLEMASI part of society and government
  - Avoid separation between KLEMASI and other ethnic groups
    - Efforts should equally benefit KLEMASI
    - Cultural sensitivity, also in relation to KPF motivation
  - GoT should positively engage with KLEMASI
    - Professional policing
    - COLDAM/CIVCAS as a result of engaging KPF might increase support for KPF and decrease support for El Kahasi
    - KLEMASI should not be blamed for KPF actions

Figure 4-1: Process Steps and Their Users [5].

In Ref. [8], FOI describes the modelling, simulation and data analysis of a multi-criteria simulation-based approach for operation planning. With this method a decision maker can analyze alternative scenarios, where the concern is the best use of available resources in military operations. The scenario is a ground combat situation of two battalions and describes the military units and their capabilities (with simulation at the platform level). Tens of thousands of alternative plans are evaluated using multiple MOE with a data farming approach. A model is developed that represent various military units and contains basic logic for various components of each unit, such as platforms, sensors, cognition models governing the behavior of different units, etc. Large amounts of data from the simulations are analyzed in order to find the best parameter values for the Blue side, e.g., number of platoons, sensors ranges, force tactical behavior, and avenues of approach for both the Red and Blue side. Since the quality of a plan is determined by several possibly contradicting MOE, a multi criteria approach based on preference analysis is used to determine overall success. Finally, visualization methods such as heat maps and box-plots show why the best plan is good. With this methodology it is possible to find which combination of parameter ranges leads to overall Blue success. Some of the methods applied in this work, are used as a basis for our work in this MSG-124 Report.

4.3 ALIGNMENT OF DFTOP TO THE PLANNING PROCESS

The Data Farming decision support is aligned with NATO's COPD; it is briefly described in this section in order to show how it is supported by Data Farming and DFTOP.

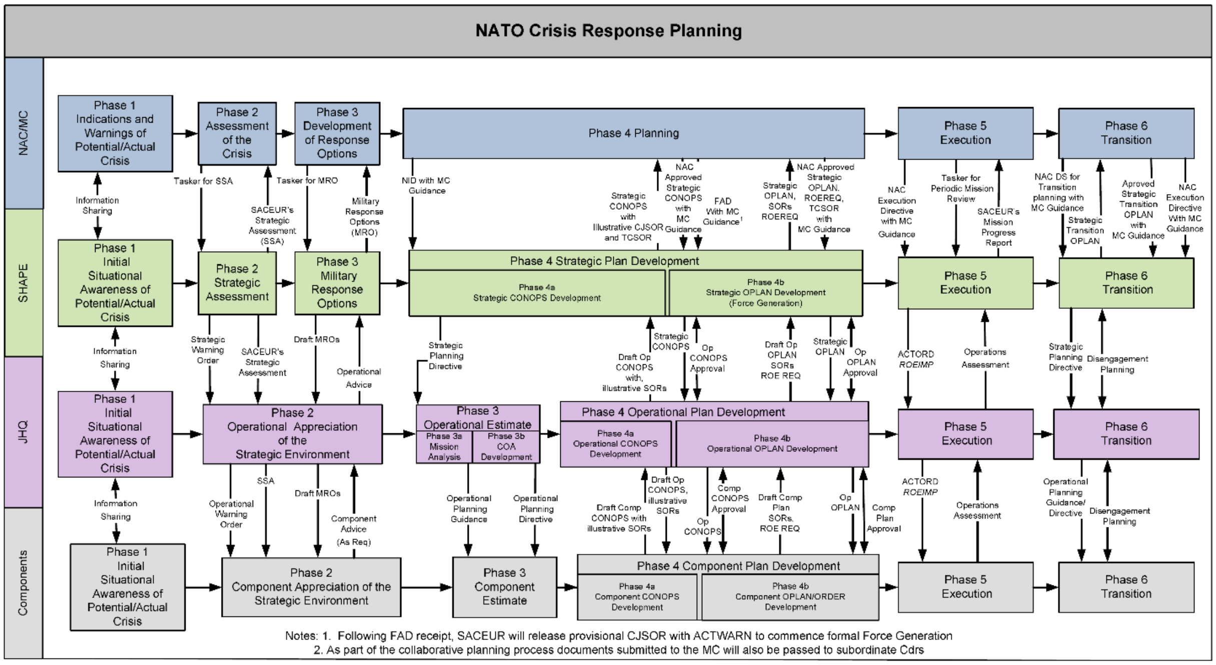
4.3.1 COPD Overview

The COPD is applicable to all operation planning activities at the NATO strategic and operational levels of command and can be adapted to the component/tactical level in order to enhance collaborative planning activity.

With regards to the Operation Planning the military strategic levels seek to translate political-strategic guidance into military-strategic directions for the operational commander.

At the operational level, planning seeks to transform strategic direction into a scheduled series of integrated military actions, carried out by joint forces to achieve operational objectives efficiently and with acceptable risks.

An overview of the COPD process is shown in Figure 4-2.


NATO Crisis Response Planning
NAC/MC
SHAPE
JHQ
Components
Phase 1 Indications and Warnings of Potential/Actual Crisis
Phase 2 Assessment of the Crisis
Phase 3 Development of Response Options
Phase 4 Planning
Phase 5 Execution
Phase 6 Transition
Information Sharing
Tasker for SSA
SACEUR's Strategic Assessment (SSA)
Tasker for MRO
Military Response Options (MRO)
NID with MC Guidance
Strategic CONOPS with Illustrative CJSOR and TCSOR
NAC Approved Strategic CONOPS with MC Guidance
FAD With MC Guidance1
Strategic OPLAN, SORs ROEREQ
NAC Approved Strategic OPLAN. ROEREQ, TCSOR with MC Guidance
NAC Execution Directive with MC Guidance
Tasker for Periodic Mission Review
SACEUR's Mission Progress Report
NAC DS for Transition planning with MC Guidance
Strategic Transition OPLAN
Aproved Strategic Transition OPLAN with MC Guidance
NAC Execution Directive With MC Guidance
Phase 1 Initial Situational Awareness of Potential/Actual Crisis
Phase 2 Strategic Assessment
Phase 3 Military Response Options
Phase 4 Strategic Plan Development
Phase 4a Strategic CONOPS Development
Phase 4b Strategic OPLAN Development (Force Generation)
Phase 5 Execution
Phase 6 Transition
Information Sharing
Strategic Warning Order
SACEUR's Strategic Assessment
Draft MROs
Operational Advice
Strategic Planning Directive
Draft Op CONOPS with, illustrative SORs
Strategic CONOPS
Op CONOPS Approval
Draft Op OPLAN SORs ROE REQ
Strategic OPLAN
Op OPLAN Approval
ACTORD ROEIMP
Operations Assessment
Strategic Planning Directive
Disengagement Planning
Phase 1 Initial Situational Awareness of Potential/Actual Crisis
Phase 2 Operational Appreciation of the Strategic Environment
Phase 3 Operational Estimate
Phase 3a Mission Analysis
Phase 3b COA Development
Phase 4 Operational Plan Development
Phase 4a Operational CONOPS Development
Phase 4b Operational OPLAN Development
Phase 5 Execution
Phase 6 Transition
Information Sharing
Operational Warning Order
SSA
Draft MROs
Component Advice (As Req)
Operational Planning Guidance
Operational Planning Directive
Draft Comp CONOPS with illustrative SORs
Draft Op CONOPS, illustrative SORs
Op CONOPS
Comp CONOPS Approval
Draft Comp Plan SORs, ROE REQ
Op OPLAN
Comp Plan Approval
ACTORD ROEIMP
Operations Assessment
Operational Planning Guidance/ Directive
Disengagement Planning
Phase 1 Initial Situational Awareness of Potential/Actual Crisis
Phase 2 Component Appreciation of the Strategic Environment
Phase 3 Component Estimate
Phase 4 Component Plan Development
Phase 4a Component CONOPS Development
Phase 4b Component OPLAN/ORDER Development
Phase 5 Execution
Phase 6 Transition

Notes: 1. Following FAD receipt, SACEUR will release provisional CJSOR with ACTWARN to commence formal Force Generation
2. As part of the collaborative planning process documents submitted to the MC will also be passed to subordinate Cdrs

Figure 4-2: Comprehensive Operations Planning Directive (COPD) Overview (COPDv2.0).

At the operational level (JHQ), the process begins with a review of the situation based on the strategic analysis of the situation and the mission to develop a clear appreciation of *what* must be accomplished, under *which* conditions and within *which* limitations. Based on this appreciation it then focuses on determining *how* operations should be arranged within an overall operational design. The operational design provides the basis for subsequent development of the operational concept as well as the detailed plan.

4.3.2 COPD JHQ Phase 3 Operational Estimate

Phase 3 *Operational Estimate* is the focal phase for the JOPG of a JHQ to identify *what* has to be done under which conditions and limitations for mission success, and subsequently to develop *how* it should be done.

The Sub-phase 3a *Mission Analysis* assists the Commander and his staff to determine *what* must be done for mission success by analysing the crisis situation in depth, determining precisely the operational problem that must be solved and appreciating the specific operational conditions that must be established.

The Sub-phase 3b *COA Development* is to determine *how* to best carry out operations that will accomplish the mission effectively and efficiently.

An overview of the interaction with DFTOP in the separate steps is given in Figure 4-3. The following chapters will describe the relevant JHQ staff planning activities within Phase 3, their input to the Data Farming process and the possibilities to support all COA Development steps by DFTOP.

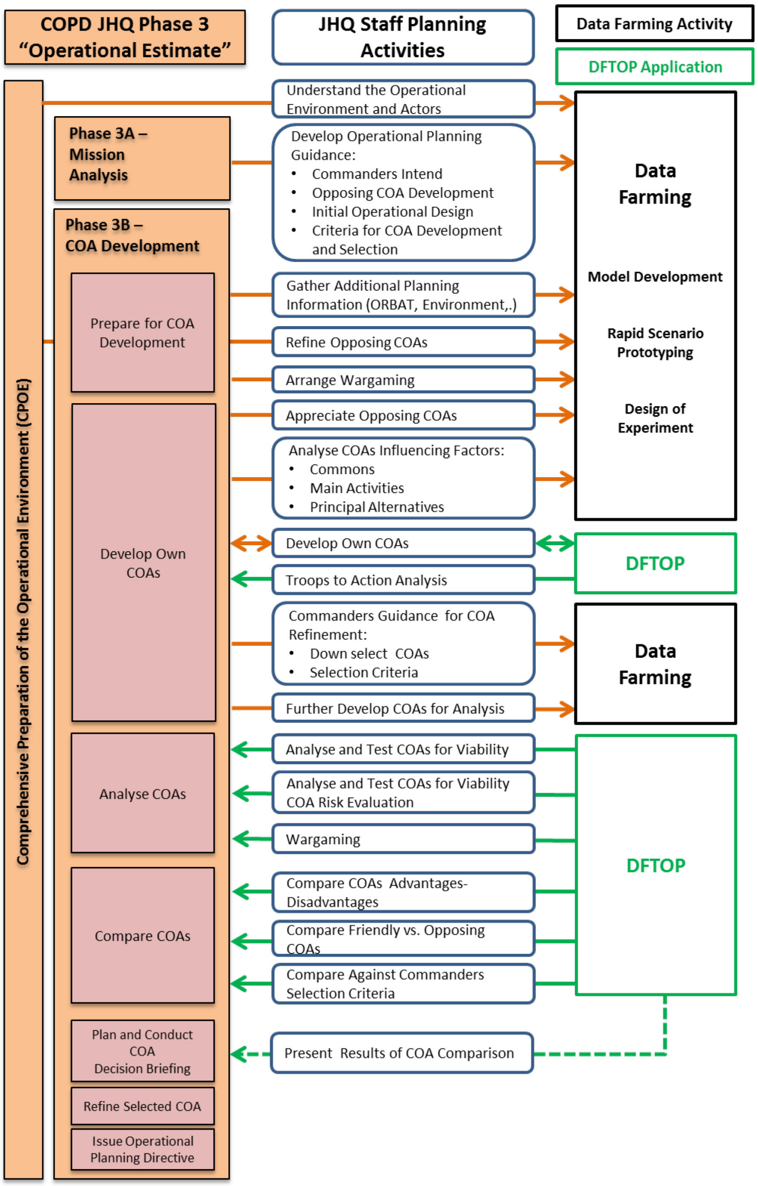

COPD JHQ Phase 3 "Operational Estimate"
JHQ Staff Planning Activities
Data Farming Activity
DFTOP Application
Comprehensive Preparation of the Operational Environment (CPOE)
Phase 3A – Mission Analysis
Phase 3B – COA Development
Prepare for COA Development
Develop Own COAs
Analyse COAs
Compare COAs
Plan and Conduct COA Decision Briefing
Refine Selected COA
Issue Operational Planning Directive
Understand the Operational Environment and Actors
Develop Operational Planning Guidance:
• Commanders Intend
• Opposing COA Development
• Initial Operational Design
• Criteria for COA Development and Selection
Gather Additional Planning Information (ORBAT, Environment,.)
Refine Opposing COAs
Arrange Wargaming
Appreciate Opposing COAs
Analyse COAs Influencing Factors:
• Commons
• Main Activities
• Principal Alternatives
Develop Own COAs
Troops to Action Analysis
Commanders Guidance for COA Refinement:
• Down select COAs
• Selection Criteria
Further Develop COAs for Analysis
Analyse and Test COAs for Viability
Analyse and Test COAs for Viability COA Risk Evaluation
Wargaming
Compare COAs Advantages-Disadvantages
Compare Friendly vs. Opposing COAs
Compare Against Commanders Selection Criteria
Present Results of COA Comparison
Data Farming
Model Development
Rapid Scenario Prototyping
Design of Experiment
DFTOP
Data Farming
DFTOP

Figure 4-3: JHQ Phase 3 Planning Activities and DFTOP Interaction.

4.3.2.1 Comprehensive Preparation of the Operational Environment

The Comprehensive Preparation of the Operational Environment (CPOE) is a crisis-specific cross-headquarters process, led by the intelligence/SME support staff, to develop a comprehensive understanding of the operational environment, the actors, and the potential threats and risks.

The intelligence and knowledge staff will lead the CPOE process, which runs in parallel to the planning process. They will also directly assist the JOPG to understand the nature of the crisis as well as the actions, capabilities and behaviour of the main actors/systems and influencing factors that account for the current situation and its development.

Exemplified inputs from the CPOE to Data Farming are:

- Theatre and environmental information.
- Anticipated intended behaviour of main actors/opposing forces.
- Capabilities, structure, quantities, and dislocation of opposing forces.

4.3.2.2 Phase 3a Mission Analysis

The relevant formal outcome from Phase 3a with regards to the follow-on planning within the JHQ is the Operational Planning Guidance (OPG). It incorporates the Commander's initial intent, the Commander's Planning Guidance (CPG) and the initial operational design.

Exemplified inputs from the OPG to Data Farming are:

- Guidance for opposing COA development.
- Guidance/fundamentals/criteria for own COA development.
- Criteria for COA selection, enabling a first draft of the definition of overall success.

4.3.2.3 Phase 3b COA Development

With regard to the application of the envisaged decision support tool the following process steps of Phase 3b are relevant.

4.3.2.3.1 Prepare for COA

The JOPG gathers any additional and updated planning information required to develop and analyse COA from the ongoing CPOE process and Operational Liaison & Reconnaissance Team activities.

This information can include opposing Order of Battle (ORBAT), actual port, airfield, road, and rail data.

Exemplified inputs to Data Farming are:

- Update on structure and dislocation of opposing forces and infrastructure.

Based on the OPG selected opposing COA are refined, including the combination of COA of multiple opponents. Often a *most likely* and a *most dangerous* opposing COA are defined in detail. This activity is part of the CPOE process.

Exemplified inputs to Data Farming are:

- Mature draft of opposing COA including parameter space for opposing capabilities, forces and systems, timing.

In the later on process step *Analyse COA* the JOPG should ideally wargame each own COA against selected opposing COA. The conduct of a wargame requires advance consideration and preparation.

Exemplified inputs to the Data Farming are:

- Administrative issues concerning time and arrangement of the wargame.
- Type of wargame and requirements for Data Farming support.

4.3.2.3.2 Develop Own COA

Before developing their own COA, the JOPG must appreciate the COA open to opposing forces. The intelligence/ knowledge staff will present their estimate of the opposing COA for each opponent and combined COA for multiple opponents as appropriate.

Exemplified inputs to the Data Farming are:

- Final adaptation of opposing COA.

At this point in time in the planning process, the JOPG will already have significant understanding of the operational factors that will impact how operations can be conducted, in particular conclusions from its analysis of time, space, forces/actors and information. The JOPG now reviews these, with the aim of establishing those key conclusions that will influence how COA are developed, focusing on the following questions:

- What are the common points applicable to all COA?
- What are the main operational activities?
- Where are the principal alternatives?

Exemplified inputs to Data Farming are:

- What are the common points and principal alternative for own COA (spatial / timely / forces/ actors).

Based on OPG, selected opposing COA and the before mentioned conclusions the JOPG develops in a creative process a set of tentative COA. Each tentative COA consists of a main idea and a brief outline of the sequence of main actions by different forces, to outline how they will create the operational effects and establish the required Decisive Conditions in the operational design.

Exemplified inputs to Data Farming:

- Initial COA ideas (combination of spatial/timely/forces/actors).

Exemplified contribution from Data Farming via DFTOP:

- General proof of Data Farming generated data and visualisation of own COA.
- First draft of *important* factors and quantities by examining a huge range of possible COA and variants within each COA.

After a first, JOPG internal, testing of the tentative COA for viability and selecting a manageable number (based on time and resources) of them for review with the Commander, the Troops-to-Action Analysis will be conducted. The JOPG, with input from subordinate commands will determine the respective military capabilities and capacities required to implement a pre-selected tentative COA. Beside others, the JOPG seeks to:

- Determine the optimum employment of operational capabilities for each operational action and desired operational effects for each phase.
- Establish the most effective/efficient mix of component capabilities.
- Determine the most effective/efficient theatre level support capabilities to support the operational force and the supplemental support capabilities required by the component.

Exemplified contribution from Data Farming via DFTOP:

- Provide data with regard to forces, forces structure, quantities and capabilities and visualize the effects of data variations.

In the follow up the JOPG presents the preselected tentative COA to the Commander in order to seek acceptance for COA and receive Commander's Guidance for the refinement of the accepted COA. In this guidance the Commander's selection criteria will be fixed, reflecting what the Commander considers to be most important for mission accomplishment based on strategic direction.

Exemplified inputs to Data Farming:

- Selection criteria for COA selection.

The COA accepted by the Commander will be refined according to his guidance and by adding the level of detail required for further analysis and war gaming. At a minimum the accepted COA will be matured by developing a first outline of a Concept of Operations (CONOPS), provisional missions for subordinate commands, draft task organization, operational graphic and timeline and Decision Points.

Exemplified inputs to Data Farming:

- Guidance and requirements to refine model and scenarios of accepted COA.

4.3.2.3.3 Analyse COA

The refined COA will be analysed in this process from different functional perspectives.

During the Analysis and Test of COA for Viability the JOPG evaluates a set of criteria, among these are:

- Suitability (does the COA accomplish the mission and comply with the OPG).
- Acceptability (are the likely achievements from the COA worth the expected costs in terms of forces deployed, resources, casualties, collateral efforts and risks levels).

Exemplified contribution from Data Farming via DFTOP:

- Provide data with regard to mission success, own and opposing losses, and visualize the effects of data variations.

The COA Risk Evaluation will be commenced by the JOPG during COA development constantly in order to look for risks and, if necessary, finding ways to mitigate them.

Exemplified contribution from Data Farming via DFTOP:

- Important factors, their quantities, their impact and their visualisation.

Wargaming of COA is necessary to evaluate their potential in accomplishing the mission against opposition foreseen in the different opposing COA and to identify and correct deficiencies. Each COA is normally wargamed against the *most* likely and *most dangerous* opposing COA, obtained according to the JOPG estimate of the mission analysis. Another value of wargaming lies in synchronizing actions and visualizes the conduct of operations.

Depending on time and resources, the method and the scope of wargaming is chosen, simulation support may be utilized at this stage.

Exemplified contribution from Data Farming via DFTOP:

- Provide data with regard to mission success, own and opposing losses, timely and spatial aspects, and visualize the effects of data variations.

4.3.2.3.4 Compare COA

COA are compared in three different contexts:

- Inherent advantages versus disadvantages;
- Own COA versus opposing COA; and
- COA against Commander's COA selection criteria.

Based on these different comparisons the JOPG should be able to recommend the COA with the highest probability for success within acceptable risks. The most important aspect of this process is the ability to articulate to the Commander why one COA is preferred over another.

Exemplified contribution from Data Farming via DFTOP:

- Provide data with regard to mission success, important factors, own and opposing losses, timely and spatial aspects and visualize the effects of data variations.

4.3.2.3.5 Plan and Conduct COA Decision Briefing

In order to come to a Commander's decision on selection of one COA, the JOPG presents during a *COA Decision* Brief the results of the Phase 3. The presentation must provide optimum information upon which to base a decision. It must be detailed enough to identify focal points but summarized for effectiveness and brevity.

Exemplified contribution from Data Farming via DFTOP:

- Most probably selected results and visualisations from DFTOP will be used during the *COA Decision Brief.*

Following the Commander's decision on a COA and his guidance, the JOPG refines the selected COA and final operational design.

The Commander's selected refined COA and the final operational design set the starting point for Phase 4 *Operational Plan Development*.

After appropriate staff preparation the Commander will issue an *Operational Planning Directive* (OPD) to the subordinate *Component Commands* (CC). The OPD will trigger the COA development at the component level.

4.3.3 Added Value for the Planning Process

Applying Data Farming in support of decision making improves the quality of the decision-making by providing a robust, reproducible, and quantitative basis. Data Farming is able to provide case driven COA analysis (based on individual scenarios comprising opposing and own COA) by statistical analysis of thousands of scenario variants (comprising a multitude of opposing and own COA variants with varying parameters).

As seen in Figure 4-3 this concept is able to cover and support the whole process of COA development. There are two main parts. The first part covers process step *Mission Analysis* until process step *Develop own COA.* Here, DFTOP supports gaining rough insights into important factors and initial ideas for own and opposing

COA. This can be performed by providing analysis of the correlation of the important factors with the overall success defined by the commander.

In the second part, from *Develop own COA* until *Decision Briefing* a refined analysis is provided based on the choices made by JOPG, e.g., answering specific questions regarding operational objectives and the consequences on own and opposing forces.

The focus of DFTOP is to translate the statistical data into actionable information in support of decision making:

- DFTOP is able to display the interdependencies between planning parameters (opposition and own COA design, force composition and location) in relation to the achieved effects (success criteria) and related consequences (e.g., losses).
- DFTOP visualisation methods highlight the most important decision factors and their correlation.
- DFTOP visualisation of statistical results enables decision makers and their staffs to capture and understand statistically derived results easily and quickly.
- DFTOP results and visualisation methods provide efficient arguments for decisions.
- DFTOP is an integrated tool combining several functionalities for decision support such as statistical analysis, success criteria definition, and visualisation.
- DFTOP provides reusable statistical workflows to non-statistical experts and the possibility adaptable to nearly any Data Farming result set to find outliers, evaluate risks and find possible and plausible outcomes.

4.4 DFTOP CONCEPT

In this section we present the DFTOP concept and how it is supporting the COPD planning process. The functional and technical requirements for DFTOP are defined using the results of the previous section. From these requirements we develop conceptual methods to address the tasks supported by DFTOP.

4.4.1 Introduction

As shown in Section 4.3, DFTOP supports the NATO COPD in the process of COA Development. DFTOP is intended as a tool for operational analysts supporting the JOPG Head and the commander, afterwards called decision maker. The operational analyst prepares analysis modules, interaction possibilities and visualisation modules based on the raw simulation output. The decision maker, on the other hand, is only confronted with visualisations and limited user interaction possibilities, and is completely detached from the raw data.

As shown in Figure 4-4, DFTOP integrates into the data farming loop of loops by supporting the analysis and visualisation step. It takes the output data of the high performance computing and either terminates the data farming loop, encourages additional analysis of specific scenarios, or shows the necessity to refine the DoE.

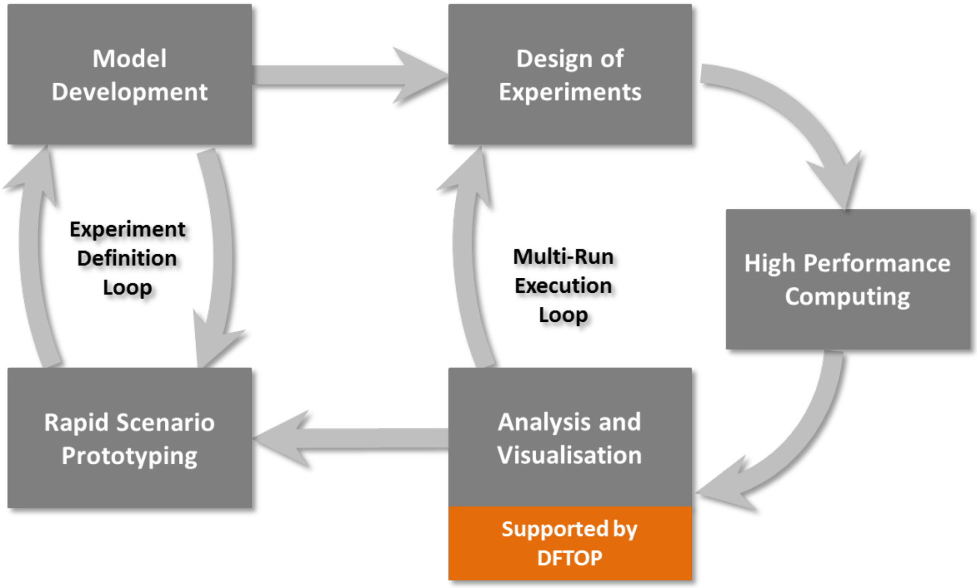

Model Development
Design of Experiments
Experiment Definition Loop
Multi-Run Execution Loop
High Performance Computing
Rapid Scenario Prototyping
Analysis and Visualisation
Supported by DFTOP

Figure 4-4: Integration of DFTOP into the Data Farming Loop.

4.4.2 Requirements

The requirements derived from operation planning define the concept of DFTOP. These are separated into two categories: functional and technical requirements.

4.4.2.1 Functional Requirements

The functionality, processes and structures of DFTOP have to be designed to efficiently support the work of the operational analyst and the decision maker. Both roles have different objectives in the planning process and need to be supported in different ways.

In general it can be assumed, that the decision maker is not a SME in statistics or data farming. Using DFTOP the decision maker wants to make sound decisions, which are backed by simulation and statistical methods. He has a set of questions formulated into objective functions (or more generally into MOE) by the analyst. The sensitivity of the MOE to certain changes in the COA needs to be evaluated to analyse the risk. This is presented to the decision maker by problem oriented visualisations. To evaluate the effect of changes in the COA, changing it must be simple. In addition, the effects of the changes must be instantly visible in order to support easy comparison.

4.4.2.2 Technical Requirements

To facilitate a long life cycle of DFTOP as a software system it has to be designed to support maintenance, expandability and customization. The presented workflows of DFTOP are based on one specific Data Farming experiment. Thus, the analysis, visualisation and interaction methods created are only a subset of all necessary methods to support the COPD planning process in general. To work as an integration tool, connecting different statistics or visualisation applications, DFTOP needs to have a long lifecycle and be open to extensions in its functional range. This was achieved by designing DFTOP as a modular system and using open and standard interfaces.

4.4.3 Functional Solution

The main idea in supporting the operational analyst is to offer the possibility to create and store standard workflows. Once defined, they can be reused in later decision making projects, independent of the data analysed. The idea of reusable workflows is based on the observation that different data farming experiments are analysed with the same statistical methods. If a single statistical method is not sufficient, the process of using several methods sequentially is also similarly reoccurring. Since the same statistical methods are used, the results have the same form and the same visualisation methods can be used. By providing a limited set of analysis and visualisation methods, the work of the analyst can be simplified and streamlined. In addition, the quality of the results will be consistent quality.

As shown in Figure 4-5 the question will come out of the previous COPD process step of the mission analysis which is a factual interpretation of the commander's intent and his guidance to tackle a certain operational problem. The analysis will break down these questions to different aspects and deliver answers based on hard facts in the COA-development which will afterwards lead to a decision of the commander.

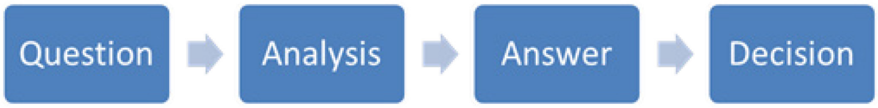


Figure 4-5: Decision Support Process.

DFTOP supports analysis and provides answers in a structured and comprehensive way (Figure 4-6). Data Farming is used to adapt questions in suitable models and simulate different outcomes in order to answer specific questions. In addition, it widens the point of view and presents different options and possibilities.

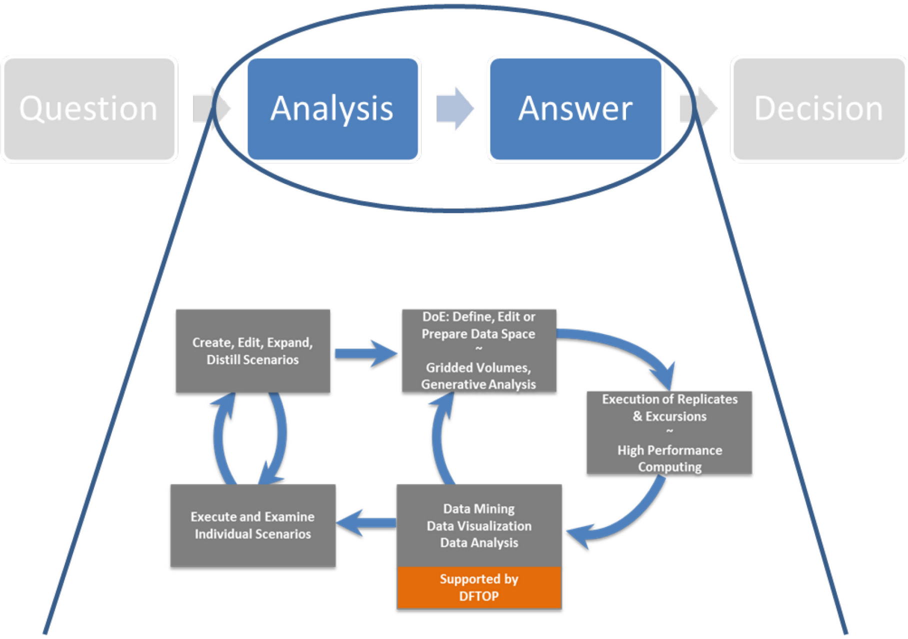

Question
Analysis
Answer
Decision
Create, Edit, Expand, Distill Scenarios
DoE: Define, Edit or Prepare Data Space ~ Gridded Volumes, Generative Analysis
Execution of Replicates & Excursions ~ High Performance Computing
Data Mining Data Visualization Data Analysis
Supported by DFTOP
Execute and Examine Individual Scenarios

Figure 4-6: DFTOP Integration into the Decision Support Process.

There are three ways of interacting with DFTOP. Data can be analysed, results of the analysis can be visualized, and the analysis can be influenced by the user. These ways of interacting are capsuled into workflow modules which provide a specific functionality and fixed in- and output channels (Figure 4-7).

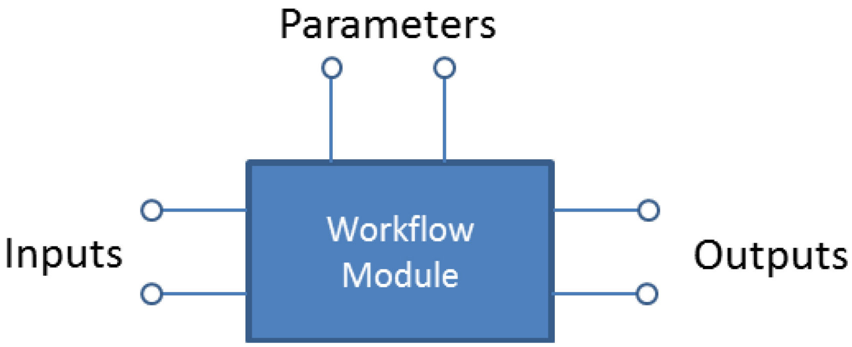


Figure 4-7: Workflow Module.

In addition each workflow module can be parameterised to adapt its algorithm to the input, or to define a specific output format.

The introduced workflows are now defined as specific ways of analysing and visualizing data using a chain of connected workflow modules. A simple example is shown in Figure 4-8.

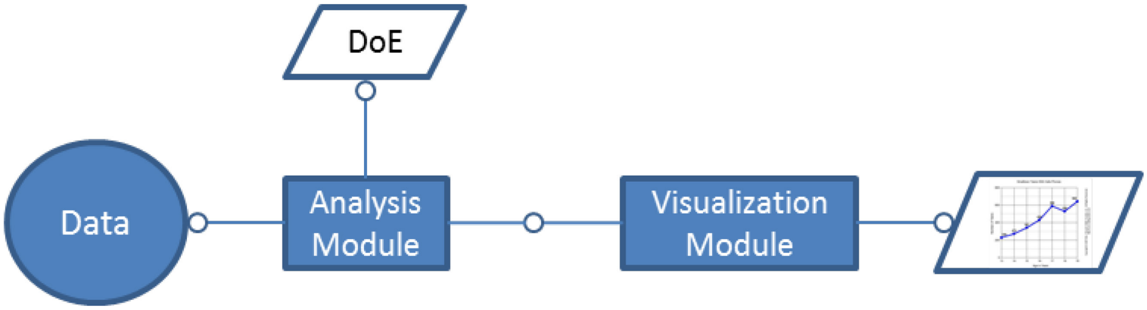


Figure 4-8: Simple Workflow Concept.

In the figure, the data is used as input to the analysis module. This Analysis module is parameterised by the DOE. After analysing the data the result is handed over to the visualisation module. The final output of the module is a visualisation that provides input to the decision support process.

An additional way of influencing the analysis is depicted in Figure 4-9. The interaction/visualisation module is a two-way-interaction module. This allows the user to show results of the analysis and interact with the result itself by filtering and scaling, etc. This interaction creates a subset of the data. If more extensive adaptions are necessary the whole workflow has to be rerun with adjusted parameters.

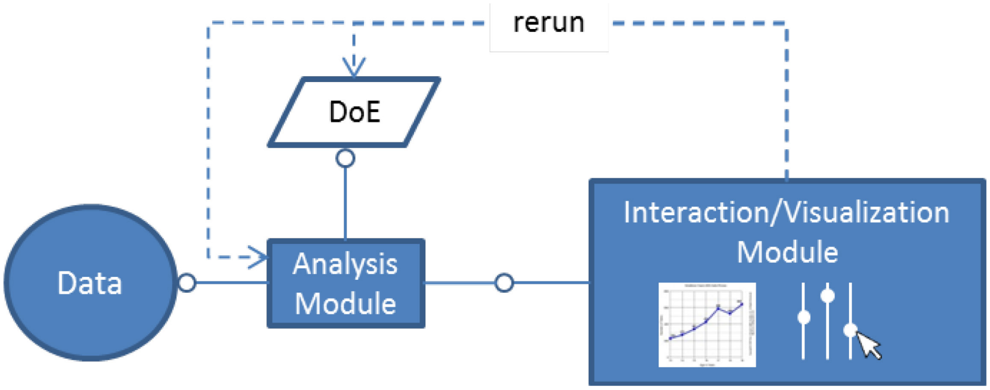


Figure 4-9: Workflow Concept with Interaction Module.

More elaborated workflows are possible, as long as the standardized input and output channels of the included modules match. Workflows can be defined once and adapted to any data source using the parameterisation. Thus, it is possible to reuse workflows in another planning cycle without big effort.

4.4.3.1 Role Scheme

Since the process of COA development is a cooperative process of different analysis steps, there are also different target audiences, which are using DFTOP.

In general we distinguish between three roles:

1) Data Technician:

   The data technician is responsible for preparing data for DFTOP. DFTOP is aligned with the realms in the Data Farming methodology and parameters and MOE has to be structured accordingly. This structuring is a required pre-processing step before the data can be used in the further analysis.

   Furthermore, the data technician is responsible for setting up the technical structure of the workflows in DFTOP. In agreement with the data analyst in charge, he incorporates new workflow modules and connects the input and output channels.

2) Data Analyst:

   The data analyst is responsible for correlating the initial questions with the analysis and visualisation methods. Therefore, he may use existing workflows or create additional ones.

   The data analyst is also responsible for the correctness of the analysis results and the adaption of the workflows to the specific COA development questions. This is done by parameterising all necessary workflow modules accordingly. In addition he will decide which visualisation is best depending on the intended target audience.

3) Decision Maker:

   The decision maker will never interact directly with DFTOP. The results of DFTOP will be presented to him by a data analyst. He will have indirect influence on DFTOP by rephrasing his initial questions, guidance, and important factors (i.e., parameters). This information is adopted by the data analyst to interact with DFTOP in the interaction/visualisation module or by re-running some workflows.

Using DFTOP the main objective of the decision maker is to draw operational conclusions from the results. In addition he may adjust basic setting of the analysis if necessary.

For all of the roles mentioned above, specific workflows with different functionalities are needed as shown in Figure 4-10.

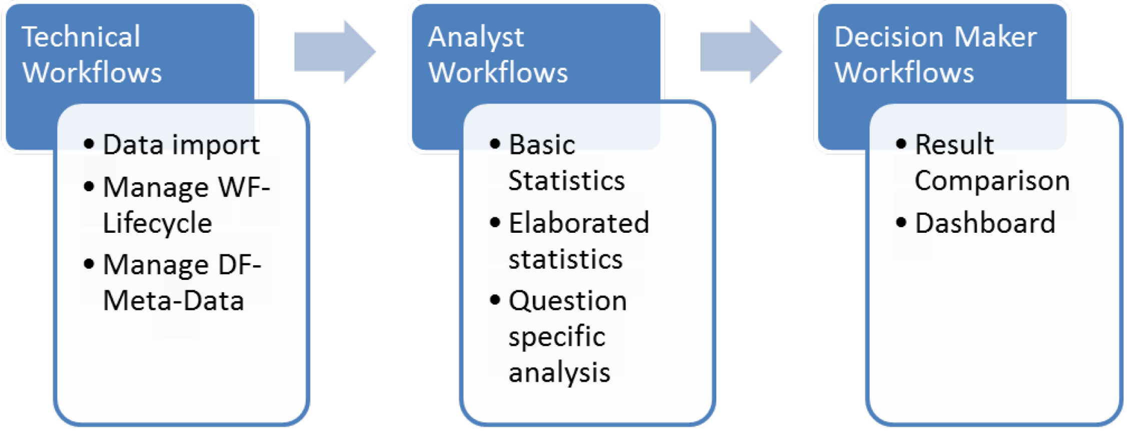


Figure 4-10: Role-Specific Workflows.

The data technician will need workflows to import the data into DFTOP and a specific expert view to manage the workflow lifecycle of creating, adjusting and deleting entire workflows or single workflow modules.

According to the COA Development process, the analyst will first get some rough insights into the data by looking at factors of importance and statistics. Accordingly, all workflows are simple to construct and well suited for reuse.

Working in an interactive manner, the analyst will take initial results and use more specialized workflows to gain further insight into the data. At the end of the process, the data analyst will present the results of the decision maker workflows to the decision maker. These decision maker workflows summarize the results of several statistical workflows and present an overview on a virtual dashboard. Additionally, interaction functionality is available to show differences between several COA, and answer possible questions from decision maker.

4.4.4 Technical Solution

In this section the technical part of the concept is presented. It takes into account the functional and technical requirements as well as the functional solution.

4.4.4.1 The Domain Model

As a standard approach in software engineering for modular systems, a domain model (Figure 4-11) is used to fulfil the requirements.

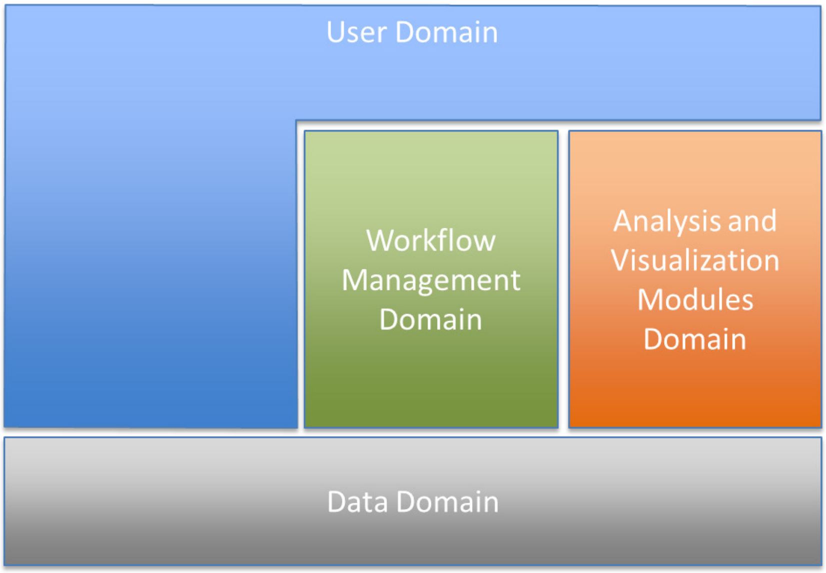
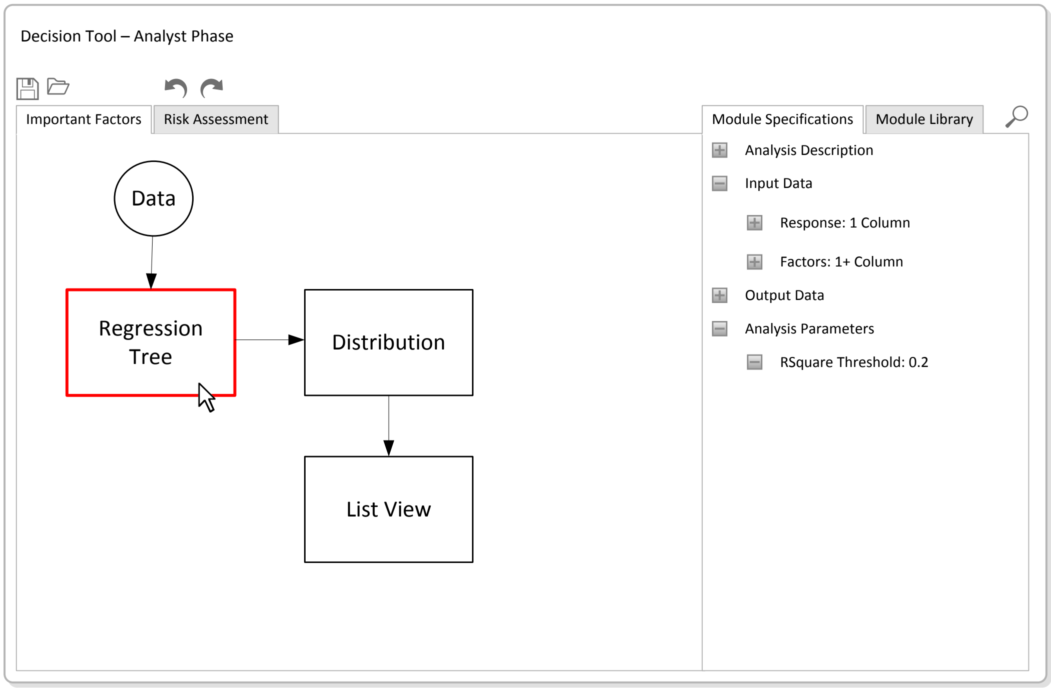

User Domain
Workflow Management Domain
Analysis and Visualization Modules Domain
Data Domain

Figure 4-11: DFTOP Domain Model.

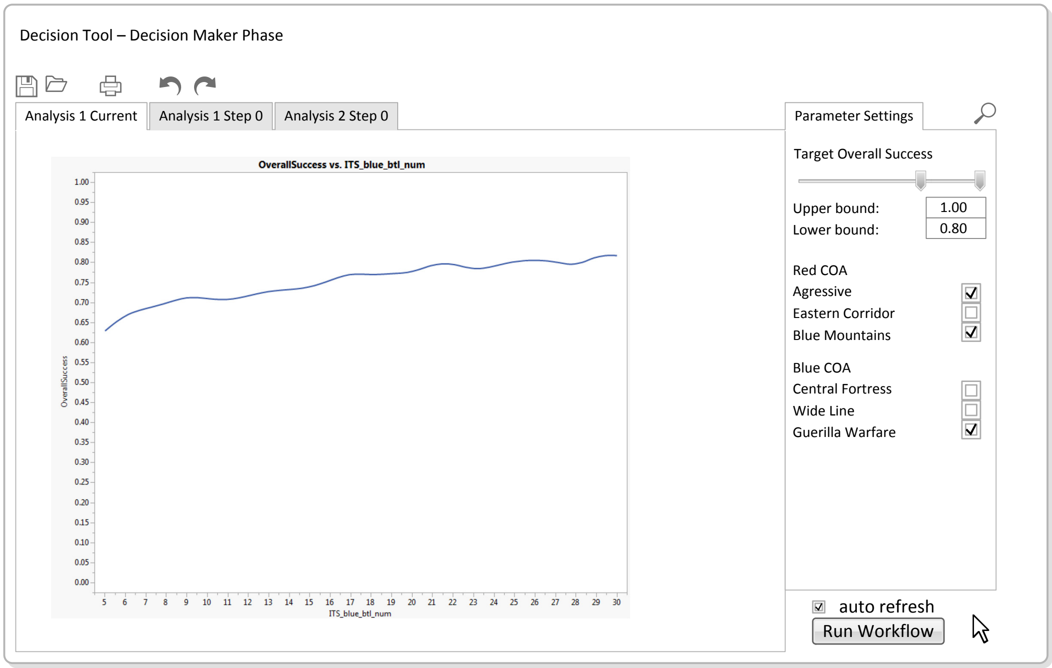
The main components of the user domain are two graphical user interfaces: one to create and modify workflows (target role: data technician) and one for workflow execution to enable visualisation and interaction (target role: data analyst and decision maker). Both GUIs feature simple and problem specific design and controls. The first GUI offers the possibility to connect and parameterise workflow modules to create workflows (Figure 4-12).


Decision Tool – Analyst Phase

- Analysis Description
- Input Data
  - Response: 1 Column
  - Factors: 1+ Column
- Output Data
- Analysis Parameters
  - RSquare Threshold: 0.2

Figure 4-12: Data Technician GUI.

The second GUI offers the possibility to choose and execute workflows and go through tabs with diagrams created by visualisation modules, some of these have interactive applications like sliders and checkboxes (Figure 4-13).



Upper bound: 1.00
Lower bound: 0.80

Red COA
Agressive ☑
Eastern Corridor □
Blue Mountains ☑

Blue COA
Central Fortress □
Wide Line □
Guerilla Warfare ☑

☑ auto refresh

Figure 4-13: Analyst and Decision Maker GUI.

The workflow management domain performs loading, saving, execution, visualisation, and interaction of workflows. In addition to orchestrate the module execution order of analysis and visualisation, it also manages the data exchange between modules.

The analysis and visualisation domain consists of two libraries, one for analysis modules and one for visualisation modules. Analysis modules perform mathematical, statistical or logical operations on data. Input and output data are both in tabular form. Visualisation modules create diagrams, histograms, etc., reading data in tabular form. Each module in this domain is an active input-output system; when input data is executed an output is automatically created. The input and output tables are both loaded and saved from and to the data domain. Examples of analysis modules are standard statistical methods like partition trees, calculation of distribution parameters, and response surface generation. There can also be tailored methods, like “List of the most important factors of success”. Visualisation modules are for instance *x*-*y*-diagrams or histograms. The modules can be run by external applications like COTS statistics tools, scientific computation tools, business intelligence tools, etc. Some of these tools provide both analysis and visualisation.

The data domain consists of one database with several different tables. The main table consist of the simulation data. Other tables contain metadata[1] or intermediate data from workflow execution. The simulation data consists of decision and noise factors of the DOE and of MOE. This data is organized in a single table where each

[1] The metadata contains descriptions of factors like names and classification into decision or noise factors.

column corresponds to a factor or MOE, and each row represents a single simulation run. DFTOP uses an import workflow to convert raw data from the simulation runs and calculate MOE before putting them into the database.

4.4.4.2 Workflow Definition

The conceptual basis of workflows was laid out in Section 4.4.3. A more detailed view on the technical definition of a workflow document is presented in this section.

The workflow document is written using Extensible Markup Language (XML) and contains the following elements:

- Description of the workflow; how it works, what questions can be answered, how the results are to be interpreted, etc.
- Connection information to the database; its address, table names, login data, etc.
- Network of analysis and visualisation modules, where each module defines:
  - Interfaces to external applications;
  - List of parameters and their values;
  - Columns and tables to load from the database;
  - List of filters, in case only a subset of the available data should be loaded;
  - Storage location for results; and
  - Predecessor or successor modules in the network.
- List of interaction modules and their links to parameters or filters.

4.4.4.3 Interfaces

The domains are connected as follows (Figure 4-14):

- As the user domain is used to start workflows it is connected to the workflow management domain. Visualisations are presented in the main GUI, thus there is a connection to the analysis and visualisation modules domain. In order to display metadata or create workflows data is loaded from the data domain.
- The workflow management domain is the central control component and is connected to the user domain, and to the analysis and visualisation modules domain.
- The analysis and visualisations modules domain is connected to the data domain to access data.

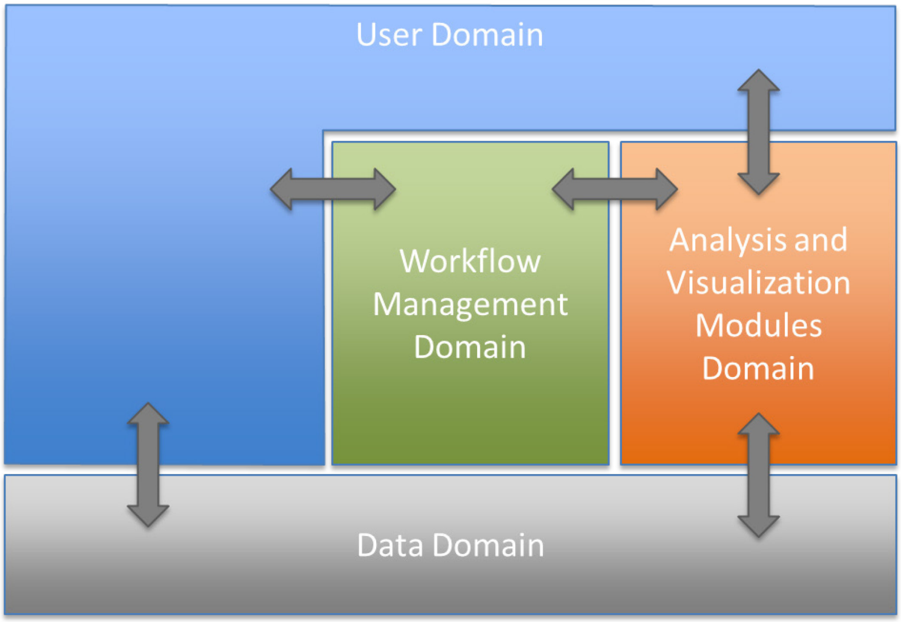

User Domain
Workflow Management Domain
Analysis and Visualization Modules Domain
Data Domain

Figure 4-14: Domain Model with Interfaces.

As all four domains are encapsulated exchangeable modules, using an open and standardized messaging system for interconnection is important. For this reason XML is chosen; it is a widely known format with standard libraries for encoding, and it is human readable. These messages are used to connect all domains except the data domain, where SQL is used. DFTOP provides an integration library which translates the XML messages to application specific commands.

4.4.5 Analysis and Visualisation: Highlighted Features

Most of the analysis and visualisation methods are straight forward and basic techniques. Nevertheless, some features stand out of the standard way of thinking and are specially developed to support decision planning, these will be described in more detail in this chapter.

4.4.5.1 Multi-Criteria Objective Function

Normally the decision maker will base his decision on more than one criterion. In operations many different aspects of the operational environment have to be taken in account. For example, one should not only minimize the number of own losses but also the duration of the operation, in addition the number of reached operational objectives should be maximized. Such MOE each have different importance. In an overall objective function used for decision making they therefore receive different weights.

This leads to a multi-criteria objective function which is set up by different MOE derived from the commander's intent and the prior mission analysis phase. The setup of this objective function is summarized in one workflow by selecting desired MOE and subsequent computing of the corresponding weights and calculation of the *overall success* value for each simulation run. This *overall success* is the only MOE created in DFTOP itself and treated as such in all other workflows. The overall success is automatically calculated based on priorities, but may also be manually adjusted in a pure interaction workflow module implemented in DFTOP.

4.4.5.2 Geo-Referenced Analysis

The geography of the area of operation is essential for military operations. Overlaying analysis results on a map is therefore important for evaluation performed by decision makers. Appropriate mathematical graphs and figures are presented with geo-reference to the operational environment of the COA Development.

As a further development, the graphical representation of a proposed COA (operation plan), should be incorporated into existing NATO planning tools.

4.4.5.3 Dashboard

The main results from the COA Development are presented to the commander in a decision brief. In order to support this brief, a special workflow incorporates the most important analysis results into one visualisation interface.

The workflow is used to summarise essential information into a single overview interface. This workflow demonstrates the possibility to merge a whole set of analysis modules into one single visualisation (Figure 4-15).

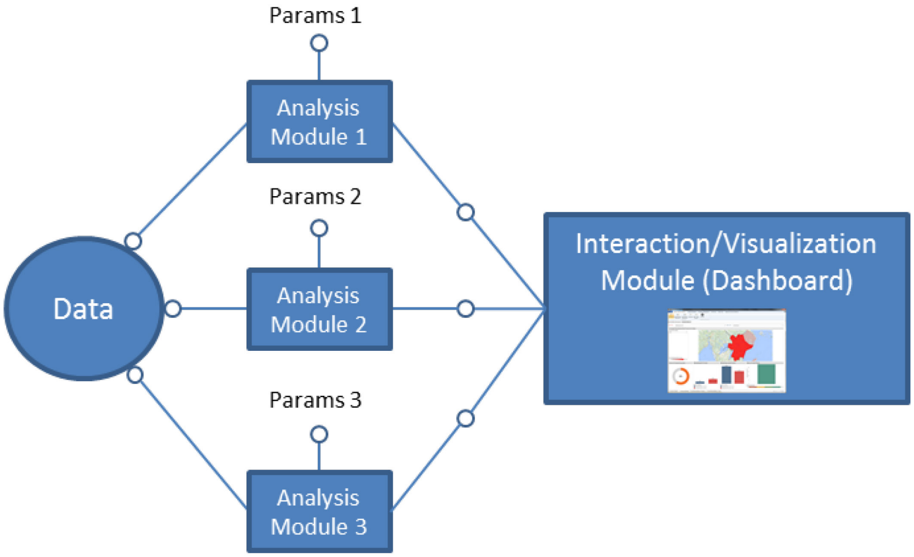


Figure 4-15: Dashboard Principle.

4.5 PROOF OF CONCEPT: DF EXPERIMENT

To demonstrate the benefit of Data Farming for actionable decision support in operation planning a large symmetrical warfare scenario is used. The scenario is presented in detail in this section. The first two phases of the scenario feature detailed inter-platform interactions. Therefore a single entity simulation tool was chosen; PAXSEM developed by Airbus Defence and Space. The third phase includes a larger number of entities, and is simulated by an aggregated planning and simulation tool; ITSimBw developed by Fraunhofer IAIS. Using two different simulation tools and models of different resolution requires the elaborate coupling of both tools to generate a coherent simulation state and output data. This section presents how the coupling is realized using standardized interfaces and how this approach is used for a large-scale Data Farming experiment.

4.5.1 The Bogaland Scenario

The scenario was provided by the Swedish Defence Research Agency (FOI) and is a derivative of the Bogaland scenario that depicts a large-scale conventional military operation. In the scenario, the operation is separated into three different phases: airstrike, entry and land attack phase. The airstrike and entry phases consist mainly of air-to-air and air-to-ground engagements. The subsequent land attack phase consists of brigade level engagements supported by airborne units.

Bogaland is a virtual country geographically located in the southeast of Sweden. It is threatened by occupation from its northern neighbour Northland (Figure 4-16). This operation is planned to take place in three phases. It is important for Northland to deny NATO allied forces in Bogaland (BFOR) involvement in this conflict.

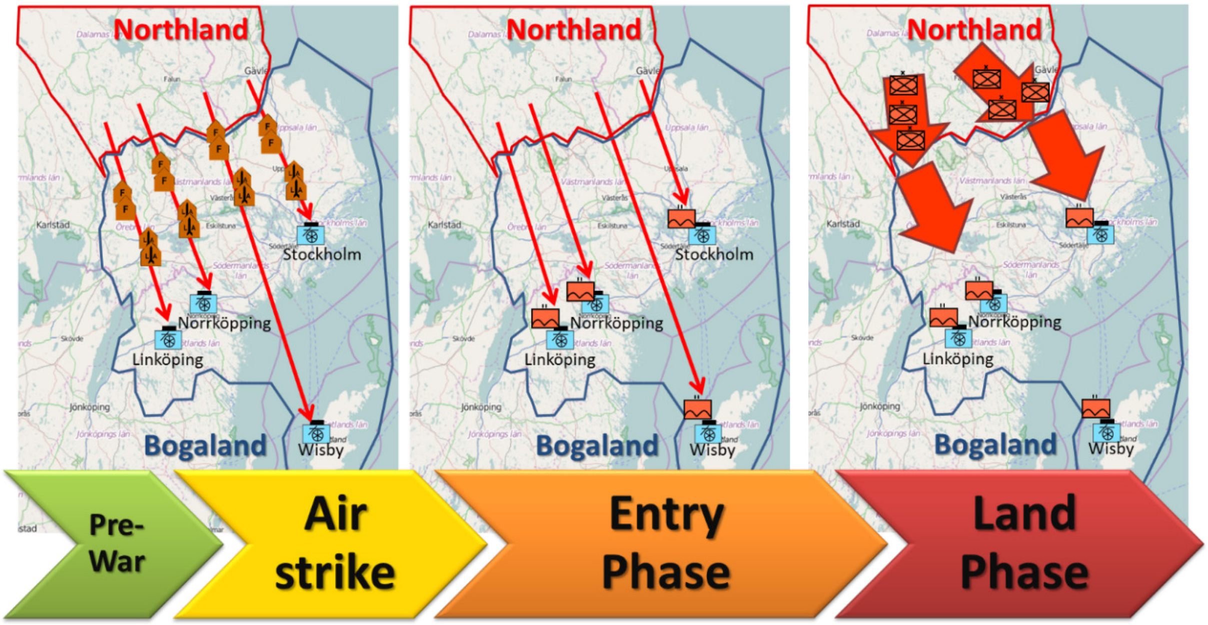


Figure 4-16: Bogaland Scenario Overview.

Bogaland defence plans are based on the support of coalition forces. Therefore, the operational objective of Bogaland's armed forces in the first phase of a Northland attack is to delay Northland's advance in order to gain time for BFOR deployment.

After a pre-war activity, the offensive starts with an airstrike phase (see Figure 4-16 left). Northland air forces conduct primarily an offensive counter-air operation in order to gain air superiority. Northland forces attack with cruise missiles, multi-role fighters and bombers against Bogaland's forces, air defence units and airbase infrastructure. The simulation of the operation terminates before the arrival of BFOR.

Bogaland's air force deploys multi-role fighters in combat air patrols or as intercept fighters. Air defence units are deployed in order to provide area defence to Bogaland's four airbases. In addition, after a short response delay, BFOR deploys fighter aircraft to reinforce Bogaland's air force defensive air operations.

The entry phase of Northland's airborne forces starts when the air defence units on Bogaland's airbases are destroyed and the runways are still operable. Airborne infantry forces are deployed using transport planes during the entry phase to seize Bogaland's four airbases (Figure 4-16 centre). This is done in order to deny their use by BFOR and to establish bridgeheads in support of the subsequent land attack phase.

After the entry phase, the land attack phase is initiated by Northland (Figure 4-16 right). Land units consisting of up to 40 armoured, mechanized infantry, and artillery battalions attack their operational target areas and are supported by the air forces that survived the airstrike phase. Northland has several optional strategies for their ground assault with varying size of the attacking force for each target area. Bogaland also has several optional strategies for how to deploy their defence forces.

4.5.2 Main Study Question

The main question to be answered by this study is:

> *"How can we in Bogaland best use what we have to defend the territory (including NATO allied forces)?"*

The goal of the study is to provide decision support for building robust COA that enables Bogaland to resist attacks from Northland. The commander's priorities are to hold important infrastructure and areas of Bogaland. Important aspects are to delay the beginning of the land phase and set good conditions for subsequent phases. It is investigated which unit types, quantities, equipment, and Tactics, Techniques, and Procedures (TTPs) are most robust against Northland's most likely and most dangerous COA.

4.5.3 Scenario Realization with PAXSEM and ITSimBw

The two simulation systems used to model the operations is described in this section. The realization of the Bogaland scenario then follows in Sections 4.5.4 and 4.5.5.

4.5.3.1 Introduction to PAXSEM

The agent-based simulation framework PAXSEM has been developed by Airbus Defence and Space on behalf of the German Armed Forces since 2008. Its main areas of application are simulation-based military analyses in Concept, Development and Experimentation (CD&E) experiments and the support to foreign missions as well as to national procurement activities.

Its high resolution 3D visualisation allows the simulation of technical-tactical scenarios and plots. Within these, military units are represented as agents in a resolution ranging from single entity to enforced company level. PAXSEM enables a detailed, physically based representation of technical systems equipped with sensors (e.g., optical/infrared/radar) and effectors (e.g., small armed fire/artillery/ rockets/guided missiles). These agents independently execute activities, perceive their environment (sensors), intervene therein (effectors) and react upon the changes in the respective ambience (dynamics). This allows multiple differential decision alternatives to be created, describing a wide sample space. The mutual interference of individual agents allows simulation of complex systems that are often impossible to predict and uniquely confined by the agents abilities [9]. Hence, valuable insights can be generated regarding the operational employment, e.g., defined TTPs of systems in use, systems under development or systems that do not yet exist at all.

4.5.3.2 Introduction to ITSimBw

ITSimBw is a long-term project of the German Armed Forces and the Fraunhofer Institute for Intelligent Analysis and Information Systems. It began as a multi-agent simulation system [10], [11], but over time focus shifted to planning and macro-simulation of military applications and operations. In several studies, interfaces to PAXSEM using Battle Management Language (BML) [12] and Military Scenario Definition Language (MSDL) [13] for interoperability on multiple resolution levels have been developed and refined. Alongside MSG-088 [14], a Data Farming framework for the German Armed Forces and a planning and macro-simulation method of ITSimBw was developed. For MSG-124 the planning and macro-simulation method was refined and extended to cope with more complex scenarios, lower levels of resolution and hierarchical command and control.

4.5.3.3 Assignment of Operation Phases to Simulation Models

PAXSEM is well suited to simulate the airstrike and entry phase, since the details of flight movement and guided missile behaviour play an important role in combat, and simulation accuracy on single entity level is crucial. The number of air combat and air defence units depicted is no more than a few hundred, which results in a manageable simulation runtime.

As the land phase consists of up to 65 land battalions, corresponding to several thousand single entities, it has to be simulated on an aggregated level. This number of entities would exceed the manageable complexity of the current version of the PAXSEM model. In ITSimBw it is possible to plan and simulate military operations with hundreds of battalions. It uses aggregated attrition models to calculate unit interaction as well as simplified movement and tactics. Thus simulation runtimes are achievable that are fractions of those of PAXSEM in this scenario. The realization of the scenario in PAXSEM and ITSimBw will be introduced in the next two sections.

4.5.4 Realization of the Airstrike and Entry Phase in PAXSEM

For a comprehensive representation of its simulated environment, PAXSEM simulates all scenarios on a 3D terrain. For the Bogaland scenario, a 400 x 800 km terrain database is generated that covers the entire country as well as the southern part of Northland where the airstrike and entry phase is initiated (Figure 4-17 left). The 3D terrain is mainly used for movement planning, intervisibility between entities, weapon trajectory, and impact computation.

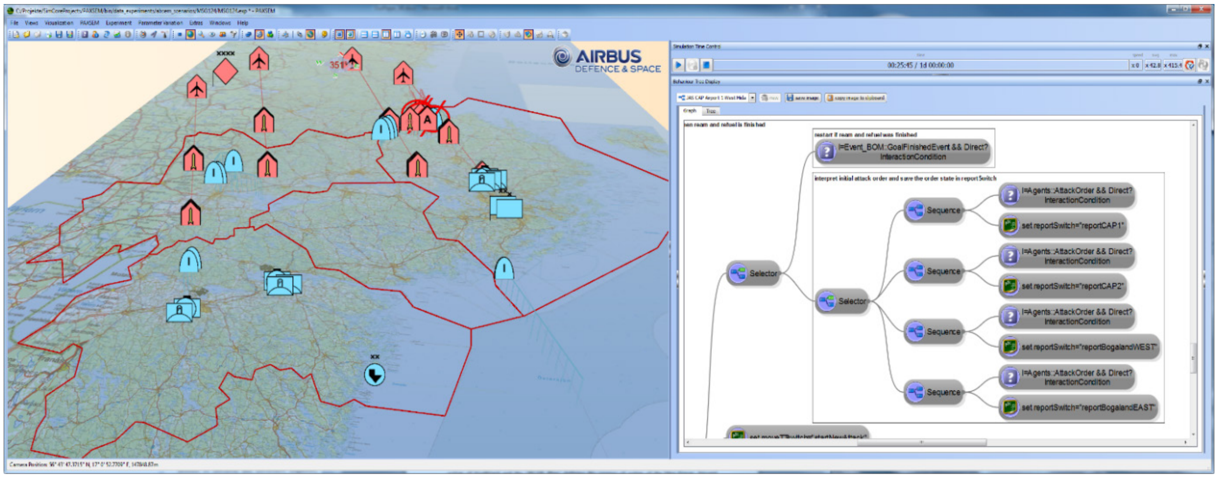

AIRBUS
DEFENCE & SPACE
Simulation Time Control
00:25:45 / 1d 00:00:00
x 0
x 42.8
x 415.4
Behaviour Tree Display
save image
copy image to clipboard
Graph
Tree
restart if ream and refuel was finished
!=Event_BOM::GoalFinishedEvent && Direct? InteractionCondition
interpret initial attack order and save the order state in reportSwitch
Selector
Selector
Sequence
!=Agents::AttackOrder && Direct? InteractionCondition
set reportSwitch="reportCAP1"
Sequence
!=Agents::AttackOrder && Direct? InteractionCondition
set reportSwitch="reportCAP2"
Sequence
!=Agents::AttackOrder && Direct? InteractionCondition
set reportSwitch="reportBogalandWEST"
Sequence
!=Agents::AttackOrder && Direct? InteractionCondition
set reportSwitch="reportBogalandEAST"

Figure 4-17: Airstrike Phase and Behaviour Tree in PAXSEM.

All entities (e.g., JAS Gripen or F-18 aircraft) are configured with their tactical symbols and 3D models as well as their technical parameters, such as maximum speed and flight level in specific mission situations. In addition, sensor and weapon systems of all entities are configured to include their hit and kill probabilities. Unclassified weapons data was mainly provided by the Swedish Defence Research Agency (FOI).

The agent behaviour is defined through a flexible set of rules using behaviour tree methodology (Figure 4-17 right). These rules are visualised in graphs that supports definition monitoring and tracking of agents' behaviour. In addition to basic tasks such as move or attack, a behaviour tree usually consists of additional control nodes like sequences, selections, conditions, loops, etc. An arbitrary set of behavioural rules can be implemented for each agent. They are activated once a relevant condition delivers a trigger thereto. These triggers can be specific sensor information, presence of entities in crucial areas, weapon threats, ammunition engagements, etc.

As an example, a JAS Gripen fighter has the behaviour to start engaging hostile air targets based on a predefined target prioritization, and has to land as soon as it runs out of ammunition or fuel. In case its own airbase is destroyed, the fighter will land on the closest alternative airbase. During the entry phase, each airborne battalion is divided into 20 platoons. These are each transported by one transport aircraft that are escorted by fighters.

4.5.5 Realization of the Land Phase in ITSimBw

The simulation environment of ITSimBw consists of two separate modules: planner and simulation. They interact using BML and MSDL. Using these standardized interfaces it is possible to connect the planner module to other simulation models, e.g., models of different scope, level of abstraction.

The planner is based on the methodology of Capability Based Planning and uses a hierarchical mind-map-like modelling methodology. This model consists of the used capabilities, available resources, resource hierarchy, and geographical locations.

The main part of the model is the operation plan (Figure 4-18 right).

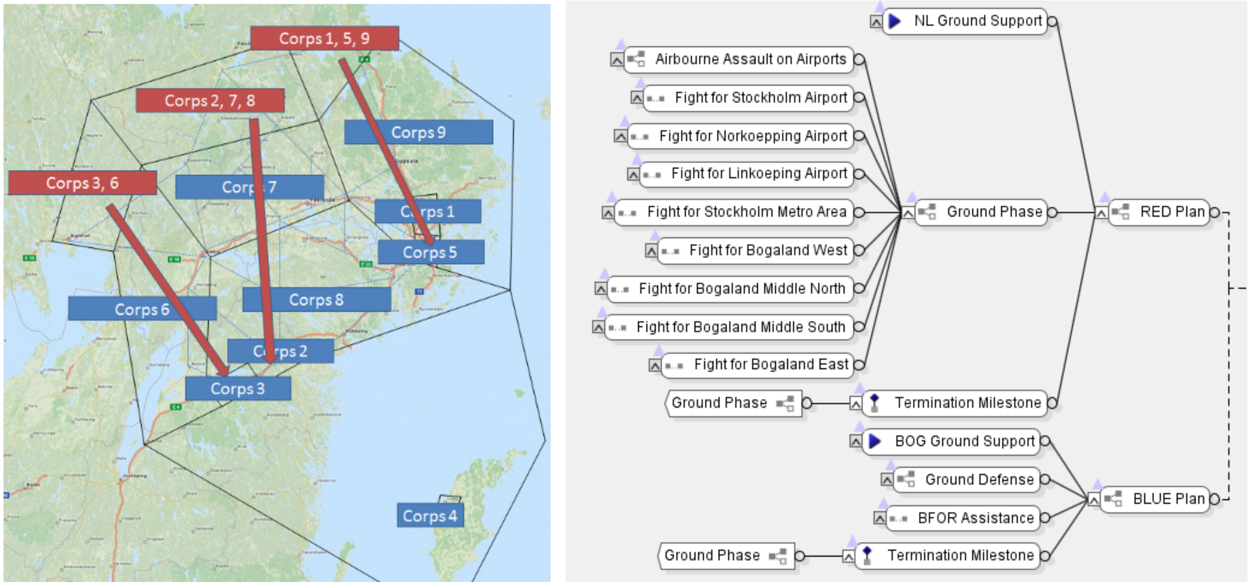


Figure 4-18: Operation Chart of the Plan and Plan Visualisation.

The plan describes how capabilities are used to disable resources of opposing forces and thereby remove enemy capabilities. The capabilities include *Air Support*, *Defend Area*, *Attack Opposing Resources in Area*, among others. Each capability needs certain types of resources to be executable. The plan defines which specific unit resources which are necessary to execute the capability.

The plans for the Bogaland scenario are shown to the right in Figure 4-18. The Red plan defines the COA of Northland, and the Blue plan defines the COA of the Bogaland coalition. Several different kinds of elements are used in these plans; the three most important elements being step (triangle, actual capability use), sequence (two squares, sequential execution of sub-elements) and parallel execution (three squares, parallel execution of sub-elements).

During simulation the plans are analysed iteratively by the planner. At every iteration, it is evaluated whether or not each step can be executed. For instance, they are executed if the required resources are available (i.e., not destroyed and not used in another step) and if the objective of the step is still unachieved. After every plan evaluation iteration, the executable steps are transmitted to the macro simulation in form of BML orders. The simulation calculates resource movement using an abstract road network, point-shaped resources, and resource attrition using an adapted Correlation of Forces [15] model. Simulation of resources continues until one or more orders are fulfilled or failed. At this point the state of the resources in the simulation is transmitted back to the planner, which then starts a new planning iteration. The initial resource state is transmitted from the planner to the simulation using MSDL.

An aggregated visualisation of the plan is provided in Figure 4-18 left. Bogaland is divided into nine areas and Northland into three. The forces of both countries are organized into corps; each corps consists of a variable number of either armoured, mechanized infantry, or artillery battalions. These battalions are dynamically generated prior to the execution of the plan according to the DOE. Each corps of Bogaland is tasked to defend one area, and each corps of Northland is assigned to attack one area of Bogaland. Depending on the assignment of battalions to different corps, a large set of possibilities are simulated.

4.5.6 Methods of Interoperation

To allow handover of the scenario after the entry phase, the simulation state of PAXSEM is transferred to ITSimBw. Since PAXSEM is an entity-based simulation its state is composed of the state of its entities. ITSimBw models the units on an aggregated level (i.e., battalion and squadron), which requires that PAXSEM entities have to be mapped to units in ITSimBw. Most entities are used in either the air and entry phase or in the land phase. This applies to air defence units (Patriots), radars, bombers, transport planes, and cruise missiles (PAXSEM), and armoured, mechanized, and artillery battalions (ITSimBw). The entities that need to be mapped are fighters and airborne battalions.

After the land phase is finished another interaction process is needed to create a collection of consistent output data. In the next sections the mapping of the simulation state and the collection of the output data are described.

4.5.6.1 Mapping of the Simulation State

PAXSEM writes the state of all entities into a MSDL file. The location of this file is defined in the DOE-file, a common XML document, which both PAXSEM and ITSimBw use to create their entities and units. ITSimBw then uses the MSDL file for initialization.

PAXSEM uses the MSDL object *EquipmentItem* to store its entities and *ScenarioTime* to store the time. The time can easily be parsed by ITSimBw, since it conforms to ISO 8601. To identify the relevant fighters and airborne units, the *SymbolIdentifier* of all equipment items is used. If the symbol identifier contains the sub-string *MFA* (fixed wing attack) or *MFFI* (fixed wing interceptor) it is a fighter according to the Common Warfighting Symbology (MIL-STD-2525C). The list of fighters is then partitioned into Red or Blue fighters. The *ForceOwnerHandle* of the equipment items is used for this partitioning by comparing it to the *ObjectHandle* of the global object *ForceSides.* The type of fighters is not modelled in ITSimBw, only the amount is relevant. The fighters for both sides are organized into one squadron each, and placed on a randomly chosen operational airport. Since the time advance model in ITSimBw is much coarser and the area of operation is rather small in relation to the fighter speed the position of the fighters are disregarded and the fighters are considered ready for operation.

The airborne platoons are identified by the sub-string *EWR*, i.e., a weapon (MIL-STD-2525C). Since the success of transportation can only be identified by evaluating the position of the platoon. The set of platoons is split into sets that are each placed close to the four separate airports, and one remainder (which is not near any of the airports). The split is performed by comparing the *Location* of the platoon with the position of each airport. If the distance is less than 5 km, it is considered successfully transported. All other platoons were either never transported or the transport plane was shot down during flight. For each airport, airborne battalions are created by defining 20 platoons as a fully operational airborne battalion. If there are less than 20 platoons or there is a remainder, a partly operational battalion is created. The position of the battalion is set as the position of the airport.

4.5.6.2 Collecting the Model Outputs

All model outputs of PAXSEM are written into a Comma Separated Values (CSV) file. The file starts with a header line, describing all simulation output columns, and continues with one line of model outputs. The outputs describe the simulation state either at a predefined simulation time, an event, or the end of the simulation run. Since there needs to be one coherent output file for the whole scenario, ITSimBw writes its simulation outputs to the same file. Therefore, the CSV filename is passed to ITSimBw to ensure that the same file is used. ITSimBw extends the header line in the CSV file with column descriptions of its additional simulation outputs and appends its values to the last line of the CSV file.

ITSimBw has an option to execute several simulation runs with varying input factors that are only relevant to the land phase (e.g., strategy combinations of red and blue). Therefore, the simulation output data of PAXSEM in the last line of the CSV file needs to be duplicated and appended by the simulation output of each ITSimBw simulation run. This approach ensures that the Data Farming environment can merge the results of all simulation runs into one single CSV file such that it can be easily analysed by using statistical tools like SAS JMP.

4.5.7 The Data Farming Experiment

This section outline the Data Farming experiment conducted to answer the main study question on how to defend Bogaland, by setting up the DOE and define all MOE.

4.5.7.1 Design Of Experiment (DOE)

According to the scenario, the following decision factors (definition of the Blue forces) and noise factors (definition of the Red forces) are listed in the following two tables.

Table 4-1: Decision Factors.

Decision Factor Name	Type	Range	Description
# F18	Integer	24 – 36	Number of F18 of BFOR
# JAS	Integer	24 – 48	Number of JAS of Bogaland
# JAS / CAP	Integer	2 – 6	Number of JAS per CAP (Combat Air Patrol)
# CAP	Integer	0 – 2	Number of CAP
# Patriot	Integer	4 – 12	Number of Patriot
# Battalions	Integer	15 – 25	Number of Battalion
NATO Arrival Time	Integer	2 – 10	Arrival time of BFOR F18 after operation start
Weapon Mix	Categorical	3	Short, medium or long range JAS weapons
Patriot Disposition	Categorical	3	One, two or no cluster of Patriots
Strategy	Categorical	4	Defence focus on areas : front, east, airports, all

Table 4-2: Noise Factors.

Noise Factor Name	Type	Range	Description
# Attack Packages	Integer	3 – 8	Number of attack packages (each containing 8 fighters + 2 bomber)
# Airborne	Integer	4 – 8	Number of airborne battalions
# Cruise Missile	Integer	24 – 48	Number of cruise missiles
# Battalions	Integer	24 – 40	Number of battalions
Strategy	Categorical	5	Attack focus on areas: front, east, airports, all

The decision and noise factors are crossed to ensure that each decision factor combination of Blue runs against each noise factor of Red.

A Nearly Orthogonal, Nearly Balanced (NONB) design [16] with 512 design points is used for all decision factors, except *Strategy*. The categorical variables *Weapon Mix* and *Patriot Disposition* are integrated into the NONB design, as the NONB handles categorical factors as well. For the noise factors a small fully gridded design is used in order to allow for individual filtering of each factor. This also allows varying the red factor values from a most likely COA to a most dangerous COA. To keep the number of design points within bounds, each noise factor except *Strategy* is varied by two levels only.

The already crossed NONB-fully gridded design is further augmented by crossing it with the categorical *Strategy* factors. There are 4 (Blue) * 5 (Red) = 20 combinations of strategy factors. The crossing of the strategies is chosen to allow for better analysis and for software architectural reasons. It is implemented by running the land phase 20 times per design point of the air and entry phase. This will not significantly increase the overall runtime since the simulation runtime of the air and entry phase is much larger than that of the land phase. The resulting number of design points, N_{DP}, of the whole DOE is:

$$N_{DP} = 512\ (decision\ factors) \cdot 16\ (noise\ factor\ design) \cdot 20\ (strategies\ design) = 163\,840 \qquad (1)$$

To keep the computation requirement within bounds, the number of simulation replications (simulations with different random seeds) is set to 5. Thus, the final number of simulation runs is 819 200 runs.

4.5.7.2 Measures Of Effectiveness (MOEs)

The development of the MOE is driven by the main study question and the commander's intent presented in Section 4.5.2. The commander's intent can be described by the following prioritized list:

1) Hold the Stockholm area;
2) Hold as many areas as possible;
3) Delay the start of the land phase;
4) Generate favourable conditions for future operations; and
5) Keep airports under control and with active Patriot systems.

Further, favourable conditions are assumed to be achieved by minimizing blue losses and maximizing red losses. The following table shows the MOE derived from the Commanders intent.

Table 4-3: Measures of Effectiveness.

MOE Name	Type	Range	Symbol	Description
Owner Stockholm	Binary	0,1	O_s	Owner of Stockholm: 0 = Red; 1 = Blue
# Blue Areas	Integer	[0,9]	A_B	Number of areas under Blue control
End-Time Entry Phase	Time	> = 0	T_{EE}	Time at the end of the entry phase. Its normalized counterpart in denoted by $\tilde{T}_{EE}$
Red and Blue Losses	Double	[0,1]	L_{RA},L_{RB}, L_{BA}, L_{BB}	Relative losses of aircraft and battalions on both sides
# Blue Airports with Active Patriot	Integer	[0,4]	A_{BAP}	Number of airports under Blue control with active Patriot system

For a multi-criteria analysis of the overall mission success the following objective function, Oms , is defined:

$$Oms = w_1\, O_S + w_2 \frac{A_B}{9} + w_3 \tilde{T}_{EE} - w_4 L_{BA} - w_5 L_{BB} + w_6 L_{RA} + w_7 L_{RB} + w_8 \frac{A_{BAP}}{4}, \qquad (2)$$

where $w_i, i \in [1,8]$ are normalized weights that sum up to 1. Each MOE also needs to be normalized. The normalization is done by using the theoretical maximum value, except for T_{EE}, which does not have a theoretical maximum. Here the maximum time over all available simulation runs is used to normalize. The weights are used to represent the priorities in the commander's intent. In order to optimize mission success the objective function has to be maximized.

4.5.7.3 High Performance Computing (HPC)

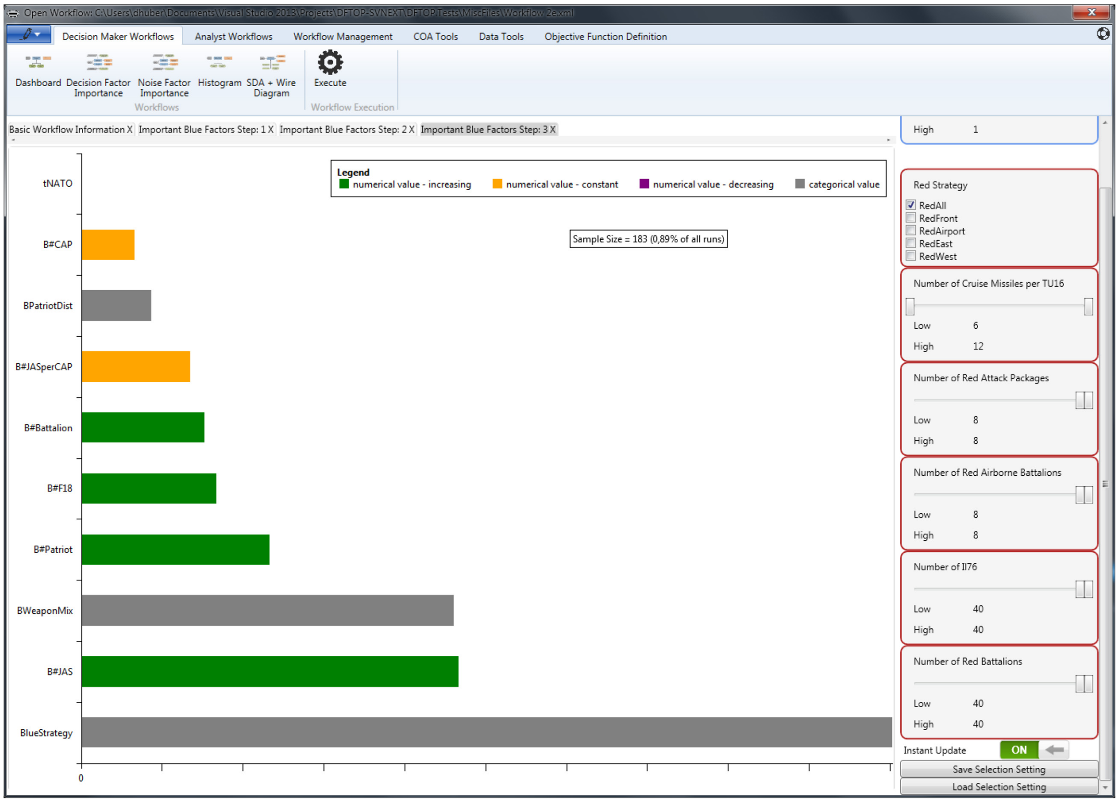
The German Armed Forces own several High Performance Computing (HPC) cluster systems. One cluster system containing 512 computer nodes which was used for this Data Farming experiment was hosted by Airbus Defence and Space in Unterschleißheim, Germany. A Data Farming software infrastructure with a web application to manage, monitor and conduct the Data Farming experiments on a PC cluster was used. The open-source software *HTCondor*, developed by the University of Wisconsin-Madison, was used as the job scheduler to distribute all simulation runs to the available computer nodes. After all Data Farming simulation runs were performed, the simulation output results were merged into a CSV file which could be downloaded through a web application. In addition, a software tool called *Data Farming GUI* was used to define the Data Farming input parameter variations and design of experiment in an easy and simulation model-independent way.

4.6 PROOF OF CONCEPT: DFTOP REALIZATION

In this section the prototype implementation of DFTOP is presented according to the concept presented in Section 4.4. The general layout of the DFTOP GUI is presented, followed by all workflows. These workflows are created to support Phase 3b COA Development of the COPD v2 planning process. By analysing the questions that need to be answered and depending on the kind of available data, one or more workflows are created for each step that DFTOP supports. The modular design of DFTOP allows for creating and modifying workflows freely. Additionally, these workflows are designed to work with general Data Farming data.

4.6.1 DFTOP Overview

The implemented GUI of DFTOP is shown in Figure 4-19. It has a ribbon menu on the top, where all functions are accessible. It has a tabbed main display area that allows for several visualisations to be accessible at the same time with easy switching. On the right side there is a column with stacked interaction modules.


Open Workflow: C:\Users\dhuber\Documents\Visual Studio 2013\Projects\DFTOP-SVNEXT\DFTOP.Tests\MiscFiles\Workflow 2e.xml
Decision Maker Workflows
Analyst Workflows
Workflow Management
COA Tools
Data Tools
Objective Function Definition
Dashboard
Decision Factor Importance
Noise Factor Importance
Histogram
SDA + Wire Diagram
Workflows
Execute
Workflow Execution
Basic Workflow Information X
Important Blue Factors Step: 1 X
Important Blue Factors Step: 2 X
Important Blue Factors Step: 3 X
Legend
numerical value - increasing
numerical value - constant
numerical value - decreasing
categorical value
tNATO
B#CAP
BPatriotDist
B#JASperCAP
B#Battalion
B#F18
B#Patriot
BWeaponMix
B#JAS
BlueStrategy
0
Instant Update
ON
Save Selection Setting
Load Selection Setting

Sample Size = 183 (0,89% of all runs)

High 1

Red Strategy

☑ RedAll
☐ RedFront
☐ RedAirport
☐ RedEast
☐ RedWest

Number of Cruise Missiles per TU16

Low 6
High 12

Number of Red Attack Packages

Low 8
High 8

Number of Red Airborne Battalions

Low 8
High 8

Number of Il76

Low 40
High 40

Number of Red Battalions

Low 40
High 40

Figure 4-19: DFTOP GUI Overview.

Each workflow can be started by selecting its respective button in the menu. The workflows are grouped by the role of the user; either decision maker or analyst. Special workflows that are necessary to start an analysis, i.e., the definition of a multi-criteria objective function, definition of courses of actions, and data import are separated into their own menus.

Interaction modules are either a group of checkboxes, one-sided sliders (selection of a specific value), or two-sided sliders (selection of a value range). Colouring is used to indicate if they are affecting the filtering of Red factors, Blue factors, or parameters configuring the workflow modules.

4.6.2 Implemented Workflows

The current version of DFTOP consists of ten workflows using five different software tools or frameworks. The most widely used tools are MathWorks' MATLAB and Microsoft's .NET, especially C#, SAS JMP, Tableau, and Java. DFTOP is an integration and control framework and is either presenting images of visualisations generated by these tools or integrating the application windows of these tools directly into its GUI. For detailed information regarding the implementation of DFTOP workflows, see Section A1.1 in Appendix 1.

4.6.2.1 Deriving Workflows from the COPD

In Figure 4-3 the relation between Data Farming and DFTOP to Phase 3 planning activities is illustrated. Referring to this, the mapping of the corresponding workflows of DFTOP to the planning activities is depicted in

Figure 4-20. The rightmost column of the figure describes how each workflow executed in DFTOP supports corresponding activities in the middle column. Arrows going to the right implies that information from the planning staff is used to set up or adjust DFTOP. Arrows going to the left implies support provided by DFTOP. Vertical arrows indicate the proposed order of execution for the workflows.

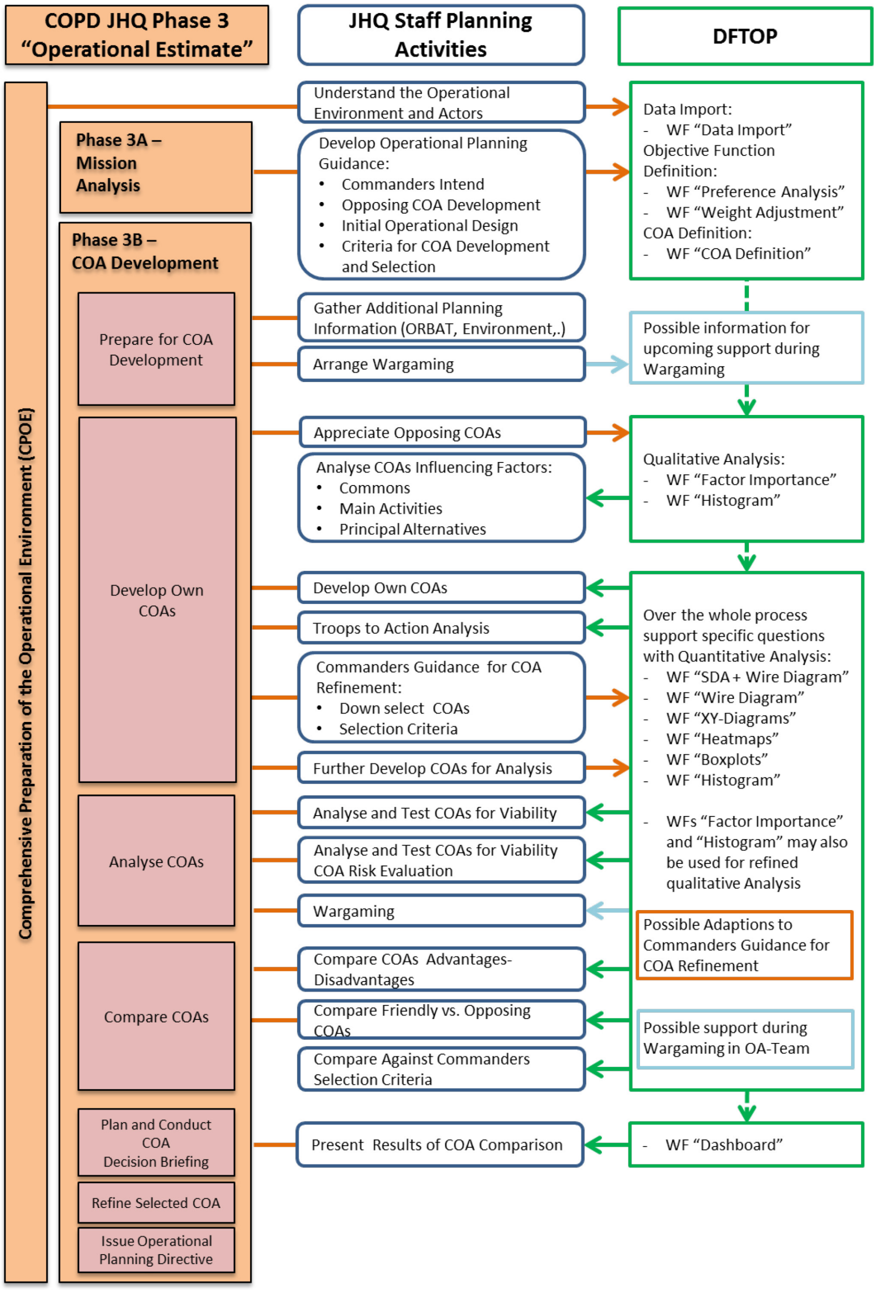
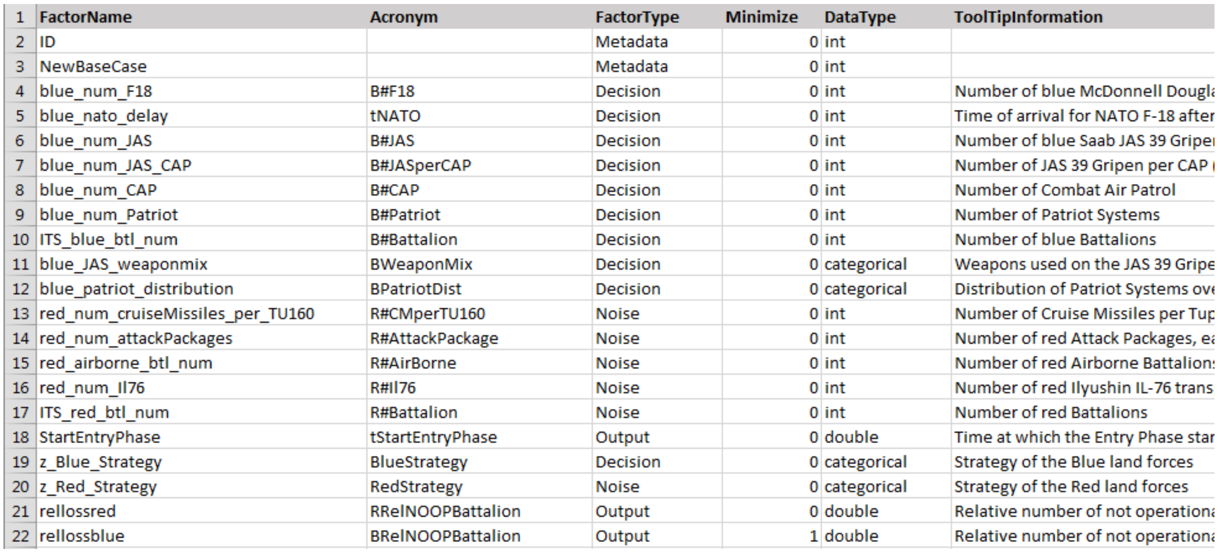

COPD JHQ Phase 3 "Operational Estimate"
JHQ Staff Planning Activities
DFTOP
Comprehensive Preparation of the Operational Environment (CPOE)
Phase 3A – Mission Analysis
Phase 3B – COA Development
Prepare for COA Development
Develop Own COAs
Analyse COAs
Compare COAs
Plan and Conduct COA Decision Briefing
Refine Selected COA
Issue Operational Planning Directive
Understand the Operational Environment and Actors
Develop Operational Planning Guidance:
• Commanders Intend
• Opposing COA Development
• Initial Operational Design
• Criteria for COA Development and Selection
Gather Additional Planning Information (ORBAT, Environment,.)
Arrange Wargaming
Appreciate Opposing COAs
Analyse COAs Influencing Factors:
• Commons
• Main Activities
• Principal Alternatives
Develop Own COAs
Troops to Action Analysis
Commanders Guidance for COA Refinement:
• Down select COAs
• Selection Criteria
Further Develop COAs for Analysis
Analyse and Test COAs for Viability
Analyse and Test COAs for Viability COA Risk Evaluation
Wargaming
Compare COAs Advantages-Disadvantages
Compare Friendly vs. Opposing COAs
Compare Against Commanders Selection Criteria
Present Results of COA Comparison
Data Import:
- WF "Data Import"
Objective Function Definition:
- WF "Preference Analysis"
- WF "Weight Adjustment"
COA Definition:
- WF "COA Definition"
Possible information for upcoming support during Wargaming
Qualitative Analysis:
- WF "Factor Importance"
- WF "Histogram"
Over the whole process support specific questions with Quantitative Analysis:
- WF "SDA + Wire Diagram"
- WF "Wire Diagram"
- WF "XY-Diagrams"
- WF "Heatmaps"
- WF "Boxplots"
- WF "Histogram"
- WFs "Factor Importance" and "Histogram" may also be used for refined qualitative Analysis
Possible Adaptions to Commanders Guidance for COA Refinement
Possible support during Wargaming in OA-Team
- WF "Dashboard"

Figure 4-20: COPD Phase 3 and DFTOP Workflows (WF).

Following the process in Phase 3b chronologically, all workflows are presented in the next sections.

4.6.2.2 Data Import

The DF data has to be imported into the DFTOP database. The first step is to define decision and noise factors and MOE to be imported. This definition is done by filling out an Excel spread sheet as shown in Figure 4-21. Next to the factor names, some metadata is included to improve usability of DFTOP. After describing the data, the import workflow has to be executed.



1	FactorName	Acronym	FactorType	Minimize	DataType	ToolTipInformation
2	ID		Metadata	0	int	
3	NewBaseCase		Metadata	0	int	
4	blue_num_F18	B#F18	Decision	0	int	Number of blue McDonnell Dougla
5	blue_nato_delay	tNATO	Decision	0	int	Time of arrival for NATO F-18 after
6	blue_num_JAS	B#JAS	Decision	0	int	Number of blue Saab JAS 39 Griper
7	blue_num_JAS_CAP	B#JASperCAP	Decision	0	int	Number of JAS 39 Gripen per CAP (
8	blue_num_CAP	B#CAP	Decision	0	int	Number of Combat Air Patrol
9	blue_num_Patriot	B#Patriot	Decision	0	int	Number of Patriot Systems
10	ITS_blue_btl_num	B#Battalion	Decision	0	int	Number of blue Battalions
11	blue_JAS_weaponmix	BWeaponMix	Decision	0	categorical	Weapons used on the JAS 39 Gripe
12	blue_patriot_distribution	BPatriotDist	Decision	0	categorical	Distribution of Patriot Systems ove
13	red_num_cruiseMissiles_per_TU160	R#CMperTU160	Noise	0	int	Number of Cruise Missiles per Tup
14	red_num_attackPackages	R#AttackPackage	Noise	0	int	Number of red Attack Packages, ea
15	red_airborne_btl_num	R#AirBorne	Noise	0	int	Number of red Airborne Battalions
16	red_num_Il76	R#Il76	Noise	0	int	Number of red Ilyushin IL-76 trans
17	ITS_red_btl_num	R#Battalion	Noise	0	int	Number of red Battalions
18	StartEntryPhase	tStartEntryPhase	Output	0	double	Time at which the Entry Phase star
19	z_Blue_Strategy	BlueStrategy	Decision	0	categorical	Strategy of the Blue land forces
20	z_Red_Strategy	RedStrategy	Noise	0	categorical	Strategy of the Red land forces
21	rellossred	RRelNOOPBattalion	Output	0	double	Relative number of not operationa
22	rellossblue	BRelNOOPBattalion	Output	1	double	Relative number of not operationa

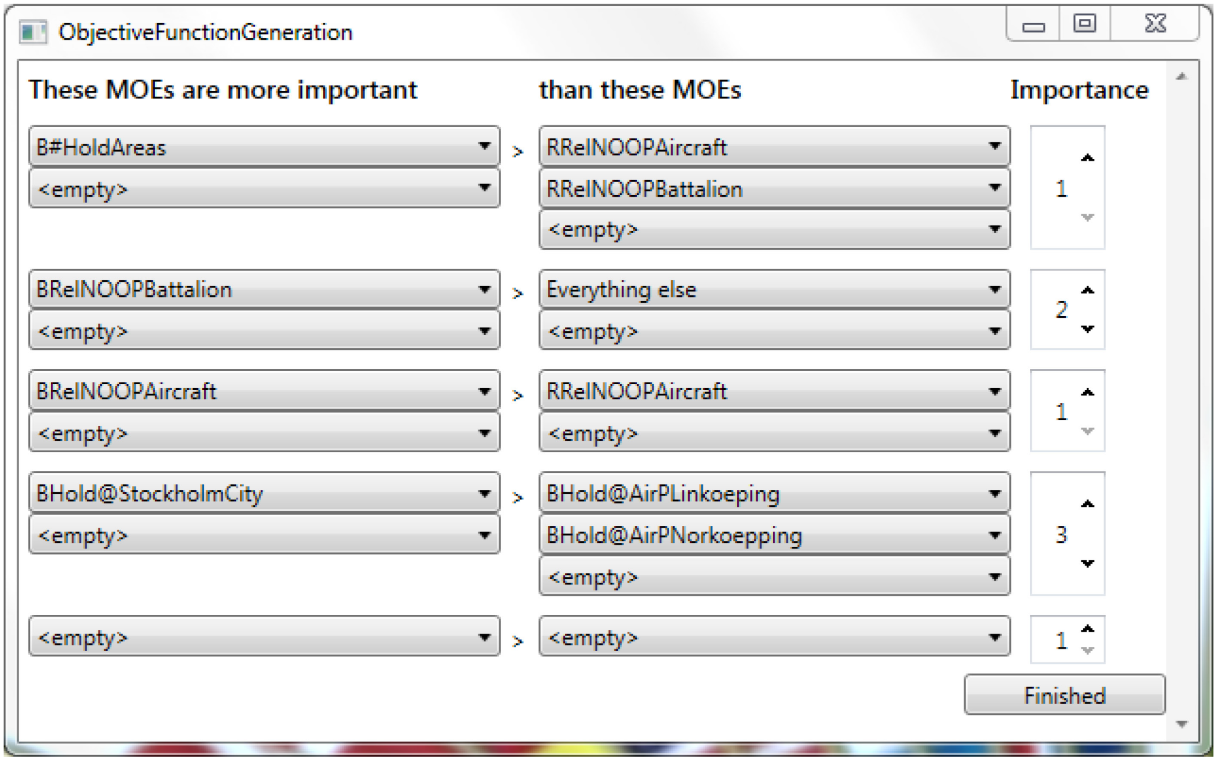
Figure 4-21: Database Definition and Metadata.

This workflow also allows setting up formulas to define a transformation from raw simulation outputs to the MOE required for the analysis.

4.6.2.3 Objective Function Definition

The commander’s intend and the commander’s planning guidance has to be incorporated into the Data Farming analysis and DFTOP in the form of a multi-criteria objective function. DFTOP offers a two-step process to do this. The first step involves identifying relevant MOE for the objective function with an automated suggestion for weights in the linear objective function for Overall mission success (*Oms*). The weights can be manually refined in the second step.

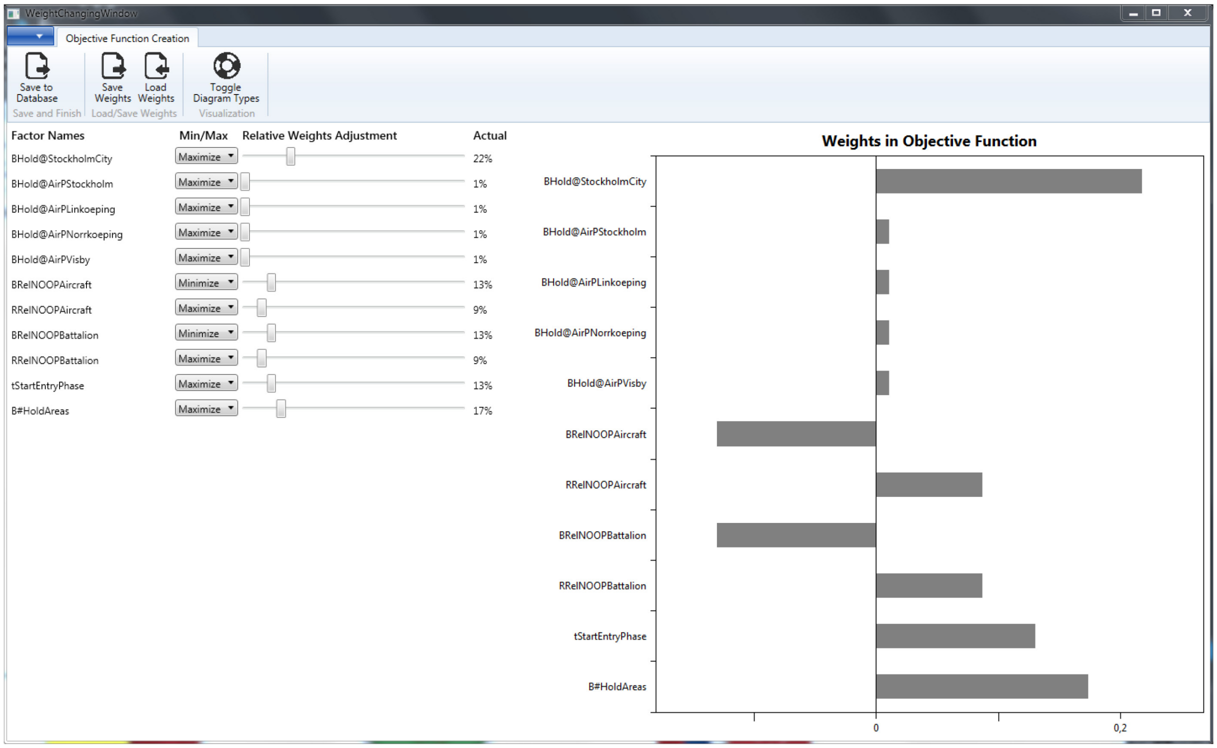
The GUI for the first step is presented in Figure 4-22. To help decision makers assign appropriate weights to all MOE, a preference based algorithm has been incorporated. The decision maker may express preferences on the importance between any two disjoint subsets of MOE using a tailored GUI. An extension of Utkin’s [17], [18] preference ranking method is used to calculate the weights. It is focused on finding the order of importance of the MOE from the preference assignments. The method is extended by Schubert’s method [19] for interpolation in belief-plausibility intervals regarding the obtained degree of preference of all different measures of effectiveness. This method accepts any preference expression about the MOE from multiple decision makers. For example, expressions such as *“measure of effectiveness number i is more important than measure of effectiveness number j”* or expressions regarding two different subsets of all measures such as *“measures i and j are more important than measures k and l”*. The GUI can be used to define these preferences and also assign an importance ranking to them, causing preferences with high importance to have large weights (for instance due to support from many decision makers). The algorithm to calculate the weights in the objective function can be seen in Section A1.2 in Appendix 1.



These MOEs are more important		than these MOEs	Importance
B#HoldAreas <empty>	>	RRelNOOPAircraft RRelNOOPBattalion <empty>	1
BRelNOOPBattalion <empty>	>	Everything else <empty>	2
BRelNOOPAircraft <empty>	>	RRelNOOPAircraft <empty>	1
BHold@StockholmCity <empty>	>	BHold@AirPLinkoeping BHold@AirPNorkoepping <empty>	3
<empty>	>	<empty>	1

Figure 4-22: Definition of Preferences.

The GUI for the second step is shown in Figure 4-23. If the first step was skipped, the initial objective function consists of all MOE having equal weights assigned to them. In this GUI the weights can be adjusted and their relative value can be seen in a bar or pie chart. Whether the MOE shall be maximised or minimised is also assigned. Since the objective functions quantify the overall success of the Blue side, it is named OverallSuccess.



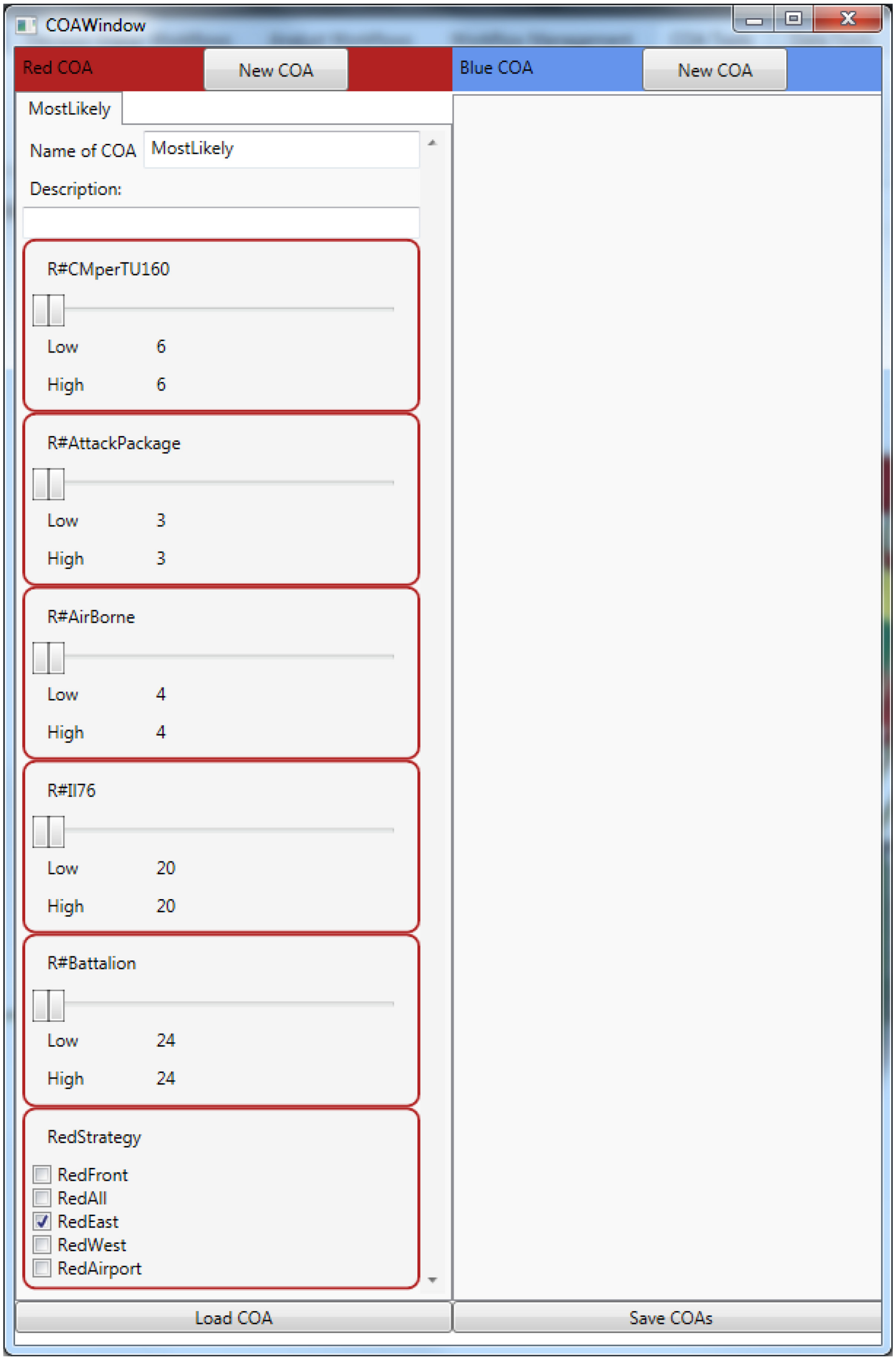
Factor Names	Min/Max	Relative Weights Adjustment	Actual
BHold@StockholmCity	Maximize		22%
BHold@AirPStockholm	Maximize		1%
BHold@AirPLinkoeping	Maximize		1%
BHold@AirPNorrkoeping	Maximize		1%
BHold@AirPVisby	Maximize		1%
BRelNOOPAircraft	Minimize		13%
RRelNOOPAircraft	Maximize		9%
BRelNOOPBattalion	Minimize		13%
RRelNOOPBattalion	Maximize		9%
tStartEntryPhase	Maximize		13%
B#HoldAreas	Maximize		17%

Figure 4-23: Weight Adjustment and Writing to Database.

After all weights are set according to the commander's intend and planning guidance, the objective function can be saved to the database. This action initiates a database update by calculating a value of OverallSuccess for every row in the database.

4.6.2.4 COA Definition

Having incorporated the commander's intent into the overall success MOE, the next workflow supports the definition of COA for both sides using the GUI shown in Figure 4-24. In DFTOP COA are defined using filters on decision and noise factors, thus defining a subset of the DF data. The definition of these filters uses the same interaction modules as in the main DFTOP GUI. After defining the COA in the COA Definition GUI, they can be saved and used in all other workflows, limiting the analysis to subsets of the DF data corresponding to respective COA.



Name of COA: MostLikely

Description:

R#CMperTU160

Low 6

High 6

R#AttackPackage

Low 3

High 3

R#AirBorne

Low 4

High 4

R#Il76

Low 20

High 20

R#Battalion

Low 24

High 24

RedStrategy

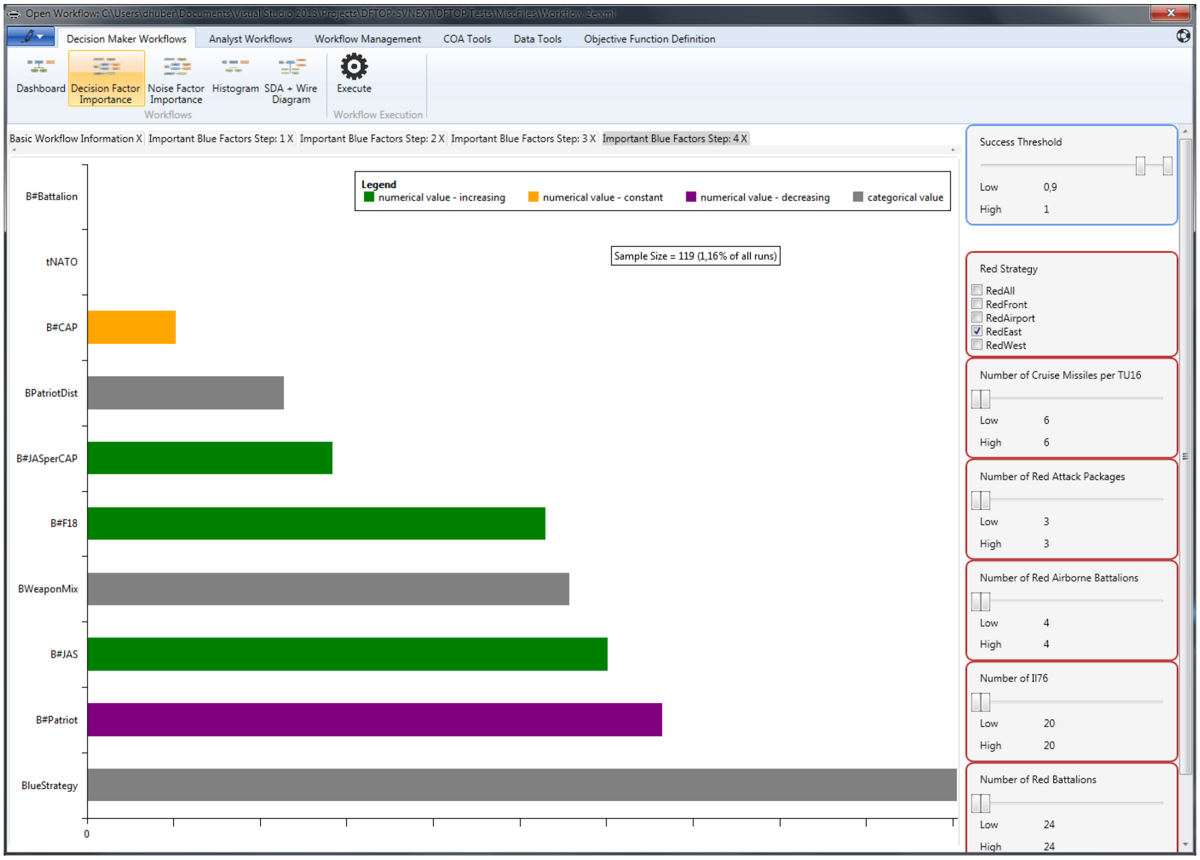
- □ RedFront
- □ RedAll
- ☑ RedEast
- □ RedWest
- □ RedAirport

Figure 4-24: COA Definition.

4.6.2.5 Factor Importance

This workflow is designed to give top-level answer to the question like: *What are the most important decision and noise factors for success?* Using this workflow is one possible way to analyse the COA influencing factors.

A successful outcome is defined by the objective function OverallSuccess. The decision maker defines an outcome as successful by setting a quantitative threshold on the OverallSuccess using an interaction module. A workflow visualisation is shown in Figure 4-25 with the threshold for success set to 0.9. In the figure an opposing COA is used to filter the data. Thus, the most important factors for success are shown for this COA.


Open Workflow: C:\Users\dhuber\Documents\Visual Studio 2013\Projects\DFTOP-SVNEXT\DFTOP.Tests\MiscFiles\Workflow 2e.xml

Sample Size = 119 (1,16% of all runs)

Success Threshold
Low 0,9
High 1

Red Strategy
☐ RedAll
☐ RedFront
☐ RedAirport
☑ RedEast
☐ RedWest

Number of Cruise Missiles per TU16
Low 6
High 6

Number of Red Attack Packages
Low 3
High 3

Number of Red Airborne Battalions
Low 4
High 4

Number of Il76
Low 20
High 20

Number of Red Battalions
Low 24
High 24

Decision Maker Workflows
Analyst Workflows
Workflow Management
COA Tools
Data Tools
Objective Function Definition
Dashboard
Decision Factor Importance
Noise Factor Importance
Histogram
SDA + Wire Diagram
Workflows
Execute
Workflow Execution
Basic Workflow Information X
Important Blue Factors Step: 1 X
Important Blue Factors Step: 2 X
Important Blue Factors Step: 3 X
Important Blue Factors Step: 4 X
Legend
🟩 numerical value - increasing
🟧 numerical value - constant
🟪 numerical value - decreasing
⬛ categorical value
B#Battalion
tNATO
B#CAP
BPatriotDist
B#JASperCAP
B#F18
BWeaponMix
B#JAS
B#Patriot
BlueStrategy
0

Figure 4-25: Most Important Factors Chart.

The result of this workflow is qualitative and gives an indication of which factors are most important. The colour coding of the bars indicate if a tendency in the values has been found. For instance, different coding is given to factors that improve success, decrease success, or are without importance. For categorical factors the tendency cannot be calculated.

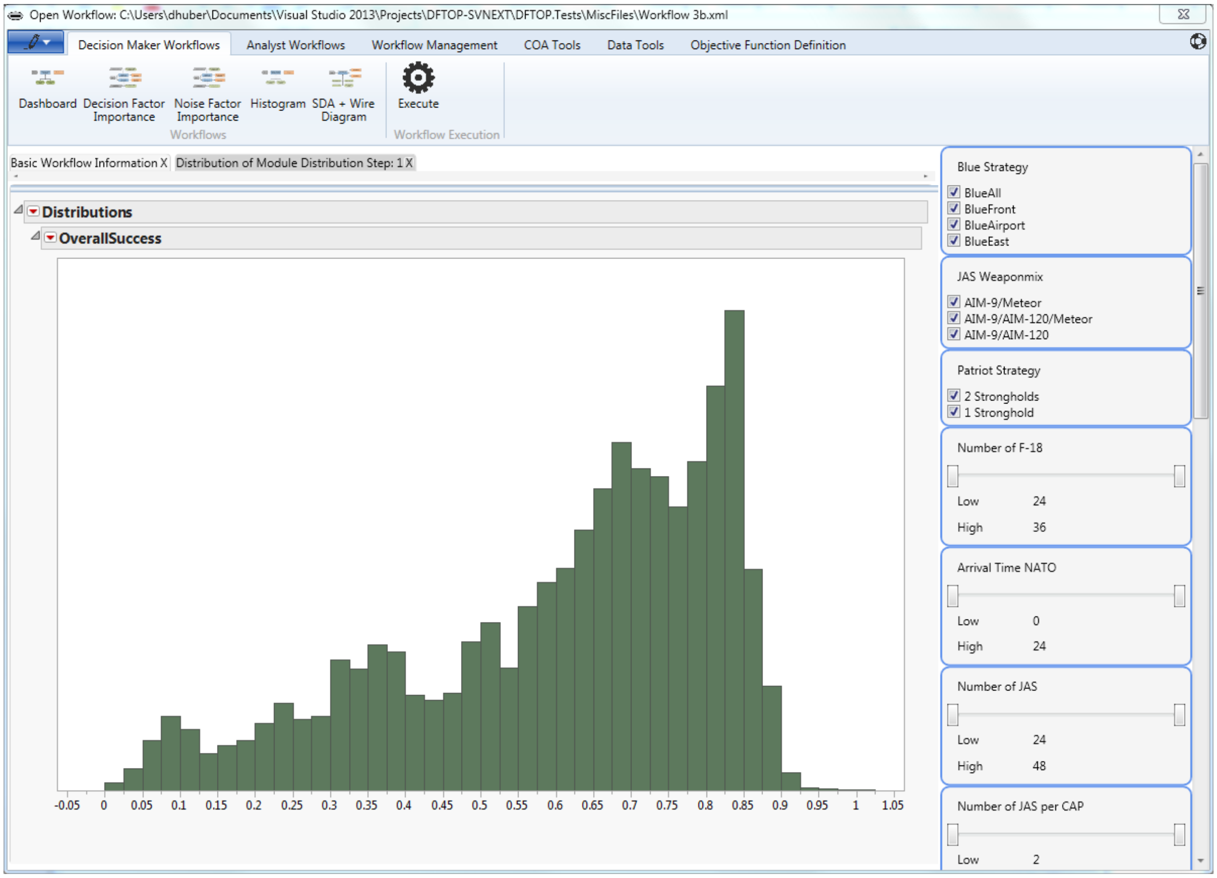
The workflow uses two modules, one for data analysis and one for visualisation. Two data sets are used in the analysis module that contains the decision and noise factors. These sets are filtered by opposing or own COA. The second data set is additionally filtered based on the OverallSuccess threshold. The difference between the two datasets for each factor is quantified using a statistical analysis. The bar size for each factor represents its influence on OverallSuccess. Factors with a high influence on OverallSuccess are important factors.

If the interaction modules are used to modify the filter, the workflow has to be re-executed. A new bar chart will be presented in a new tab.

4.6.2.6 Histogram

This workflow is designed to give a top-level overview of the distribution of OverallSuccess, especially when applying filters, e.g., looking at specific COA and combination of COA. The histogram can be used to get an estimate of success and of the risk existing in the selected COA combination. This workflow can also be used to modify COA interactively, or to get a better understanding of the data.

This workflow uses only one module, which is running in JMP. The module creates and visualizes a histogram of the selected data. Figure 4-26 shows a histogram of OverallSuccess for all simulation runs, and Figure 4-27 shows the same histogram, filtered by a selection of red strategies.



Blue Strategy

☑ BlueAll
☑ BlueFront
☑ BlueAirport
☑ BlueEast

JAS Weaponmix

☑ AIM-9/Meteor
☑ AIM-9/AIM-120/Meteor
☑ AIM-9/AIM-120

Patriot Strategy

☑ 2 Strongholds
☑ 1 Stronghold

Number of F-18

Low 24
High 36

Arrival Time NATO

Low 0
High 24

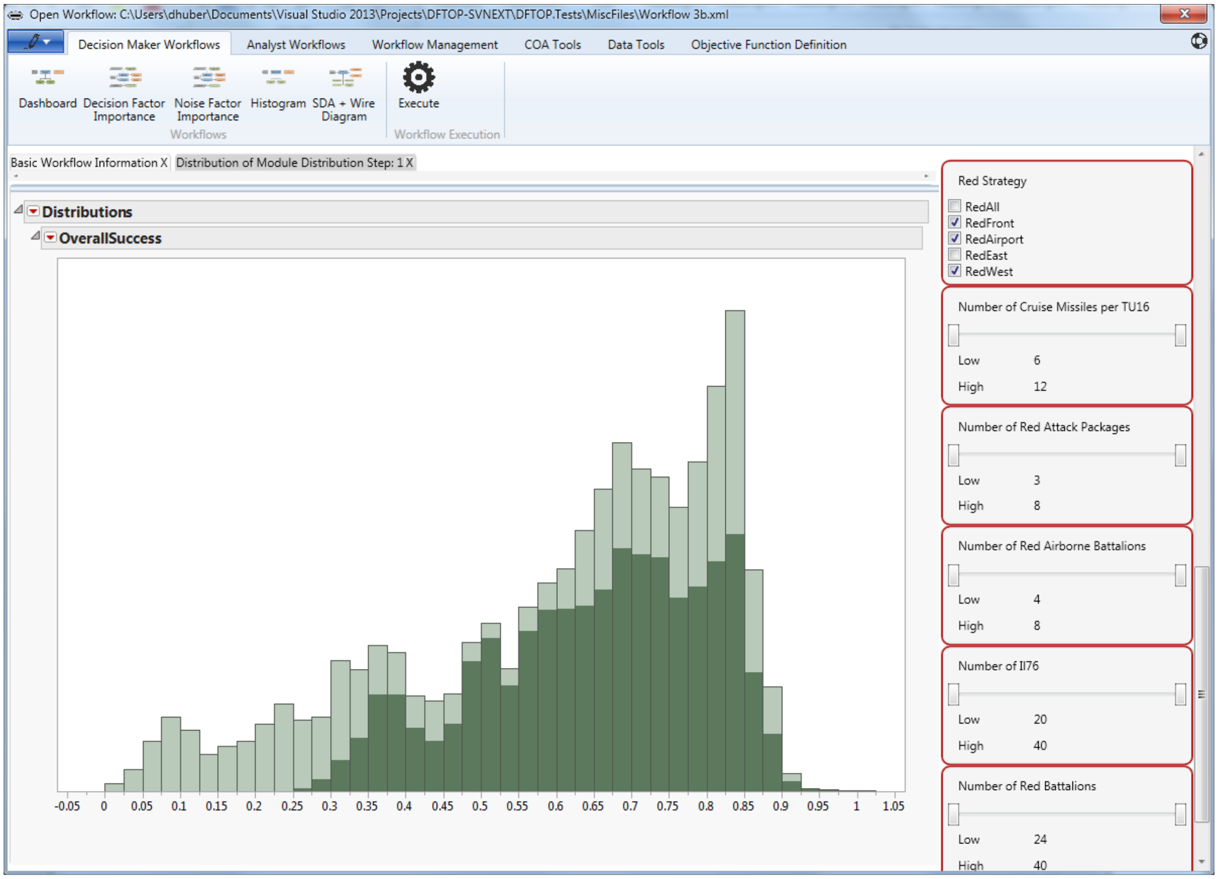
Number of JAS

Low 24
High 48

Number of JAS per CAP

Low 2

Figure 4-26: Histogram of OverallSuccess Showing All Blue Strategies Against All Red Strategies.



Open Workflow: C:\Users\dhuber\Documents\Visual Studio 2013\Projects\DFTOP-SVNEXT\DFTOP.Tests\MiscFiles\Workflow 3b.xml

Red Strategy

- □ RedAll
- ☑ RedFront
- ☑ RedAirport
- □ RedEast
- ☑ RedWest

Number of Cruise Missiles per TU16

Low	6
High	12

Number of Red Attack Packages

Low	3
High	8

Number of Red Airborne Battalions

Low	4
High	8

Number of Il76

Low	20
High	40

Number of Red Battalions

Low	24
High	40

Figure 4-27: Histogram of OverallSuccess Filtered by a Selection of Red Strategies.

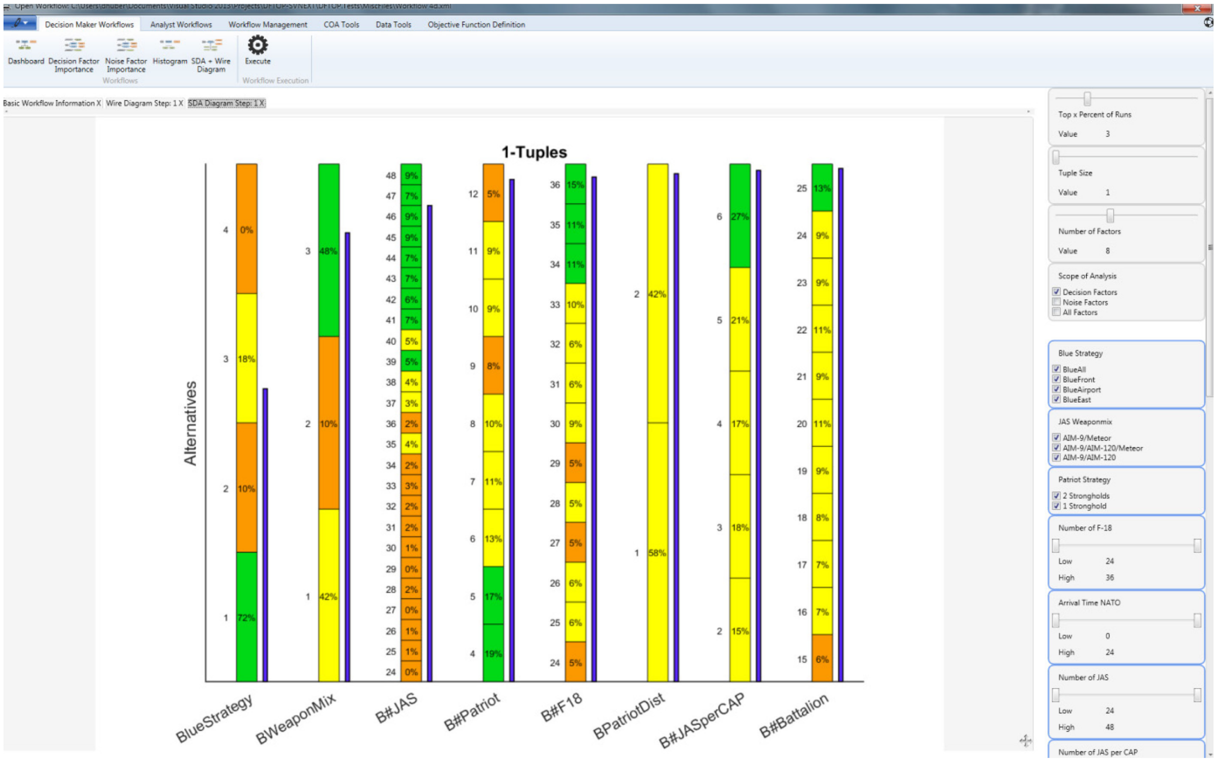
4.6.2.7 Skewed Distribution Analysis

An alternative factor analysis is the *Skewed Distribution Analysis* (SDA) approach [20] where we consider a subset of simulations that achieved the best operational result[2]. The frequency distributions of the factors can then reveal their importance.

The idea behind SDA is that, if a factor is important for the operational outcome, the value of this factor is significant in differentiating between success and failure. This implies that the frequency of values within the subset of best simulations should be highly uneven, that is *skewed*. The *skewedness* can be measured using Shannon entropy [21]. This analysis can also be performed for several factors simultaneously, to discover correlated factors (where we measure the combined factor skewedness by their *joint* Shannon entropy, we call a combination of *k* factors a *k*-tuple). Low entropy of a factor means a highly skewed distribution and suggests that the operational outcome is highly sensitive to the value of that factor (or set of factors). The minimum entropy value, zero, is achieved when only one factor value leads to success. Conversely, high (joint) entropy indicates that the operational result is more or less independent on the factor(s) and may be ignored.

[2] Best with respect to a combination of multiple MOEs.

When using this module, the first step is to study single factors. After that, the interaction of several factors (higher *k*-tuples) should be studied. In our experience, studying multiple factors seems frequently to yield lower entropy than when studying fewer. When increasing the number of factors, this advantage diminishes at some point as the complexity of dealing with too many multiple factors becomes practically too high. The next step is to rank the *k*-tuples for further analysis. In Figure 4-28, we present an example of factors and factor value ranges yielding the lowest entropy in increasing order.



Top x Percent of Runs

Value 3

Tuple Size

Value 1

Number of Factors

Value 8

Scope of Analysis

☑ Decision Factors
☐ Noise Factors
☐ All Factors

Blue Strategy

☑ BlueAll
☑ BlueFront
☑ BlueAirport
☑ BlueEast

JAS Weaponmix

☑ AIM-9/Meteor
☑ AIM-9/AIM-120/Meteor
☑ AIM-9/AIM-120

Patriot Strategy

☑ 2 Strongholds
☑ 1 Stronghold

Number of F-18

Low 24
High 36

Arrival Time NATO

Low 0
High 24

Number of JAS

Low 24
High 48

Number of JAS per CAP

Figure 4-28: Skewed Distribution Analysis for 1-Tuples, the Blue Bars Indicate the (Normalized) Entropy.

The lowest entropy factors to the left tend to have skewed distributions with particular value ranges of importance. On the right in Figure 4-28 we have factors that did not turn out to be decisive for the outcome of the simulations.

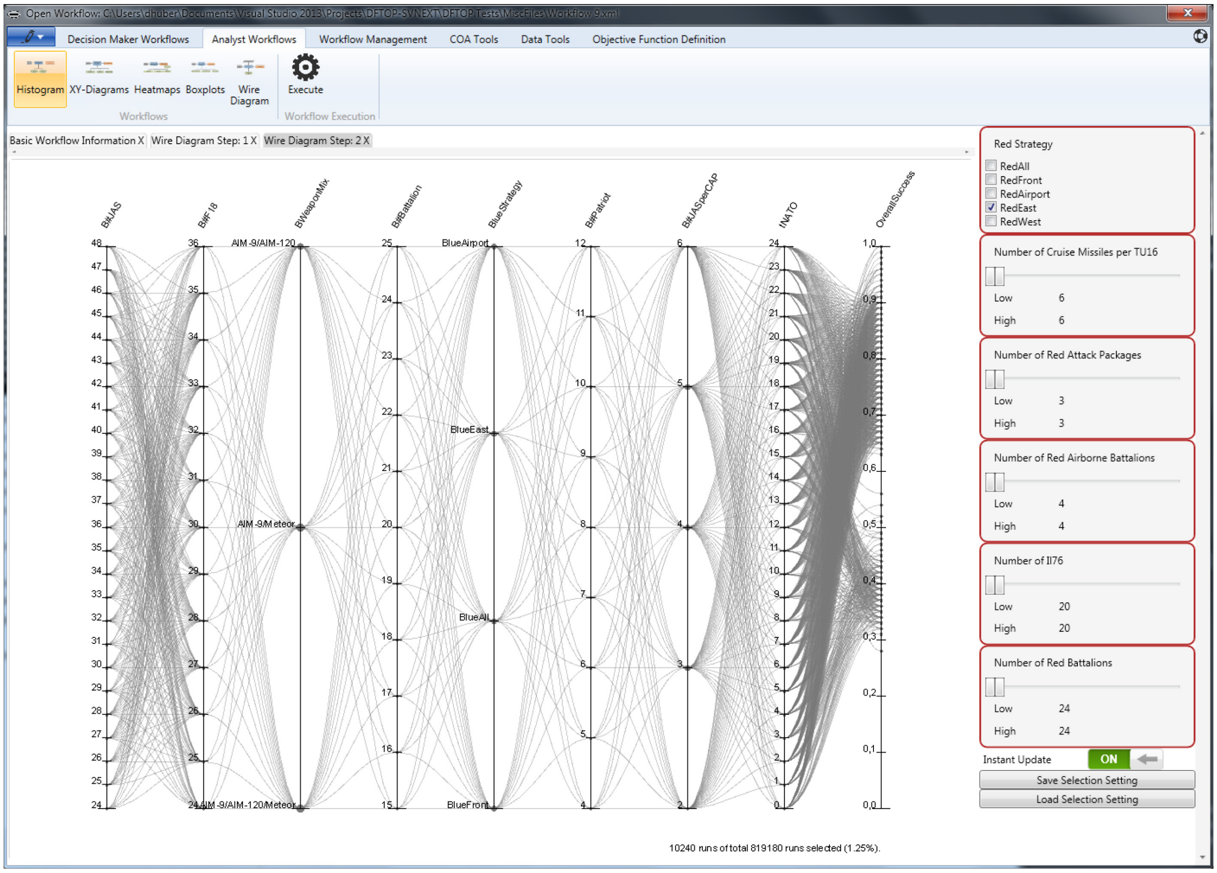
4.6.2.8 Wire Diagram

The Wire Diagram workflow provides immediate visualization of the effect of chosen factor values on the OverallSuccess. It is designed to support development of COA, and is used for an interactive analysis of interdependencies between the factors and their influence on OverallSuccess.

The diagram type used is called Parallel Coordinates Plot [22], which creates parallel vertical axis for a set of factors and OverallSuccess. Each simulation run is represented by a line combining the input values of all decision factors with the resulting output value for OverallSuccess. If many lines cross the same points, the lines are drawn thicker. If many simulation runs realize the same axis value, the relevant dots are drawn thicker.

The Wire Diagram is set up to support COA development, thus only decision factors are integrated and there is a possibility to filter by opposing COA. The analysis provided with the Wire Diagram is closely related to the SDA, the Wire Diagram is therefore also set up as an extra in the SDA workflow, integrating the same factors as the SDA and showing matching colour coding on the axes. The latter case is designed to evaluate concrete factor value combinations and constraints based on the SDA analysis.

In Figure 4-29 data regarding one specific opposing COA is shown against all own COA. It is seen that all factor values are equally distributed, which is a consequence of the DOE.



Red Strategy
☐ RedAll
☐ RedFront
☐ RedAirport
☑ RedEast
☐ RedWest

Number of Cruise Missiles per TU16
Low 6
High 6

Number of Red Attack Packages
Low 3
High 3

Number of Red Airborne Battalions
Low 4
High 4

Number of Il76
Low 20
High 20

Number of Red Battalions
Low 24
High 24

Instant Update ON

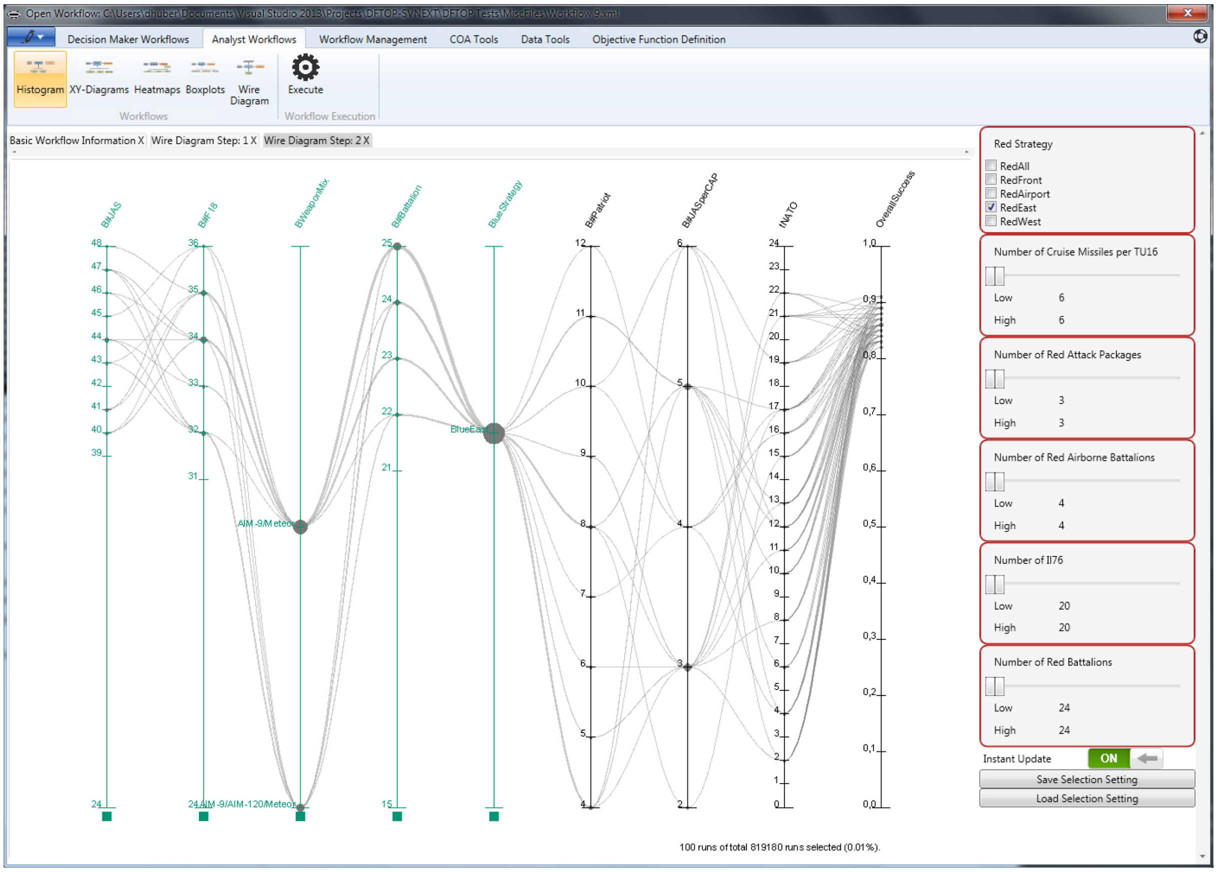
Save Selection Setting

Load Selection Setting

10240 runs of total 819180 runs selected (1.25%).

Figure 4-29: Wire Diagram Showing All Own COA Against One Opposing COA.

When we select the most successful simulation runs, a diagram state as shown in Figure 4-30 is obtained.



Red Strategy

☐ RedAll
☐ RedFront
☐ RedAirport
☑ RedEast
☐ RedWest

Number of Cruise Missiles per TU16

Low 6
High 6

Number of Red Attack Packages

Low 3
High 3

Number of Red Airborne Battalions

Low 4
High 4

Number of Il76

Low 20
High 20

Number of Red Battalions

Low 24
High 24

100 runs of total 819180 runs selected (0.01%).

Figure 4-30: Wire Diagram Showing the Most Successful Own COA Against One Opposing COA.

Data farming is a question-driven process, typical questions that can be answered with the Wire Diagram are:

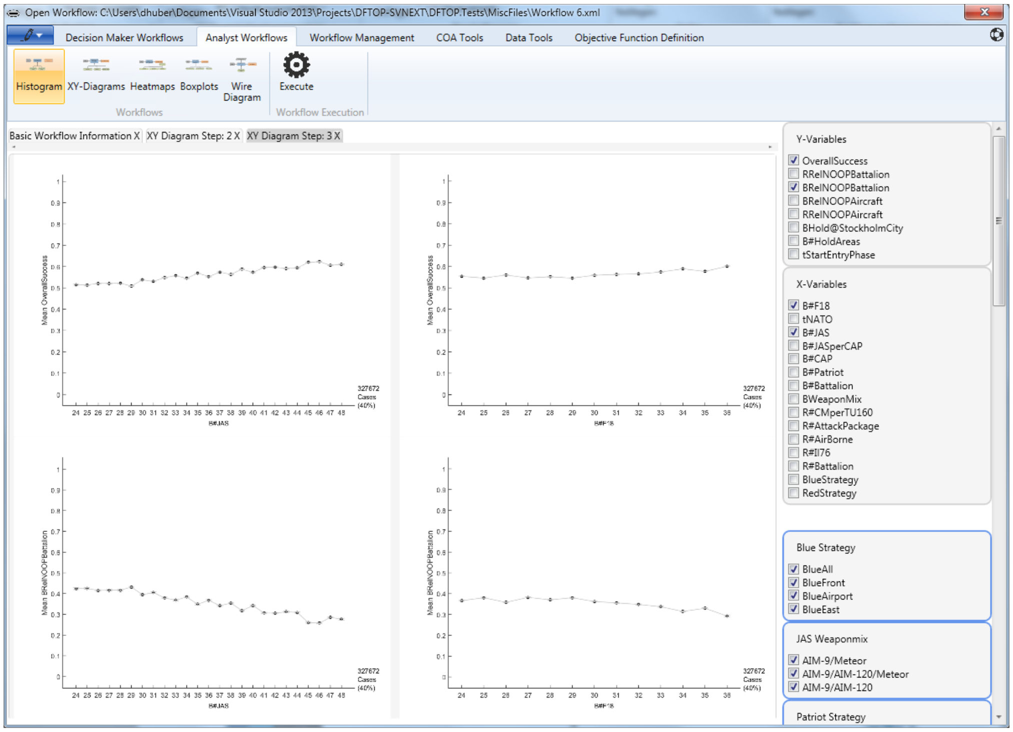
1) Which set of own COA results in a certain range of OverallSuccess? or
2) What is the range of OverallSuccess for a specific COA?

One should be careful not to filter out too many simulation runs; therefore the number of runs is presented.

4.6.2.9 *xy*-Diagrams

The workflow generates a set of *xy*-diagrams. Each diagram shows the effect of a factor on an MOE. These show the mean value of an MOE for each factor value. Each data point features an error indicator, displaying the standard deviation of the mean.

Several MOE and factors can be selected, creating a grid of diagrams (Figure 4-31). Pan and zoom functionality allows the user to zoom in on each diagram, such that it can be viewed in detail as shown in Figure 4-32.



Y-Variables

☑ OverallSuccess
☐ RRelNOOPBattalion
☑ BRelNOOPBattalion
☐ BRelNOOPAircraft
☐ RRelNOOPAircraft
☐ BHold@StockholmCity
☐ B#HoldAreas
☐ tStartEntryPhase

X-Variables

☑ B#F18
☐ tNATO
☑ B#JAS
☐ B#JASperCAP
☐ B#CAP
☐ B#Patriot
☐ B#Battalion
☐ BWeaponMix
☐ R#CMperTU160
☐ R#AttackPackage
☐ R#AirBorne
☐ R#Il76
☐ R#Battalion
☐ BlueStrategy
☐ RedStrategy

Blue Strategy

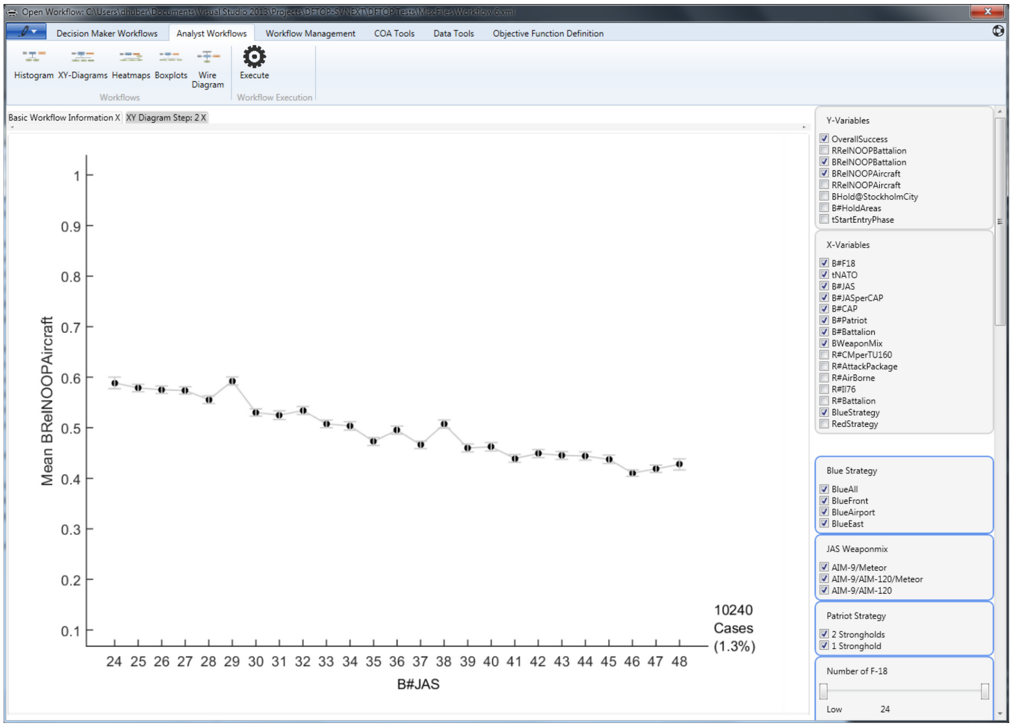
☑ BlueAll
☑ BlueFront
☑ BlueAirport
☑ BlueEast

JAS Weaponmix

☑ AIM-9/Meteor
☑ AIM-9/AIM-120/Meteor
☑ AIM-9/AIM-120

Patriot Strategy

Figure 4-31: *xy*-Diagram (Grid).



Y-Variables

☑ OverallSuccess
☐ RRelNOOPBattalion
☑ BRelNOOPBattalion
☑ BRelNOOPAircraft
☐ RRelNOOPAircraft
☐ BHold@StockholmCity
☐ B#HoldAreas
☐ tStartEntryPhase

X-Variables

☑ B#F18
☑ tNATO
☑ B#JAS
☑ B#JASperCAP
☑ B#CAP
☑ B#Patriot
☑ B#Battalion
☑ BWeaponMix
☐ R#CMperTU160
☐ R#AttackPackage
☐ R#AirBorne
☐ R#Il76
☐ R#Battalion
☑ BlueStrategy
☐ RedStrategy

Blue Strategy

☑ BlueAll
☑ BlueFront
☑ BlueAirport
☑ BlueEast

JAS Weaponmix

☑ AIM-9/Meteor
☑ AIM-9/AIM-120/Meteor
☑ AIM-9/AIM-120

Patriot Strategy

☑ 2 Strongholds
☑ 1 Stronghold

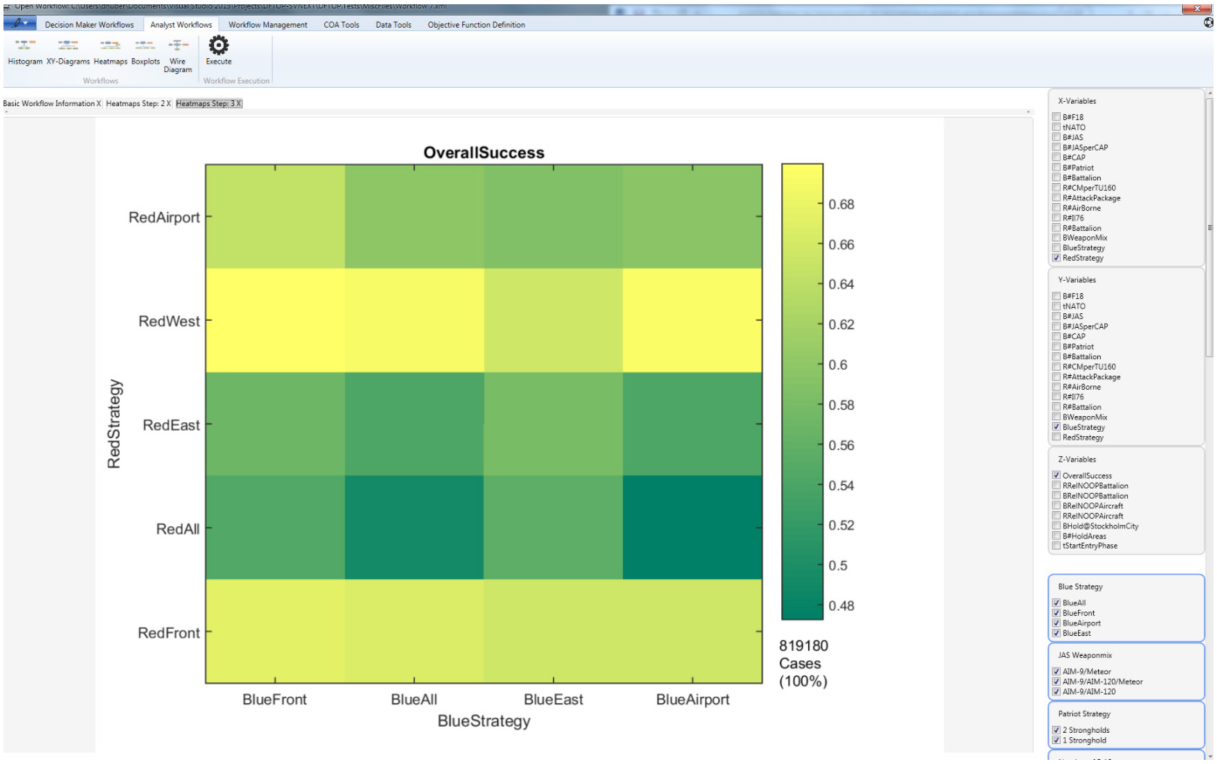
Number of F-18

Low 24

Figure 4-32: *xy*-Diagram (Detail).

4.6.2.10 Heat Map

A *heat map* can be used to see how an MOE varies as a function of two factors. The ranges of the two factors span the *x*- and *y*-axes, and the MOE is mapped to a colour scale. This is a way to use colours for the third dimension. The colour scale uses a coding as shown in the legend. Combinations of MOE values for which there are no simulations are coloured grey. Below in Figure 4-33 we show one example of a heat map on our data set.



Open Workflow: C:\Users\dhuber\Documents\Visual Studio 2013\Projects\DFTOP-SVNEXT\DFTOP.Tests\MiscFiles\Workflow 7.xml

X-Variables
□ B#F18
□ tNATO
□ B#JAS
□ B#JASperCAP
□ B#CAP
□ B#Patriot
□ B#Battalion
□ R#CMperTU160
□ R#AttackPackage
□ R#AirBorne
□ R#Il76
□ R#Battalion
□ BWeaponMix
□ BlueStrategy
☑ RedStrategy

Y-Variables
□ B#F18
□ tNATO
□ B#JAS
□ B#JASperCAP
□ B#CAP
□ B#Patriot
□ B#Battalion
□ R#CMperTU160
□ R#AttackPackage
□ R#AirBorne
□ R#Il76
□ R#Battalion
□ BWeaponMix
☑ BlueStrategy
□ RedStrategy

Z-Variables
☑ OverallSuccess
□ RRelNOOPBattalion
□ BRelNOOPBattalion
□ BRelNOOPAircraft
□ RRelNOOPAircraft
□ BHold@StockholmCity
□ B#HoldAreas
□ tStartEntryPhase

Blue Strategy
☑ BlueAll
☑ BlueFront
☑ BlueAirport
☑ BlueEast

JAS Weaponmix
☑ AIM-9/Meteor
☑ AIM-9/AIM-120/Meteor
☑ AIM-9/AIM-120

Patriot Strategy
☑ 2 Strongholds
☑ 1 Stronghold

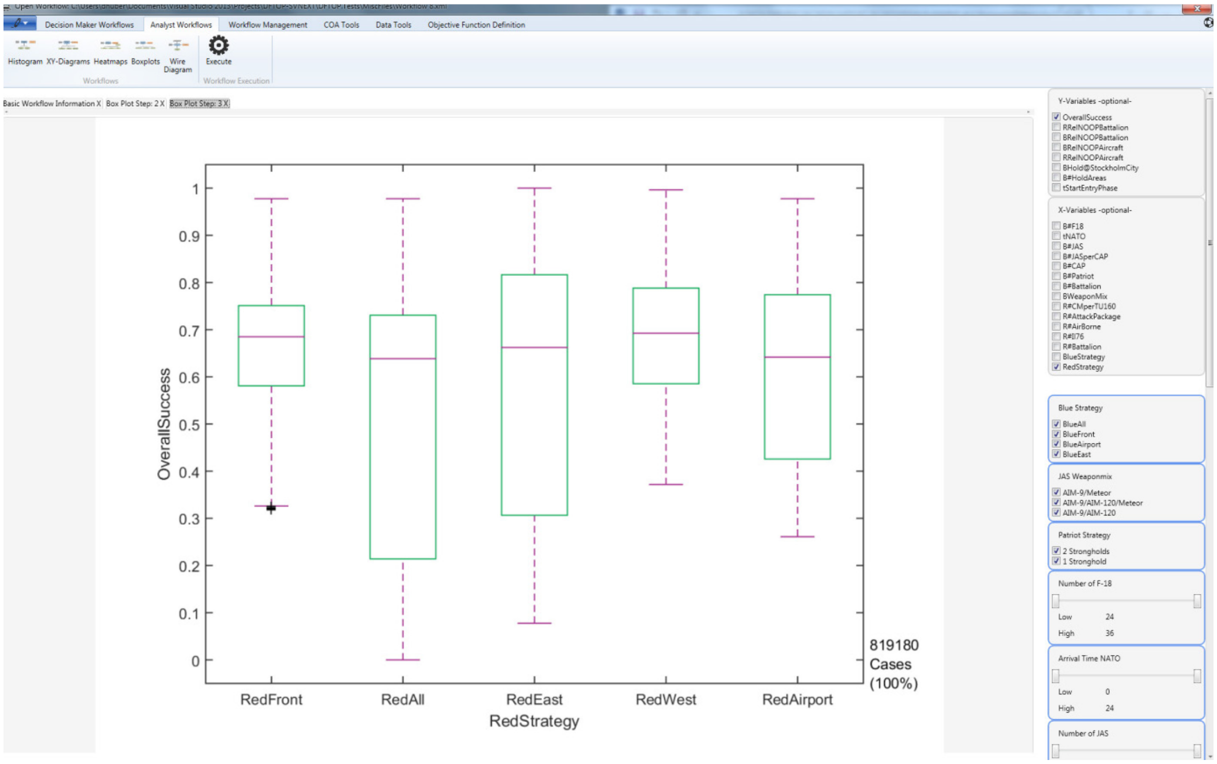
Figure 4-33: OverallSuccess.

We study several combinations of factor pairs, both concerning the Red side and the Blue side. Such an analysis is performed in the *Analyst View* process to get an overview based on the entire data set. To answer more specific questions regarding opposing COA of interest to the decision maker, we restrict the data set to specific subsets that match those questions [23]. This is done by restricting some of the noise factors. Filtering can also be used to put restrictions on decision factors. This narrows down the scenario and makes the heat maps easier to interpret. However, to impose too hard restrictions might provide too low statistical confidence of the heat map.

One can also put restrictions on MOE. For instance, one can focus on simulations that have the best outcome for the Blue side by limiting the value of OverallSuccess, thereby analysing only the scenarios where the Blue side has large success.

4.6.2.11 Box Plot

While heat maps are used to show how an MOE varies as a function of two factors, a *box plot* is used to plot a condensed representation of the distribution for each factor value, see Figure 4-34.



Y-Variables -optional-

☑ OverallSuccess
☐ RRelNOOPBattalion
☐ BRelNOOPBattalion
☐ BRelNOOPAircraft
☐ RRelNOOPAircraft
☐ BHold@StockholmCity
☐ B#HoldAreas
☐ tStartEntryPhase

X-Variables -optional-

☐ B#F18
☐ tNATO
☐ B#JAS
☐ B#JASperCAP
☐ B#CAP
☐ B#Patriot
☐ B#Battalion
☐ BWeaponMix
☐ R#CMperTU160
☐ R#AttackPackage
☐ R#AirBorne
☐ R#Il76
☐ R#Battalion
☐ BlueStrategy
☑ RedStrategy

Blue Strategy

☑ BlueAll
☑ BlueFront
☑ BlueAirport
☑ BlueEast

JAS Weaponmix

☑ AIM-9/Meteor
☑ AIM-9/AIM-120/Meteor
☑ AIM-9/AIM-120

Patriot Strategy

☑ 2 Strongholds
☑ 1 Stronghold

Number of F-18

Low 24
High 36

Arrival Time NATO

Low 0
High 24

Number of JAS

Figure 4-34: Box Plot.

The central horizontal line in a box is the median value. The upper and lower edges of each box represent the upper and lower quartiles, i.e., half of all simulation runs are inside the box. The dashed lines on each side of a box are called the *whiskers*. They extend to maximum 1.5 times the box height. (For normally distributed data, this means that 99.3% of all data are within the whiskers). Data outside the whiskers are defined as outliers and are marked as crosses.

Using filters, we can narrow down the intervals of other factors than those in the plot, which would normally give narrower distributions due to the smaller variation in factor values that are included in each box.

The variation of OverallSucess values in the five box-plots is a clear example on how we gain a much broader view of the range of possible outcomes using data farming. We may use data farming to compare between the different values of a specific factor, and see how the output varies as a function of the variation in other factors when that specific factor has a fixed value. From the figure, it is seen that on average the RedAirport strategy is more dangerous than the RedWest strategy since the mean, upper and lower quartiles are all lower for RedAirport.

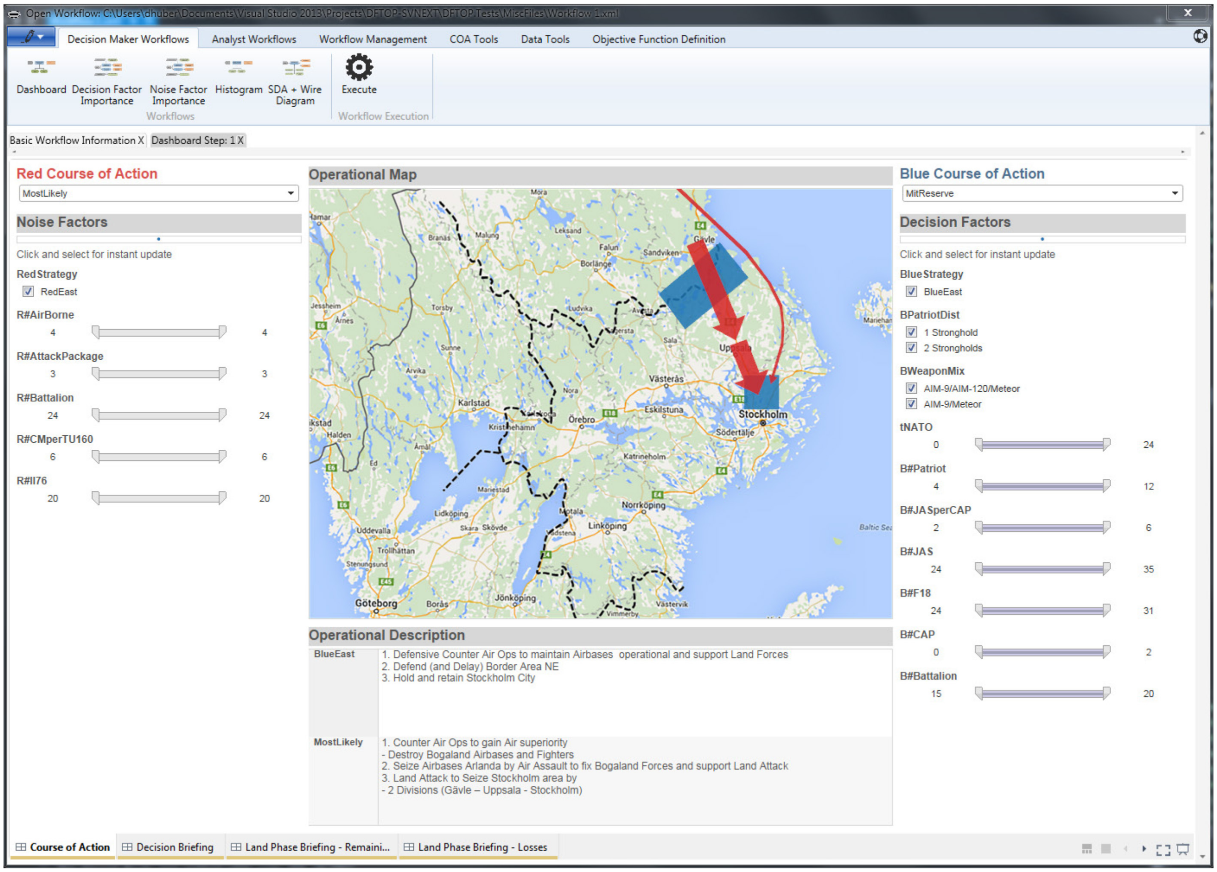
4.6.2.12 Dashboard

This workflow is designed to support the decision brief in COPD Phase 3b. The Dashboard delivers a comprehensive overview of COA design and evaluation on three tabs:

- COA specifications (own and opposing) displayed on a map (Figure 4-35).

- OverallSuccess of a given COA combination, and a detailed look at its criteria (Figure 4-36).
- A geographical view of losses and remaining forces (Figure 4-37).

On the COA page (Figure 4-35), one COA for each side can be selected from the set of COA developed in a previous analysis step (Section 4.6.2.4) and presented on a map. All Red and Blue factors can be interactively modified by sliders.



Red Course of Action

MostLikely

Noise Factors

Click and select for instant update

RedStrategy

☑ RedEast

R#AirBorne 4 4

R#AttackPackage 3 3

R#Battalion 24 24

R#CMperTU160 6 6

R#Il76 20 20

Blue Course of Action

MitReserve

Decision Factors

Click and select for instant update

BlueStrategy

☑ BlueEast

BPatriotDist

☑ 1 Stronghold

☑ 2 Strongholds

BWeaponMix

☑ AIM-9/AIM-120/Meteor

☑ AIM-9/Meteor

tNATO 0 24

B#Patriot 4 12

B#JASperCAP 2 6

B#JAS 24 35

B#F18 24 31

B#CAP 0 2

B#Battalion 15 20

Operational Description

BlueEast

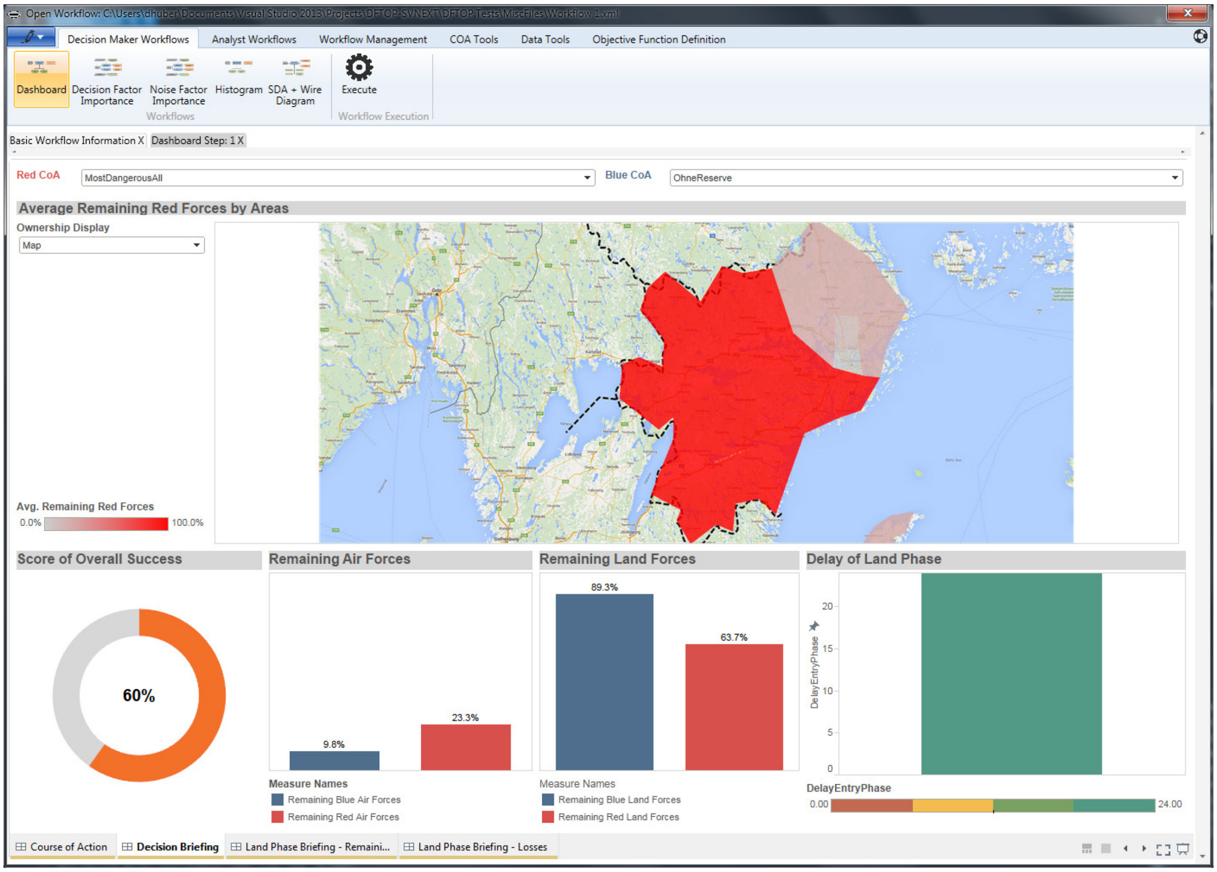
1. Defensive Counter Air Ops to maintain Airbases operational and support Land Forces
2. Defend (and Delay) Border Area NE
3. Hold and retain Stockholm City

MostLikely

1. Counter Air Ops to gain Air superiority
- Destroy Bogaland Airbases and Fighters
2. Seize Airbases Arlanda by Air Assault to fix Bogaland Forces and support Land Attack
3. Land Attack to Seize Stockholm area by
- 2 Divisions (Gävle – Uppsala - Stockholm)

Figure 4-35: Dashboard (COA).

On the OverallSuccess tab (Figure 4-36) the mean value of OverallSuccess is presented, as well as the mean of its composing MOE. If feasible, the MOE are presented on a map for better understanding. On this tab there is again the possibility to select different COA.



Open Workflow: C:\Users\dhuber\Documents\Visual Studio 2013\Projects\DFTOP-SVNEXT\DFTOP.Tests\MiscFiles\Workflow 1.xml

Red CoA: MostDangerousAll

Blue CoA: OhneReserve

Ownership Display: Map

Figure 4-36: Dashboard (OverallSuccess).

On the last tab (Figure 4-37) the average number of remaining forces still able to operate is presented. If the area of operation is separated into sub-areas, like in Figure 4-37, the respective values are presented in the form of a bar chart as well as a pie chart for each sub-area.

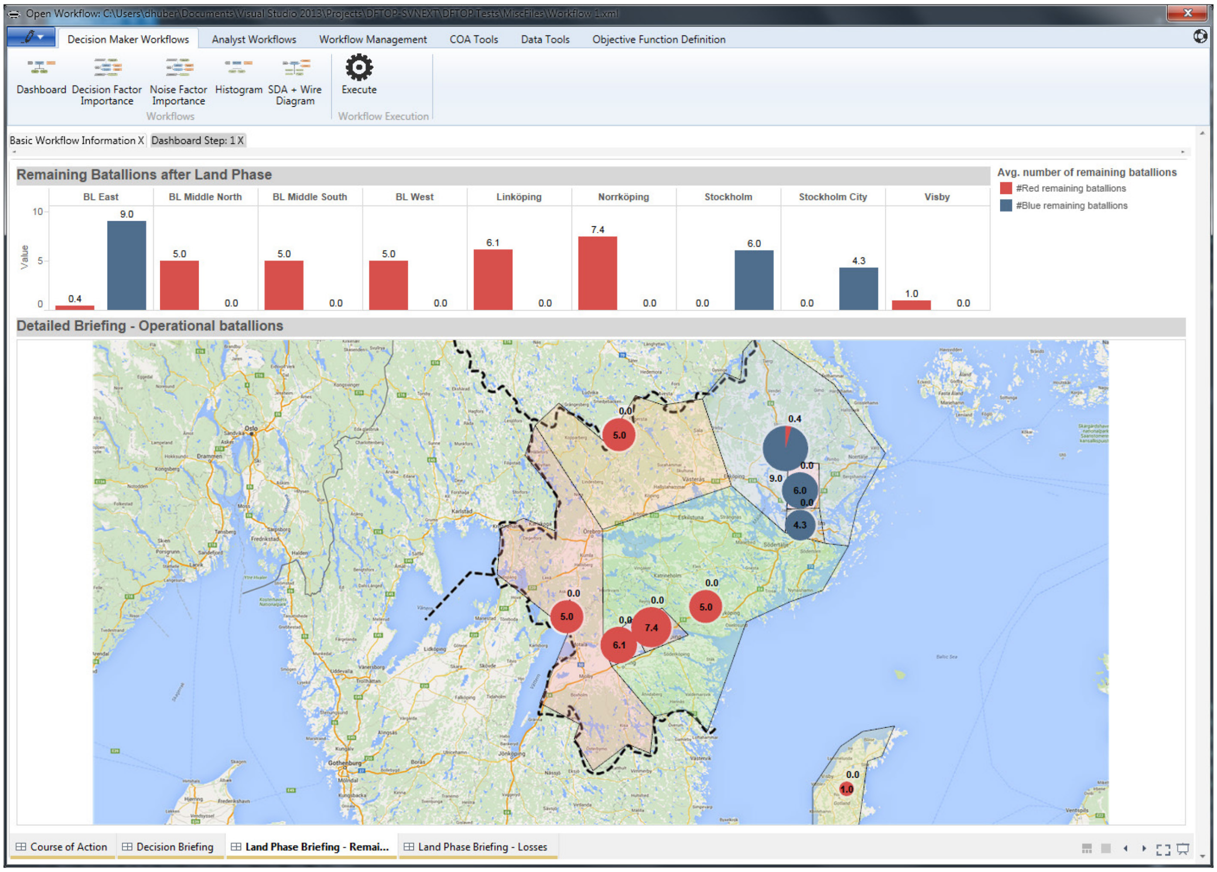

Open Workflow: C:\Users\dhuber\Documents\Visual Studio 2013\Projects\DFTOP-SVNEXT\DFTOP.Tests\MiscFiles\Workflow 1.xml
Decision Maker Workflows
Analyst Workflows
Workflow Management
COA Tools
Data Tools
Objective Function Definition
Dashboard
Decision Factor Importance
Noise Factor Importance
Histogram
SDA + Wire Diagram
Workflows
Execute
Workflow Execution
Basic Workflow Information X
Dashboard Step: 1 X
Remaining Batallions after Land Phase
Value
10
5
0
BL East
0.4
9.0
BL Middle North
5.0
0.0
BL Middle South
5.0
0.0
BL West
5.0
0.0
Linköping
6.1
0.0
Norrköping
7.4
0.0
Stockholm
0.0
6.0
Stockholm City
0.0
4.3
Visby
1.0
0.0
Avg. number of remaining batallions
#Red remaining batallions
#Blue remaining batallions
Detailed Briefing - Operational batallions
Course of Action
Decision Briefing
Land Phase Briefing - Remai...
Land Phase Briefing - Losses

Figure 4-37: Dashboard (Remaining Forces).

4.7 CONCLUSIONS

DFTOP is a tool that supports the Commander to evaluate operation plans, analysing a broad set of COA. The support is aligned with the COPD, here exemplified at the joint level, providing support for the JOPG in Phase 3b. This allows the Commander to get better insights into his operations, and make decisions based on much broader decision grounds. With DFTOP, the possibilities of quantitative simulation-based analysis are made readily available to decision makers and planners at the operational level.

DFTOP aids the JOPG to analyse the whole spectrum of feasible COA. This assists the JOPG in developing plans based on a robust and reproducible dataset, and makes objective recommendations to the Commander. This aids decisions based on much broader decision grounds in selecting the best COA to achieve the goal with minimum risk. In addition, every outcome can be traced back to the most important factors and their corresponding crucial values.

The tool is flexible, as open standardized interfaces ensure its interoperability with either simulation and/or analysis systems. With automated and reusable workflows, the analysis in the planning process becomes standardized, reproducible, traceable and objective, which helps the JOPG to perform the planning process in a more transparent and efficient way. This adds operational value by increasing the quality of the decisions.

The DFTOP prototype was demonstrated in a relevant environment at the *Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise* (CWIX) in 2016 and is planned to be used at CWIX 2017. The demonstration in 2016 was a milestone in establishing Technology Readiness Level 6 (TRL 6). The Bundeswehr Joint Forces Command followed the demonstration of DFTOP, and found it to be promising for operation planning decision support. After the successful demonstration of DFTOP at CWIX it was presented to the Multinational Joint Headquarters Ulm, led by Germany. They decided to perform further testing of DFTOP. A new demonstration at CWIX in 2017 will utilize another simulation model than described in this report, proving the flexibility of DFTOP and test and validate interoperability with the NATO planning tool in use: *Tool for Operational Planning Functional Area Service* (TOPFAS).

Experience from CWIX confirms that DFTOP successfully brings Data Farming into the *actionable* decision support domain, translating the results of the analysis to visualizations directly adapted to the decision maker's needs.

4.8 REFERENCES

[1] Hannay, J.E., Bråthen, K. and Hyndøy, J.I. (2015). On how simulation can support adaptive thinking in operations planning, in *Proceedings of the NATO Symposium on Modelling and Simulation Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence*, Munich, Germany, 15–16 October 2015, paper 18, pp. 1-14.

[2] Khimeche, L. and de Champs, P. (2004). M&S in decision support for course of action analysis, APLET, in *Proceedings of the NATO Symposium on Modelling and Simulation to Address NATO's New and Existing Military Requirements*, Koblenz, Germany, 7-8 October 2004, paper 4, pp. 1-22.

[3] Schubert, J., Moradi, F., Asadi, H., Luotsinen, L., Sjöberg, E., Hörling, P., Linderhed, A. and Oskarsson, D. (2015). Simulation-based decision support for evaluating operational plans, *Operations Research Perspectives* **2**:36-56. doi:10.1016/j.orp.2015.02.002.

[4] Veldhuis, G. and de Reus, N.M. (2016). The application of modelling and simulation in support of the operations process, in *Proceedings of the NATO Symposium on Ready for the Predictable, Prepared for the Unexpected – M&S for Collective Defence in Hybrid Environments and Hybrid Conflicts*, Bucharest, Romania, 20-21 October 2016, paper 13, pp. 1-20.

[5] Veldhuis, G., Keijser, B. and de Reus, N.M. (2017). Continued development of a concept to implement M&S in support of the operations process, in *Proceedings of the 35th International Conference of the System Dynamics Society*, Cambridge, MA, USA, 16-20 July 2017, to appear.

[6] Vensim. [Online] available: http://vensim.com (April 2017).

[7] JMP. [Online] Available: http://jmp.com (April 2017).

[8] Moradi, F. and Schubert, J. (2014). Simulation-based defense planning, in *Proceedings of the NATO Symposium on Integrating Modelling & Simulation in the Defence Acquisition Lifecycle and Military Training Curriculum*, Washington, DC, USA, 23-24 October 2014, paper 6, pp. 1-16.

[9] Kallfass, D. and Schlaak, T. (2012). NATO MSG-088 case study results to demonstrate the benefit of using data farming for military decision support, in *Proceedings 2012 Winter Simulation Conference*, Berlin, Germany, 9-12 December 2012, pp. 2481-2492.

[10] Hügelmeyer, P., Steffens, T. and Zöller, T. (2006). Specifying and simulating modern warfare scenarios with ITSimBw, in *Proceedings of the 2006 Winter Simulation Conference*, Monterey, CA, USA, 3-6 December 2006, pp. 1273-1279.

[11] Hügelmeyer, P., Schade, U. and Zöller, T. (2007). Application of BML to inter-agent communication in the ITSimBw simulation environment, in *Proceedings of the 2007 Winter Simulation Conference*, Washington, D.C., USA, 9-12 December 2007, pp. 1337-1343.

[12] Carey, S.A., Kleiner, M.S., Hieb, M.R. and Brown, R. (2001). Standardizing battle management language - A vital move towards the army transformation, in *Proceedings of the 2001 Fall Simulation Interoperability Workshop*, Orlando, FL, USA, 9-14 September 2001, pp. 1-13.

[13] Standard for: Military Scenario Definition Language (MSDL), SISO-STD-007-2008. Orlando, FL: Simulation Interoperability Standards Organization (SISO), 2008.

[14] Horne, G. and Seichter, S. (2013). Data farming support to NATO: A summary of MSG-088 work, in *Proceedings of the Symposium on M&S Support to Transitioning Forces and Emerged/Emerging Disruptive M&S Technologies*, Sydney, Australia, 17-18 October 2013, paper 14, pp. 1-10.

[15] Zanella, J.A. (2012). *Combat Power Analysis is Combat Power Density*. Fort Leavenworth, KS: School for Advanced Military Studies.

[16] Vieira, Jr., H. (2012). NOB_Mixed_512DP_template_v1.xlsx. [Online] Available: http://harvest.nps.edu (April 2017).

[17] Utkin, L.V. (2009). A new ranking procedure by incomplete pairwise comparisons using preference subsets. *Intelligent Data Analysis* **13**(2):229-241.

[18] Schubert, J. and Hörling, P. (2014). Preference-based Monte Carlo weight assignment for multiple-criteria decision making in defense planning, in *Proceedings of the 17th International Conference on Information Fusion*, Salamanca, Spain, 7-10 July 2014, paper 189, pp. 1-8.

[19] Schubert, J. (1995). On ρ in a decision-theoretic apparatus of Dempster-Shafer theory. *International Journal of Approximate Reasoning* **13**(3):185-200.

[20] Schubert, J., Johansson, R. and Hörling, P. (2015). Skewed distribution analysis in simulation-based operation planning, in *Proceedings of the 9th Operations Research and Analysis Conference*, Ottobrunn, Germany, 22-23 October 2015, paper 5, pp. 1-14.

[21] Shannon, C.E. (1948). A mathematical theory of communication, *The Bell System Technical Journal* **27**(3/4):379-423, 623-656, July/October 1948.

[22] Parallel coordinates. [Online] Available: https://en.wikipedia.org/wiki/Parallel_coordinates (April 2017).

[23] Schubert, J. and Hörling, P. (2016). Decision support for simulation-based operation planning, in *Proceedings of SPIE Volume 9848 Modeling and Simulation for Defense Systems and Applications XI*, Baltimore, USA, 17 April 2016, paper 984805, pp. 1-20. doi:10.1117/12.2222172.

Chapter 5 − DATA FARMING DECISION SUPPORT FOR CYBER DEFENCE

5.1 INTRODUCTION

Data farming has been in continuous development for nearly two decades. During this period, a multitude of military questions have been examined using the data farming process. Developing techniques along with new modelling and simulation efforts have allowed for decision support to include the examination of vast possibility spaces and the identification of outliers that can be significantly informative. Support to decision makers has progressed in many contexts to include the three-year NATO Modelling and Simulation Task Group, MSG-088: "Data Farming Support to NATO", which is described in detail in Chapter 3.

The work described in this Chapter seeks to leverage past work in data farming, the recent documentation of the data farming process achieved by MSG-088, and NATO ACT capabilities development work to orchestrate the use of data farming to address current and emerging NATO cyber security challenges.

ACT participated in the formation of syndicates within MSG-124 addressing application areas to be undertaken by this task group. Here we describe the work of the Cyber Defence Syndicate of MSG-124.

The cyber study team involved other cyber experts from the attending nations in order to ensure the results would be as comprehensive as possible. This part was exercised at international workshops hosted near Washington DC in June 2013, October 2015, and March 2017 and hosted in Finland in January 2014, March 2015, and October 2016. Also, in February 2016 the University of Catania, Italy, hosted an international workshop. These international workshops with the participation of the larger data farming community served to enhance the methodology and application of data farming along with the MSG-124-only task group meetings that took place in September 2013 in Istanbul, June 2014 in Munich, June 2015 in Stockholm, October 2015 in Ottawa, June 2016 in Oslo.

The Cyber Team used data farming techniques to explore solutions to improve NATO's resilience to cyber-attacks. The scenarios considered spanned the threat spectrum, ranging from lone hackers to cyber espionage organizations. The team leveraged a NetLogo model [1] developed by the team in working meetings 1 through 4 of MSG-124 [2], [3], and evolved the model as its behaviours and the needs of the stakeholders were better understood. The initial analyses focused on exploring the value of various network topologies and organizations, firewall policies and intrusion detection systems.

The overall goal of this syndicate is to leverage the current research, develop a suitable simulation, and explore possible scenarios through data farming that could facilitate the understanding of some aspects of cyber defence important to NATO. The supporting tasks for this goal were as follows:

- Conduct background research and work in the area of the application of data farming methodology to cyber security, perform exploration work up to and including the data farming workshops, and build on the workshops results on the application of data farming to cyber security questions. The models and the scenarios developed allowed for the exploration of the parameter space in a data farming environment.
- Define questions within the cyber defence area in conjunction with cyber defence experts at ACT, within the MSG-124 nations, and in general. Assist in the analysis and iterative exploration of "What-If?" questions to reveal the landscape of possibilities inherent in the scenarios and enable the study of any "outliers" that are discovered.

- Provide modelling and simulation support for various cyber defence questions. The simulation developed used the NetLogo model, open source software that could be easily shared by work teams such as the MSG-124 Cyber Defence Syndicate.

Quantitative analysis is predicated on a set of measurable relations between the factors of interest and the metrics that determine performance and effectiveness of a potential solution in a given scenario (i.e., combination of factors). For this purpose, a useful abstraction − i.e., a model − is required to capture these relationships.

Networks are complex dynamic systems, and understanding how to best protect them and the information they contain and transmit only makes the problem more difficult. The system behaviour of networks is well-suited for event driven modelling, because of their technological characteristics and the actions of the human operators using, maintaining, and attacking them.

There is a wide range of metrics that can be used to assess the performance and effectiveness of a secure network. The information security (InfoSec) CIA paradigm (Confidentiality, Integrity, and Availability) serves as a well-established and comprehensive reference from which to derive the set of measures, but it does not provide a universally ideal framework. Therefore, it is important to understand the strengths and limitations of this approach.

The team mainly used the following metrics:

- Number of attackers sensed.
- Number of compromised data files. In order to evaluate such metric it was assumed that each server stores a certain number of files containing operationally relevant information. When an attacker achieves control of a data server, all files stored by such server are considered compromised.
- Availability of the network service. Such parameters will be evaluated as the probability that a host can reach a server offering the desired service or piece of data. Calculation of such a metric can be expensive from a computational point of view because it requires verifying that a path exists and is operational between the requesting host and one of the servers offering the requested service or storing the needed data. Algorithms exist (Bellman-Ford) that perform such operation with complexity that increases linearly with the product between the number of nodes and the number of links in the network. Due to time and resource constraints a full implementation of the availability assessment could not be produced, but the "availability" of the network is estimated as the fraction of systems that are "up", disregarding intermediary systems that would be required to connect them to the other parts of the network.

The syndicate developed the *Data-farmable Agent-based Cyber Defence Assessment Model* (DACDAM) as an extensible proof-of-concept model to tests the ideas of Data Farming and how they may apply to supporting decision making. It is critical that:

1) The model is easy to distribute;
2) It could be extended by others in and outside the Group; and
3) It does not violate any export control restrictions.

For this reason the team decided to use an open-source framework and develop a model from the ground up to address the first and third requirements. The agent-based[1] framework NetLogo was selected because of its lower

[1] There are various modeling paradigms (e.g., system dynamics, discrete event simulation) that could have been used, but based on the experience of the team, and the initial needs of project, the team decided to use an agent-based time step approach.

barrier of entry (it was developed to teach agent-based programming to high-school students), it is open source, and counts with a very active development team and user community.

The agent-based model focused primarily on the network and the cyber actors, but it is critical that the effects of network attacks be linked to the operational capabilities of a force like NATO. For this purpose the team devised a risk-based series of mappings to capture the effect that compromising and denying certain services would have on various operational tasks. These tasks were then aggregated into higher level groupings that reflected the overall mission a force may be performing in a theatre of operations. The services were mapped to systems on the network. The mappings were integrated into DACDAM to allow users to simultaneously assess the network and operational metrics.

DACDAM was not developed with the intention of capturing every possible cyber threat. It does not explicitly address natural or inadvertent user errors, instead it is focused on intentional attacks, in particular, penetration attacks. The insider threat is not explicitly modeled, but it could be included by integrating a formal insider threat framework. [4]

The model, its elements, and the overall modelling effort is described in more detail in Section 5.3. Section 5.4 describes the initial data farming efforts with DACDAM and some of the preliminary results. Before diving into the details of the model, the authors would like to highlight some of the potential benefits of including cyber defence as part of the planning process.

5.2 CYBER DEFENCE AS A PART OF THE PLANNING PROCESS

The Data Farming approach can be useful when planning an operation within a variety of processes. One example is within the important Federated Mission Network (FMN) construct. [5] Modelling itself will improve the defender's own familiarity/knowledge and understanding of the network, its components and interactions between subsystems, i.e., it supports understanding of a complex system of systems environment. Secondly, it facilitates understanding of complex sub-system behaviours that contribute to the overall mission level cyber security. Thirdly, it may pinpoint or confirm vulnerabilities or weak spots in the overall network and thus direct additional security measures to be implemented to those.

When planning military operations, cyber factors need to be considered at every phase of the planning process, as the use and dependence of cyberspace grows:

- What is this Cyber Defence planning process about?
- Description of the need in the planning process.
- Potential benefits by applying Data Farming in the process. What advantages can we offer?

This section is based on the handbook and guidelines for integrating cyber defence into the operational planning process. [6], [7] These documents were developed to aid in identifying how cyber aspects can be integrated into the planning process at the operational level. The guidelines are intended for use in a Joint Operations Planning Group (JOPG) and follow the process described in the Comprehensive Operational Planning Directive v2.0 (COPDv2.0).

The planning process comprises the following phases:

1) Initial Situational Awareness of Potential/Actual Crisis.

2) Operational Appreciation of the Strategic Environment.

3) Operational Estimate:
   a) Mission Analysis; and
   b) Courses of Action Development.

4) Operational Plan Development:
   a) Operational CONOPS Development; and
   b) Operational OPLAN Development.

5) Execution.

6) Transition.

The main cyber-related questions for COPD JHQ Phases 1 – 4 are listed in Table 5-1. The terms cyber factors/ aspects refer to circumstances where the cyber domain may impact the conduct of military operations.

Table 5-1: Main Questions Related to the Cyber Domain in COPD JHQ Phases 1 – 4.

Phase	Main Questions Related to the Cyber Domain
Phase 1 Initial Situational Awareness of Potential/Actual Crisis	How do the actors make use of the cyber domain to pursue their interests? What characterizes the actors' Cyber Key Terrain?
Phase 2 Operational Appreciation of the Strategic Environment	How do strategic cyber threats affect operations at the operational level? How do practical aspects related to coordination and organization affect strategic Military Response Options?
Phase 3a Mission Analysis	How do cyber factors affect the operation? What efforts could be made to reduce unfortunate consequences?
Phase 3b Courses of Action Development	How do cyber factors affect COAs? When and where in the operation is a network or a cyber asset critical to the accomplishment of the operation? What cyber defence activities should be synchronized with other activities? What cyber defence considerations should be de-conflicted and coordinated with other considerations?
Phase 4a Operational CONOPS Development	What cyber factors are important to address in the State of Requirements? What aspects should be described in a Cyber Defence Annex?
Phase 4b Operational OPLAN Development	Who should have the authority to release information to external partners? What are the best mechanisms for optimal information-sharing with external partners? How should cyber defence units be organized in the C2 plan?

All phases are, of course, important, but Phases 1 and 2 provide input for the Data Farming process, in particular Rapid Scenario Prototyping. Also, in the Mission Analysis phase (3A) we assess how cyber factors affect the operation and what measures can be taken to mitigate negative consequences.

5.2.1 Cyber Situational Awareness

The purpose of cyber SA is to define operational status, possibilities and limitations and should also include own vulnerabilities. Cyber expertise in a Joint Operations Planning Group (JOPG) is necessary in order to recognize how various cyber effects are relevant.

Comprehensive Preparation of the Operational Environment (CPOE) includes information on key terrain, main actors, their capacities and intentions. Cyber elements of the CPOE deal with appreciating the nature of relevant cyber factors and what threats and risks they pose to the mission. Consequently, cyber threats need to be assessed with an emphasis on actors' intentions and capacities to challenge our freedom of action in our own cyber domain.

Cyberspace has a wide range of actors with different levels of education, training, skills, motivation and capacity. [8] Threat actors fall into six broad categories: nation states, terrorists, criminals, patriotic hackers, "hacktivists", and insiders. [9] Each group can vary greatly in terms of sophistication, scale and motive and may pose differing types of threat.

Cyber threats to military operations can broadly be divided into two types. Computer Network Attack (CNA) is defined as "Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or network itself." [10] Computer Network Exploitation (CNE) is defined as "Action taken to make use of a computer or computer network, as well as the information hosted therein, in order to gain advantage." [10]

Other threats to freedom of action in own cyber domain include:

- Kinetic attacks on the physical components of the cyber domain, including electromagnetic pulse.
- Electronic warfare.
- Third party infrastructure on which the mission depends.
- Agents and insiders who cause damage or gain access to systems or assets.

Lockheed Martin coined the term "cyber kill chain" [11], to describe the seven phases comprising offensive cyber activity [9]:

- Understanding;
- Payload development;
- Delivery;
- Exploitation;
- Installation;
- Command and control; and
- Desired effect created.

5.2.2 Courses of Action

The way cyber defence comes into play in COA development depends heavily on the scenario, the operation's objectives and other actors.

The Handbook for Integrating Cyber Defense into the Operational Planning Process v1.0 states that due to a lack of empirical grounds for precisely predicting the impacts of cyber factors, wargaming is an important activity for trying them out in a specific context.

Critical events and phases are of importance when including cyber defence in the COA-phase. Wargaming such events and situations may reveal how cyber defence can be utilized to mitigate threats. Furthermore, opposing COAs may include offensive cyber operations against our networks, and should be included.

Wargaming may provide answers to the following questions:

- How can adversaries challenge our freedom of action in our own cyber domain?
- What happens when one of our critical capabilities is targeted?
- Is there anything we could do to proactively counter unfortunate situations?

To cope with the complexity of the cyber domain, simulation-based decision support could be utilized, as illustrated later in this chapter with the use of data farming, DACDAM, and DFTOP.

5.2.3 Considerations for the Joint Planning Process

Applying data farming to cyber defence with a data visualization as provided by DFTOP could assist planners to assess questions. The handbook raises the following questions to be addressed in operational planning:

- What are the technological consequences of a given change to the information systems?
- What are the operational consequences of any technical implementation?
- Does the increase in security measures outweigh the corresponding loss of operational effectiveness?
- What efforts can be initiated to mitigate the loss of operational effectiveness?

These questions are essential to mission planners, but they did not guide the design of the DACDAM model as the model and the handbook were being developed concurrently. In consideration of this limited information, the model was designed to assess the validity of applying data farming to cyber defence.

5.3 DATA-FARMABLE AGENT-BASED CYBER DEFENCE ASSESSMENT MODEL

The work of this syndicate was focused on the cyber defence procurement and policy decision makers. Although the model itself depicts an operational environment, higher level decision makers can use a lower level model to understand the implications of their options [12]. This problem is challenging and requires a significant level of effort on part of organizations to understand the problem and potential solutions [13]. The team developed DACDAM to assess the applicability of data farming in support of the decision making process.

5.3.1 Purpose

The question of interest is: “how should organizations invest their resources to maximize their ability to defend themselves against cyberattacks?” This question opens the door to a variety of issues and concerns. The most salient ones are listed below:

- What things can a resource investment in cyber defence impact?
- How do we measure the impact of a cyberattack?
- What things are not under the control of the organization?
- What things are under the control of the organization?
- How do attackers interact with one another?
- How do system administrators interact with one another?
- How much freedom is in modifying the policies of the organization?

These questions align themselves well with the principles of data farming, in that one should identify:

1) The metrics of interest;
2) The control factors;
3) The noise factors; and
4) The primary behaviours of the system of interest.

Quantitative analysis is predicated on a set of measurable relations between the factors of interest and the metrics that determine performance and effectiveness of a potential solution in a given scenario (i.e., combination of factors). For this purpose, it follows that a useful abstraction − i.e., a model − is required to capture these relationships.

Networks are complex dynamic systems, comprised of a large number of entities, that act nonlinearly (small changes in a factor can have a large effect on another, and vice versa) through a non-trivial set of connections (the connections are not fully random nor perfectly ordered), and the entities comprising the network modify their states based on the actions of other entities and their internal rules as they imperfectly and myopically observe their surroundings. The system’s behaviour is by its very nature discrete and event driven, and is dictated by the technological characteristics of the network and the actions of the human operators using it, maintaining it, and attacking it.

5.3.2 Related Efforts

As cyber security is a particularly large field of study, numerous studies have been performed on different ways of modelling attacks, responses, and defence [14]. Despite the idiom that security through obscurity is not desirable, an argument can be made that all security is ultimately obscurity because even the secret keys are still obscured data [15]. Systems can be deeply compromised, all the way to cryptographic keys, thus defenders must be highly responsive, rapidly update and refresh their systems, and minimize costs for responsiveness in order to have a resilient system [16].

According to the Verizon data breach report [17], a widely read and cited report in cyber security industries, the vast majority of breaches that have occurred in the public sector are results of malicious actors using software backdoors, malware, and phishing(social) attacks. The relationships of the actions of using these attack vectors with the network attributes affected over 100,000 incidents has been analysed by Verizon and is shown in the following figure.

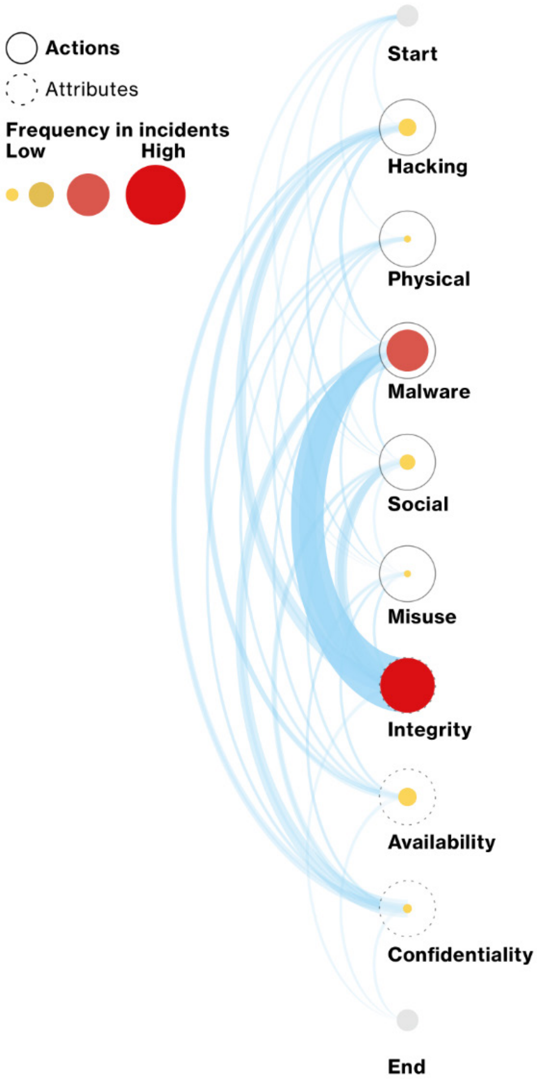


Figure 5-1: Actions and Attribute Relationships in 100,000 Real-World Cyber Incidents [17].

5.3.3 Metrics

There is a wide range of Measures Of Effectiveness (MOEs), also referred to as metrics, that can be used to assess the performance and effectiveness of a secure network. The information security (InfoSec) CIA paradigm shown in Figure 5-2 serves as a well-established and comprehensive reference from which to derive the set of measures, but it does not provide a universally ideal framework [18]. Therefore, it is important to understand the strengths and limitations of this approach.

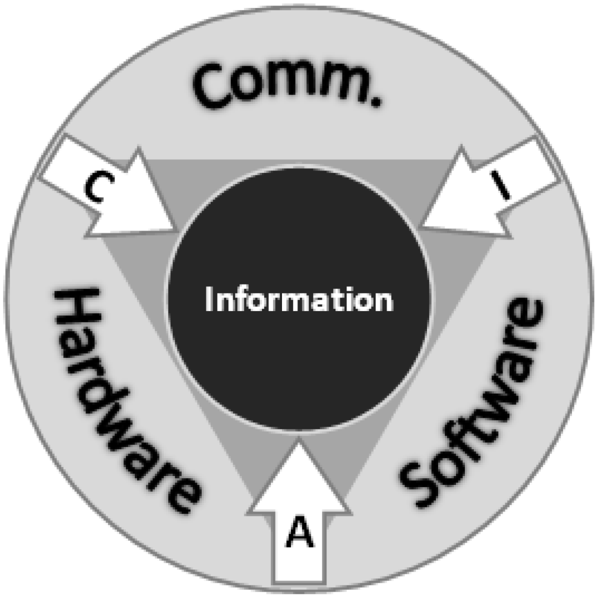


Figure 5-2: The Confidentiality-Integrity-Availability Information Security Paradigm [18].

The CIA paradigm is based on the three concepts described below:

- Confidentiality (C): The ability to grant access to authorized users and deny access to unauthorized users;
- Integrity (I): The ability to guarantee that some information or message hasn't been manipulated; and
- Availability (A): The ability to access information or use services at any moment we demand it, with appropriate performance.

The first two concepts are concerned with protecting the information, while the third ensures that the systems provide the necessary services for the users. These two key concepts form the basis for the metrics of the model. These two concepts must be traded off, as maximizing confidentiality and integrity negatively impacts availability. To illustrate this concept, one can think of an extremely secure system where the information is so protected, locked down to such a degree, that its availability is extremely limited, as only a few users can physically access it, and only after extensive efforts and commitment of time.

The CIA paradigm is nonetheless highly abstract and for the purposes of this paper just serves as a means to classify the types of goals for maintaining a secure network. The authors recognize that the focus on effects rather than causes makes the CIA paradigm not scientific for purposes of analysing attacks, but this is not the purpose of using this framework. The paradigm can also be used to categorize the elements of a network, namely the hardware, software and communications systems.

A final note regarding the metrics is that they will be time dependent, for example the number of attackers sensed, or the amount of compromised data. This makes the analysis more difficult and impedes the understanding of large option spaces, because analysts must understand these time domain results for each combination of interest. For this reason, it is necessary to condense these metrics to single value scalars. It is possible to record the last value, but because most of these are not monotonically increasing, this is not a suitable approach as it could potentially vary depending on where the simulation was terminated. Another approach is to take an average, but averages do not capture the variance of a metric, which is important when analysing the risk of an option, as it is not the mean amount of data that was compromised that is of interest, but an understanding of the worst case scenarios, e.g., with 95% confidence, how much data was compromised? This requires the analysis to sort the observations after a warm up period has been removed (as notionally described in Figure 5-3 with the distribution in green for the metric 'attackers sensed'). Since attackers sensed is a "higher is better" metric, we are interested in the lower tail (right tail) so we can state with 95% confidence, these many attackers will be sensed in this scenario. This approach was replicated for the three main metrics of interest derived from the CIA paradigm.

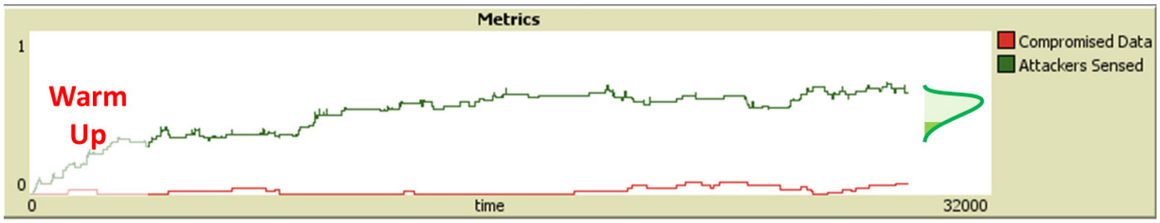


Figure 5-3: Statistical Derivation of the Metrics.

5.3.4 Model Parameters

The way the model parameters, or factors, can also be informed by the CIA paradigm by decomposing the elements that compose a secure information system, i.e., hardware, software and communications. For the purposes of this model, a few parameters that characterize the hardware, software and communications elements have been selected. The selection of these elements was informed by NATO's perceived tradespace and concepts and ideas communicated by the subject matter experts from the nations. The model was intended to demonstrate how data farming can help decision makers identify options within the DOTMLPF-I (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability) spectrum. The factors can either be controllable or non-controllable (i.e., noise factors). The list of major DACDAM model parameters is presented in Table 5-2.

Table 5-2: Major Model Parameters.

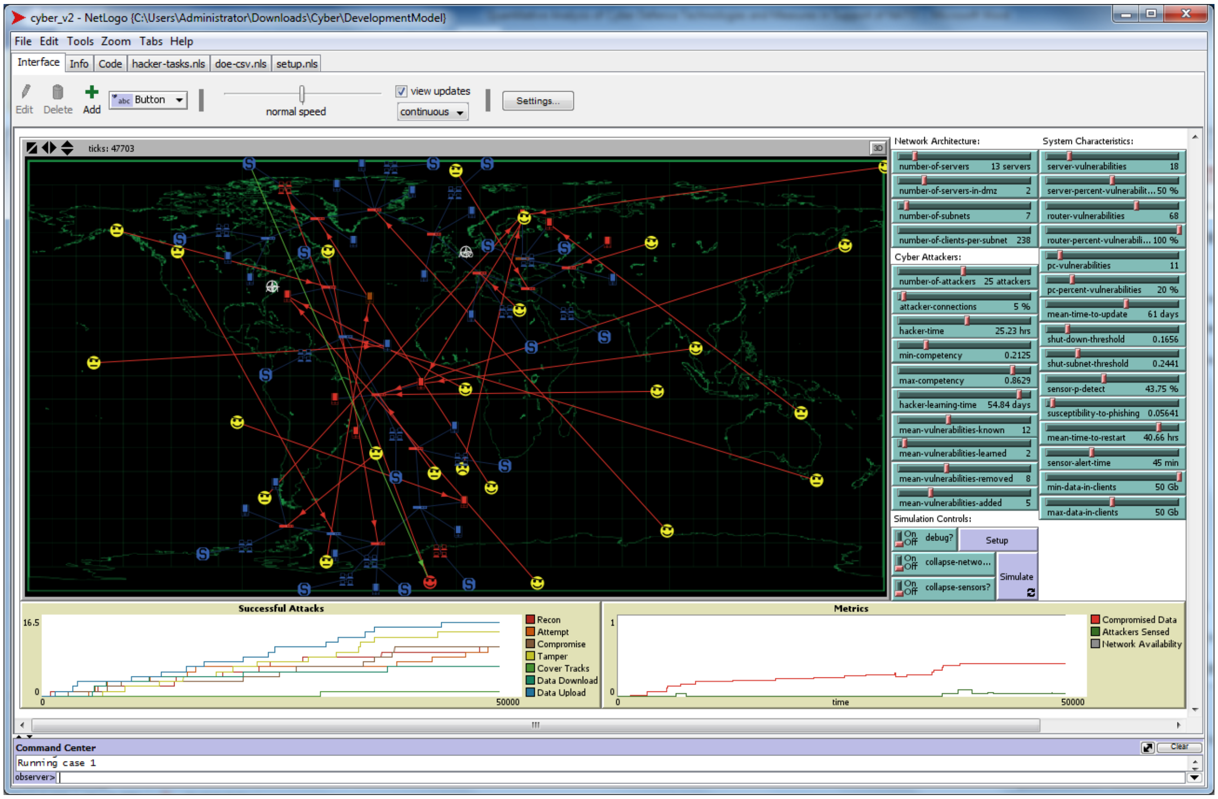
Name	**Unit**	**Description**	**Factor Type**
number-of-servers	int	The number of servers in the network.	Facilities
number-of-servers-in-dmz	int	The number of servers that are in the demilitarized zone. This value can range between 0 and the number-of-servers.	Doctrine
number-of-subnets	int	The number of subnets in each of the networks.	Facilities
number-of-clients-per-subnet	int	The average number of clients in each of the sub networks.	Organization
server-vulnerabilities	int	Number of vulnerabilities that exist for servers.	Noise
server-percent-vulnerabilities	%	Fraction of vulnerabilities present in any one server. Used to model application/vendor commonality.	Noise, Doctrine, Facilities

Name	Unit	Description	Factor Type
router-vulnerabilities	int	Number of vulnerabilities that exist for the routers/switches.	Noise
router-percent-vulnerabilities	%	Fraction of vulnerabilities present in any one router/switch. Used to model application/vendor commonality.	Noise, Doctrine, Facilities
pc-vulnerabilities	int	Number of vulnerabilities that exist for the clients in the subnets.	Noise
pc-percent-vulnerabilities	%	Fraction of vulnerabilities present in the clients inside a subnet. Used to model application/vendor commonality.	Noise, Doctrine, Facilities
mean-time-to-update	days	Average time it takes for the network to issue an update.	Doctrine, Training
mean-vulnerabilities-removed	int	Average number of vulnerabilities removed by any update.	Doctrine, Training
mean-vulnerabilities-added	int	Average number of vulnerabilities added by any update.	Noise
shut-down-threshold	%	Percentage of sensors that have to issue an alarm before the system administrator will shut it down.	Doctrine
shut-subnet-threshold	%	Percentage of sensors that have to issue an alarm before the system administrator will shut down the affected subnets.	Doctrine
sensor-p-detect	%	Sensor probability of detecting an attack.	Materiel
susceptibility-to-phishing	%	Probability that any user of the subnet is susceptible to a phishing attack.	Training, Personnel, Leadership
mean-time-to-restart	hrs	Average time it takes for the system administrators to restart the elements of the network after the shutdown.	Training, Doctrine, Materiel
number-of-attackers	int	The total number of attackers (hackers).	Noise
mean-attack-time	hrs	Average time it takes a hacker to perform an attack. This is the nominal time that is extended/contracted by the different tasks the hacker performs.	Noise
min-competency	%	Minimum competency that the hackers possess. This is a non-dimensional factor between 0 and max-competency.	Noise
max-competency	%	Maximum competency that the hackers possess. This is a non-dimensional factor between min-competency and 1.	Noise

Name	Unit	Description	Factor Type
hacker-learning-time	days	Average time it takes for the hackers to learn new vulnerabilities. This is the mean value from an exponential distribution.	Noise
mean-vulnerabilities-known	int	Average number of vulnerabilities the hackers may know at time zero.	Noise
mean-vulnerabilities-learned	int	Average number of vulnerabilities the attackers learn each time they elapse their randomly generated time to learn.	Noise

5.3.5 Approach

The approach consisted of developing an extensible agent-based model on which to conduct stochastic simulations. It was considered paramount that the model should be easy to distribute and share with the nations, forcing the data and processes modelled to remain unclassified and the framework to be freely distributable. NetLogo was selected as it is a free agent-based modelling framework with a wide community of users and an ever-growing list of extensions and features. Figure 5-4 below is a screen capture of one version of DACDAM.



ticks: 47703

Network Architecture:

number-of-servers 13 servers
number-of-servers-in-dmz 2
number-of-subnets 7
number-of-clients-per-subnet 238

Cyber Attackers:

number-of-attackers 25 attackers
attacker-connections 5 %
hacker-time 25.23 hrs
min-competency 0.2125
max-competency 0.8629
hacker-learning-time 54.84 days
mean-vulnerabilities-known 12
mean-vulnerabilities-learned 2
mean-vulnerabilities-removed 8
mean-vulnerabilities-added 5

Simulation Controls:

On Off debug?
On Off collapse-netwo...
On Off collapse-sensors?

System Characteristics:

server-vulnerabilities 18
server-percent-vulnerabilit... 50 %
router-vulnerabilities 68
router-percent-vulnerabili... 100 %
pc-vulnerabilities 11
pc-percent-vulnerabilities 20 %
mean-time-to-update 61 days
shut-down-threshold 0.1656
shut-subnet-threshold 0.2441
sensor-p-detect 43.75 %
susceptibility-to-phishing 0.05641
mean-time-to-restart 40.66 hrs
sensor-alert-time 45 min
min-data-in-clients 50 Gb
max-data-in-clients 50 Gb

```
Running case 1
observer>
```

Figure 5-4: Screen Capture of the NetLogo User Interface Running DACDAM.

5.3.6 Elements of the Model

This simulation is not an attempt to model every possible cyber threat. It is focused on intentional attacks, in particular, penetration attacks. It does not currently address natural or inadvertent user errors. The simulation was composed of three primary elements:

1) The network;
2) The system administrator; and
3) The attackers.

The sections below will describe the three elements in more detail.

5.3.6.1 The Network

The modelled network is composed of three primary elements, routers/switches, servers and subnets with terminals. All the networks in the model have systems in the Demilitarized Zone (DMZ)[2], with at least one router which serves as the portal between the DMZ and the Wide Area Network (WAN), and a user-specified number of servers. The final element is the sensors to detect the cyber-attacks. The sensor model is general and does not differentiate between the different types of cyber-attack sensors, e.g., NetFlow, honeypots, Samhain. The sensors are associated with the other elements of the network and can detect attacks based on their probability of detection. The model currently does not allow attackers to exploit the sensors, as evidenced by recently published vulnerabilities [19], which should be noted as a potential future development for DACDAM.

The routers (or switches) connect other elements of the network, and even though firewalls are not modeled explicitly, when attackers attempt to penetrate the network, they must be able to exploit a vulnerability on these nodes before they can compromise other parts of the network. If one portion of the network can be easily accessed from another, a direct connection between these two elements can be created.

The network generation algorithm can currently create bus, tree, star, ring, fully connected, mesh or line networks. Bus networks were deemed the most representative for the applications of interest by the groups of subject-matter experts (SMEs) consulted. The algorithms follow a process for creating the networks, e.g., the bus networks are generated by creating the world facing router first, and then sequentially adding routers for each subnet specified in series and finally the servers are randomly associated with the routers except for the number of routers that are placed in the DMZ. The algorithms for generating the network can be modified if required. It is also possible to load a specific network from a network input file, an example of which is shown below. The value of the item is a numeric representation of the utility an attacker would gain if that item is compromised.

Table 5-3: Example of a Partial Custom Network Definition Input File.

ID	Type	Value	In the DMZ	Connected To
1	Server	0	TRUE	2
2	Router	0	TRUE	3
3	Router	0.35	FALSE	2

[2] The DMZ is modeled as an area that can accept traffic from the general internet. Real life network implementations may have more security layers than what is currently modeled in DACDAM.

ID	Type	Value	In the DMZ	Connected To
4	Subnet	0.15	FALSE	3
5	Sensor	0	FALSE	3
6	Server	0.65	FALSE	3
7	Subnet	0.85	FALSE	3

5.3.6.2 The System Administrator

The System Administrator (SA) is currently modelled using a simple algorithm using the shutdown thresholds specified and the alarms communicated by the sensors. The system administrator monitors the sensor alarms and either shuts down affected subnets, or the entire network depending on the number of alarms and the threshold parameters (i.e., shut-down-threshold and shut-subnet-threshold).

The following example illustrates the activity of the SA. The SA monitors a network of 4 subnets with a total of 5 sensors, with a shut-subnet-down threshold of 18% and a shut-down-threshold of 28%. As an attack is detected, the sensors will trigger an alarm. If one sensor issues an alarm, that represents 20% of the sensors, which will force the SA to shut down the affected subnets. If two sensors issue an alarm, it will trigger a total network shutdown as that represents 40% of the network.

The logic of the SA is simple, but provides a first iteration for the logic that a reactive administrator may follow. It could clearly be improved if the sensors were specialized and the risk of the different activities that the specialized sensors could detect was defined. This would produce more accurate reactions. Ideally, sensor fusion algorithms could be evaluated, potentially defining requirements for data fusion algorithms, such as accuracy, false positive and negative rates, etc.

5.3.6.3 Attackers

There are multitudes of ways that the actions of cyber attackers can be modelled. The key concept is to do so in the simplest manner possible while still capturing the primary behaviours and traits. A model developed by de Souza et al. provides a series of tasks that hackers follow and all their potential sequences. Figure 5-5 reproduces the task model by de Souza *et al.* [20], where the blocks represent the tasks hackers perform and the arrows the transitions. For the model, each hacker follows a different strategy by having different probabilities for transitioning between states. A multitude of cyber-attack models were reviewed, including the Hacker Attack Representation Model (HARM) by Karpati *et al.* [21], generic attack graphs, e.g., [22], and agent-based models, e.g., [23], and other procedural models, e.g., [24]. The main drawback of these approaches for this particular application is the level of detail and complexity required to represent cyber-attacks. The De Souza *et al.* model provides a simple framework on which more complex representations for cyber attackers' activities can be modelled. We employed a rapid-prototyping methodology of modelling with the simplest model possible and adding complexity as needed.

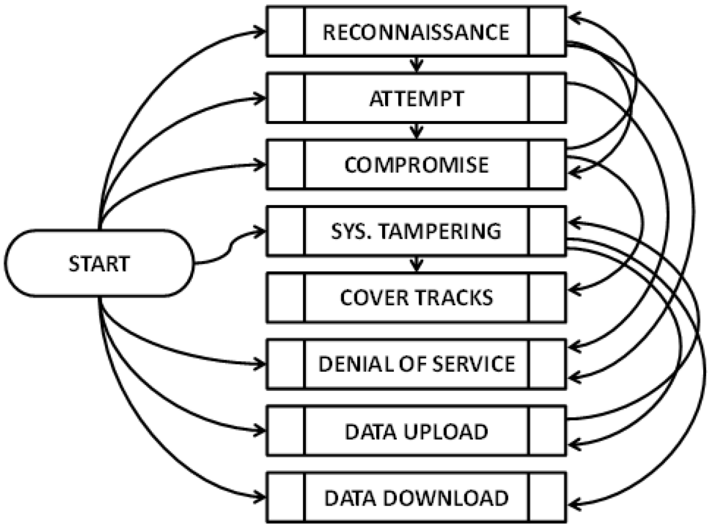


Figure 5-5: Attacker Task Model (based on Ref. [20]).

5.4 DATA FARMING WITH DACDAM

The data farming effort using DACDAM concentrated on demonstrating potential analyses that could be performed using the model and data farming techniques. The results are not meant to be predictive in nature, but illustrative of the types of trade-offs that may be studied. The ultimate goal is to provide insight to decision makers as to which protocols, topologies and configurations of the systems produce the most secure networks. Alternatively, the model can indicate under which conditions which combination of network control factors produce the best results. This can help decision makers' downselect combinations to be considered for further analysis. Additionally, decision makers can gain a better understanding of parameters that drive the behaviour of the model. The overarching process is a simplified version of the data farming loop-of-loops and is presented in Figure 5-6. The authors, with support from subject matter experts, iterated through this cycle half a dozen times. The analyses presented below will highlight some of the results discovered through a few of the later iterations.

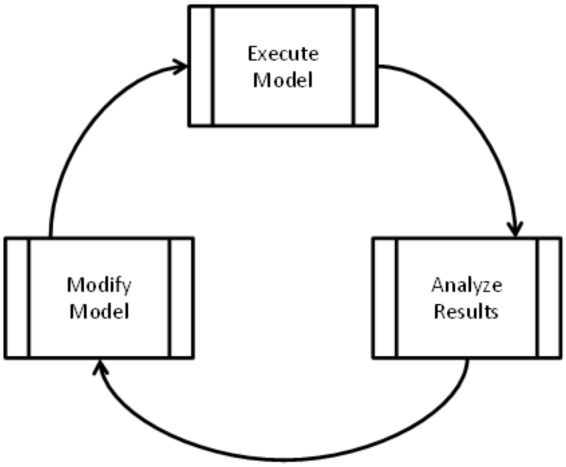


Figure 5-6: The Feedback Process and Evolution of the Model.

5.4.1 Setting Up DACDAM for Data Farming

As described in Chapter 3 of this Report, the centre of the data farming methodology is based on the question or questions at hand. Then data farming is used to try to achieve insights into this question base using an iterative approach with six realms. The first realm, rapid prototyping, works with the second realm, model development, iteratively in an experiment definition loop. A rapidly prototyped model provides a starting point in examining the initial questions and the model development regimen supports the model implementation, defining the resolution, scope, and data requirements. The third realm, design of experiments, enables the execution of a broad input factor space while keeping the computational requirements within feasible limits. High performance computing, realm four, allows for the execution of the many simulation runs that is both a necessity and a major advantage of data farming. The fifth realm, analysis and visualization, involves techniques and tools for examining the large output of data resulting from the data farming experiment. The final realm, collaborative processes, underlies the entire data farming process and these processes will be described in detail in this section.

One scenario generated is a generic multinational peacekeeping operation with possible escalation to violence and even to peace enforcement at times thus enabling potential cyber threats to escalate in scope and impact. Secondly, this scenario is based on the assumption of the Federated Mission Network that potentially would be set up by a host nation (NATO), framework nation (EU), or by a third entity (e.g., NCIA/NATO), and to which national network segments (enclaves) are interconnected. This also implies joint security management or administration (e.g., Security Accreditation Board) to which already approved members of the federated network contribute, in a similar fashion as being prepared for NATO Federated Mission Networks [5]. Operations (and the network operations) are supported by strategic reach-back capability (potentially NCIRC in NATO, EU Intcen/EUMS in EU context).

A number of national network segments were modelled in the scenario. Details and parameters of the scenario are generic and thus operational use of the model may require significant amount of research and compilation of statistics to produce parameter sets that are relevant, valid and verifiable within the operational context in question.

In one data farming exploration of this illustrative scenario, the syndicate decided to focus on one question: *What factors are the most crucial to each of the metrics?* The team decided to use a robust screening design [25] to assess the impact of 14 factors. This type of design was selected because of the minimal number of cases required and its ability to minimize the confounding of second-order effects with first-order effects, i.e., interactions between factors. The factors and their units and ranges are shown in the table below. The cells are coloured by the minimum and maximum value of each column to provide a visually friendlier indication of the combinations included.

The experimental design consisted of 29 cases generated by the robust screening design approach. Each case was repeated 150 times, for a total of 4,350 cases. The operations metrics assessed were:

1) Cordon and Search;
2) Counter-Insurgency (COIN) Patrols;
3) Civil Security; and
4) Support and Economic Infrastructure.

These were deemed different enough to capture the diversity in the potential types of operations to be analysed. The 4 operational metrics were augmented with the three CIA metrics, for a total of 7 metrics.

Table 5-4: Robust Screening Design with 14 Factors (Columns) and 29 Cases (Rows).

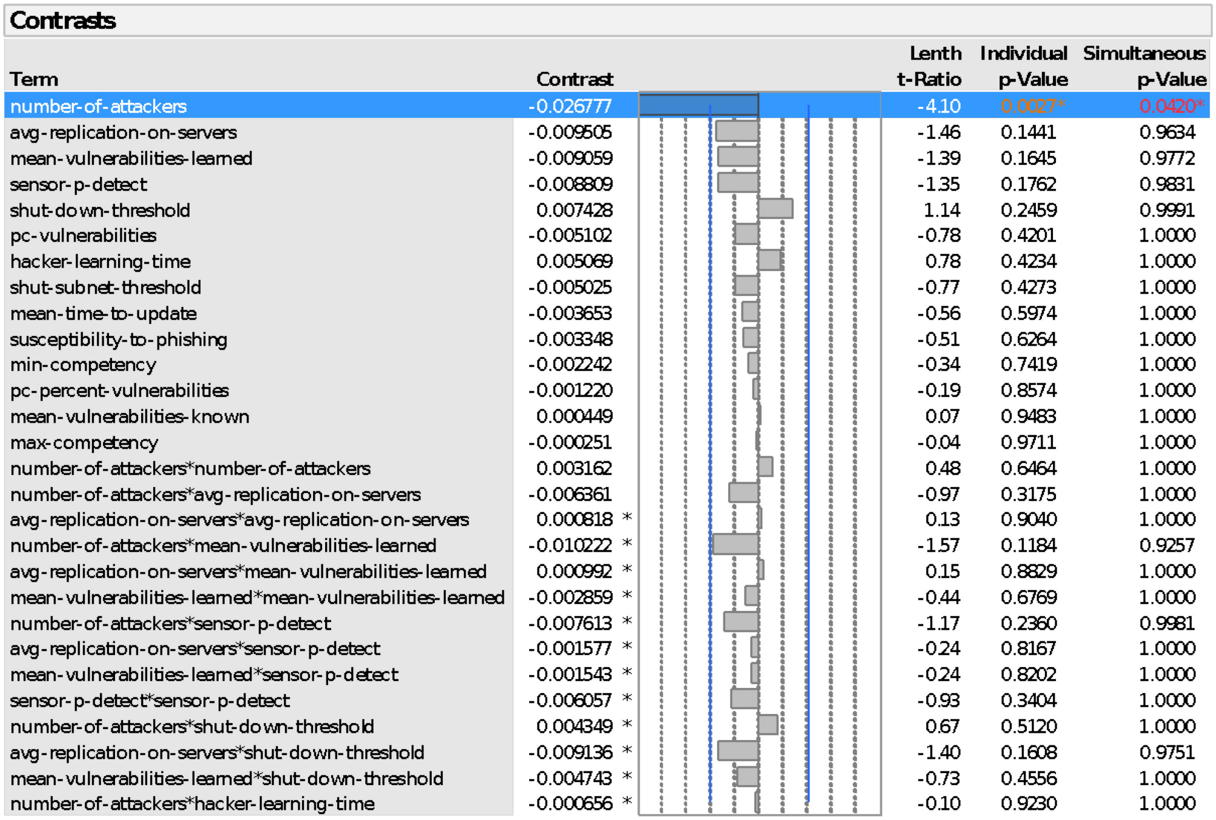
Case #	mean-time-to-update	sensor-p-detect	susceptibility-to-phishing	hacker-learning-time	min-competency	max-competency	mean-vulnerabilities-known	mean-vulnerabilities-learned	number-of-attackers	shut-down-threshold	shut-subnet-threshold	pc-percent-vulnerabilities	pc-vulnerabilities	avg-replication-on-servers
	days	%	%	days	%	%	int	int	int	%	%	%	int	int
1	45	85	5	45	10	50	20	1	22	4	4	30	10	9
2	45	15	2.55	10	45	50	2	5	40	15	4	30	10	9
3	45	85	0.1	27.5	10	95	2	1	40	15	4	80	10	1
4	45	85	5	10	10	95	2	3	4	15	1	30	80	9
5	45	15	0.1	45	10	72.5	2	5	4	4	4	80	80	9
6	5	85	0.1	45	27.5	95	2	5	40	4	1	30	10	9
7	5	15	5	27.5	45	50	20	5	4	4	1	30	80	9
8	5	85	0.1	45	45	50	2	1	4	15	4	30	80	5
9	5	15	5	45	10	95	11	5	4	15	4	30	10	1
10	45	85	5	45	45	50	2	5	4	9.5	1	80	10	1
11	45	15	5	10	27.5	50	20	1	4	15	4	80	80	1
12	5	85	5	10	10	50	2	5	40	4	4	55	80	1
13	5	15	0.1	45	45	50	20	3	40	4	4	80	10	1
14	5	15	5	45	10	50	2	1	40	15	1	80	45	9
15	45	50	0.1	45	10	50	20	5	40	15	1	30	80	1
16	45	85	0.1	10	45	50	11	1	40	4	1	80	80	9
17	45	15	0.1	45	45	95	20	1	4	15	1	55	10	9
18	5	15	0.1	10	45	95	2	5	22	15	1	80	80	1
19	45	15	5	10	10	95	20	5	40	4	1	80	10	5
20	25	85	5	45	45	95	20	5	40	15	4	80	80	9
21	45	15	5	45	45	95	2	1	40	4	2.5	30	80	1
22	5	15	0.1	10	10	95	20	1	40	9.5	4	30	80	9
23	5	85	2.55	45	10	95	20	1	4	4	1	80	80	1
24	25	50	2.55	27.5	27.5	72.5	11	3	22	9.5	2.5	55	45	5
25	5	50	5	10	45	95	2	1	4	4	4	80	10	9
26	5	85	0.1	10	10	50	20	5	4	15	2.5	80	10	9
27	5	85	5	10	45	72.5	20	1	40	15	1	30	10	1
28	45	85	0.1	10	45	95	20	5	4	4	4	30	45	1
29	25	15	0.1	10	10	50	2	1	4	4	1	30	10	1

5.4.2 Data Farming Results and Assessments of Possible Courses of Action

The results from the experimental design were analysed using JMP a statistical analysis tool developed by the SAS Institute. The authors were able to execute sufficient runs to estimate the mean value and standard deviation for each of the 7 metrics. This permitted to not only analyse the impact of each factor and the interactions on the estimated value of each of the metrics, but also assess their variability.

5.4.2.1 Cordon and Search

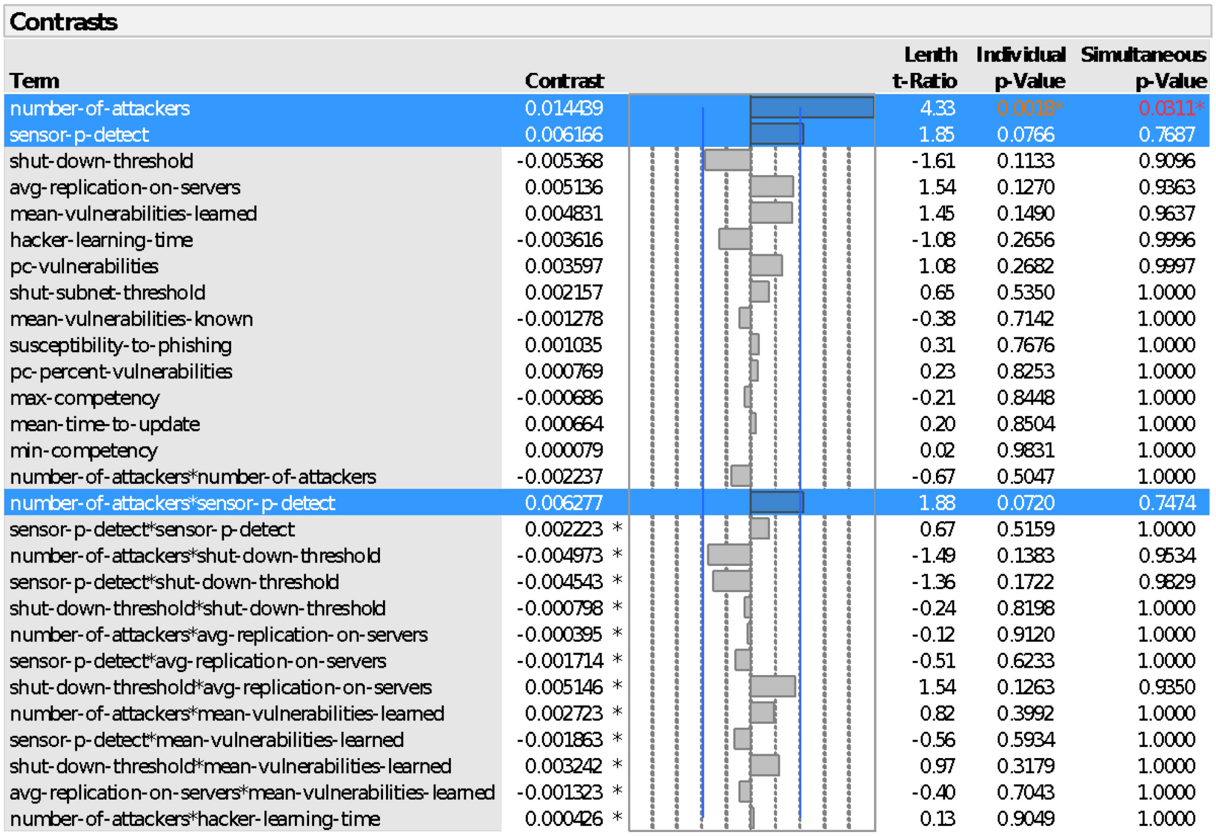
For Cordon and Search, the results of which are shown in Figure 5-7 and Figure 5-8, the number of attackers is the most important factor affecting the expected value of performing this task, and the only one that is statistically significant. The relationship is intuitive, in that increasing the number of attackers decreases the ability to perform the mission. Nonetheless, the variability of this metric is also affected by the sensor's probability of detecting an attack (sensor-p-detect) and its interaction with the number of attackers. The results indicate that increasing the sensor-p-detect increases the variability in the metric, as does increasing the number of attackers. If both increase then the variability is further increased due to interactions between the two factors. If one increases but the other decreases, the interaction factor reduces the variability. If both decrease, the interaction factor has a sub-additive effect in diminishing the variance of the metric.



Contrasts

Term	Contrast	Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
number-of-attackers	-0.026777	-4.10	0.0027*	0.0420*
avg-replication-on-servers	-0.009505	-1.46	0.1441	0.9634
mean-vulnerabilities-learned	-0.009059	-1.39	0.1645	0.9772
sensor-p-detect	-0.008809	-1.35	0.1762	0.9831
shut-down-threshold	0.007428	1.14	0.2459	0.9991
pc-vulnerabilities	-0.005102	-0.78	0.4201	1.0000
hacker-learning-time	0.005069	0.78	0.4234	1.0000
shut-subnet-threshold	-0.005025	-0.77	0.4273	1.0000
mean-time-to-update	-0.003653	-0.56	0.5974	1.0000
susceptibility-to-phishing	-0.003348	-0.51	0.6264	1.0000
min-competency	-0.002242	-0.34	0.7419	1.0000
pc-percent-vulnerabilities	-0.001220	-0.19	0.8574	1.0000
mean-vulnerabilities-known	0.000449	0.07	0.9483	1.0000
max-competency	-0.000251	-0.04	0.9711	1.0000
number-of-attackers*number-of-attackers	0.003162	0.48	0.6464	1.0000
number-of-attackers*avg-replication-on-servers	-0.006361	-0.97	0.3175	1.0000
avg-replication-on-servers*avg-replication-on-servers	0.000818 *	0.13	0.9040	1.0000
number-of-attackers*mean-vulnerabilities-learned	-0.010222 *	-1.57	0.1184	0.9257
avg-replication-on-servers*mean-vulnerabilities-learned	0.000992 *	0.15	0.8829	1.0000
mean-vulnerabilities-learned*mean-vulnerabilities-learned	-0.002859 *	-0.44	0.6769	1.0000
number-of-attackers*sensor-p-detect	-0.007613 *	-1.17	0.2360	0.9981
avg-replication-on-servers*sensor-p-detect	-0.001577 *	-0.24	0.8167	1.0000
mean-vulnerabilities-learned*sensor-p-detect	-0.001543 *	-0.24	0.8202	1.0000
sensor-p-detect*sensor-p-detect	-0.006057 *	-0.93	0.3404	1.0000
number-of-attackers*shut-down-threshold	0.004349 *	0.67	0.5120	1.0000
avg-replication-on-servers*shut-down-threshold	-0.009136 *	-1.40	0.1608	0.9751
mean-vulnerabilities-learned*shut-down-threshold	-0.004743 *	-0.73	0.4556	1.0000
number-of-attackers*hacker-learning-time	-0.000656 *	-0.10	0.9230	1.0000

Figure 5-7: Impact of Each Factor on the Expected Value of Successfully Conducting Cordon and Search.



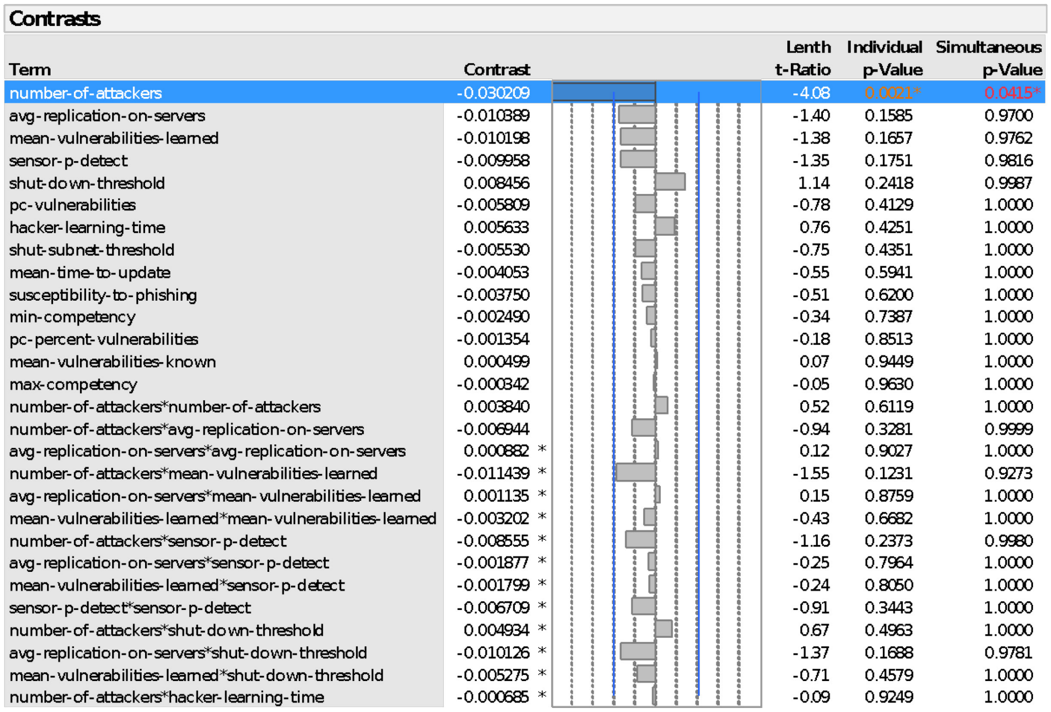
Contrasts

Term	Contrast	Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
number-of-attackers	0.014439	4.33	0.0018*	0.0311*
sensor-p-detect	0.006166	1.85	0.0766	0.7687
shut-down-threshold	-0.005368	-1.61	0.1133	0.9096
avg-replication-on-servers	0.005136	1.54	0.1270	0.9363
mean-vulnerabilities-learned	0.004831	1.45	0.1490	0.9637
hacker-learning-time	-0.003616	-1.08	0.2656	0.9996
pc-vulnerabilities	0.003597	1.08	0.2682	0.9997
shut-subnet-threshold	0.002157	0.65	0.5350	1.0000
mean-vulnerabilities-known	-0.001278	-0.38	0.7142	1.0000
susceptibility-to-phishing	0.001035	0.31	0.7676	1.0000
pc-percent-vulnerabilities	0.000769	0.23	0.8253	1.0000
max-competency	-0.000686	-0.21	0.8448	1.0000
mean-time-to-update	0.000664	0.20	0.8504	1.0000
min-competency	0.000079	0.02	0.9831	1.0000
number-of-attackers*number-of-attackers	-0.002237	-0.67	0.5047	1.0000
number-of-attackers*sensor-p-detect	0.006277	1.88	0.0720	0.7474
sensor-p-detect*sensor-p-detect	0.002223 *	0.67	0.5159	1.0000
number-of-attackers*shut-down-threshold	-0.004973 *	-1.49	0.1383	0.9534
sensor-p-detect*shut-down-threshold	-0.004543 *	-1.36	0.1722	0.9829
shut-down-threshold*shut-down-threshold	-0.000798 *	-0.24	0.8198	1.0000
number-of-attackers*avg-replication-on-servers	-0.000395 *	-0.12	0.9120	1.0000
sensor-p-detect*avg-replication-on-servers	-0.001714 *	-0.51	0.6233	1.0000
shut-down-threshold*avg-replication-on-servers	0.005146 *	1.54	0.1263	0.9350
number-of-attackers*mean-vulnerabilities-learned	0.002723 *	0.82	0.3992	1.0000
sensor-p-detect*mean-vulnerabilities-learned	-0.001863 *	-0.56	0.5934	1.0000
shut-down-threshold*mean-vulnerabilities-learned	0.003242 *	0.97	0.3179	1.0000
avg-replication-on-servers*mean-vulnerabilities-learned	-0.001323 *	-0.40	0.7043	1.0000
number-of-attackers*hacker-learning-time	0.000426 *	0.13	0.9049	1.0000

Figure 5-8: Impact of Each Factor on the Variance of Cordon and Search.

5.4.2.2 Counter Insurgency Patrols

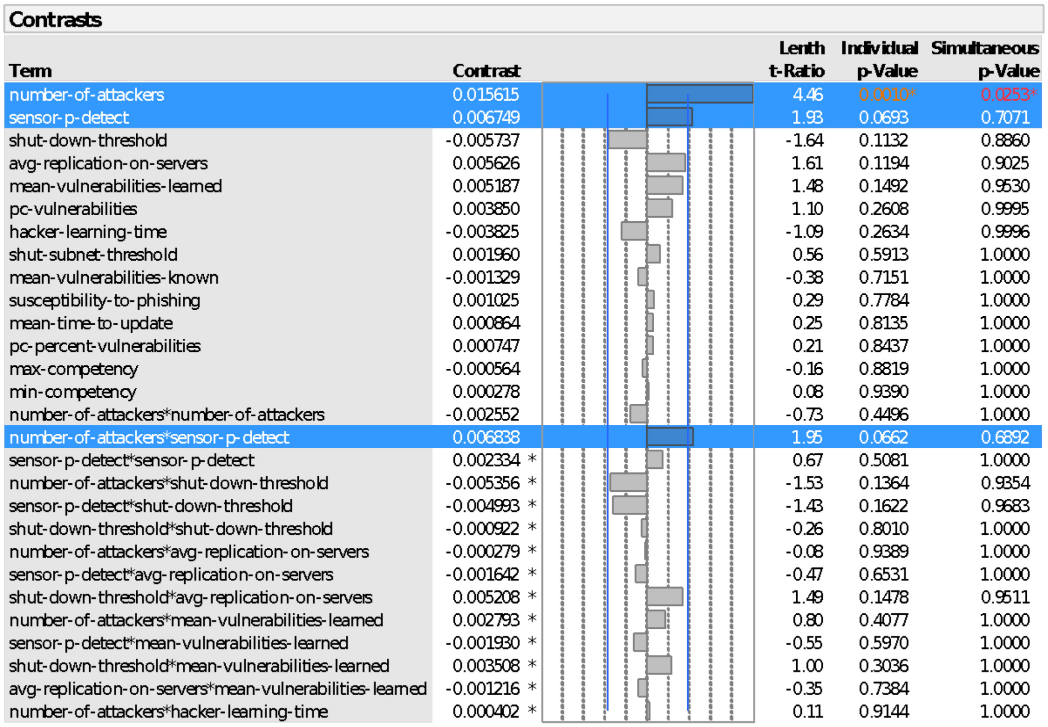
Counter Insurgency (COIN) Patrols, the results of which are presented in Figure 5-9 and Figure 5-10, are affected almost identically to Cordon and Search. These results are to be expected, as the two types of operations are similar in the types of services they require and the threats they face.



Contrasts

Term	Contrast	Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
number-of-attackers	-0.030209	-4.08	0.0021*	0.0415*
avg-replication-on-servers	-0.010389	-1.40	0.1585	0.9700
mean-vulnerabilities-learned	-0.010198	-1.38	0.1657	0.9762
sensor-p-detect	-0.009958	-1.35	0.1751	0.9816
shut-down-threshold	0.008456	1.14	0.2418	0.9987
pc-vulnerabilities	-0.005809	-0.78	0.4129	1.0000
hacker-learning-time	0.005633	0.76	0.4251	1.0000
shut-subnet-threshold	-0.005530	-0.75	0.4351	1.0000
mean-time-to-update	-0.004053	-0.55	0.5941	1.0000
susceptibility-to-phishing	-0.003750	-0.51	0.6200	1.0000
min-competency	-0.002490	-0.34	0.7387	1.0000
pc-percent-vulnerabilities	-0.001354	-0.18	0.8513	1.0000
mean-vulnerabilities-known	0.000499	0.07	0.9449	1.0000
max-competency	-0.000342	-0.05	0.9630	1.0000
number-of-attackers*number-of-attackers	0.003840	0.52	0.6119	1.0000
number-of-attackers*avg-replication-on-servers	-0.006944	-0.94	0.3281	0.9999
avg-replication-on-servers*avg-replication-on-servers	0.000882 *	0.12	0.9027	1.0000
number-of-attackers*mean-vulnerabilities-learned	-0.011439 *	-1.55	0.1231	0.9273
avg-replication-on-servers*mean-vulnerabilities-learned	0.001135 *	0.15	0.8759	1.0000
mean-vulnerabilities-learned*mean-vulnerabilities-learned	-0.003202 *	-0.43	0.6682	1.0000
number-of-attackers*sensor-p-detect	-0.008555 *	-1.16	0.2373	0.9980
avg-replication-on-servers*sensor-p-detect	-0.001877 *	-0.25	0.7964	1.0000
mean-vulnerabilities-learned*sensor-p-detect	-0.001799 *	-0.24	0.8050	1.0000
sensor-p-detect*sensor-p-detect	-0.006709 *	-0.91	0.3443	1.0000
number-of-attackers*shut-down-threshold	0.004934 *	0.67	0.4963	1.0000
avg-replication-on-servers*shut-down-threshold	-0.010126 *	-1.37	0.1688	0.9781
mean-vulnerabilities-learned*shut-down-threshold	-0.005275 *	-0.71	0.4579	1.0000
number-of-attackers*hacker-learning-time	-0.000685 *	-0.09	0.9249	1.0000

Figure 5-9: Impact of Each Factor on the Expected Value of Successfully Conducting COIN Patrols.



Contrasts

Term	Contrast	Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
number-of-attackers	0.015615	4.46	0.0010*	0.0253*
sensor-p-detect	0.006749	1.93	0.0693	0.7071
shut-down-threshold	-0.005737	-1.64	0.1132	0.8860
avg-replication-on-servers	0.005626	1.61	0.1194	0.9025
mean-vulnerabilities-learned	0.005187	1.48	0.1492	0.9530
pc-vulnerabilities	0.003850	1.10	0.2608	0.9995
hacker-learning-time	-0.003825	-1.09	0.2634	0.9996
shut-subnet-threshold	0.001960	0.56	0.5913	1.0000
mean-vulnerabilities-known	-0.001329	-0.38	0.7151	1.0000
susceptibility-to-phishing	0.001025	0.29	0.7784	1.0000
mean-time-to-update	0.000864	0.25	0.8135	1.0000
pc-percent-vulnerabilities	0.000747	0.21	0.8437	1.0000
max-competency	-0.000564	-0.16	0.8819	1.0000
min-competency	0.000278	0.08	0.9390	1.0000
number-of-attackers*number-of-attackers	-0.002552	-0.73	0.4496	1.0000
number-of-attackers*sensor-p-detect	0.006838	1.95	0.0662	0.6892
sensor-p-detect*sensor-p-detect	0.002334 *	0.67	0.5081	1.0000
number-of-attackers*shut-down-threshold	-0.005356 *	-1.53	0.1364	0.9354
sensor-p-detect*shut-down-threshold	-0.004993 *	-1.43	0.1622	0.9683
shut-down-threshold*shut-down-threshold	-0.000922 *	-0.26	0.8010	1.0000
number-of-attackers*avg-replication-on-servers	-0.000279 *	-0.08	0.9389	1.0000
sensor-p-detect*avg-replication-on-servers	-0.001642 *	-0.47	0.6531	1.0000
shut-down-threshold*avg-replication-on-servers	0.005208 *	1.49	0.1478	0.9511
number-of-attackers*mean-vulnerabilities-learned	0.002793 *	0.80	0.4077	1.0000
sensor-p-detect*mean-vulnerabilities-learned	-0.001930 *	-0.55	0.5970	1.0000
shut-down-threshold*mean-vulnerabilities-learned	0.003508 *	1.00	0.3036	1.0000
avg-replication-on-servers*mean-vulnerabilities-learned	-0.001216 *	-0.35	0.7384	1.0000
number-of-attackers*hacker-learning-time	0.000402 *	0.11	0.9144	1.0000

Figure 5-10: Impact of Each Factor on the Variance of COIN Patrols.

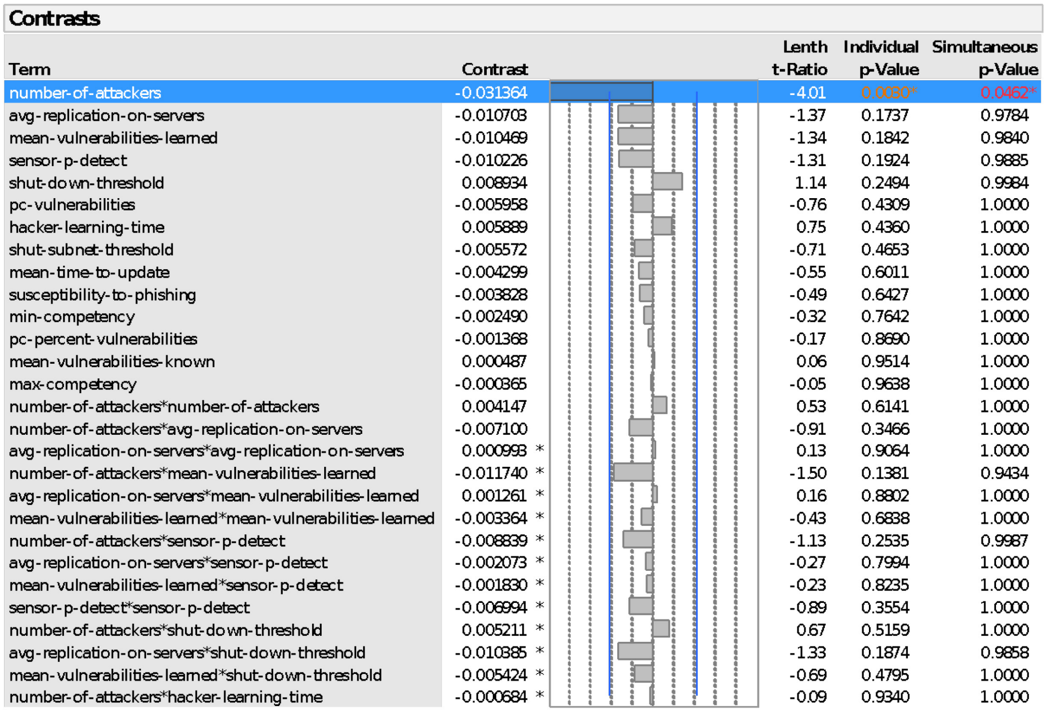
5.4.2.3 Civil Security and Support Economic and Infrastructure Operations

Civil Security and Support Economic and Infrastructure Operations both displayed very similar results as shown by Figure 5-11 through Figure 5-14. This similarity is a strong indication that the ranges chosen were not comparable, as the number of attackers dominates the behaviour of the model.

If this were a verified, validated and accredited model, it would be important to re-assess the ranges for the factors. If the ranges were deemed to be correct, two primary options would be available to the analysts:

1) Spend considerable effort attempting to quantify the expected number of attackers to narrow its variability.

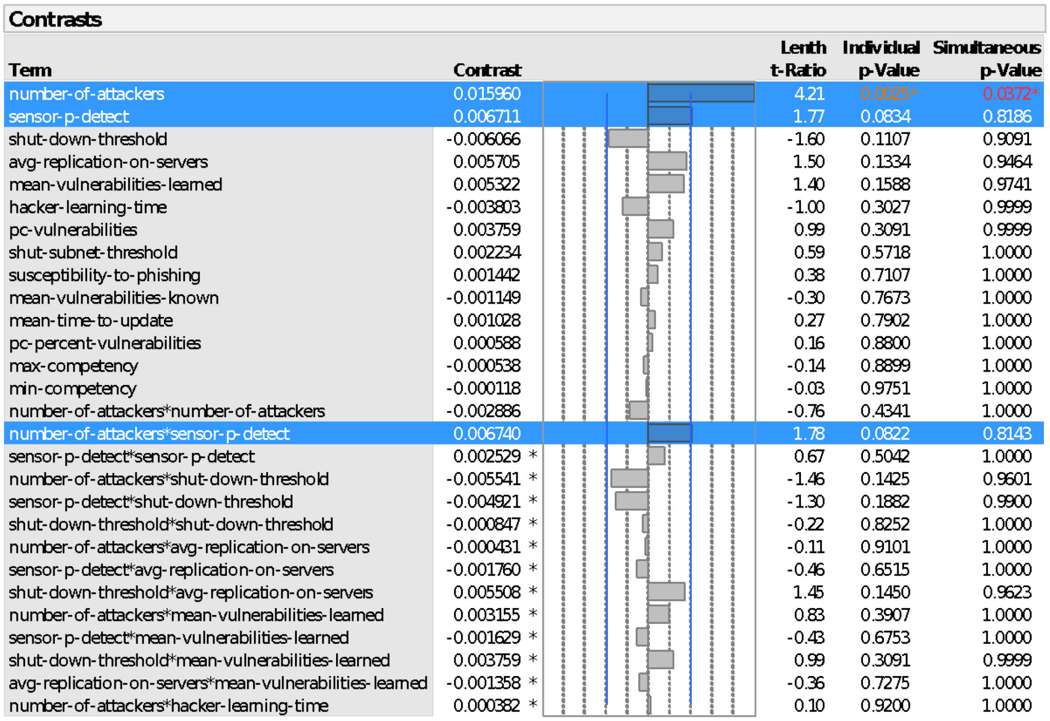
2) Create a number of scenarios, e.g., select a worse-case or conservative number and a nominal number of attackers and repeat the analysis to identify the factors that are most critical in each case.



Contrasts

		Lenth	Individual	Simultaneous
Term	Contrast	t-Ratio	p-Value	p-Value
number-of-attackers	-0.031364	-4.01	0.0030*	0.0462*
avg-replication-on-servers	-0.010703	-1.37	0.1737	0.9784
mean-vulnerabilities-learned	-0.010469	-1.34	0.1842	0.9840
sensor-p-detect	-0.010226	-1.31	0.1924	0.9885
shut-down-threshold	0.008934	1.14	0.2494	0.9984
pc-vulnerabilities	-0.005958	-0.76	0.4309	1.0000
hacker-learning-time	0.005889	0.75	0.4360	1.0000
shut-subnet-threshold	-0.005572	-0.71	0.4653	1.0000
mean-time-to-update	-0.004299	-0.55	0.6011	1.0000
susceptibility-to-phishing	-0.003828	-0.49	0.6427	1.0000
min-competency	-0.002490	-0.32	0.7642	1.0000
pc-percent-vulnerabilities	-0.001368	-0.17	0.8690	1.0000
mean-vulnerabilities-known	0.000487	0.06	0.9514	1.0000
max-competency	-0.000365	-0.05	0.9638	1.0000
number-of-attackers*number-of-attackers	0.004147	0.53	0.6141	1.0000
number-of-attackers*avg-replication-on-servers	-0.007100	-0.91	0.3466	1.0000
avg-replication-on-servers*avg-replication-on-servers	0.000993 *	0.13	0.9064	1.0000
number-of-attackers*mean-vulnerabilities-learned	-0.011740 *	-1.50	0.1381	0.9434
avg-replication-on-servers*mean-vulnerabilities-learned	0.001261 *	0.16	0.8802	1.0000
mean-vulnerabilities-learned*mean-vulnerabilities-learned	-0.003364 *	-0.43	0.6838	1.0000
number-of-attackers*sensor-p-detect	-0.008839 *	-1.13	0.2535	0.9987
avg-replication-on-servers*sensor-p-detect	-0.002073 *	-0.27	0.7994	1.0000
mean-vulnerabilities-learned*sensor-p-detect	-0.001830 *	-0.23	0.8235	1.0000
sensor-p-detect*sensor-p-detect	-0.006994 *	-0.89	0.3554	1.0000
number-of-attackers*shut-down-threshold	0.005211 *	0.67	0.5159	1.0000
avg-replication-on-servers*shut-down-threshold	-0.010385 *	-1.33	0.1874	0.9858
mean-vulnerabilities-learned*shut-down-threshold	-0.005424 *	-0.69	0.4795	1.0000
number-of-attackers*hacker-learning-time	-0.000684 *	-0.09	0.9340	1.0000

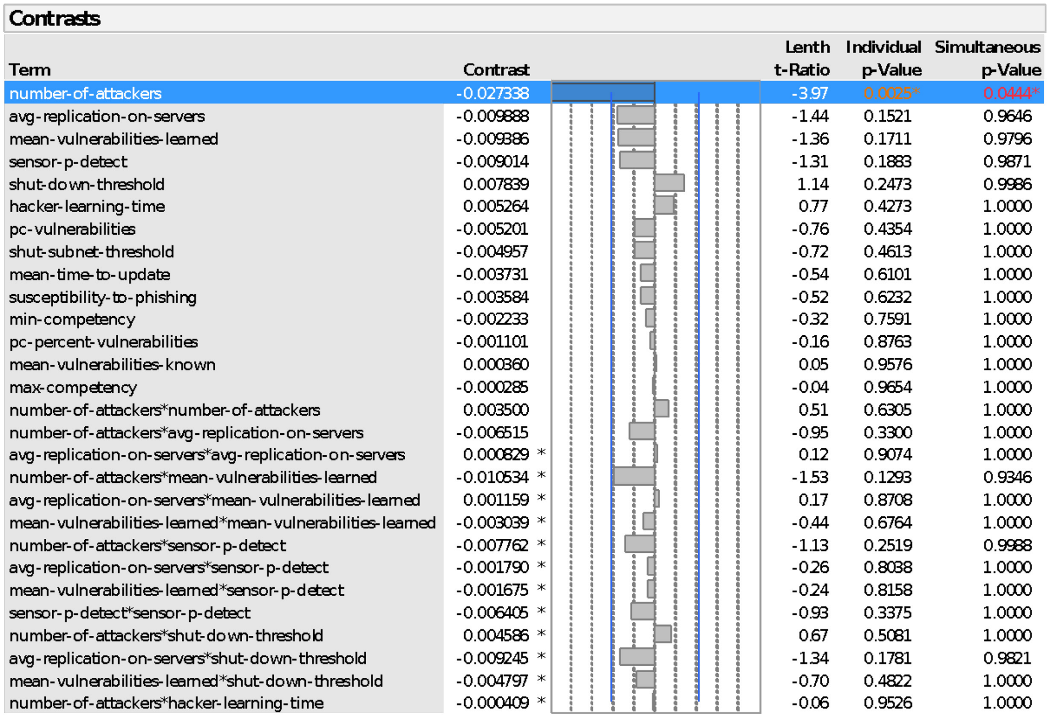
Figure 5-11: Impact of Each Factor on the Expected Value of Successfully Conducting Civil Security Operations.



Contrasts

Term	Contrast	Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
number-of-attackers	0.015960	4.21	0.0025*	0.0372*
sensor-p-detect	0.006711	1.77	0.0834	0.8186
shut-down-threshold	-0.006066	-1.60	0.1107	0.9091
avg-replication-on-servers	0.005705	1.50	0.1334	0.9464
mean-vulnerabilities-learned	0.005322	1.40	0.1588	0.9741
hacker-learning-time	-0.003803	-1.00	0.3027	0.9999
pc-vulnerabilities	0.003759	0.99	0.3091	0.9999
shut-subnet-threshold	0.002234	0.59	0.5718	1.0000
susceptibility-to-phishing	0.001442	0.38	0.7107	1.0000
mean-vulnerabilities-known	-0.001149	-0.30	0.7673	1.0000
mean-time-to-update	0.001028	0.27	0.7902	1.0000
pc-percent-vulnerabilities	0.000588	0.16	0.8800	1.0000
max-competency	-0.000538	-0.14	0.8899	1.0000
min-competency	-0.000118	-0.03	0.9751	1.0000
number-of-attackers*number-of-attackers	-0.002886	-0.76	0.4341	1.0000
number-of-attackers*sensor-p-detect	0.006740	1.78	0.0822	0.8143
sensor-p-detect*sensor-p-detect	0.002529 *	0.67	0.5042	1.0000
number-of-attackers*shut-down-threshold	-0.005541 *	-1.46	0.1425	0.9601
sensor-p-detect*shut-down-threshold	-0.004921 *	-1.30	0.1882	0.9900
shut-down-threshold*shut-down-threshold	-0.000847 *	-0.22	0.8252	1.0000
number-of-attackers*avg-replication-on-servers	-0.000431 *	-0.11	0.9101	1.0000
sensor-p-detect*avg-replication-on-servers	-0.001760 *	-0.46	0.6515	1.0000
shut-down-threshold*avg-replication-on-servers	0.005508 *	1.45	0.1450	0.9623
number-of-attackers*mean-vulnerabilities-learned	0.003155 *	0.83	0.3907	1.0000
sensor-p-detect*mean-vulnerabilities-learned	-0.001629 *	-0.43	0.6753	1.0000
shut-down-threshold*mean-vulnerabilities-learned	0.003759 *	0.99	0.3091	0.9999
avg-replication-on-servers*mean-vulnerabilities-learned	-0.001358 *	-0.36	0.7275	1.0000
number-of-attackers*hacker-learning-time	0.000382 *	0.10	0.9200	1.0000

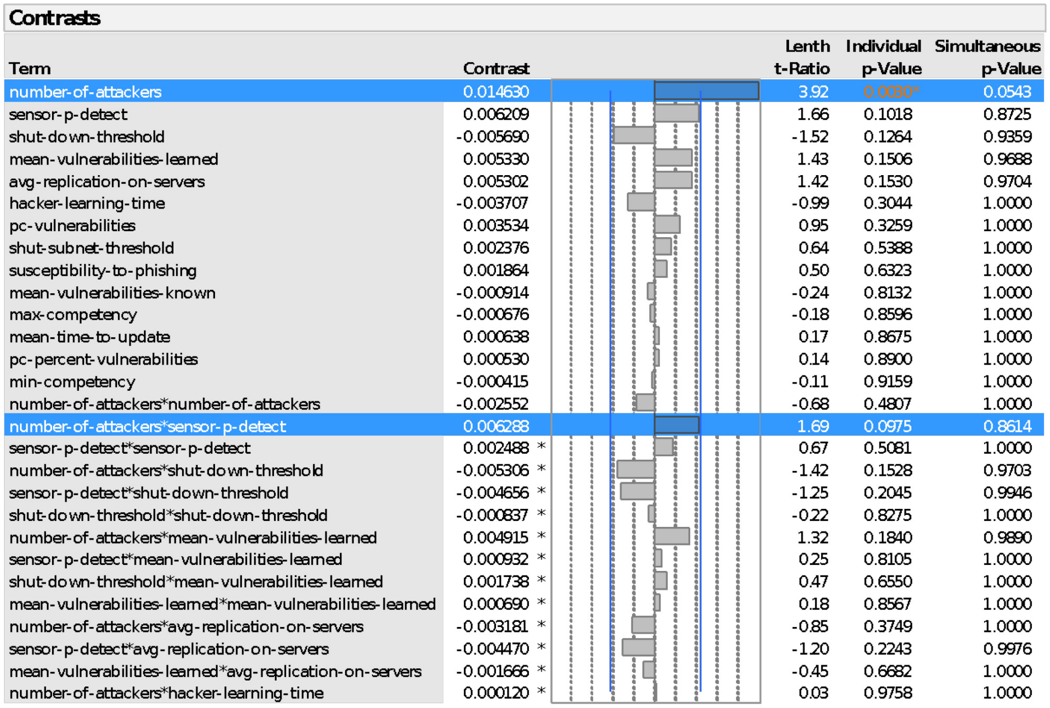
Figure 5-12: Impact of Each Factor on the Variance of Civil Security Patrols.



Contrasts

Term	Contrast	Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
number-of-attackers	-0.027338	-3.97	0.0025*	0.0444*
avg-replication-on-servers	-0.009888	-1.44	0.1521	0.9646
mean-vulnerabilities-learned	-0.009386	-1.36	0.1711	0.9796
sensor-p-detect	-0.009014	-1.31	0.1883	0.9871
shut-down-threshold	0.007839	1.14	0.2473	0.9986
hacker-learning-time	0.005264	0.77	0.4273	1.0000
pc-vulnerabilities	-0.005201	-0.76	0.4354	1.0000
shut-subnet-threshold	-0.004957	-0.72	0.4613	1.0000
mean-time-to-update	-0.003731	-0.54	0.6101	1.0000
susceptibility-to-phishing	-0.003584	-0.52	0.6232	1.0000
min-competency	-0.002233	-0.32	0.7591	1.0000
pc-percent-vulnerabilities	-0.001101	-0.16	0.8763	1.0000
mean-vulnerabilities-known	0.000360	0.05	0.9576	1.0000
max-competency	-0.000285	-0.04	0.9654	1.0000
number-of-attackers*number-of-attackers	0.003500	0.51	0.6305	1.0000
number-of-attackers*avg-replication-on-servers	-0.006515	-0.95	0.3300	1.0000
avg-replication-on-servers*avg-replication-on-servers	0.000829 *	0.12	0.9074	1.0000
number-of-attackers*mean-vulnerabilities-learned	-0.010534 *	-1.53	0.1293	0.9346
avg-replication-on-servers*mean-vulnerabilities-learned	0.001159 *	0.17	0.8708	1.0000
mean-vulnerabilities-learned*mean-vulnerabilities-learned	-0.003039 *	-0.44	0.6764	1.0000
number-of-attackers*sensor-p-detect	-0.007762 *	-1.13	0.2519	0.9988
avg-replication-on-servers*sensor-p-detect	-0.001790 *	-0.26	0.8038	1.0000
mean-vulnerabilities-learned*sensor-p-detect	-0.001675 *	-0.24	0.8158	1.0000
sensor-p-detect*sensor-p-detect	-0.006405 *	-0.93	0.3375	1.0000
number-of-attackers*shut-down-threshold	0.004586 *	0.67	0.5081	1.0000
avg-replication-on-servers*shut-down-threshold	-0.009245 *	-1.34	0.1781	0.9821
mean-vulnerabilities-learned*shut-down-threshold	-0.004797 *	-0.70	0.4822	1.0000
number-of-attackers*hacker-learning-time	-0.000409 *	-0.06	0.9526	1.0000

Figure 5-13: Impact of Each Factor on the Expected Value of Successfully Conducting Support Economic and Infrastructure Operations.



Contrasts

Term	Contrast	Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
number-of-attackers	0.014630	3.92	0.0030*	0.0543
sensor-p-detect	0.006209	1.66	0.1018	0.8725
shut-down-threshold	-0.005690	-1.52	0.1264	0.9359
mean-vulnerabilities-learned	0.005330	1.43	0.1506	0.9688
avg-replication-on-servers	0.005302	1.42	0.1530	0.9704
hacker-learning-time	-0.003707	-0.99	0.3044	1.0000
pc-vulnerabilities	0.003534	0.95	0.3259	1.0000
shut-subnet-threshold	0.002376	0.64	0.5388	1.0000
susceptibility-to-phishing	0.001864	0.50	0.6323	1.0000
mean-vulnerabilities-known	-0.000914	-0.24	0.8132	1.0000
max-competency	-0.000676	-0.18	0.8596	1.0000
mean-time-to-update	0.000638	0.17	0.8675	1.0000
pc-percent-vulnerabilities	0.000530	0.14	0.8900	1.0000
min-competency	-0.000415	-0.11	0.9159	1.0000
number-of-attackers*number-of-attackers	-0.002552	-0.68	0.4807	1.0000
number-of-attackers*sensor-p-detect	0.006288	1.69	0.0975	0.8614
sensor-p-detect*sensor-p-detect	0.002488 *	0.67	0.5081	1.0000
number-of-attackers*shut-down-threshold	-0.005306 *	-1.42	0.1528	0.9703
sensor-p-detect*shut-down-threshold	-0.004656 *	-1.25	0.2045	0.9946
shut-down-threshold*shut-down-threshold	-0.000837 *	-0.22	0.8275	1.0000
number-of-attackers*mean-vulnerabilities-learned	0.004915 *	1.32	0.1840	0.9890
sensor-p-detect*mean-vulnerabilities-learned	0.000932 *	0.25	0.8105	1.0000
shut-down-threshold*mean-vulnerabilities-learned	0.001738 *	0.47	0.6550	1.0000
mean-vulnerabilities-learned*mean-vulnerabilities-learned	0.000690 *	0.18	0.8567	1.0000
number-of-attackers*avg-replication-on-servers	-0.003181 *	-0.85	0.3749	1.0000
sensor-p-detect*avg-replication-on-servers	-0.004470 *	-1.20	0.2243	0.9976
mean-vulnerabilities-learned*avg-replication-on-servers	-0.001666 *	-0.45	0.6682	1.0000
number-of-attackers*hacker-learning-time	0.000120 *	0.03	0.9758	1.0000

Figure 5-14: Impact of Each Factor on the Variance of Support Economic and Infrastructure Operations.

5.4.2.4 Overall Significance

Most metrics did not have a large or consistent impact on the system, but some factors were almost significant and deserve to be mentioned. These are listed below with a short explanation and potential implication.

Average replication of files on servers: This factor appears to be almost significant in all cases, and it is inversely correlated with the metrics, indicating that if a file is replicated more on different servers, the ability to perform the mission is jeopardized. This is an indication that confidentiality and data integrity are more important than availability. This confirms the model behaves as designed, as the effects of availability are not fully implemented as discussed previously. If the effects of availability were modelled more comprehensively, it would be possible that increased replication would improve availability and become a positively correlated factor.

Mean vulnerabilities learned vs mean vulnerabilities known: DUE to the long term over which the simulation is executed, the initial number of vulnerabilities the attackers know is not as critical as to how many vulnerabilities they learn. As expected the more vulnerabilities the attackers learn during each period, the lower the ability of the defender to perform the mission.

Sensor Detection Probability: This factor is non-intuitively correlated with the expected value for the ability to perform the operations. The statistical analyses indicate that higher probabilities of detecting an attack reduce the ability to perform the mission. This is an indication that availability is decreasing. This may not be the case in reality but reflects the design of the model and the simplifications made to the system administrators and the way the services are architectured.

Shutdown Threshold is one factor that seems to provide improvement in both increasing the expected value and reducing the variability. Increasing the factor implies neglecting more alarms and only shutting down the portions of the network when the number of activated sensors is sufficient. This again implies that the model is operating in a scenario where the availability of the services is driving the ability of the operational forces to conduct their respective missions.

5.4.2.5 CIA Metrics

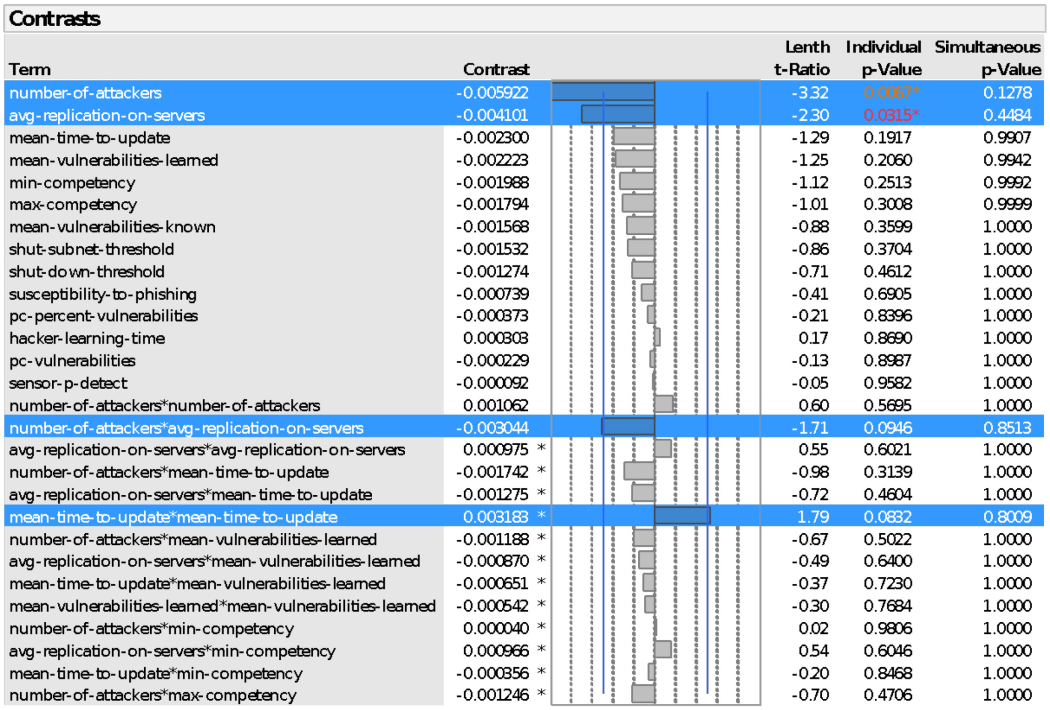
The operational metrics can be contrasted with the more technical CIA metrics, i.e., those that cyber-defence experts may be more familiar with. It is important to note that the CIA metrics are not a well-established and agreed upon concept, but the authors used the concepts described in the CIA paradigm to develop metrics that are aligned with the concerns of each of the elements of the CIA paradigm.

The first metric to be considered is confidentiality, which is concerned with maintaining the secrecy of the information. As shown in Figure 5-15, the ability to maintain confidentiality is mostly impacted by the number of attackers and the number of times files are replicated on the server. These results are logical and agree with that is expected. In addition to these two factors and their linear interaction, which is reinforcing, the mean time to update the systems is also important in maintaining confidentiality. The effect correlates better with a quadratic relationship than a linear relationship, which is indicative that there are additional benefits to updating more often, as has been proposed by other relevant studies [16].

Figure 5-16 illustrates the impact of each factor on the variance in confidentiality. In this case, the variance is dominated by the number of attackers and the average replication of the data files in the servers. The time to update the system is marginally under the statistical significance threshold. While the number of attackers and the average replication increase the variability, the longer times to update decreases the variability of the metric.

While confidentiality is interested in maintaining the secrecy of the data, integrity is concerned with maintaining the accuracy or veracity, i.e., to avoid having attackers manipulate the data. Figure 5-17 shows that the expected value of integrity is driven by the same factors as confidentiality.

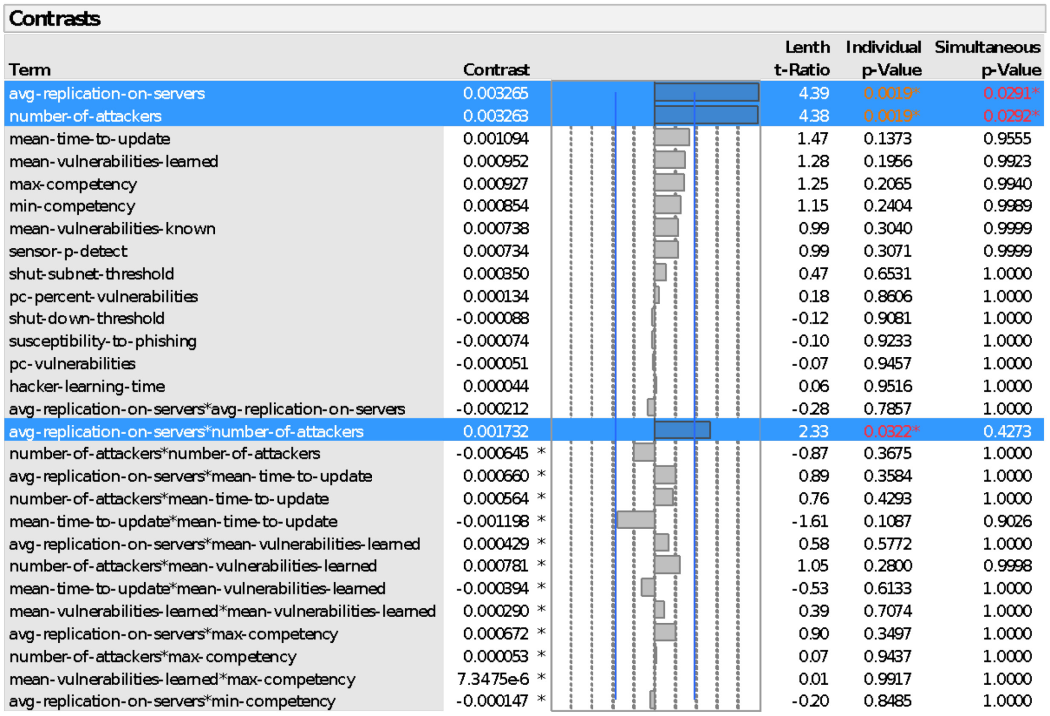
The variance in the value of integrity on the other hand is impacted by other factors, as shown in Figure 5-18. In particular, the competency of the attackers increases the variability. This is an indication of that the model for the penetration attacks that exploits manipulation of data is more heavily impacted by how competent the attackers are.



Contrasts

Term	Contrast	Lenth	Individual	Simultaneous
		t-Ratio	p-Value	p-Value
number-of-attackers	-0.005922	-3.32	0.0067*	0.1278
avg-replication-on-servers	-0.004101	-2.30	0.0315*	0.4484
mean-time-to-update	-0.002300	-1.29	0.1917	0.9907
mean-vulnerabilities-learned	-0.002223	-1.25	0.2060	0.9942
min-competency	-0.001988	-1.12	0.2513	0.9992
max-competency	-0.001794	-1.01	0.3008	0.9999
mean-vulnerabilities-known	-0.001568	-0.88	0.3599	1.0000
shut-subnet-threshold	-0.001532	-0.86	0.3704	1.0000
shut-down-threshold	-0.001274	-0.71	0.4612	1.0000
susceptibility-to-phishing	-0.000739	-0.41	0.6905	1.0000
pc-percent-vulnerabilities	-0.000373	-0.21	0.8396	1.0000
hacker-learning-time	0.000303	0.17	0.8690	1.0000
pc-vulnerabilities	-0.000229	-0.13	0.8987	1.0000
sensor-p-detect	-0.000092	-0.05	0.9582	1.0000
number-of-attackers*number-of-attackers	0.001062	0.60	0.5695	1.0000
number-of-attackers*avg-replication-on-servers	-0.003044	-1.71	0.0946	0.8513
avg-replication-on-servers*avg-replication-on-servers	0.000975 *	0.55	0.6021	1.0000
number-of-attackers*mean-time-to-update	-0.001742 *	-0.98	0.3139	1.0000
avg-replication-on-servers*mean-time-to-update	-0.001275 *	-0.72	0.4604	1.0000
mean-time-to-update*mean-time-to-update	0.003183 *	1.79	0.0832	0.8009
number-of-attackers*mean-vulnerabilities-learned	-0.001188 *	-0.67	0.5022	1.0000
avg-replication-on-servers*mean-vulnerabilities-learned	-0.000870 *	-0.49	0.6400	1.0000
mean-time-to-update*mean-vulnerabilities-learned	-0.000651 *	-0.37	0.7230	1.0000
mean-vulnerabilities-learned*mean-vulnerabilities-learned	-0.000542 *	-0.30	0.7684	1.0000
number-of-attackers*min-competency	0.000040 *	0.02	0.9806	1.0000
avg-replication-on-servers*min-competency	0.000966 *	0.54	0.6046	1.0000
mean-time-to-update*min-competency	-0.000356 *	-0.20	0.8468	1.0000
number-of-attackers*max-competency	-0.001246 *	-0.70	0.4706	1.0000

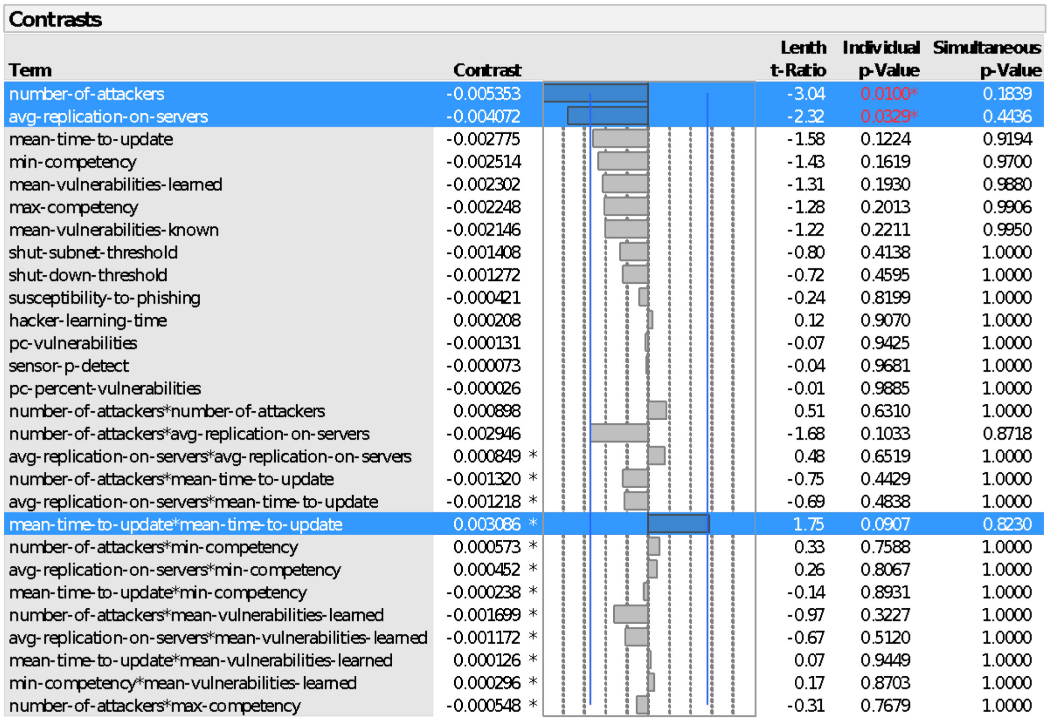
Figure 5-15: Impact of Each Factor on the Expected Value of Confidentiality.



Contrasts

Term	Contrast	Lenth	Individual	Simultaneous
		t-Ratio	p-Value	p-Value
avg-replication-on-servers	0.003265	4.39	0.0019*	0.0291*
number-of-attackers	0.003263	4.38	0.0019*	0.0292*
mean-time-to-update	0.001094	1.47	0.1373	0.9555
mean-vulnerabilities-learned	0.000952	1.28	0.1956	0.9923
max-competency	0.000927	1.25	0.2065	0.9940
min-competency	0.000854	1.15	0.2404	0.9989
mean-vulnerabilities-known	0.000738	0.99	0.3040	0.9999
sensor-p-detect	0.000734	0.99	0.3071	0.9999
shut-subnet-threshold	0.000350	0.47	0.6531	1.0000
pc-percent-vulnerabilities	0.000134	0.18	0.8606	1.0000
shut-down-threshold	-0.000088	-0.12	0.9081	1.0000
susceptibility-to-phishing	-0.000074	-0.10	0.9233	1.0000
pc-vulnerabilities	-0.000051	-0.07	0.9457	1.0000
hacker-learning-time	0.000044	0.06	0.9516	1.0000
avg-replication-on-servers*avg-replication-on-servers	-0.000212	-0.28	0.7857	1.0000
avg-replication-on-servers*number-of-attackers	0.001732	2.33	0.0322*	0.4273
number-of-attackers*number-of-attackers	-0.000645 *	-0.87	0.3675	1.0000
avg-replication-on-servers*mean-time-to-update	0.000660 *	0.89	0.3584	1.0000
number-of-attackers*mean-time-to-update	0.000564 *	0.76	0.4293	1.0000
mean-time-to-update*mean-time-to-update	-0.001198 *	-1.61	0.1087	0.9026
avg-replication-on-servers*mean-vulnerabilities-learned	0.000429 *	0.58	0.5772	1.0000
number-of-attackers*mean-vulnerabilities-learned	0.000781 *	1.05	0.2800	0.9998
mean-time-to-update*mean-vulnerabilities-learned	-0.000394 *	-0.53	0.6133	1.0000
mean-vulnerabilities-learned*mean-vulnerabilities-learned	0.000290 *	0.39	0.7074	1.0000
avg-replication-on-servers*max-competency	0.000672 *	0.90	0.3497	1.0000
number-of-attackers*max-competency	0.000053 *	0.07	0.9437	1.0000
mean-vulnerabilities-learned*max-competency	7.3475e-6 *	0.01	0.9917	1.0000
avg-replication-on-servers*min-competency	-0.000147 *	-0.20	0.8485	1.0000

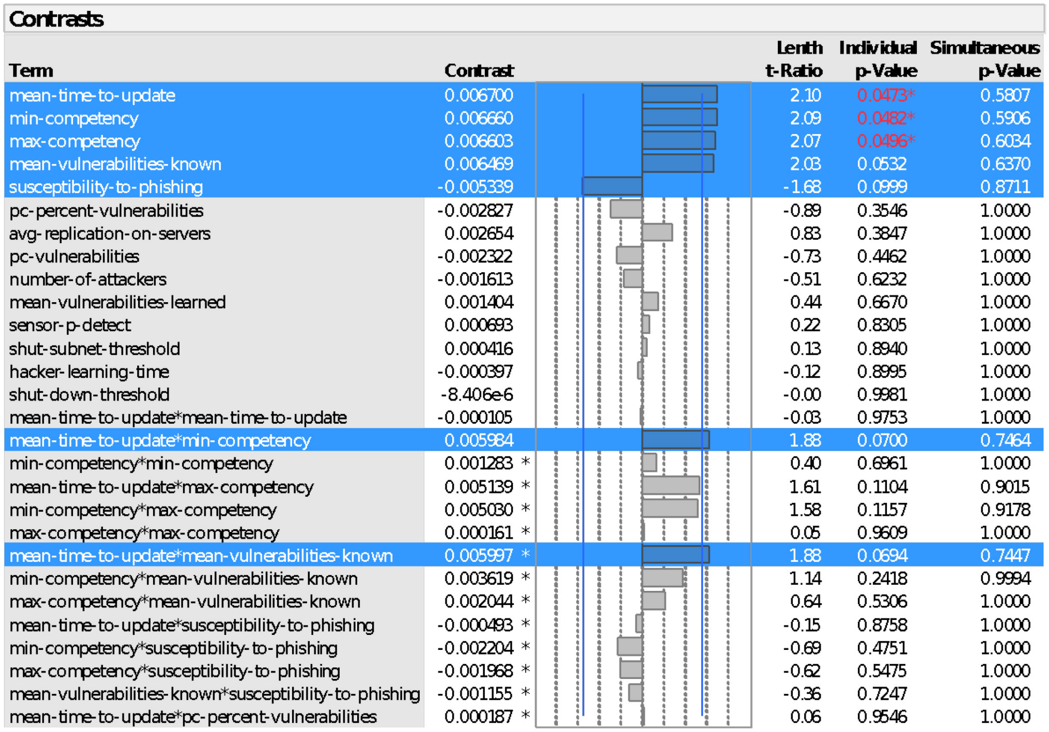
Figure 5-16: Impact of Each Factor on the Variance of Confidentiality.



Contrasts

		Lenth	Individual	Simultaneous
Term	Contrast	t-Ratio	p-Value	p-Value
number-of-attackers	-0.005353	-3.04	0.0100*	0.1839
avg-replication-on-servers	-0.004072	-2.32	0.0329*	0.4436
mean-time-to-update	-0.002775	-1.58	0.1224	0.9194
min-competency	-0.002514	-1.43	0.1619	0.9700
mean-vulnerabilities-learned	-0.002302	-1.31	0.1930	0.9880
max-competency	-0.002248	-1.28	0.2013	0.9906
mean-vulnerabilities-known	-0.002146	-1.22	0.2211	0.9950
shut-subnet-threshold	-0.001408	-0.80	0.4138	1.0000
shut-down-threshold	-0.001272	-0.72	0.4595	1.0000
susceptibility-to-phishing	-0.000421	-0.24	0.8199	1.0000
hacker-learning-time	0.000208	0.12	0.9070	1.0000
pc-vulnerabilities	-0.000131	-0.07	0.9425	1.0000
sensor-p-detect	-0.000073	-0.04	0.9681	1.0000
pc-percent-vulnerabilities	-0.000026	-0.01	0.9885	1.0000
number-of-attackers*number-of-attackers	0.000898	0.51	0.6310	1.0000
number-of-attackers*avg-replication-on-servers	-0.002946	-1.68	0.1033	0.8718
avg-replication-on-servers*avg-replication-on-servers	0.000849 *	0.48	0.6519	1.0000
number-of-attackers*mean-time-to-update	-0.001320 *	-0.75	0.4429	1.0000
avg-replication-on-servers*mean-time-to-update	-0.001218 *	-0.69	0.4838	1.0000
mean-time-to-update*mean-time-to-update	0.003086 *	1.75	0.0907	0.8230
number-of-attackers*min-competency	0.000573 *	0.33	0.7588	1.0000
avg-replication-on-servers*min-competency	0.000452 *	0.26	0.8067	1.0000
mean-time-to-update*min-competency	-0.000238 *	-0.14	0.8931	1.0000
number-of-attackers*mean-vulnerabilities-learned	-0.001699 *	-0.97	0.3227	1.0000
avg-replication-on-servers*mean-vulnerabilities-learned	-0.001172 *	-0.67	0.5120	1.0000
mean-time-to-update*mean-vulnerabilities-learned	0.000126 *	0.07	0.9449	1.0000
min-competency*mean-vulnerabilities-learned	0.000296 *	0.17	0.8703	1.0000
number-of-attackers*max-competency	-0.000548 *	-0.31	0.7679	1.0000

Figure 5-17: Impact of Each Factor on the Expected Value of Integrity.



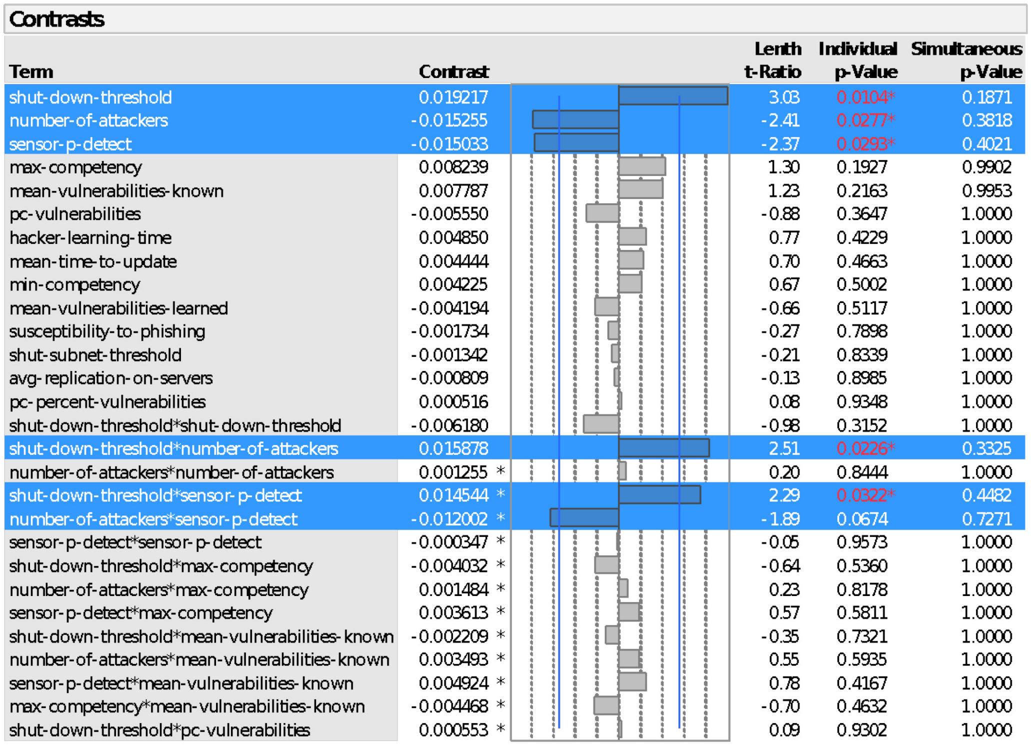
Contrasts

		Lenth	Individual	Simultaneous
Term	Contrast	t-Ratio	p-Value	p-Value
mean-time-to-update	0.006700	2.10	0.0473*	0.5807
min-competency	0.006660	2.09	0.0482*	0.5906
max-competency	0.006603	2.07	0.0496*	0.6034
mean-vulnerabilities-known	0.006469	2.03	0.0532	0.6370
susceptibility-to-phishing	-0.005339	-1.68	0.0999	0.8711
pc-percent-vulnerabilities	-0.002827	-0.89	0.3546	1.0000
avg-replication-on-servers	0.002654	0.83	0.3847	1.0000
pc-vulnerabilities	-0.002322	-0.73	0.4462	1.0000
number-of-attackers	-0.001613	-0.51	0.6232	1.0000
mean-vulnerabilities-learned	0.001404	0.44	0.6670	1.0000
sensor-p-detect	0.000693	0.22	0.8305	1.0000
shut-subnet-threshold	0.000416	0.13	0.8940	1.0000
hacker-learning-time	-0.000397	-0.12	0.8995	1.0000
shut-down-threshold	-8.406e-6	-0.00	0.9981	1.0000
mean-time-to-update*mean-time-to-update	-0.000105	-0.03	0.9753	1.0000
mean-time-to-update*min-competency	0.005984	1.88	0.0700	0.7464
min-competency*min-competency	0.001283 *	0.40	0.6961	1.0000
mean-time-to-update*max-competency	0.005139 *	1.61	0.1104	0.9015
min-competency*max-competency	0.005030 *	1.58	0.1157	0.9178
max-competency*max-competency	0.000161 *	0.05	0.9609	1.0000
mean-time-to-update*mean-vulnerabilities-known	0.005997 *	1.88	0.0694	0.7447
min-competency*mean-vulnerabilities-known	0.003619 *	1.14	0.2418	0.9994
max-competency*mean-vulnerabilities-known	0.002044 *	0.64	0.5306	1.0000
mean-time-to-update*susceptibility-to-phishing	-0.000493 *	-0.15	0.8758	1.0000
min-competency*susceptibility-to-phishing	-0.002204 *	-0.69	0.4751	1.0000
max-competency*susceptibility-to-phishing	-0.001968 *	-0.62	0.5475	1.0000
mean-vulnerabilities-known*susceptibility-to-phishing	-0.001155 *	-0.36	0.7247	1.0000
mean-time-to-update*pc-percent-vulnerabilities	0.000187 *	0.06	0.9546	1.0000

Figure 5-18: Impact of Each Factor on the Variance of Integrity.

The number of vulnerabilities known by the hackers at the beginning of the simulation also increases the variability of the integrity metric. The more vulnerabilities the attackers know at the beginning of the simulation, the faster they may penetrate the network. As they penetrate the network, it may be easier for them to manipulate the configuration data files and obtain deeper footholds in the network. Lastly, increasing the susceptibility to phishing decreases the variability in the integrity. This is an interesting result because as the other factors mentioned in this paragraph and the prior, are not shown to be statistically significant to the expected value of integrity. What can explain this phenomenon is that as more users fall for phishing attacks, the attackers gain deeper access to the network more easily, making it easier for them to hop from one part of the network that contains integrity information to the other. The model is apparently indicating that attackers will penetrate the network modelled regardless of the propensity of users to fall for phishing attacks, but the lower the phishing, the more variability in the impact they will have on the integrity of the data in the network.

The last of the CIA metrics is availability, and the one that must traditionally be traded off against the first two. Figure 5-19 shows that the shutdown threshold, the number of attackers, and the probability of a sensor detecting an attack are the primary parameters that drive the availability of the network. The higher the threshold, i.e., the less sensitive to alarms, the higher the availability. The more attackers, or the more sensitive the sensors, the lower the availability. There are interesting interactions between these factors, e.g., if both number of attackers and the shutdown threshold increase, the availability goes up, as it does if shut-down threshold and the sensors' sensitivity increases. In addition, if one increases and the other decreases the availability is reduced. If both decrease, the availability increases. These interactions indicate that there are effects from these factors that put the model in different states and are critical when trying to find good balances between confidentiality, integrity and availability. Furthermore, these factors are doctrinal, materiel and noise parameters, once again, highlighting the complexity of the cyber problem and the need to assess them jointly.

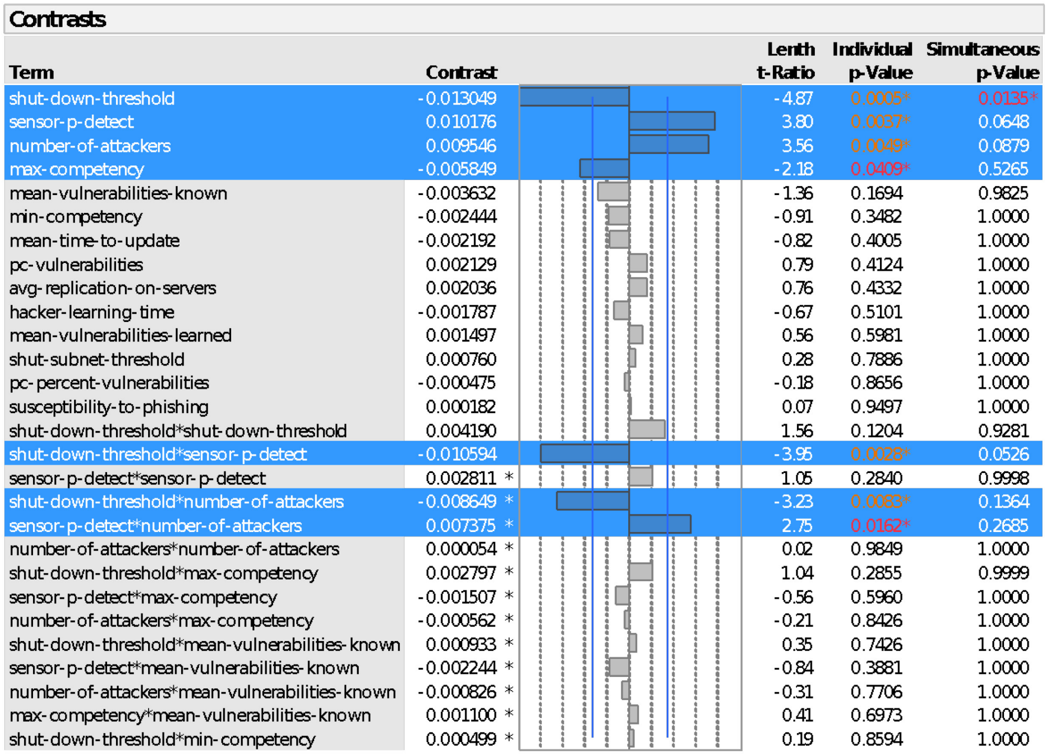


Contrasts

Term	Contrast	Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
shut-down-threshold	0.019217	3.03	0.0104*	0.1871
number-of-attackers	-0.015255	-2.41	0.0277*	0.3818
sensor-p-detect	-0.015033	-2.37	0.0293*	0.4021
max-competency	0.008239	1.30	0.1927	0.9902
mean-vulnerabilities-known	0.007787	1.23	0.2163	0.9953
pc-vulnerabilities	-0.005550	-0.88	0.3647	1.0000
hacker-learning-time	0.004850	0.77	0.4229	1.0000
mean-time-to-update	0.004444	0.70	0.4663	1.0000
min-competency	0.004225	0.67	0.5002	1.0000
mean-vulnerabilities-learned	-0.004194	-0.66	0.5117	1.0000
susceptibility-to-phishing	-0.001734	-0.27	0.7898	1.0000
shut-subnet-threshold	-0.001342	-0.21	0.8339	1.0000
avg-replication-on-servers	-0.000809	-0.13	0.8985	1.0000
pc-percent-vulnerabilities	0.000516	0.08	0.9348	1.0000
shut-down-threshold*shut-down-threshold	-0.006180	-0.98	0.3152	1.0000
shut-down-threshold*number-of-attackers	0.015878	2.51	0.0226*	0.3325
number-of-attackers*number-of-attackers	0.001255 *	0.20	0.8444	1.0000
shut-down-threshold*sensor-p-detect	0.014544 *	2.29	0.0322*	0.4482
number-of-attackers*sensor-p-detect	-0.012002 *	-1.89	0.0674	0.7271
sensor-p-detect*sensor-p-detect	-0.000347 *	-0.05	0.9573	1.0000
shut-down-threshold*max-competency	-0.004032 *	-0.64	0.5360	1.0000
number-of-attackers*max-competency	0.001484 *	0.23	0.8178	1.0000
sensor-p-detect*max-competency	0.003613 *	0.57	0.5811	1.0000
shut-down-threshold*mean-vulnerabilities-known	-0.002209 *	-0.35	0.7321	1.0000
number-of-attackers*mean-vulnerabilities-known	0.003493 *	0.55	0.5935	1.0000
sensor-p-detect*mean-vulnerabilities-known	0.004924 *	0.78	0.4167	1.0000
max-competency*mean-vulnerabilities-known	-0.004468 *	-0.70	0.4632	1.0000
shut-down-threshold*pc-vulnerabilities	0.000553 *	0.09	0.9302	1.0000

Figure 5-19: Impact of Each Factor on the Expected Value of Availability.

The variance in availability, shown in Figure 5-20, is also impacted by the maximum competency of the attackers. The variance in availability decreases when the maximum competency of the attackers increases. This can be attributed to the fact that more competent attackers may penetrate the network more easily and spend less time trying to enter, which reduces the likelihood that they will be detected by one of the sensors.



Contrasts

Term	Contrast		Lenth t-Ratio	Individual p-Value	Simultaneous p-Value
shut-down-threshold	-0.013049		-4.87	0.0005*	0.0135*
sensor-p-detect	0.010176		3.80	0.0037*	0.0648
number-of-attackers	0.009546		3.56	0.0049*	0.0879
max-competency	-0.005849		-2.18	0.0409*	0.5265
mean-vulnerabilities-known	-0.003632		-1.36	0.1694	0.9825
min-competency	-0.002444		-0.91	0.3482	1.0000
mean-time-to-update	-0.002192		-0.82	0.4005	1.0000
pc-vulnerabilities	0.002129		0.79	0.4124	1.0000
avg-replication-on-servers	0.002036		0.76	0.4332	1.0000
hacker-learning-time	-0.001787		-0.67	0.5101	1.0000
mean-vulnerabilities-learned	0.001497		0.56	0.5981	1.0000
shut-subnet-threshold	0.000760		0.28	0.7886	1.0000
pc-percent-vulnerabilities	-0.000475		-0.18	0.8656	1.0000
susceptibility-to-phishing	0.000182		0.07	0.9497	1.0000
shut-down-threshold*shut-down-threshold	0.004190		1.56	0.1204	0.9281
shut-down-threshold*sensor-p-detect	-0.010594		-3.95	0.0028*	0.0526
sensor-p-detect*sensor-p-detect	0.002811 *		1.05	0.2840	0.9998
shut-down-threshold*number-of-attackers	-0.008649 *		-3.23	0.0083*	0.1364
sensor-p-detect*number-of-attackers	0.007375 *		2.75	0.0162*	0.2685
number-of-attackers*number-of-attackers	0.000054 *		0.02	0.9849	1.0000
shut-down-threshold*max-competency	0.002797 *		1.04	0.2855	0.9999
sensor-p-detect*max-competency	-0.001507 *		-0.56	0.5960	1.0000
number-of-attackers*max-competency	-0.000562 *		-0.21	0.8426	1.0000
shut-down-threshold*mean-vulnerabilities-known	0.000933 *		0.35	0.7426	1.0000
sensor-p-detect*mean-vulnerabilities-known	-0.002244 *		-0.84	0.3881	1.0000
number-of-attackers*mean-vulnerabilities-known	-0.000826 *		-0.31	0.7706	1.0000
max-competency*mean-vulnerabilities-known	0.001100 *		0.41	0.6973	1.0000
shut-down-threshold*min-competency	0.000499 *		0.19	0.8594	1.0000

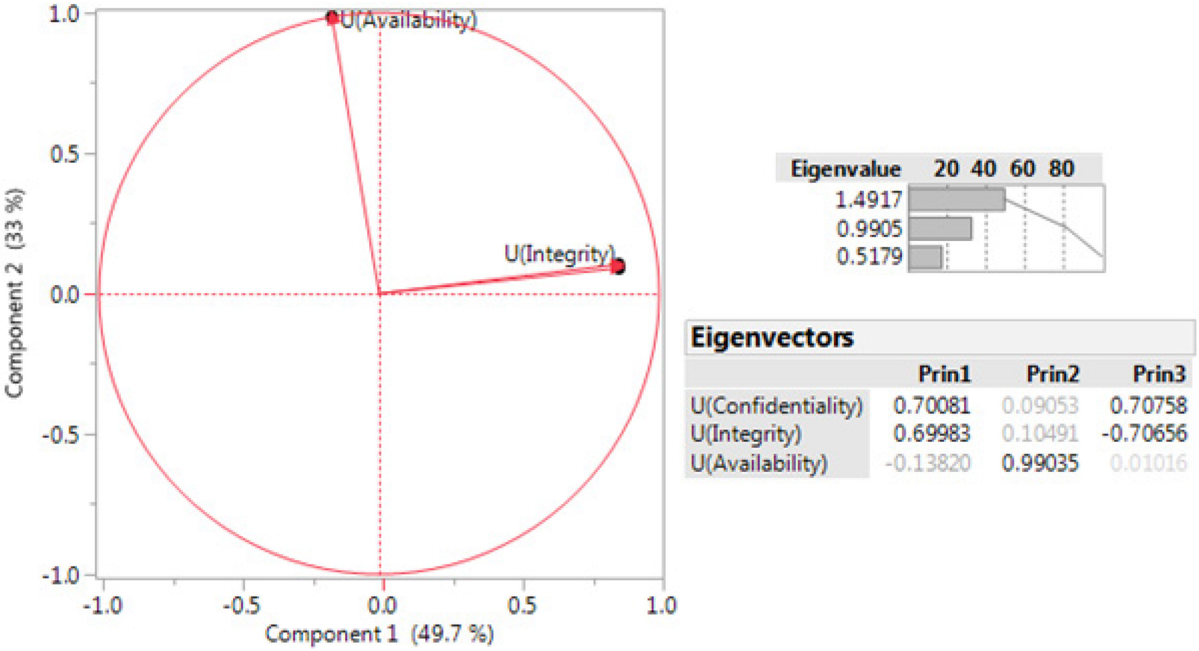
Figure 5-20: Impact of Each Factor on the Variance of Availability.

The variance in availability is reduced when the shutdown threshold is increased, but it increases with higher number of attackers and more sensitive sensors. The interaction factors are also statistically significant in explaining the variability in the availability of the systems.

5.4.3 Additional Analyses

The intent for additional analyses is to continue exploring the non-intuitive results and obtain high-performance computing resources to execute more explorations with smaller ranges for the number of attackers. Also, analysis using principal component analysis and a partition model would be beneficial and are illustrated in the three figures below.

Figure 5-21 depicts the principal component analysis of the three CIA metrics. As can be observed, the confidentiality and integrity metrics are highly correlated and relatively orthogonal to availability. This indicates that results with high integrity tend to have high confidentiality, and vice versa. These metrics are thus independent, from network availability.



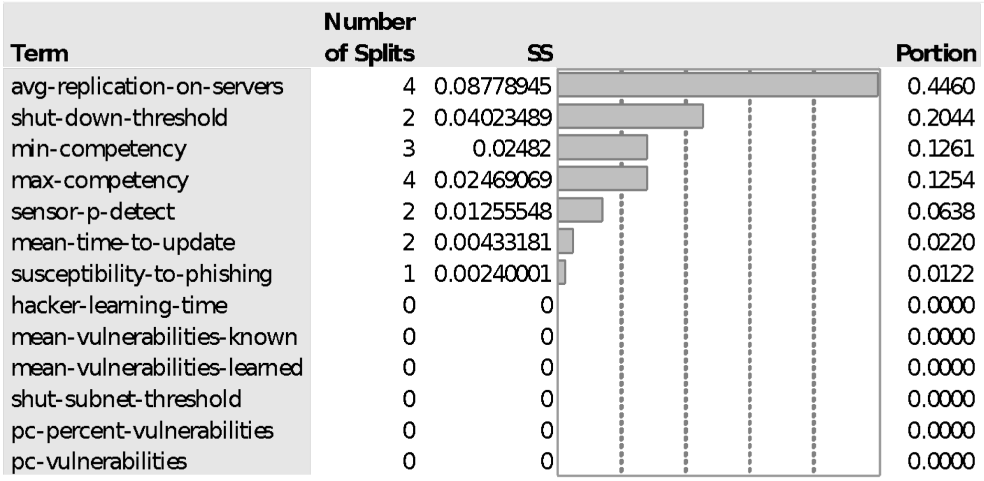
Eigenvalue
1.4917
0.9905
0.5179

Eigenvectors

	Prin1	Prin2	Prin3
U(Confidentiality)	0.70081	0.09053	0.70758
U(Integrity)	0.69983	0.10491	-0.70656
U(Availability)	-0.13820	0.99035	0.01016

Figure 5-21: Principal Component Analysis of Availability and Integrity as an Example.

Figure 5-22 shows the sorted factors from the partition tree, in this example, the average replication on servers describes 44% of the data, the network shutdown threshold an additional 20%, and so forth.



Term	Number of Splits	SS	Portion
avg-replication-on-servers	4	0.08778945	0.4460
shut-down-threshold	2	0.04023489	0.2044
min-competency	3	0.02482	0.1261
max-competency	4	0.02469069	0.1254
sensor-p-detect	2	0.01255548	0.0638
mean-time-to-update	2	0.00433181	0.0220
susceptibility-to-phishing	1	0.00240001	0.0122
hacker-learning-time	0	0	0.0000
mean-vulnerabilities-known	0	0	0.0000
mean-vulnerabilities-learned	0	0	0.0000
shut-subnet-threshold	0	0	0.0000
pc-percent-vulnerabilities	0	0	0.0000
pc-vulnerabilities	0	0	0.0000

Figure 5-22: Contribution of Control and Noise Factors on Cordon and Search Operations.

Figure 5-23 represents the results, using Cordon and Search Operations to exemplify, from the C4.5 algorithm [26]. The tree depicts the most efficient way for subdiving the data, where the most significant factors and their dividing limits are listed at the top of the tree, and subsequent less important factors and their limits are shown as leaves.

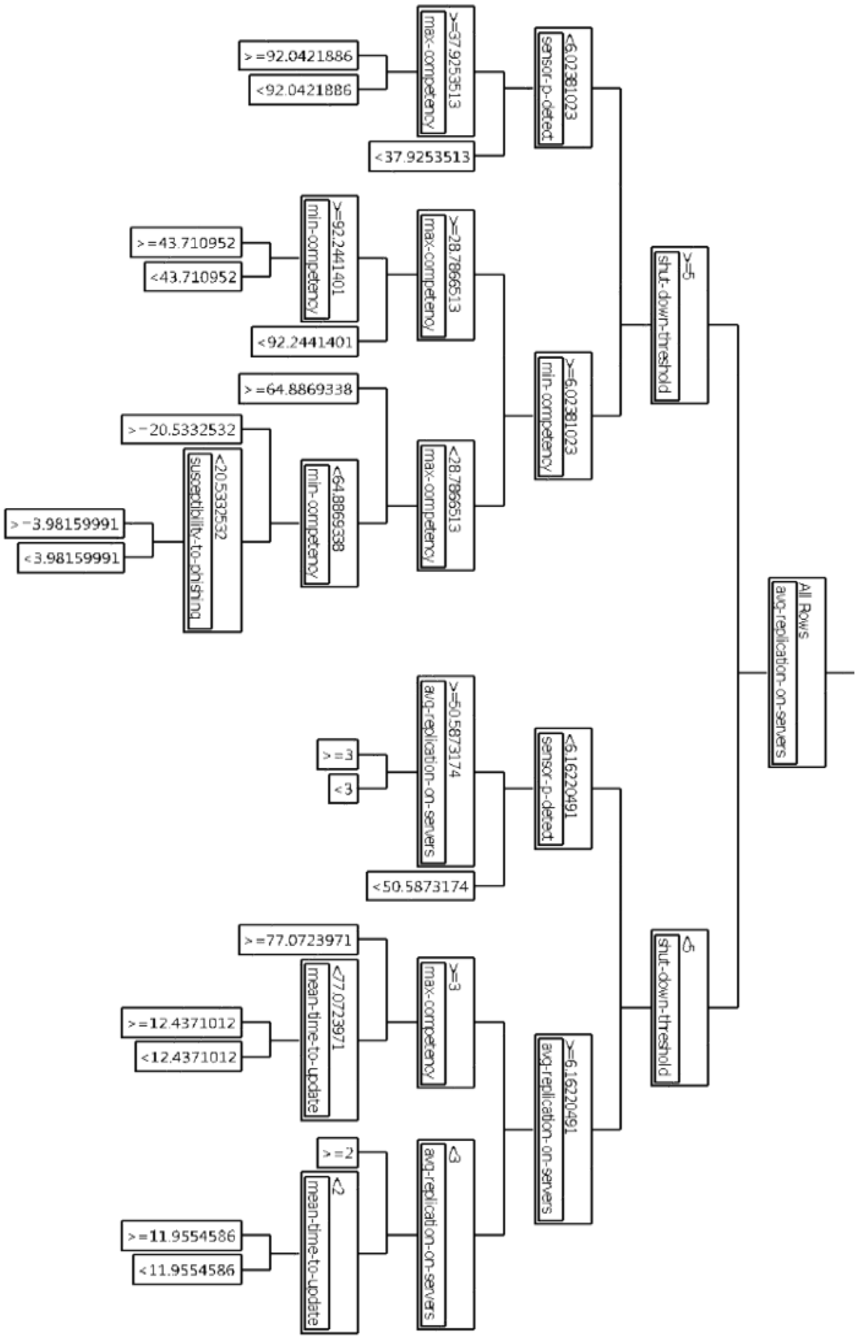


Figure 5-23: Partition Tree for Cordon and Search Operations.

The importance of conducting these additional analyses is twofold:

1) They test the model and offer an opportunity to improve it and ensure that it reflects SME expectations.
2) They offer decision makers a glimpse into the underlying behaviours that dominate the overall phenomena modelled.

5.4.4 Additional Explorations

The cyber syndicate members also evaluated changes to the model and performed some preliminary validation analysis. Some recent changes involving network shutdown were found to be unduly cautious and harmful to network operations. These changes were removed. The confidentiality, integrity, and availability metrics now reflect a more accurate representation of a network under targeted attacks.

One previous shortcoming of the model is that the competency of network operators was very simple and was more of a sliding scale between an operator's ability to detect intruders and attacks versus an operator's ability to handle known attacks. This scale was based on the uniform distribution. We experimented with using competency scores which reflected greater abilities to detect intruders and attacks rather than handling them. We found that a sigmoid distribution of probability based on the inverse cumulative distribution function of the normal distribution was a more realistic model of competency. The normal distribution minimizes assumptions for a given mean and variance of performance, and allows modellers to control scores on a wider, more intuitive range.

We found that focusing the operator's competency towards detecting rather than acting yielded improvements in confidentiality, about 4/1000ths of a "9" in uptime (where one 9 of uptime is 90%, two 9s are 99%, three 9s are 99.9%, etc.). We did not find any significant changes to the integrity or availability scores. These results suggest that focusing operator training on detection is a better investment than performing corrective actions.

5.4.5 DFTOP Applications to Cyber Defence Decision Making

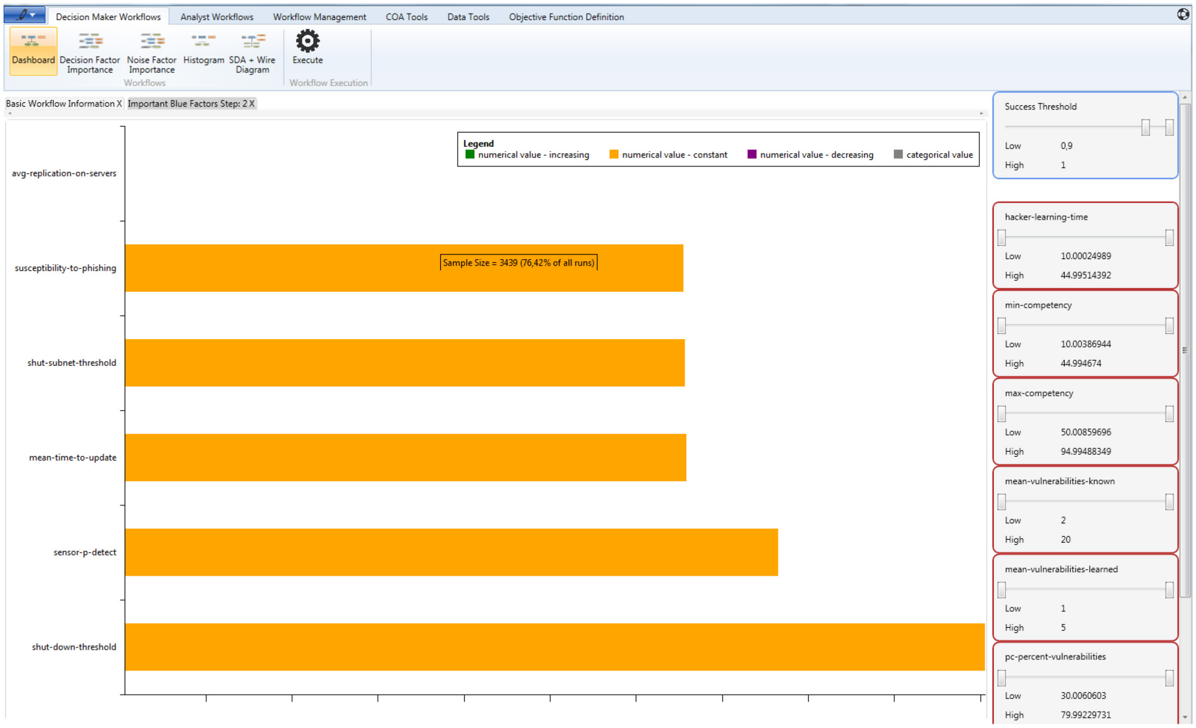
DFTOP was developed and applied successfully within the Operational Planning syndicate of MSG-124, as described in the previous chapter. It is a tool for multi-criteria decision making support. DFTOP was developed to support the collaborative processes of Data Farming between the analysts (knowing what and how they are analysing), between analysts and decision makers and between decision makers. Furthermore, it lowers the effort needed to perform iterative analysis, using reusable workflows.

The application of DFTOP is possible for all question bases with decision factors, noise factors and MOEs on both sides in a result output data base. It consolidates all outputs to facilitate understanding independently of specialized statistics tools (e.g., JMP) and combines the results with the intuition of the decision maker which is expressed in a highly flexible preference analysis. The application of DFTOP to our Cyber question base is a proof of that principle.

This section describes the application of DFTOP on simulation results generated by the Cyber Defence Syndicate using its DACDAM model. It should be emphasized that the DFTOP output presented herein is only an illustration on how the presentation of simulation results can be enhanced by using the DFTOP tool. Though the results are simply illustrative, they basically highlight the salient features of DFTOP such as user friendliness and versatility, and give tangible examples for the types of trades and analyses that DFTOP can support.

Figure 5-24 displays how the most important (critical) decision factors influence the success, where we set the success threshold for simulation runs at 0.9. Figure 5-24 highlights that out of all the critical factors (vertical axis) under examination, shutdown threshold has the highest effect on the success (horizontal axis). It should be emphasized that the graph only depicts the qualitative measures of the critical factor; highest numerical value on a critical factor indicates it has more influence on the overall success than the other critical factors.

For the top 10 per cent (best 10%) runs contributing to the overall success, the most important (critical) factors and their specific value ranges are summarized in Figure 5-25. Green parameter values (or attributes) contribute the most to overall success, whereas orange parameter values degrade the overall success by the most.


Decision Maker Workflows
Analyst Workflows
Workflow Management
COA Tools
Data Tools
Objective Function Definition
Dashboard
Decision Factor Importance
Noise Factor Importance
Histogram
SDA + Wire Diagram
Workflows
Execute
Workflow Execution
Basic Workflow Information X
Important Blue Factors Step: 2 X
Legend
numerical value - increasing
numerical value - constant
numerical value - decreasing
categorical value
avg-replication-on-servers
susceptibility-to-phishing
Sample Size = 3439 (76,42% of all runs)
shut-subnet-threshold
mean-time-to-update
sensor-p-detect
shut-down-threshold

Success Threshold
Low 0,9
High 1

hacker-learning-time
Low 10.00024989
High 44.99514392

min-competency
Low 10.00386944
High 44.994674

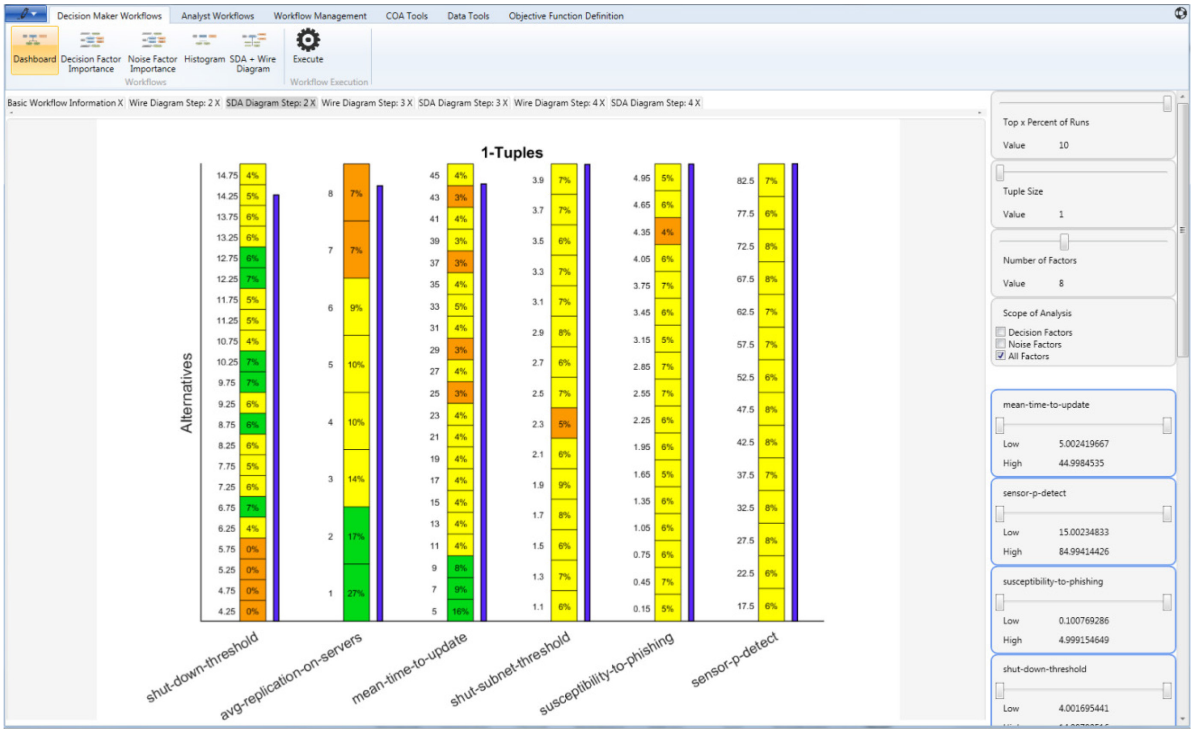
max-competency
Low 50.00859696
High 94.99488349

mean-vulnerabilities-known
Low 2
High 20

mean-vulnerabilities-learned
Low 1
High 5

pc-percent-vulnerabilities
Low 30.0060603
High 79.99229731

Figure 5-24: Most Important Decision Factors Influencing Overall Success.



Top x Percent of Runs
Value 10

Tuple Size
Value 1

Number of Factors
Value 8

Scope of Analysis
☐ Decision Factors
☐ Noise Factors
☑ All Factors

mean-time-to-update
Low 5.002419667
High 44.9984535

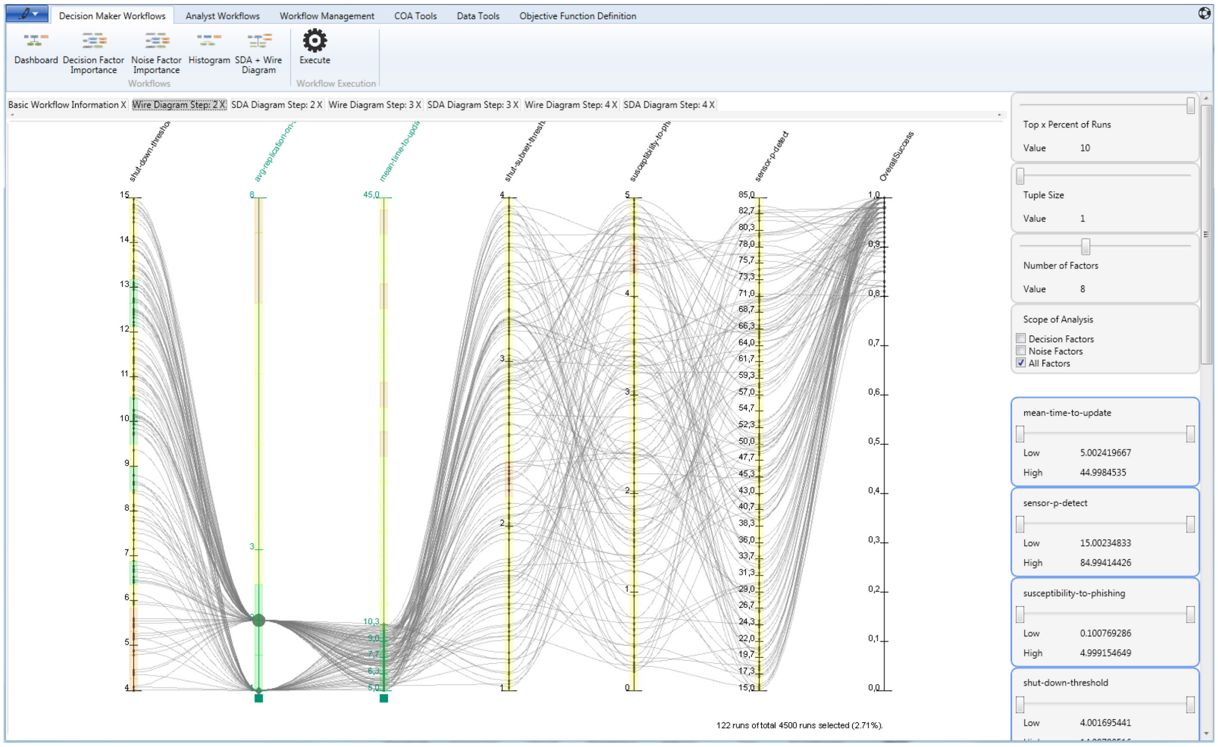
sensor-p-detect
Low 15.00234833
High 84.99414426

susceptibility-to-phishing
Low 0.100769286
High 4.999154649

shut-down-threshold
Low 4.001695441

Figure 5-25: SDA Diagram for the Most Important Factors.

In Figure 5-26, the most important (critical) factor and their specific value ranges contributing to the overall success are represented by vertical straight lines. By tracing each curve line (representing an individual simulation run) and its intercept with each vertical line, the various combinations of critical factor values on the overall success can be studied. The interrelationships between the critical factors are easily highlighted by the figure. The figure displays results for the top 20% runs, the scales of the critical factors are in accordance with those in Figure 5-24 and Figure 5-25. The figure represents a particular set of parameter values pre-specified by the user only for illustrative purposes.



Top x Percent of Runs
Value 10

Tuple Size
Value 1

Number of Factors
Value 8

Scope of Analysis
☐ Decision Factors
☐ Noise Factors
☑ All Factors

mean-time-to-update
Low 5.002419667
High 44.9984535

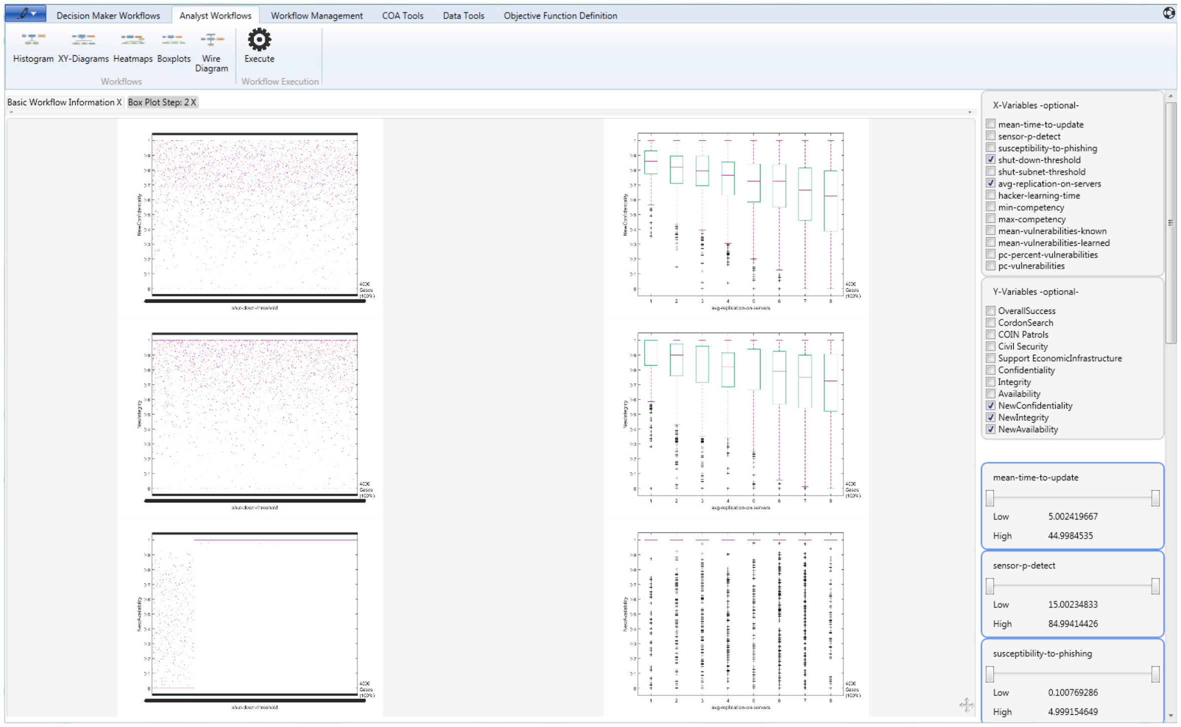
sensor-p-detect
Low 15.00234833
High 84.99414426

susceptibility-to-phishing
Low 0.100769286
High 4.999154649

shut-down-threshold
Low 4.001695441

Figure 5-26: Wire Diagrams with SDA Overlay for the Most Important Factors.

The box-plots and heat-maps in Figure 5-27 and Figure 5-28 illustrate the influence of parameter values on a single MOE (confidentiality, integrity, availability) and their subsequent contribution to the overall success. The relative shades of green and yellow indicate the degree of low and high values respectively.



X-Variables -optional-

- ☐ mean-time-to-update
- ☐ sensor-p-detect
- ☐ susceptibility-to-phishing
- ☑ shut-down-threshold
- ☐ shut-subnet-threshold
- ☑ avg-replication-on-servers
- ☐ hacker-learning-time
- ☐ min-competency
- ☐ max-competency
- ☐ mean-vulnerabilities-known
- ☐ mean-vulnerabilities-learned
- ☐ pc-percent-vulnerabilities
- ☐ pc-vulnerabilities

Y-Variables -optional-

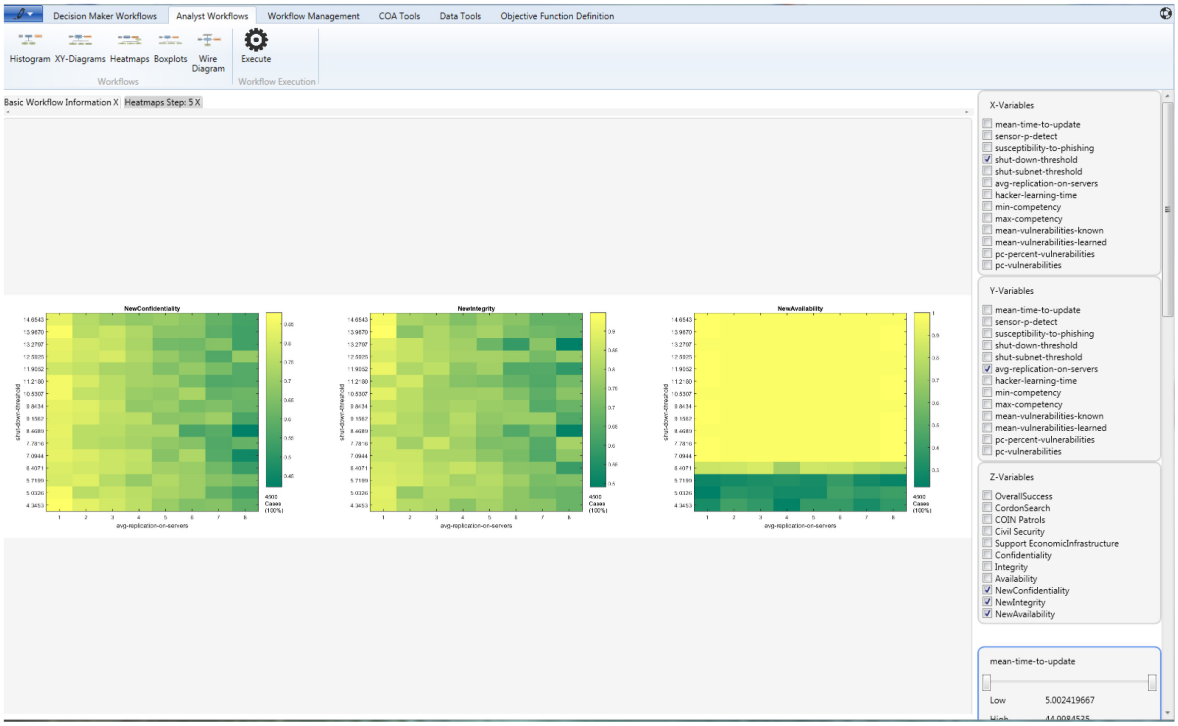
- ☐ OverallSuccess
- ☐ CordonSearch
- ☐ COIN Patrols
- ☐ Civil Security
- ☐ Support EconomicInfrastructure
- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☑ NewConfidentiality
- ☑ NewIntegrity
- ☑ NewAvailability

mean-time-to-update
Low 5.002419667
High 44.9984535

sensor-p-detect
Low 15.00234833
High 84.99414426

susceptibility-to-phishing
Low 0.100769286
High 4.999154649

Figure 5-27: Box Plots.



X-Variables

- ☐ mean-time-to-update
- ☐ sensor-p-detect
- ☐ susceptibility-to-phishing
- ☑ shut-down-threshold
- ☐ shut-subnet-threshold
- ☐ avg-replication-on-servers
- ☐ hacker-learning-time
- ☐ min-competency
- ☐ max-competency
- ☐ mean-vulnerabilities-known
- ☐ mean-vulnerabilities-learned
- ☐ pc-percent-vulnerabilities
- ☐ pc-vulnerabilities

Y-Variables

- ☐ mean-time-to-update
- ☐ sensor-p-detect
- ☐ susceptibility-to-phishing
- ☐ shut-down-threshold
- ☐ shut-subnet-threshold
- ☑ avg-replication-on-servers
- ☐ hacker-learning-time
- ☐ min-competency
- ☐ max-competency
- ☐ mean-vulnerabilities-known
- ☐ mean-vulnerabilities-learned
- ☐ pc-percent-vulnerabilities
- ☐ pc-vulnerabilities

Z-Variables

- ☐ OverallSuccess
- ☐ CordonSearch
- ☐ COIN Patrols
- ☐ Civil Security
- ☐ Support EconomicInfrastructure
- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☑ NewConfidentiality
- ☑ NewIntegrity
- ☑ NewAvailability

mean-time-to-update
Low 5.002419667
High 44.9984535

Figure 5-28: Heat Maps.

As can be seen in the above illustrations, the effects of the critical factors on the overall success are displayed in summary forms with the DFTOP tool. It can enable valuable and meaningful insights to be gathered easily and conveyed to military decision-makers in a timely manner.

5.5 DISCUSSION AND POSSIBLE FURTHER WORK

The work that went into the cyber model presented above represents just a start of a potentially much larger modelling effort. Many improvements can be made and the first improvement we are considering is to increase the fidelity and granularity of the sensors to be considered as well as including the possibility for the attacker to attack the sensors themselves. This effort will involve creating a catalogue of sensors and compiling their characteristics. These characteristics can then be mapped to the behaviour of the agents in the simulation and their processes. The outcome of this improvement will not only be a more accurate representation of the sensors, but it will also augment the fidelity of the system administrator and the attackers by requiring their processes to be adapted to capture the implications of the different sensor families on their own tasks and processes.

The behaviour model of the system administrator can also be improved by accounting for the type of sensor triggering the alarm, and adding a memory aspect to it, such that it can associate certain type of attacks effects with attacks. The ultimate level of complexity is a learning system administrator that adapts as the attackers perform their actions. Conversely, the attackers could adapt their tactics and processes as a function of the network, the system administrator and the sensors. This will require extensive effort, as the possible behaviour space of both the system administrator and the attackers must first be fully characterized and parameterized. With this parametric behaviour space for both types of agents, an evolutionary algorithm can be implemented to evolve the most successful tactics and procedures. In this implementation, a genetic algorithm could be included to vary the threshold parameters as a function of the network availability and the number of detected attacks. It is important not to imbue unrealistic abilities to these algorithms, i.e., making the fitness a function of properties that are not observable in reality.

Networks are frequently instrumented with numerous types of detections of and protections against intrusions and attacks. The current model uses generic sensors to indicate questionable or malicious events. Greater fidelity may be achieved by adding honeypots, Intrusion Detection Systems (IDSs), and Intrusion Prevention Systems (IPSs). Honeypots are decoy network elements, nodes, or data that look like targets the attackers would like to obtain, but instead are traps that indicate that an intrusion has taken place and sometimes can reveal details about the attacker. Honeypots are a part of a larger IDS, which attempts to detect intruders based on traffic, usage patterns, policies, malware signatures, and sometimes machine learning. When an IDS is considered sufficiently reliable, an IPS can be deployed which automatically blocks, shuts down, disables, or otherwise attempts to prevent active attacks from happening in real-time. The challenge with IPSs is that if the IDS determines that legitimate traffic or use is intrusion, the IPS can needlessly shutdown services or lock out legitimate users. For these reasons, IPSs are often more expensive to train and maintain. Honeypots, IDSs, and IPSs can be implemented within the model as trade-offs that can be made in the network, and data farming can be utilized to help answer questions related to where and when these types of systems should be deployed to maximize mission objectives. Another strong and growing trend within data centre deployments is the use of virtualisation and sandboxing to separate applications and data to increase the total number of layers that attackers must penetrate to be successful. Containers, virtual machines, and other sandbox environments can improve the ease of deployability and increase the granularity of access that admins can be granted, so that a single compromised account is of lower liability. The drawback of using different types of sandboxing and virtualisation is that there can be associated performance, management, and licensing costs. Modelling these types of trade-offs is another area where data farming could provide recommendations and insight from both security and operational perspectives.

The current model has a single attack type for phishing. Phishing is when an attacker attempts to send emails, messages, or other forms of communication in order to trick a user into accepting malicious information that may cause harm to the system or relinquish control or data to the attacker. When IT systems are well-protected, advanced attackers will often choose to attempt spearphishing. Spearphishing is a form of highly targeted phishing in which the attacker learns personal and work details about a single target and attempts to bypass normal scepticism and gain the trust of a single individual to compromise their account. Successful spearphishing attacks can yield powerful credentials. Though they are more difficult than phishing and target only one or a very small number of users, successful attacks typically yield more valuable results. The model can be modified such that phishing attacks can be parameterised and split into phishing and spearphishing attacks.

Attackers frequently look for different types of data and use different kinds of attacks for different purposes. Similarly, attackers can range vastly in scale, from an individual hacker with few resources all the way up to sophisticated state-sponsored actors. Though the current model can describe a range of attackers, the behaviours typically change with scale. Some attackers may be more interested in shutting down the network or services, whereas other attackers may be looking for sensitive strategic information, and yet another kind of attacker may simply be looking for information by which to shame or embarrass the target. In real-world attacks, attackers frequently use one type of attack for feints while performing a more nefarious attack or exfiltration that they hope will go unnoticed. Attacks which perform some sort of denial of service may also be used to increase confusion and reduce target resiliency in conjunction with a kinetic attack. Adding richer core motivations of denial or exfiltration, improving attack patterns to encompass multiple simultaneous attacks, and modelling different kinds and sensitivities of information in different parts of the network with different interests to the target and implications to the attacker are all ways that would improve the quality of data farming results.

Implementing different types of Denial of Service (DoS) are also of interest to improving the attacker’s arsenal to better represent real-world scenarios. The current model employs a vulnerability-based denial of service attack. This attack is more prevalent against military and healthcare targets, the former for reduction in capabilities or to measure responses and the latter for encrypting large amounts of sensitive data to be ransomed back to the provider (known as ransomware). A Distributed Denial of Service (DDoS) attack is when many devices are used across many networks attempt to continually request service at the same time. Attackers utilizing DDoS typically use botnets of compromised machines, but may also have a large amount of network and computing facilities. With the growing Internet of Things (IoT), many vendors are selling cheap devices that have very little security, making it easier for attackers to easily compromise those devices and assemble vast botnets to create large DDoS attacks. Handling DDoS attacks are a bit different than the aforementioned vulnerability-based DoS attacks, and typically require some form of IDS/IPS combination or increasing capacity to mitigate the DDoS load while still providing the needed services. DDoS are more likely to be targeted at externally available services or using a large number of internally compromised nodes, whereas a vulnerability-based DoS is more likely to target a specific kind of data or service that may be more hardened. A third type of DoS is physical DoS, which can include power or other utility outages, kinetic attacks, and flooding. A sufficiently resilient network should be able to handle all three of these DoS attacks, vulnerability-based DoS, DDoS, and physical DoS. A richer DoS model could better inform network design to handle a wider range of attacks.

Availability is vitally important within the CIA triad (Confidentiality, Integrity, Availability). Though the current model assigns value to each property of the CIA triad, network security is often about tradeoffs between security, costs, and performance. The value and performance models can be improved to include operational values such as quality of service such as bandwidth and latency in its aggregation of availability. Similarly, although network value is often quadratic for communication purposes, the value that availability of IT systems brings to missions may add linearly or nonlinearly based on the data.

When modelling, it is crucial to have an understanding of the question that is to be answered. These recommended improvements to the model assume that the direction that has been undertaken aligns with the needs to NATO and the nations. For this reason the changes recommended are essentially improvements and refinements of the existing model.

The agent-based modelling paradigm, using NetLogo in particular, is suitable for exploratory studies such as this one, but it is not the most computationally efficient approach to analysing systems such as these. Discrete Event Simulation provides a more efficient approach to analysing such networks, but it requires a more rigid modelling approach and is more difficult to adapt. If the model was to be translated into a discrete event simulation form, it could leverage the lessons learnt from the development of the agent-based model, such as the method for modelling the cyber-attackers, the generation of the network, the processes the attackers use to attack the network, etc.

Although data farming is useful for understanding system behaviour in the current implementation, adversaries in the cyber domain may act strategically and can optimize their decisions with respect to their own objectives rather than engage in predictable behaviour. DACDAM currently uses simple attacker motivations and behaviour, and does not consider strategic optimization techniques of combining actions to maximize ambiguity, minimize detection, and maximize damage. Real world attackers may behave consistently over a period of time, but may behave quite differently under unusual circumstances. This fact means that the current model is useful for modelling typical situations of expected value, but may not be applicable to more active cyber conflict situations. Game theoretic approaches, reputation analysis, ambiguity management, and decision theory could all be used to augment attacker behaviour and greatly improve the reliability of the results of data farming for network resiliency. Any operational deployment of data farming should include an advanced model for optimizing attackers.

5.6 CONCLUSIONS

The overall goal of this syndicate was to leverage the current research, develop a suitable simulation, and explore possible scenarios through data farming that could facilitate the understanding of some aspects of cyber defence important to NATO. The supporting tasks for this goal were as follows:

- Conduct background research and work in the area of the application of data farming methodology to cyber security, perform exploration work up to and including the data farming workshops, and build on the workshops results on the application of data farming to cyber security questions. The models and the scenarios developed allowed for the exploration of the parameter space in a data farming environment.
- Define questions within the cyber defence area in conjunction with cyber defence experts at ACT, within the MSG-124 nations, and in general. Assist in the analysis and iterative exploration of “What-If?” questions to reveal the landscape of possibilities inherent in the scenarios and enable the study of any “outliers” that are discovered.
- Provide modelling and simulation support for various cyber defence questions. The simulation developed used the NetLogo model, open source software that could be easily shared by work teams such as the MSG-124 Cyber Defence Syndicate.

The work of this syndicate was focused on the decision maker as the DACDAM concept and simulation was developed. DACDAM was developed to be interactive with data visualisation to support decision making using the construct of data farming.

Data farming techniques proved to be useful as evidenced by the accomplishment of the tasks of this syndicate as well as achieving the overall goal as documented in this report. Some of the most notable results that can be inferred from the notional model as exercised by the data farming process were:

- Confidentiality and integrity were orthogonal to availability; and
- The attack volume was the driving parameter of all the resiliency and performance metrics.

It is logical to recognize that confidentiality and integrity can be improved by reducing availability. DACDAM as exercised by the data farming process illustrated by the principal component analysis of the CIA metrics.

Our findings confirm and agree with tenets espoused by Van Dijk *et al*. [16] in their study of cyberspace operations. Their three takeaways were:

- Everything can be compromised, including cryptographic keys;
- Aggressive offense dominates, but if not possible due to other constraints, an efficient defence is paramount; and
- Closely monitor your resources.

This notional application of data farming to cyber defence highlights the importance and burden of acquiring appropriate data and validating the relationships thereof. For this process to be used in real decision support, considerable effort must be expended to develop and validate an accurate model (which includes gathering all the appropriate data) and set of scenarios that are pertinent to the questions at hand.

The team conducted background research, and developed proof-of-concept models and scenarios to explore a notional parameter space. This report presents an application of data farming to cyber security that can serve as a baseline for future applications.

The authors defined a series of questions within the cyber defence domain in conjunction with cyber defence experts at ACT and within the MSG-124 nations. The developed simulation used the NetLogo model, open source software that could be easily shared by multinational and multidisciplinary work teams.

In summary, the cyber syndicate considers that the cyber defence objectives set out in the TAP for MSG-124 have been achieved. In a package separate from this final report, but as part of the final deliverables for MSG-124, the parameter data, the model source code, and the resulting data are compiled into a data storage media and provided to NATO STO Secretariat for dissemination and archiving purposes.

5.7 REFERENCES

[1] Wilensky, U., NetLogo, Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL, 1999. http://ccl.northwestern.edu/netlogo/.

[2] Scythe, Proceedings and Bulletin of the International Data Farming Community, Issue 16, Workshop 28, Publication date: October 2014.

[3] Scythe, Proceedings and Bulletin of the International Data Farming Community, Issue 17, Workshop 29, Publication date: September 2015.

[4] Nurse, J.R.C., et al. Understanding insider threat: A framework for characterising attacks. Security and Privacy Workshops (SPW), 2014 IEEE. IEEE, 2014.

[5] Brannsten, M.R., Johnsen, F.T., Bloebaum, T.H. and Lund, K. Toward federated mission networking in the tactical domain, in IEEE Communications Magazine, vol. 53, no. 10, pp. 52-58, October 2015.

[6] Siedler, R.E. and Johnsen, S.T., Handbook for Integrating Cyber Defense into the Operational Planning Process v1.0, Multinational Capability Development Campaign (MCDC) 2013-14: Combined Operational Access, 2014.

[7] Siedler, R.E. and Johnsen, S.T., Guidelines for Integrating Cyber Defense into the Operational Planning Process v1.0, Multinational Capability Development Campaign (MCDC) 2013-14: Combined Operational Access, 2014.

[8] U.S. Army Training and Doctrine Command (TRADOC), The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, TRADOC Pamphlet 525-7-8, 22 February 2010.

[9] Cyber Primer, 2nd Edition, UK Ministry of Defence, 2016.

[10] APP-06 Edition 2014, NATO Glossary and Definitions (English and French), NATO Standardization Agency, 2014.

[11] Hutchins, E., Cloppert, M. and Amin, R. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 6th International Conference on i-Warfare and Security, 2011.

[12] Anteroinen, J., Enhancing the Development of Military Capabilities by a Systems Approach. National Defence University. PhD Thesis. Series 1: Publication no. 33, August 2013.

[13] Dinsmore, P., et al. "NIPRNet/SIPRNet Cyber Security Architecture Review." US Government publication. Presented at the 2016 AFCEA Symposium. 21 April 2016.

[14] Ouyang, M., "Review on modeling and simulation of interdependent critical infrastructure systems." Reliability engineering & System safety 121 (2014): 43-60.

[15] Pavlovic, D., "Gaming security by obscurity." Proceedings of the 2011 workshop on New security paradigms workshop. ACM, 2011.

[16] Van Dijk, M., et al. "FlipIt: The game of 'stealthy takeover'." Journal of Cryptology 26.4 (2013): 655-713.

[17] "2016 data breach investigations report." Verizon RISK Team, (2016): 1-80, Available: www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf, PDF, accessed 27 March 2017.

[18] Canal, V.A., "On Information Security Paradigms," ISSA Journal, September 2005.

[19] Koret, J. and Bachaalany, E. The antivirus hacker's handbook. John Wiley & Sons, 2015.

[20] de Souza, I.G., Berk, V.H., Giani, A., Bakos, G., Bates, M., Cybenko, G. and Madory, D. "Detection of Complex Cyber Attacks," Proc. SPIE 6201, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defence V, 620106, May 10, 2006.

[21] Karpati, P., Opdahl, A.L. and Sindre, G. "HARM: Hacker Attack Representation Method," Software and Data Technologies, vol. 170, pp. 156-175, 2013.

[22] Eom, J.H., Han, Y.J., Park, S.H. and Chung, T.M. "Active Cyber Attack Model for Network System's Vulnerability Assessment," in proceedings of the International Conference on Information Science and Security, pp. 153-158, 2008.

[23] Kotenko, I. "Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in Internet," in 19th European Simulation Multiconference Simulation in wider Europe, 2005.

[24] Tidwell, T., Larson, R., Fitch, K. and Hale, J. "Modeling internet attacks," in proceedings of the 2001 IEEE Workshop on Information Assurance and security, vol. 59, 2001.

[25] Jones, B. and Nachtsheim, C.J. "A Class of Screening Designs Robust to Active Second-Order Effects." mODa 9–Advances in Model-Oriented Design and Analysis. Physica-Verlag HD, 2010. 105-112.

[26] Quinlan, J.R. C4.5: programs for machine learning. Elsevier, 2014.

Chapter 6 − SUMMARY AND RECOMMENDATIONS TO NATO

Through MSG-124, the capabilities of NATO, PfP, and Contact Countries, schools, and agencies have been harnessed to document the potential value of applying data farming in an actionable way to provide military benefit. The core objective of this Task Group was to apply actionable data farming in order to support capabilities within NATO, PfP, and contact countries and agencies that could contribute to the development of improved decision making of relevance to NATO forces. Explorations involving two questions of interest to NATO decision makers were undertaken. These areas were operation planning and cyber defence. The Task Group took the results of concept explorations and assessments of possible Courses Of Action (COA) in these question areas to recommend and demonstrate a way forward.

Data farming has always been question-based, but an insight that drives action is more valuable than one that simply answers a question. Data farming enables the examination of a vast number of possibilities, transforming data into insights through analysis. This exploratory analysis can produce information that subsequently can be used to guide decision makers. These insights become actionable when they are developed quickly enough to be aligned with the decision making process to produce relevant options reflecting the Commanders' intent.

Based on the work performed on operation planning and cyber defence, we conclude that data farming can be applied to actionable decision support. We now summarize our recommendations on how to proceed with the development of data farming within NATO.

6.1 OPERATION PLANNING

One of the products from this Task Group is the *Data Farming Tool for Operation Planning* (DFTOP), a tool that supports the Commander in evaluating operation plans, analysing a broad set of COA. The support is aligned with the NATO planning process COPD, here exemplified at the joint level, providing support for the JOPG in Phase 3b. This allows the JOPG to get better insights into operations, and make decisions based on much broader decision grounds. With DFTOP, the possibilities of quantitative simulation-based analysis are made readily available to decision makers and planners at the operational level.

DFTOP enables the JOPG to analyse the spectrum of feasible COA. This process allows the JOPG to develop plans based on a robust and reproducible dataset, and to make objective recommendations to the Commander. The DFTOP prototype was demonstrated in a relevant environment at the *Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise* (CWIX) in 2016. Experience from CWIX confirms that DFTOP successfully brings data farming into the *actionable* decision support domain, translating the results of the analysis to visualizations directly adapted to the decision maker's needs.

To provide actionable decision support, it is important that insights are developed quickly enough to be aligned with the decision making process. Therefore, we recommend integration with the existing NATO *Tool for Operational Planning Functional Area Service* (TOPFAS). In order to succeed in this endeavour, further testing, validation and experimentation with potential end-users and other stakeholders is necessary.

We recommend further testing with other simulation models to extend the current application area to other areas of interest and to demonstrate the full flexibility of DFTOP. This may also facilitate an extension of the decision support to other organizational levels. It could also be useful to extend DFTOP with additional workflows in order to support other steps in the planning process, e.g., Phase 3a (mission analysis).

6.2 CYBER DEFENCE

To address questions related to cyber defence we conducted background research and developed proof-of-concept models and scenarios to explore a notional parameter space. As a result we developed the *Data-farmable Agent-based Cyber Defence Assessment Model* (DACDAM). This model was intended to test the applicability of data farming to cyber defence. Even though the model was a proof-of-concept effort and the results were intended to be illustrative, they did seem to agree at the highest levels with reputable research in the cyber domain.

We conclude that data farming is a suitable approach to answer the strategic and operational questions that may arise within the cyber domain. It is imperative that the organizations supporting these studies are willing and able to do so, as it may require a non-trivial level of effort. While researching the topic, we discovered that there are very few efforts employing quantifiable decision support means to strategic planning of cyber defence systems and networks. Data farming is shown to be a suitable framework for developing the quantifiable analysis required to answer these questions in a defensible and traceable manner. The rapid scenario prototyping has proven to be one of the most valuable steps in the data farming process, given the level of maturity of publicly available cyber defence modelling capabilities.

6.3 OVERALL DATA FARMING RECOMMENDATIONS

Any operational deployment of data farming should include an advanced model of strategically optimizing attackers or Red forces. We recommend that future approaches use data farming in conjunction with established techniques and algorithms like game theory, reputation analysis, ambiguity management, and decision theory to augment attacker behaviour.

One of the benefits of DFTOP is reducing the effort needed to perform data farming analysis. The DFTOP concept streamlines the analysis, but it is flexible enough to be adapted to a set of widely different simulation models. This was demonstrated with the integration of DACDAM with DFTOP. With DFTOP, we have mainly focused on the *analysis and visualisation* step. The positive experience from DFTOP motivates a recommendation to extend it to the other data farming realms. In making the process easier to use, we lower the effort required to apply data farming in any application area. We recommend development of a tool suite for data farming services supporting all the steps in the data farming process, in order to make analysis and simulation-based decision support more readily available.

Based on the results obtained by this Task Group, the final conclusion and recommendation to military leaders is that data farming is feasible for NATO and nations, and should be used as a methodology for actionable decision support in operation planning and cyber defence.

Appendix 1 – DFTOP IMPLEMENTATION

A1.1 DFTOP IMPLEMENTATION DETAILS

In this section the technologies used to implement DFTOP is presented. This covers the used development platform, programming languages, software architecture, and statistical and visualisation tools. Furthermore, a brief presentation of the GUI, GUI elements, GUI usage and key processes in the DFTOP application are presented.

A1.1.1 Technology Selection

The following technologies were selected to implement DFTOP:

- The user and workflow management domain is built in C# using the Visual Studio.
- Analysis and visualisation modules are implemented using the programs MATLAB, JMP, C#, Java and Tableau.
- Visualisations of MATLAB are saved as images which are shown in DFTOP, C# visualisations are created directly in DFTOP and the application windows of JMP and Tableau are integrated into DFTOP.
- The data domain is based on a Microsoft SQL Server Local database which is shipped with Visual Studio. Data import is supported using Microsoft Excel spreadsheets.
- Workflows are defined using XAML documents.
- Data exchange between domains is either done by transferring data via the database, images on the file system, direct method invocation or XAML string objects.

This technology selection offers the possibility to use the highly sophisticated analysis and visualisation capabilities of MATLAB, JMP and Tableau with a seamless integration of them all into a single DFTOP application. The main DFTOP application will require an interface library for each external application, i.e., MATLAB, JMP. Using this modular approach, additional applications can be added to DFTOP by providing this small library. Furthermore all parts of DFTOP that do not require a certain external application will work, even if that application is not available on the specific computer.

DFTOP will only work on computers running Windows, but this should not be a problem since it is the standard operation system in industry and military. Running a fully functional DFTOP requires MATLAB and JMP. Since the local MS SQL database is used, also a license of Visual Studio is necessary, even if no development is planned on a specific computer. For Tableau the Tableau Desktop version is recommended, which also adds license costs, but if no workflow development is planned, the free Tableau Reader version of the application can be used. Also for using Java no license costs incur. Additionally Microsoft Excel is mandatory for DFTOP execution.

A1.1.2 Architecture Overview

Development was conducted using Visual Studio 2013, JMP 11, MATLAB 2015a (+ Statistics and Database toolboxes), MS SQL Server using the localdb\v11.0 setting shipped with Visual Studio, Tableau 9, Java 7 and .NET 4.5.1. Downward compatibility of MATLAB, .NET and Visual Studio was only partially tested. MATLAB must be available in version 2014a or newer. Upward compatibility is (as of September 2015) not available for

Java programs, since the JDBC-ODBC-bridge was removed from Java 8 and ODBC is the protocol used to access the database. The missing JDBC-ODBC-bridge in Java8 and future releases can also result in the future unavailable upward compatibility/ usability of other tools. In C# the external libraries WPF Toolkit (http://wpf toolkit.codeplex.com/) and Oxyplot (http://oxyplot.org/) were used, which can be installed in Visual Studio using the nuget package manager.

As defined in the concept, separate software projects were created to implement functionality defined in the domain model (see Figure A1-1). The User, Workflow Management and Data domain are each implemented in one project. The first two using C# in .NET, the latter MS SQL Server. The functionality in the Analysis Methods is implemented in several projects, defined by which tools or libraries they are using. Obviously the projects JMPAccess and MatlabAccess implement the control of JMP and MATLAB. Both projects use COM to implement the control / automation of these tools. The CSharp project contains analysis and visualisation methods written in C# and the project NativeEXEs is used to start executable programs from a command line environment.

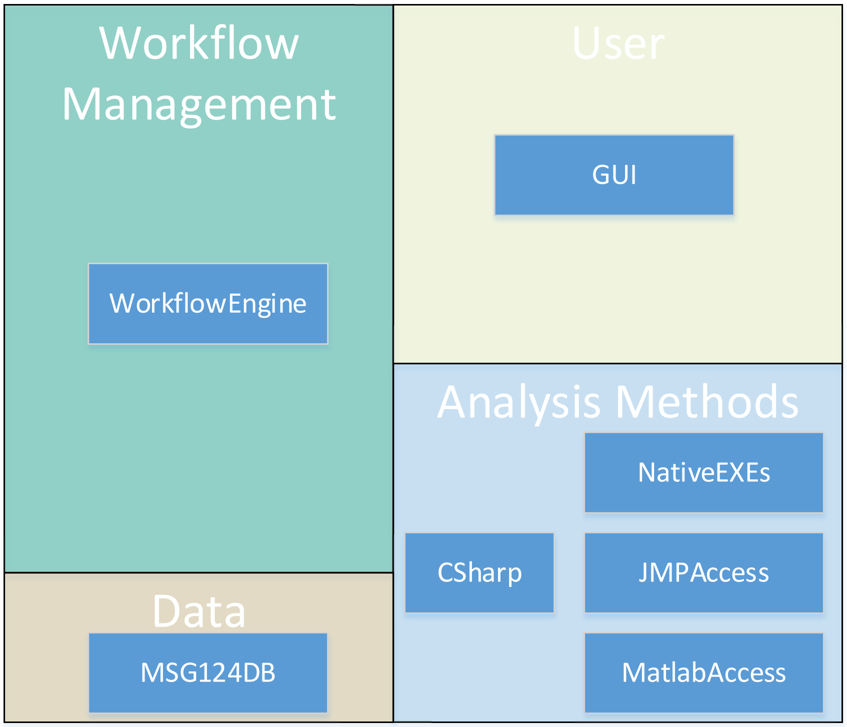


Figure A1-1: Domain Model with Associated Software Projects.

The AccessInterface library is holding all these projects together, since each of them has to implement some of the interfaces defined in AccessInterface (see Figure A1-2). Additionally, the data structure of workflows is defined in this library. A central part of the communication between projects is XAML-messages. Methods to de-serialize or serialize objects or elements of workflows to and from XAML are provided in AccessInterface.

Workflows are defined in the data structure sketched in Figure A1-3 and are saved in the file system as a human readable XAML-file. Until the creation of a workflow editor, modifying or creating workflows requires the editing of these XAML files.

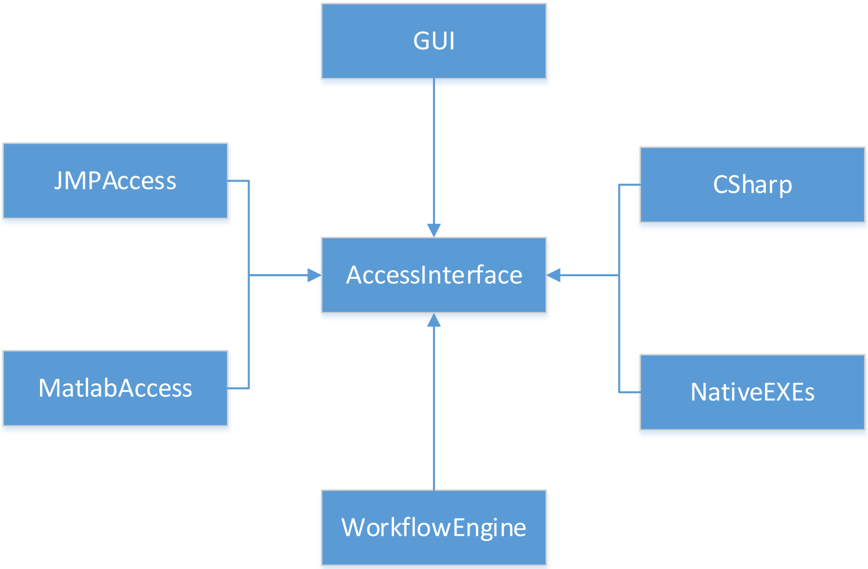


Figure A1-2: Referencing Structure of the Projects.

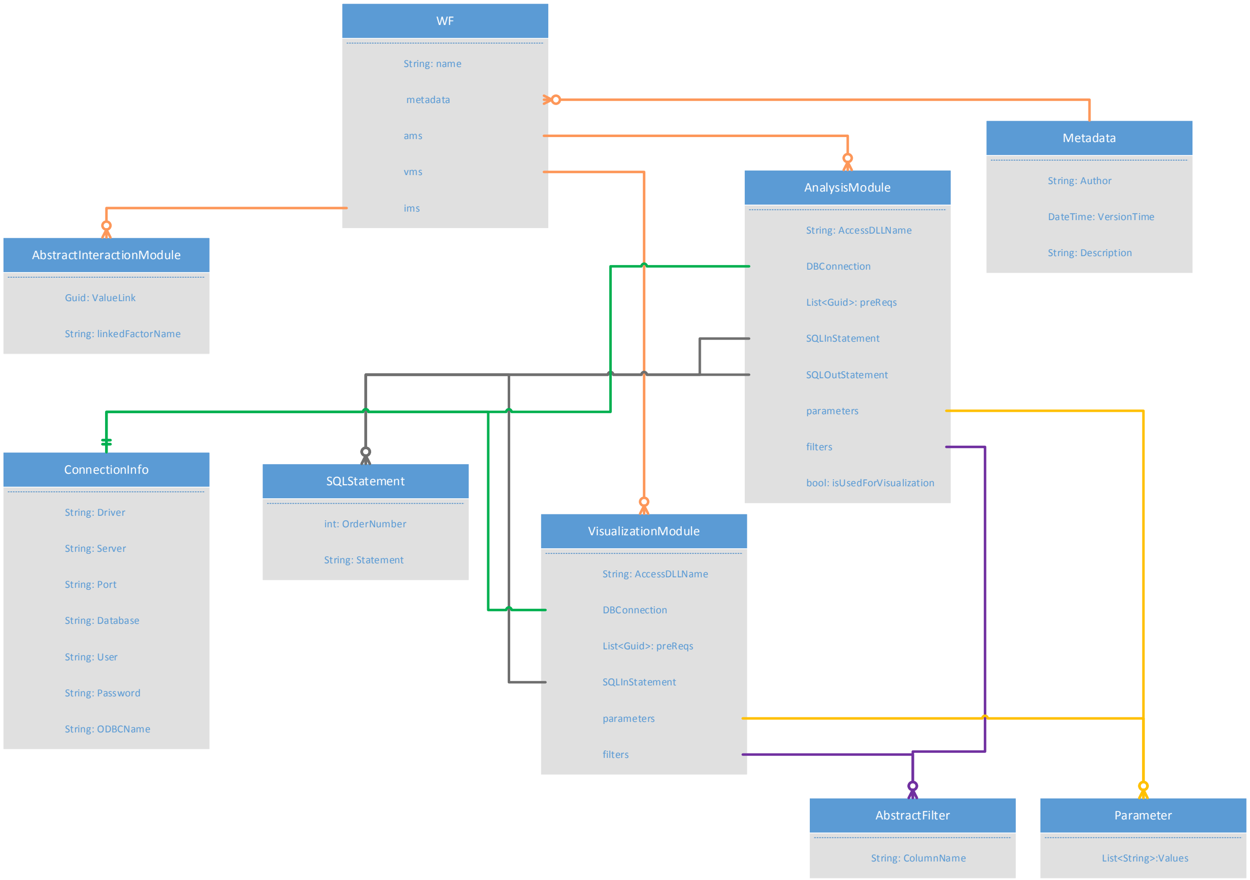


Figure A1-3: Workflow Data Structure.

A1.1.3 Workflow Object Definition

The class WF represents the base of a workflow (Figure A1-3). Each workflow has a name and metadata and it has lists of analysis-, visualisation- and interaction modules. All these modules and most other objects in the workflow have the base class AbstractModule (Figure A1-4). AbstractModule defines that each object has a name and a moduleID. This ID is of the type Guid and is used to reference objects in the workflow.

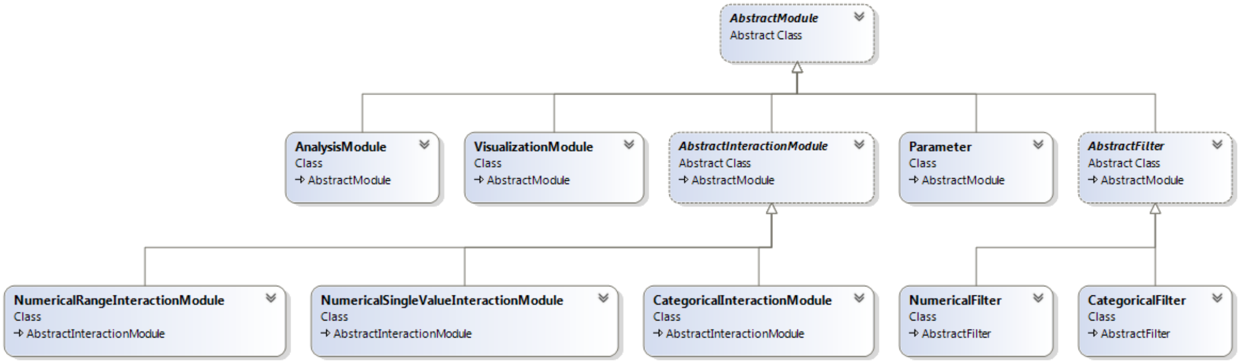


Figure A1-4: AbstractModule Inheritance Structure.

Since analysis and visualisation modules are very similar, only the analysis module is presented in the following (see Figure A1-3). The field AccessDLLName specifies the name of the library, which implements this analysis module (e.g., MatlabAccess.dll). The field DBConnection specifies connection information for the database. The object ConnectionInfo has a bigger scope than necessary, since only Driver and Database are required to access the local MS SQL database; the other fields can be used if a dedicated database server is used.

The field preReqs is a list of references to modules, which executions have to be finished before the execution of this analysis module can begin. By using preReqs a process graph of modules is created. Since the data exchange between modules in general is conducted via the database, SQL statements are used to specify which data to load or where to store result data. If two subsequent modules are executed in the same library (e.g., C#) data can be passed from one module to the next by storing it in memory. To reference this data a Binding structure can be used in the workflow definition.

The analysis module can have a list of Parameters which themselves are a list of 1 to *n* values. There is also an optional list of AbstractFilters, which can either be a numerical filter, defining a numerical interval (upper and lower bound), or a categorical filter, defining a set of words. Filters can either be integrated into SQL-statements, where numerical values must fall in the interval and categorical value must match an element of the set of words, or they can be directly used in the control of external applications or parameterization of algorithms. The last field in an analysis module defines whether it also produces a visualisation, such that no visualisation module has to be present.

Besides analysis and visualisation modules, an additional aspect of the workflow data structure is the AbstractInteractionModules. These can either be a categorical or a numerical module which is again split up into defining one value or an interval. Each of these three has a special visualisation in the GUI. Interaction modules are linked to parameters or filters referenced by their moduleID in the field ValueLink and additionally for visualisation purposes the name of the filter or parameter as linkedFactorName.

An extraction of an XAML serialization of a workflow is presented in the following listing:

```
<WF metadata="{x:Null}" Name="Name"
xmlns="clr-namespace:DFTOP.AccessInterface.WFDataStructure;
assembly=DFTOP.AccessInterface"
xmlns:s="clr-namespace:System;assembly=mscorlib"
xmlns:scg="clr-namespace:System.Collections.Generic;
assembly=mscorlib"
xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml">
 <WF.DBConnection>
  <ConnectionInfo Driver="{x:Null}" x:Name="__ReferenceID0" Database="NA" OdbcName="ODBC" Password="pwd"
   Port="NA" Server="NA" User="user" />
 </WF.DBConnection>
 <WF.ams>
  <scg:List x:TypeArguments="AnalysisModule" Capacity="4">
   <AnalysisModule DBConnection="{x:Reference __ReferenceID0}"
    AccessDLLName="DLL.dll"Name="Name"isUsedForVisualisation="False" moduleID="388ce067-87e5-4c7f-a8a3
    575ad7671873">
    <AnalysisModule.SQLInStatements>
     <scg:List x:TypeArguments="SQLStatement" Capacity="4">
      <SQLStatement OrderNumber="1" Statement="SELECT * FROM table" />
     </scg:List>
    </AnalysisModule.SQLInStatements>
    <AnalysisModule.SQLOutStatements>
     <scg:List x:TypeArguments="SQLStatement" Capacity="0" />
    </AnalysisModule.SQLOutStatements>
    <AnalysisModule.filters>
     <scg:List x:TypeArguments="AbstractFilter" Capacity="4">
      <NumericalFilter Name="{x:Null}" ColumnName="Name" LowerBound="0.1" UpperBound="0.4"
       moduleID="43ff0fca-ea15-4946-b7ea-960ee25d562a" />
     </scg:List>
    </AnalysisModule.filters>
    <AnalysisModule.parameters>
     <scg:List x:TypeArguments="Parameter" Capacity="0" />
    </AnalysisModule.parameters>
    <AnalysisModule.preReqs>
     <scg:List x:TypeArguments="s:Guid" Capacity="0" />
    </AnalysisModule.preReqs>
   </AnalysisModule>
  </scg:List>
 </WF.ams>
 <WF.ims>
  <scg:List x:TypeArguments="AbstractInteractionModule" Capacity="4">
   <NumericalRangeInteractionModule LowerBound="0" LowerValue="0.4" Name="Name" StepSize="0"
    UpperBound="1" UpperValue="0.6"
    ValueLink="1ce0af87-5faf-42f2-861d-dd4b71b77847"
    moduleID="e72df55d-54fa-4531-994d-b01962f3bdf4" />
  </scg:List>
 </WF.ims>
 <WF.vms>
  <scg:List x:TypeArguments="VisualisationModule" Capacity="4">
   <VisualisationModule DBConnection="{x:Reference
    __ReferenceID0}"AccessDLLName="DLL.dll"Name="Name"moduleID="a12030a6-a29c-45d5-b9ea-af6c23499854">
    <VisualisationModule.SQLInStatements>
     <scg:List x:TypeArguments="SQLStatement" Capacity="0" />
    </VisualisationModule.SQLInStatements>
    <VisualisationModule.filters>
     <scg:List x:TypeArguments="AbstractFilter" Capacity="0" />
    </VisualisationModule.filters>
    <VisualisationModule.parameters>
     <scg:List x:TypeArguments="Parameter" Capacity="4">
      <Parameter Name="Name" moduleID="1ce0af87-5faf-42f2-861d-dd4b71b77847">
       <Parameter.values>
        <scg:List x:TypeArguments="x:String" Capacity="4">
         <x:String>Value</x:String>
        </scg:List>
       </Parameter.values>
      </Parameter>
     </scg:List>
    </VisualisationModule.parameters>
    <VisualisationModule.preReqs>
     <scg:List x:TypeArguments="s:Guid" Capacity="4">
      <s:Guid>388ce067-87e5-4c7f-a8a3-575ad7671873</s:Guid>
     </scg:List>
    </VisualisationModule.preReqs>
   </VisualisationModule>
  </scg:List>
 </WF.vms>
</WF>
```

A1.1.4 Modules and Their Use in Workflows

The first workflows are related to data import, definition of the OverallSucess (Objective Function Definition), and defining COA. The workflows for analysis are described below:

- Factor Importance: Using a set of standard statistical key indicators a benchmark value is calculated in C# to rate the decision factors importance for blue success. One parameter defines the threshold of the objective function defining success. The benchmark values are stored in the C# library and can be visualized with a C# visualisation module.
- Histogram: Using the Distribution method from JMP, a histogram of the distribution of the objective function is presented. The JMP windows needs to be caught by and integrated into the GUI.
- SDA: Developed by FOI it calculates the importance of factors for achieving high values in the objective function using MATLAB functions. A graph is presented showing the *n* most important factors and the value intervals for success (high values of objective function are regarded as success). Parameters define how many of the best simulation runs are considered success and if the calculation should be done on single factors or on 2-*m* factor combinations. The SDA diagram is saved as an image file in the file system.
- Wire Diagram: Developed by Fraunhofer IAIS using Java, the wire diagram visualizes the input factor values and MOE values of simulation runs. Each factor or MOE has its own vertical axis or pole and each visualized simulation runs create one wire spanning each pole, connecting at the specific value. When visualizing hundreds or more runs, similarities and differences between runs are visible. When putting filters on poles also dependencies can present themselves.
- *xy*-diagram: Using the MATLAB Graph toolbox by Jörn Diedrichsen (j.diedrichsen@ucl.ac.uk), *xy*-diagrams are created showing the mean of an MOE (and the interval of its standard deviation) versus a factor. The diagrams are saved as an image file in the file system.
- Heat-Map: Developed by FOI in MATLAB, diagrams are created showing one MOE versus 2 factors. The mean values of the MOE are presented by colour gradient. The diagrams are saved as an image file in the file system.

- Box-Plot: Using standard MATLAB boxplots, either the distribution of single factors or the distribution of one factor grouped by another factor can be plotted. Boxplot diagrams are saved as an image file in the file system.
- Dashboard: Using complex SQL-statements and the JMP graph builder, the mean of an MOE can be visualized on a geographical map. Additional tables for Geo-Location are necessary to allow the geo-referencing of MOE. The JMP graph builder windows need to be caught by and integrated into the GUI.

All of these analysis modules can be combined with COA or general filtering.

The following dedicated visualisation modules are available:

- Dashboard: Using Tableau a set of MOE, factors and the objective function can be presented in a full screen fashion and further manipulated and analysed in the Tableau software. The Tableau window needs to be caught by and integrated into the GUI.
- ImageGrid: Presents a set of pictures in an *n* x *m* matrix. The matrix can be panned and zoomed.
- ChartView: Using the Oxyplot library data is presented in a bar chart.
- ListView: Using standard C# user controls, a list of text elements is presented as a list featuring a gradient of font sizes.

A1.1.5 Procedure to Integrate Additional Modules

To integrate new modules, either the existing projects in the Analysis Methods domain (see Figure 4-11) must be modified or a new project must be created and integrated into DFTOP. To start a new project a C# library that has a class named Access implementing IAccess of the AccessInterface library has to created.

All communication with the DFTOP framework is bundled into the object implementing the IApplicationToWFECommunicationObject. This object is handed to the function runModules from the WorkflowEngine library when the new library is used. The definition of the modules to run is handed over as a XAML string serialization of an AbstractModel object. To integrate and specify a module of the new project in the workflow definition, the field AccessDLLName has to set to the name of the library created. This library must be placed into the DLLs subdirectory of the DFTOP install directory or in the folder %USERHOME%\.DFTOP\DLLs.

A1.1.6 GUI Functionality

In this section the GUI design and functionality is presented briefly.

Figure A1-5 shows the start-up view of the DFTOP GUI. It has a Microsoft Office 2007 style ribbon menu with several different ribbons, each of which is presented later in this section. The main area for displaying visualisation modules is at that point occupied by a picture of the flags of the NATO countries. The white space in the right of the picture is the area for interaction modules.

The options window (Figure A1-6) can be accessed by opening the sub-menu, which is opened when clicking the dark blue button on the top-left of the ribbon menu. The window size of DFTOP can be set in the options menu. This is the only way to resize the DFTOP window. It can either be set to a specific size (width by height) in pixels or set to full-screen. The paths to the database file and to the workflow files have to be set before any workflow can be executed. When enabling the *always on top* option, DFTOP will never be overlaid by windows of other applications.

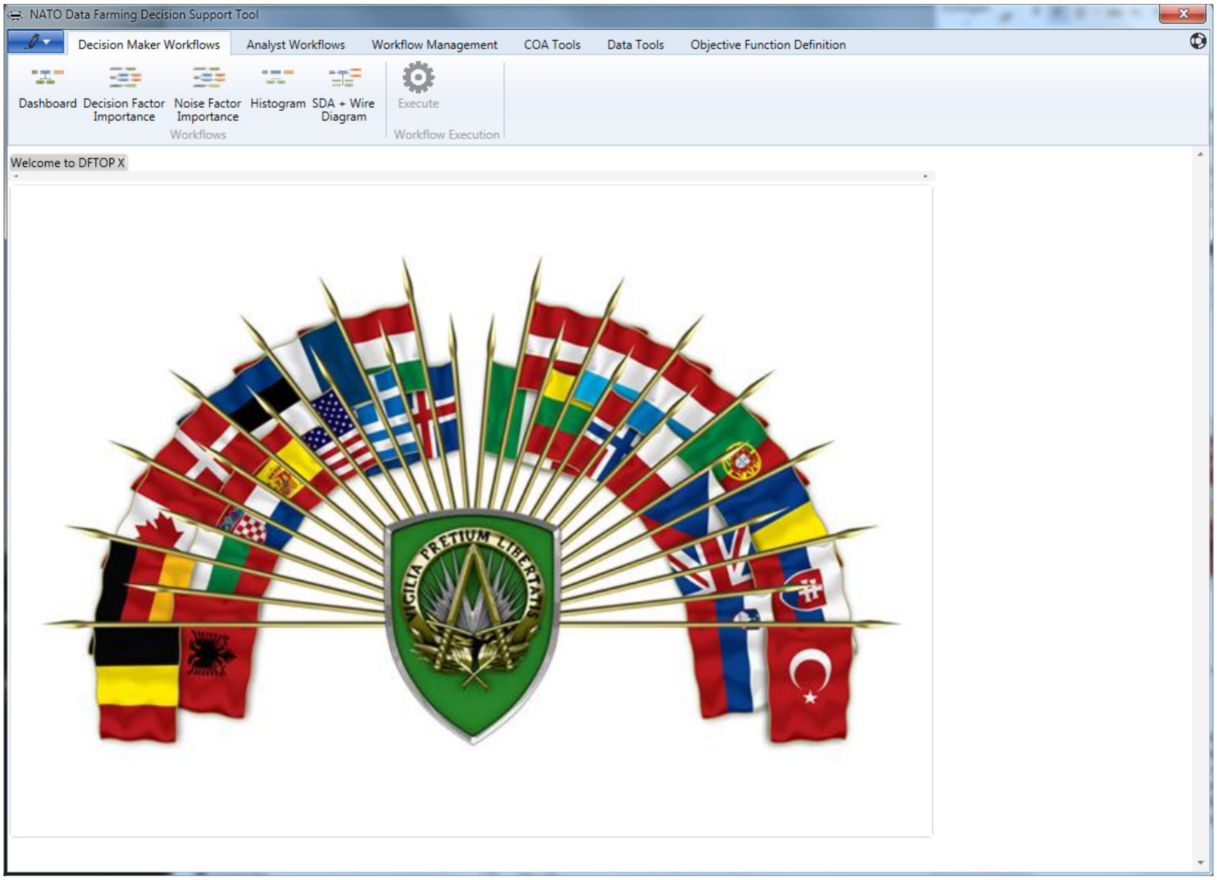
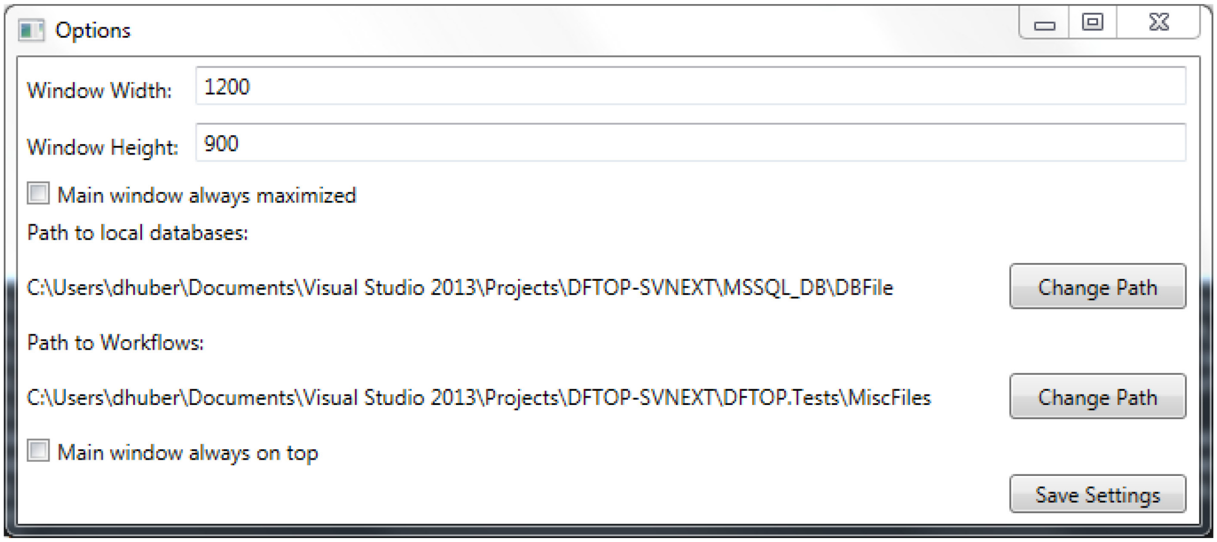


Figure A1-5: DFTOP Start-Up View.


Options

Window Width: 1200

Window Height: 900

□ Main window always maximized

Path to local databases:

C:\Users\dhuber\Documents\Visual Studio 2013\Projects\DFTOP-SVNEXT\MSSQL_DB\DBFile [Change Path]

Path to Workflows:

C:\Users\dhuber\Documents\Visual Studio 2013\Projects\DFTOP-SVNEXT\DFTOP.Tests\MiscFiles [Change Path]

□ Main window always on top

[Save Settings]

Figure A1-6: Options Window.

The workflows that are designed for use by the decision maker are grouped in the *Decision Maker Workflows* ribbon menu presented in Figure A1-7. When clicking on the buttons for one of the workflows a general description of the workflow opens in the main area (Figure A1-8) and that workflow is selected for execution. After selecting a workflow the *Execute* button can be clicked.

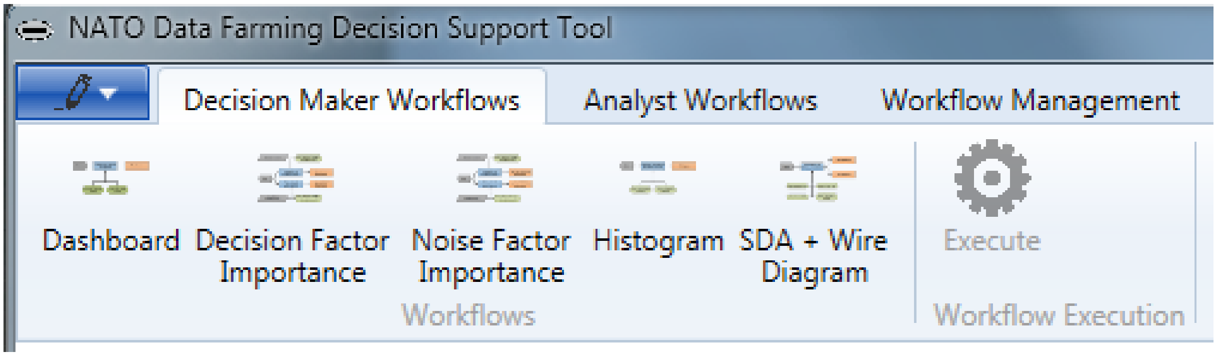
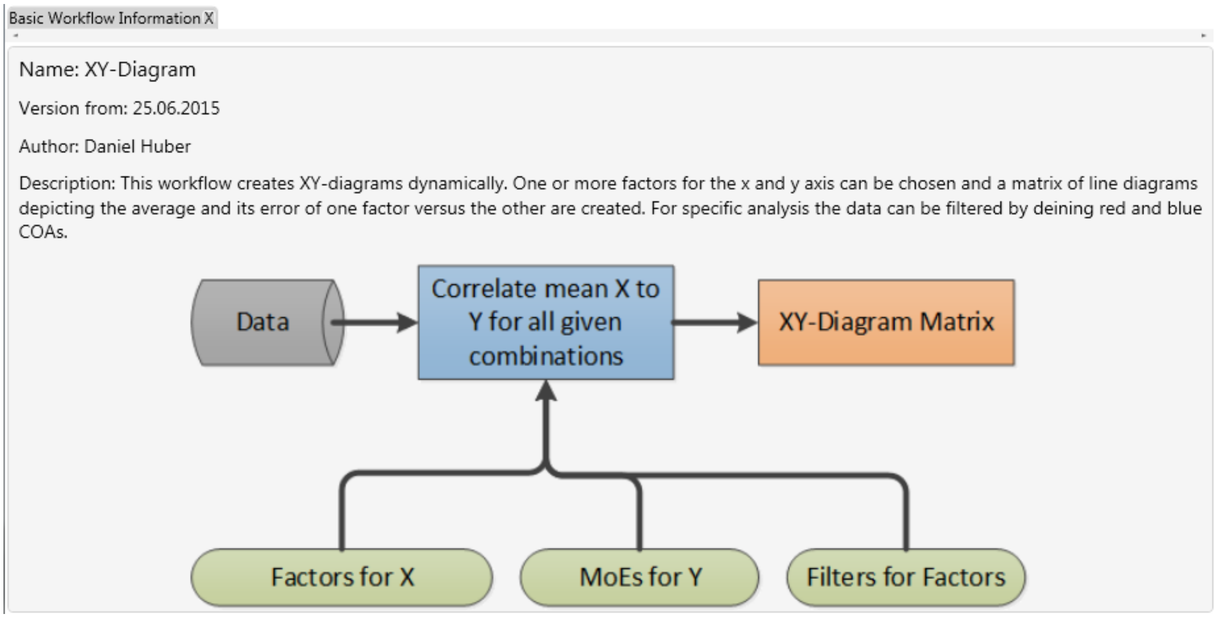


Figure A1-7: Decision Maker Ribbon Menu.


Basic Workflow Information X

Name: XY-Diagram

Version from: 25.06.2015

Author: Daniel Huber

Description: This workflow creates XY-diagrams dynamically. One or more factors for the x and y axis can be chosen and a matrix of line diagrams depicting the average and its error of one factor versus the other are created. For specific analysis the data can be filtered by deining red and blue COAs.

Figure A1-8: Basic Workflow Information.

Analogous to the above, the workflows designed for the analyst are grouped in the *Analyst Workflows* ribbon is presented in Figure A1-9.

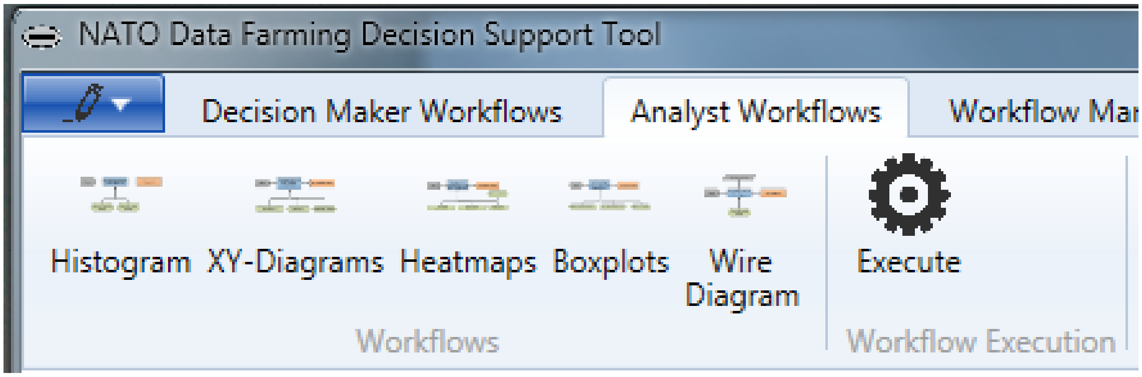


Figure A1-9: Analyst Workflow Ribbon Menu.

Figure A1-10 shows the ribbon *Workflow Management*. Here, arbitrary workflow files can be loaded, executed and saved. When saving a workflow, it is saved with the actual settings of all its interaction modules. The buttons for editing and creating workflow files are opening an XML editor in which the workflow XAML description can be edited. When editing a workflow, an existing workflow file has to be selected. When creating one, an *empty* workflow is opened.

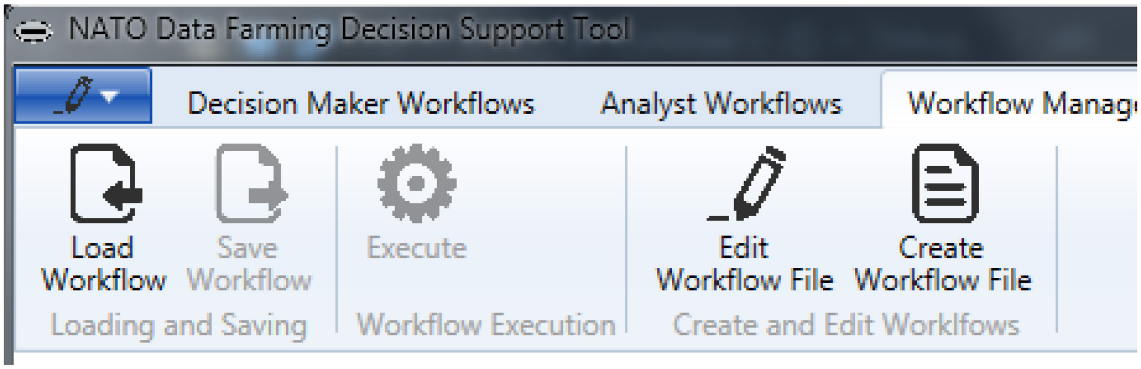


Figure A1-10: Workflow Management Ribbon Menu.

The *COA Tools* ribbon presented in Figure A1-11 features only one button to open a window for defining COA (Figure A1-12).

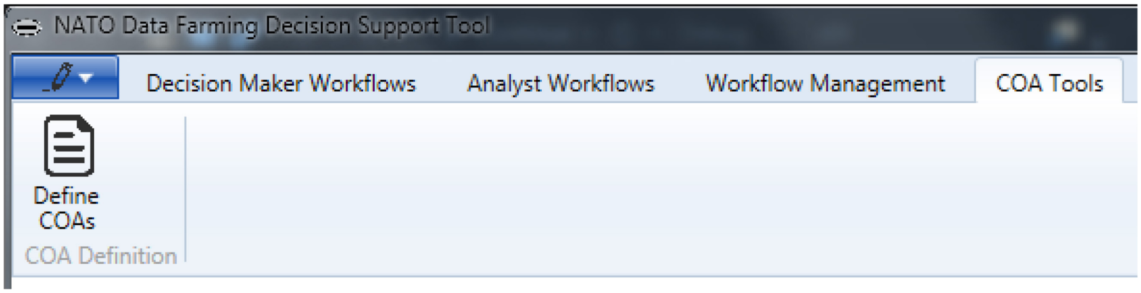
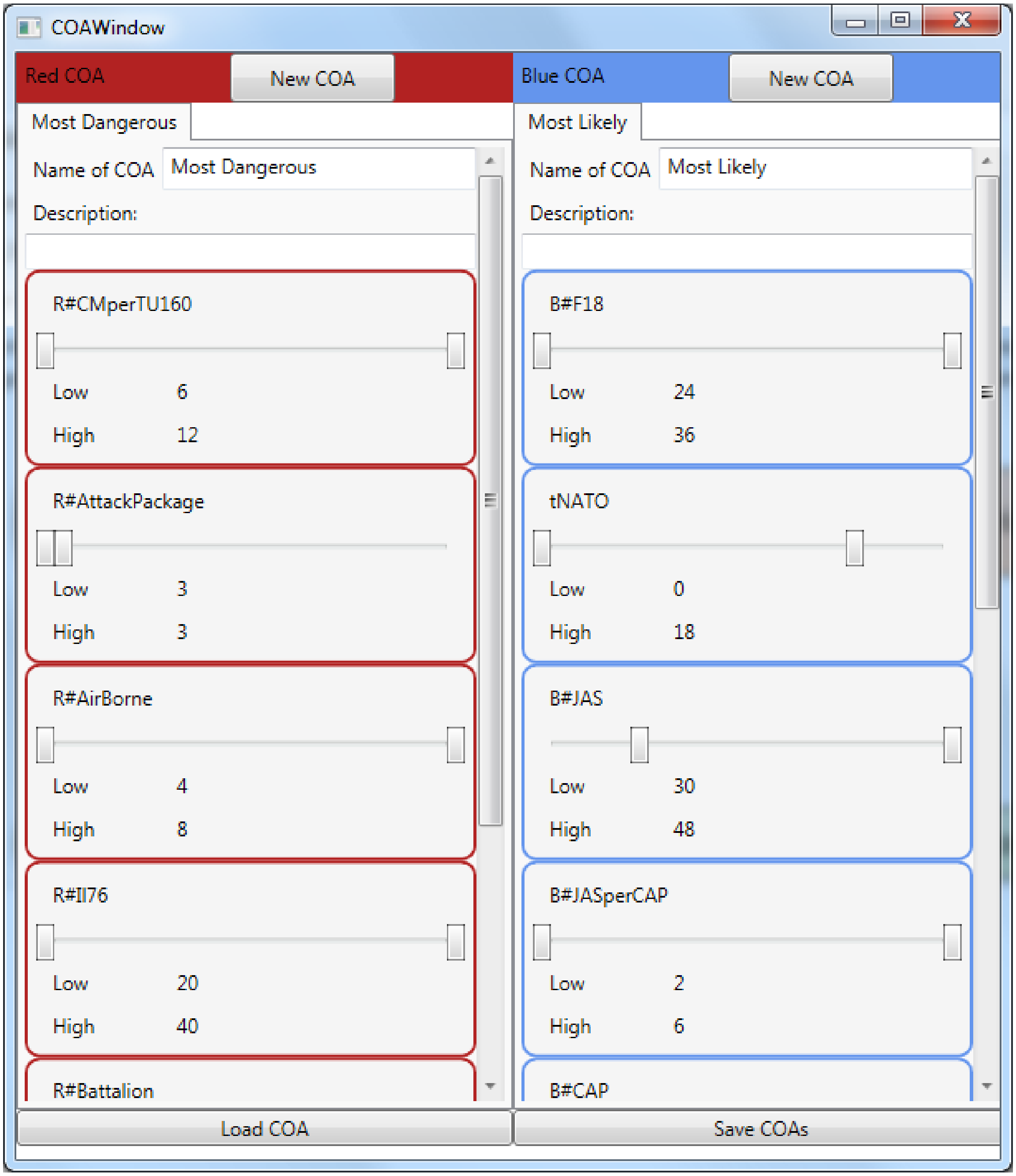


Figure A1-11: COA Tools Ribbon Menu.



Red COA – Most Dangerous

Name of COA: Most Dangerous

Description:

R#CMperTU160: Low 6, High 12

R#AttackPackage: Low 3, High 3

R#AirBorne: Low 4, High 8

R#Il76: Low 20, High 40

R#Battalion

Blue COA – Most Likely

Name of COA: Most Likely

Description:

B#F18: Low 24, High 36

tNATO: Low 0, High 18

B#JAS: Low 30, High 48

B#JASperCAP: Low 2, High 6

B#CAP

Figure A1-12: COA Window.

When opening the COA window, the metadata of the current DF data is loaded from the database, and interaction modules for each decision and noise factors are created. Several COA can be created for the Red and the Blue side by clicking the *New COA* button. After creating a new COA, it must be named and the sliders and checkboxes can be used to define the specific factor ranges and values. When clicking *Save,* XAML files for each COA are saved to the file system in the DFTOP-folder in the user home folder.

The *Data Tools* ribbon features many different buttons and functions (Figure A1-13). Data farming *raw data* can be imported into the DFTOP database when clicking on the *DF-Data Import to DB* button. Data is expected in one single csv-file. Since some analysis modules cannot handle categorical text values, there needs to be a mapping table (Figure A1-14). In this table for each categorical factor and for each categorical value there needs to be an integer value assigned. When clicking *Cat2Num Mapping Import to DB* an Excel-file can be imported to the database. This file can be created (start with an empty file) or edited (load an existing file) when clicking the appropriate buttons in this ribbon. To show the current values of the mapping table, as it is in the database, the button *Show Mapping Table* can be clicked and the values will be presented in the interaction module section of the main window (Figure A1-15).

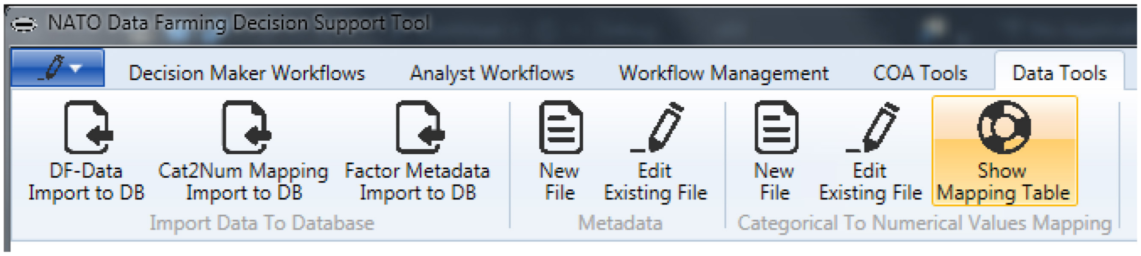
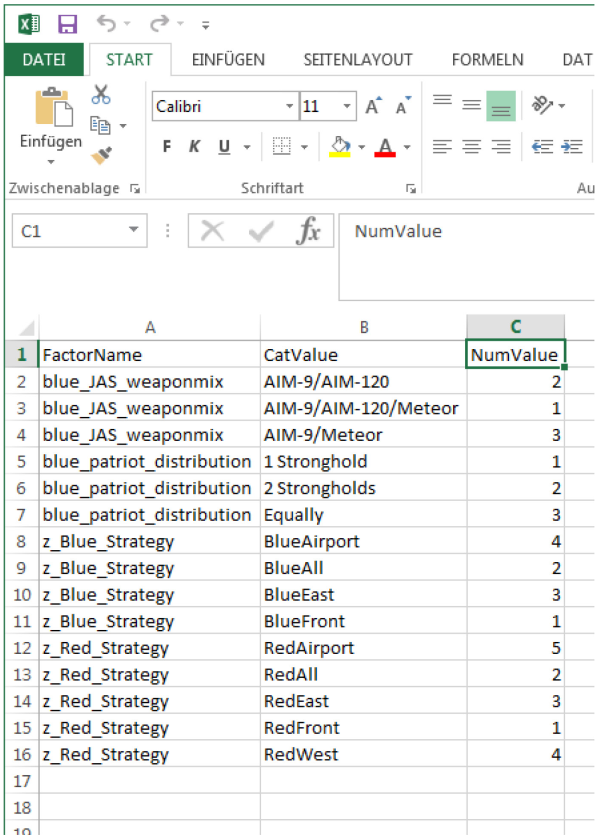
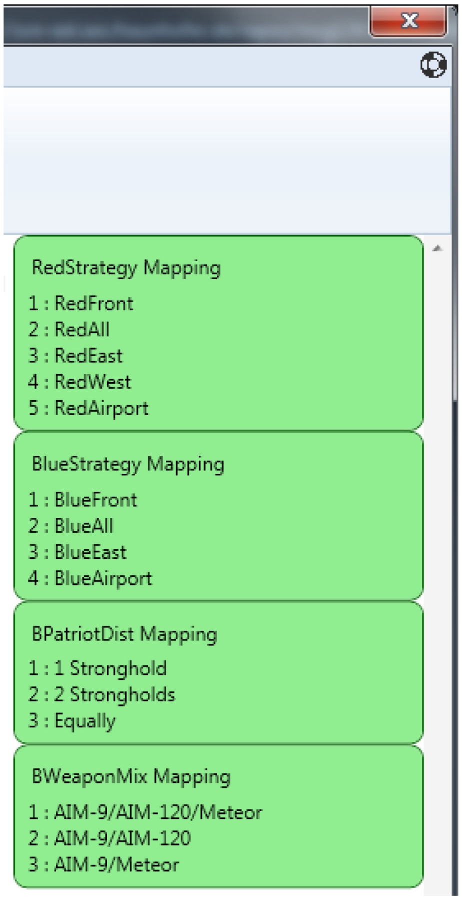


Figure A1-13: Data Tools Ribbon Menu.



	A	B	C
1	FactorName	CatValue	NumValue
2	blue_JAS_weaponmix	AIM-9/AIM-120	2
3	blue_JAS_weaponmix	AIM-9/AIM-120/Meteor	1
4	blue_JAS_weaponmix	AIM-9/Meteor	3
5	blue_patriot_distribution	1 Stronghold	1
6	blue_patriot_distribution	2 Strongholds	2
7	blue_patriot_distribution	Equally	3
8	z_Blue_Strategy	BlueAirport	4
9	z_Blue_Strategy	BlueAll	2
10	z_Blue_Strategy	BlueEast	3
11	z_Blue_Strategy	BlueFront	1
12	z_Red_Strategy	RedAirport	5
13	z_Red_Strategy	RedAll	2
14	z_Red_Strategy	RedEast	3
15	z_Red_Strategy	RedFront	1
16	z_Red_Strategy	RedWest	4
17			
18			

Figure A1-14: Categorical to Numerical Values Mapping File.



RedStrategy Mapping

1 : RedFront
2 : RedAll
3 : RedEast
4 : RedWest
5 : RedAirport

BlueStrategy Mapping

1 : BlueFront
2 : BlueAll
3 : BlueEast
4 : BlueAirport

BPatriotDist Mapping

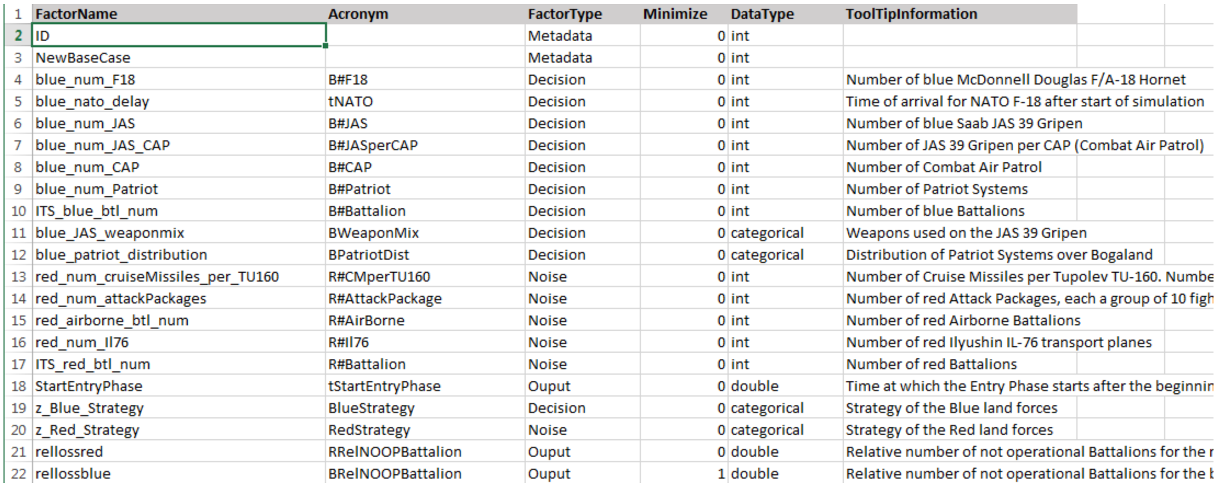
1 : 1 Stronghold
2 : 2 Strongholds
3 : Equally

BWeaponMix Mapping

1 : AIM-9/AIM-120/Meteor
2 : AIM-9/AIM-120
3 : AIM-9/Meteor

Figure A1-15: Categorical to Numerical Values Mapping Visualisation.

Nearly all workflows use metadata of the data in the database for presentation and calculation purposes. This metadata can be created, edited and imported into the database by using the buttons in the *Data Tools* ribbon (Figure A1-13). Figure A1-16 shows a screenshot of an exemplary Excel file, which could open when clicking the edit button. All variables in the database must be covered in the table and only cells in the column *Acronym* can be left empty if those factors are not used in any analysis. The Excel file is created in a way such that only allowed values can be entered into the cells of columns *FactorType*, *Minimize* and *Datatype*.



FactorName	Acronym	FactorType	Minimize	DataType	ToolTipInformation
ID		Metadata	0	int	
NewBaseCase		Metadata	0	int	
blue_num_F18	B#F18	Decision	0	int	Number of blue McDonnell Douglas F/A-18 Hornet
blue_nato_delay	tNATO	Decision	0	int	Time of arrival for NATO F-18 after start of simulation
blue_num_JAS	B#JAS	Decision	0	int	Number of blue Saab JAS 39 Gripen
blue_num_JAS_CAP	B#JASperCAP	Decision	0	int	Number of JAS 39 Gripen per CAP (Combat Air Patrol)
blue_num_CAP	B#CAP	Decision	0	int	Number of Combat Air Patrol
blue_num_Patriot	B#Patriot	Decision	0	int	Number of Patriot Systems
ITS_blue_btl_num	B#Battalion	Decision	0	int	Number of blue Battalions
blue_JAS_weaponmix	BWeaponMix	Decision	0	categorical	Weapons used on the JAS 39 Gripen
blue_patriot_distribution	BPatriotDist	Decision	0	categorical	Distribution of Patriot Systems over Bogaland
red_num_cruiseMissiles_per_TU160	R#CMperTU160	Noise	0	int	Number of Cruise Missiles per Tupolev TU-160. Numbe
red_num_attackPackages	R#AttackPackage	Noise	0	int	Number of red Attack Packages, each a group of 10 figh
red_airborne_btl_num	R#AirBorne	Noise	0	int	Number of red Airborne Battalions
red_num_Il76	R#Il76	Noise	0	int	Number of red Ilyushin IL-76 transport planes
ITS_red_btl_num	R#Battalion	Noise	0	int	Number of red Battalions
StartEntryPhase	tStartEntryPhase	Ouput	0	double	Time at which the Entry Phase starts after the beginnin
z_Blue_Strategy	BlueStrategy	Decision	0	categorical	Strategy of the Blue land forces
z_Red_Strategy	RedStrategy	Noise	0	categorical	Strategy of the Red land forces
rellossred	RRelNOOPBattalion	Ouput	0	double	Relative number of not operational Battalions for the r
rellossblue	BRelNOOPBattalion	Ouput	1	double	Relative number of not operational Battalions for the b

Figure A1-16: Experiment Data File.

The *Objective Function Definition* ribbon (Figure A1-17) contains two buttons; the first opens the window depicted in Figure A1-18.

In this window an unrestricted number of preference inequalities can be defined. The left side is a set of MOE that are more important than the MOE on the right side. There is also the option to select *everything else*. Each inequality can be weighted by an importance factor, the higher the more important it is.

After clicking the *Finished* button in Figure A1-18 or clicking the right button in the *Objective Function Definition* ribbon shown in Figure A1-17, the window presented in Figure A1-19 opens. If the preference input window was bypassed, the standard objective function is shown. Otherwise, the MOE in the objective function and their weights are calculated from the preferences.

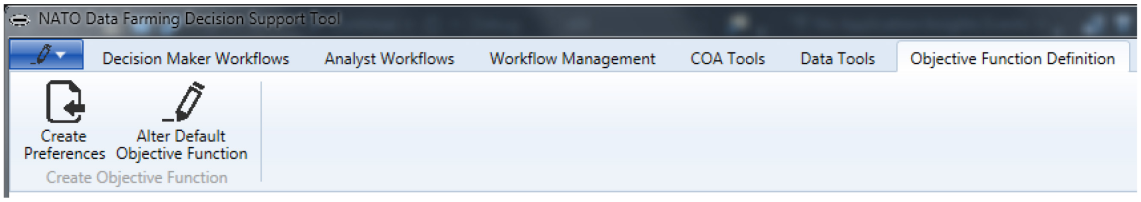
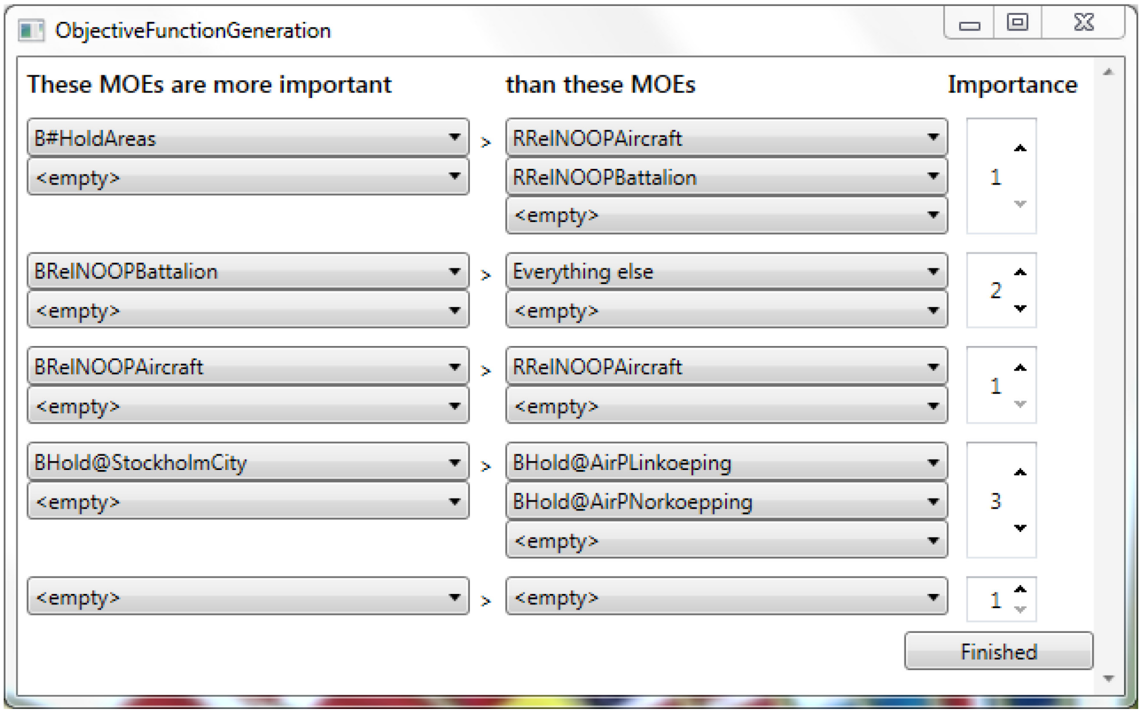
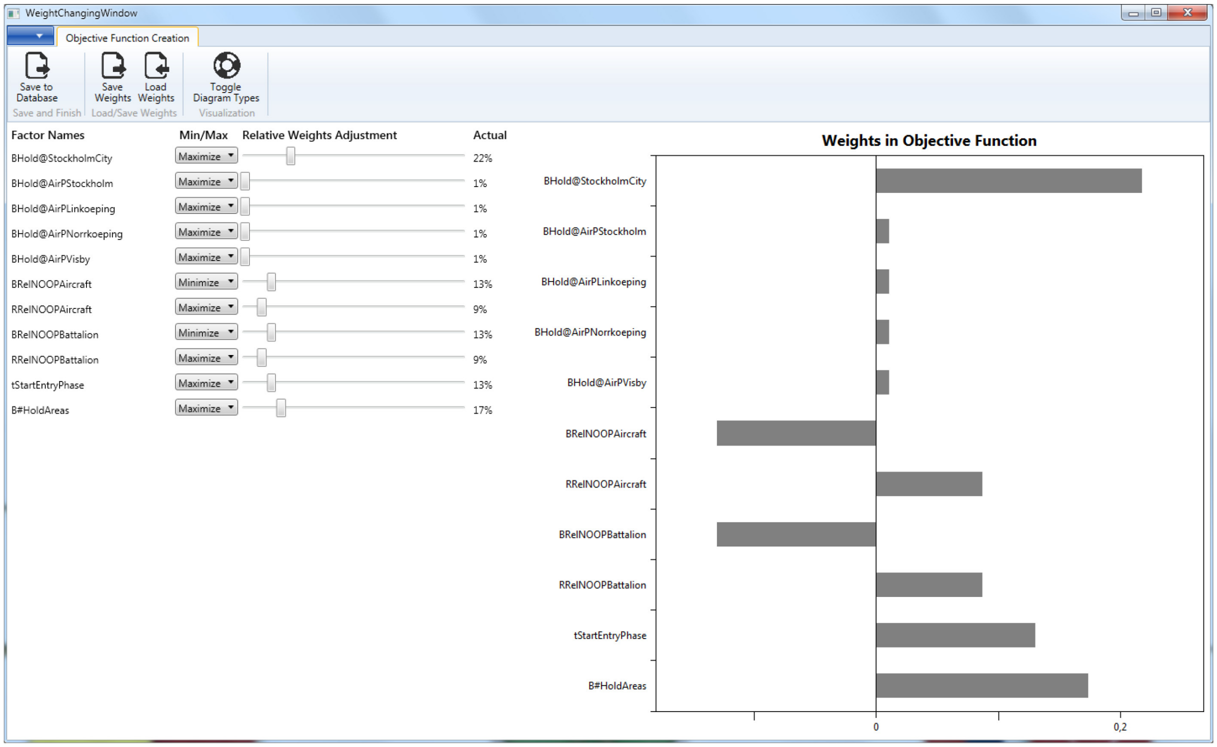

NATO Data Farming Decision Support Tool
Decision Maker Workflows
Analyst Workflows
Workflow Management
COA Tools
Data Tools
Objective Function Definition
Create Preferences
Alter Default Objective Function
Create Objective Function

Figure A1-17: Objective Function Ribbon Menu.



These MOEs are more important		than these MOEs	Importance
B#HoldAreas	>	RRelNOOPAircraft	1
<empty>		RRelNOOPBattalion	
		<empty>	
BRelNOOPBattalion	>	Everything else	2
<empty>		<empty>	
BRelNOOPAircraft	>	RRelNOOPAircraft	1
<empty>		<empty>	
BHold@StockholmCity	>	BHold@AirPLinkoeping	3
<empty>		BHold@AirPNorkoepping	
		<empty>	
<empty>	>	<empty>	1

Figure A1-18: Preference Analysis Input Window.



Factor Names	Min/Max	Actual
BHold@StockholmCity	Maximize	22%
BHold@AirPStockholm	Maximize	1%
BHold@AirPLinkoeping	Maximize	1%
BHold@AirPNorrkoeping	Maximize	1%
BHold@AirPVisby	Maximize	1%
BRelNOOPAircraft	Minimize	13%
RRelNOOPAircraft	Maximize	9%
BRelNOOPBattalion	Minimize	13%
RRelNOOPBattalion	Maximize	9%
tStartEntryPhase	Maximize	13%
B#HoldAreas	Maximize	17%

Relative Weights Adjustment

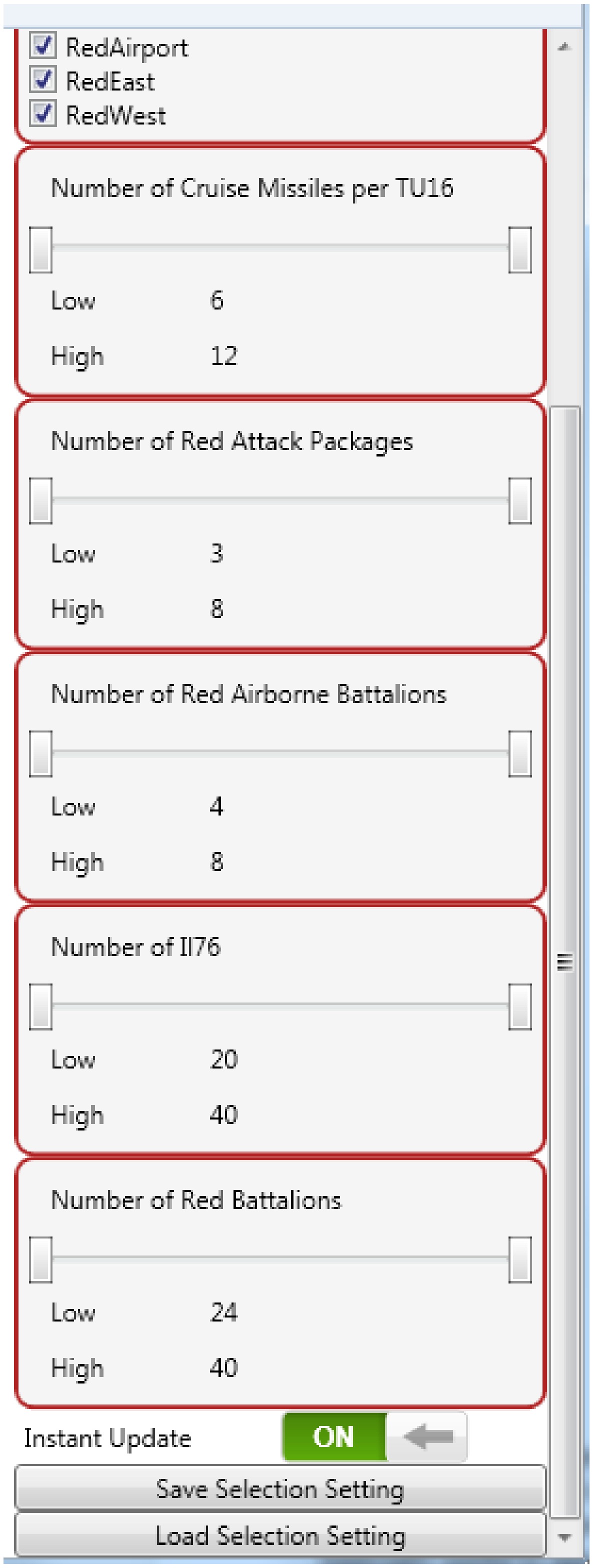
Figure A1-19: Objective Function Modification Window.

In this window you can adjust the relative weights of MOE. You can also select if the MOE should be minimized or maximized when maximizing Blue success. The metadata in the database already contain a suggested (default) value, but can be changed. This window also has its own ribbon menu, allowing it to save or load objective functions and to import the current objective function into the database. If doing so, a new column called *OverallSuccess* is created and the values in this column are calculated according to the defined objective function. If that column already exists, its values are overwritten. Every time the objective function values are written to the database, the objective function itself is saved to the file system, to be able to look at the current objective function composition.

After executing a workflow, a set of interaction modules are presented on the right side of the DFTOP window. The interaction modules are used to modify the workflow or the visualisation. As can be seen in Figure A1-20, the interaction modules are stacked on top of each other (if there are too many to fit the window, a scroll bar appears). There is an *Instant Update* switch. When it is set to *On*, modifications of interaction modules are instantly transmitted to the analysis or visualisation modules. If set to *Off*, these modifications are buffered and send if the switch is set back to *On*, or if the workflow is re-executed.

Under this switch, there are two buttons for loading and saving. When loading a set of saved interaction modules, matching modules are searched and their values updated. After loading, a message appears and shows the number of updated interaction modules. This feature is especially useful to apply the defined COA (see Figure A1-12) to the current workflow.

In Figure A1-21 the DFTOP window is shown after executing a workflow. For each workflow, execution a new tab is created, its name indicates the visualisation module's name and a counter of workflow executions. In this example the *xy-diagram* module was executed for a second time. Each tab can be closed when clicking on the cross in the tab header. If pictures are presented in the visualisation tab, they are pan- and zoomable. This can either be done by dragging and turning the mouse wheel or by opening the pan and zoom micro-window in the button right side of the tab area.



☑ RedAirport
☑ RedEast
☑ RedWest

Number of Cruise Missiles per TU16
Low 6
High 12

Number of Red Attack Packages
Low 3
High 8

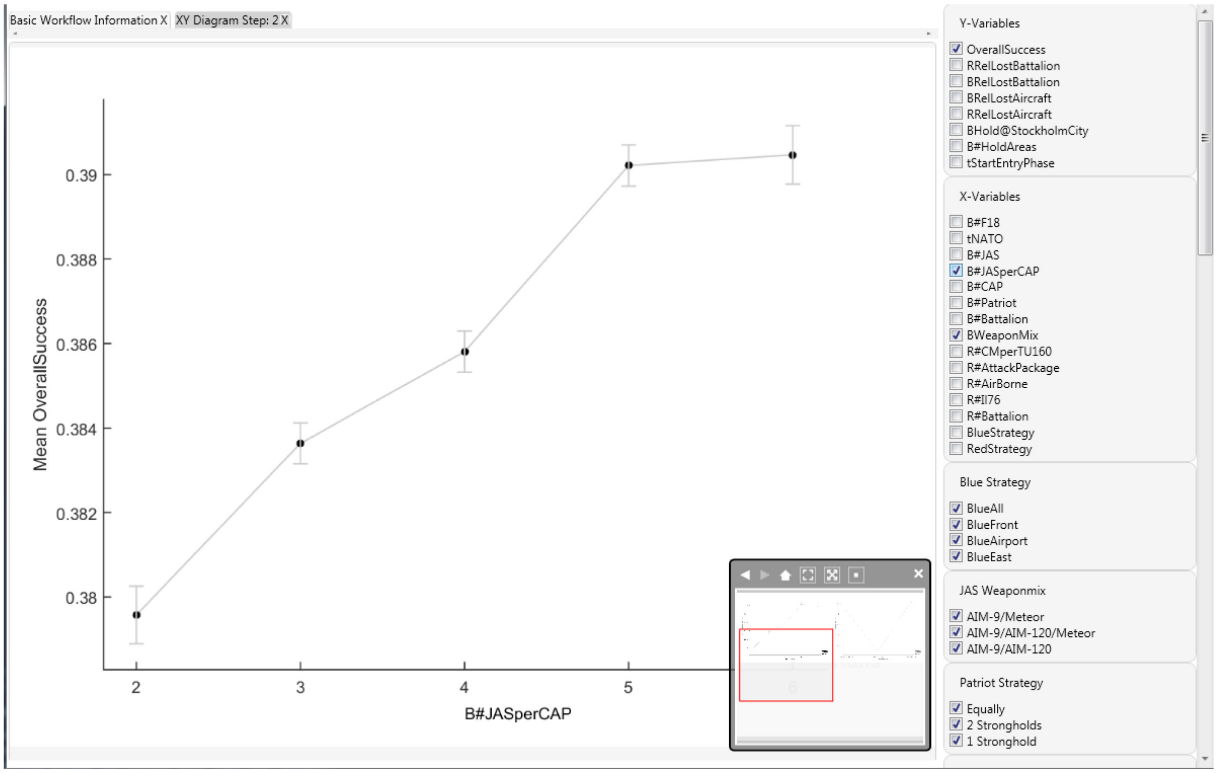
Number of Red Airborne Battalions
Low 4
High 8

Number of Il76
Low 20
High 40

Number of Red Battalions
Low 24
High 40

Instant Update ON

Figure A1-20: Interaction Modules Window Section.



Y-Variables

- ☑ OverallSuccess
- □ RRelLostBattalion
- □ BRelLostBattalion
- □ BRelLostAircraft
- □ RRelLostAircraft
- □ BHold@StockholmCity
- □ B#HoldAreas
- □ tStartEntryPhase

X-Variables

- □ B#F18
- □ tNATO
- □ B#JAS
- ☑ B#JASperCAP
- □ B#CAP
- □ B#Patriot
- □ B#Battalion
- ☑ BWeaponMix
- □ R#CMperTU160
- □ R#AttackPackage
- □ R#AirBorne
- □ R#Il76
- □ R#Battalion
- □ BlueStrategy
- □ RedStrategy

Blue Strategy

- ☑ BlueAll
- ☑ BlueFront
- ☑ BlueAirport
- ☑ BlueEast

JAS Weaponmix

- ☑ AIM-9/Meteor
- ☑ AIM-9/AIM-120/Meteor
- ☑ AIM-9/AIM-120

Patriot Strategy

- ☑ Equally
- ☑ 2 Strongholds
- ☑ 1 Stronghold

Figure A1-21: Visualisation Module Window Section.

A1.1.7 Main DFTOP Processes

In this section, two processes in DFTOP are presented using flow diagrams (Figure A1-22 and Figure A1-23).

The colour code is as follows:

- Red border: User action.
- Light blue: Process in the Analysis Methods domain.
- Beige: Process in the User domain.
- Bluegreen: Process in Workflow Management domain.

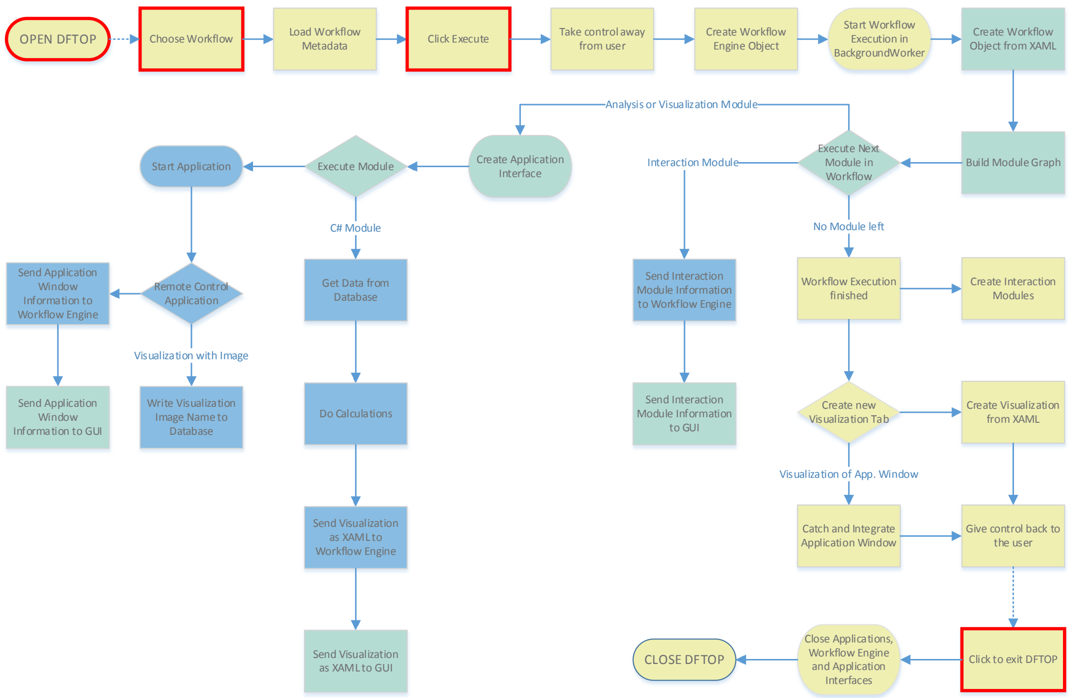

OPEN DFTOP
Choose Workflow
Load Workflow Metadata
Click Execute
Take control away from user
Create Workflow Engine Object
Start Workflow Execution in BackgroundWorker
Create Workflow Object from XAML
Analysis or Visualization Module
Build Module Graph
Execute Next Module in Workflow
Interaction Module
Create Application Interface
Execute Module
Start Application
C# Module
No Module left
Send Application Window Information to Workflow Engine
Remote Control Application
Get Data from Database
Send Interaction Module Information to Workflow Engine
Workflow Execution finished
Create Interaction Modules
Visualization with Image
Send Application Window Information to GUI
Write Visualization Image Name to Database
Do Calculations
Send Interaction Module Information to GUI
Create new Visualization Tab
Create Visualization from XAML
Visualization of App. Window
Send Visualization as XAML to Workflow Engine
Catch and Integrate Application Window
Give control back to the user
Send Visualization as XAML to GUI
CLOSE DFTOP
Close Applications, Workflow Engine and Application Interfaces
Click to exit DFTOP

Figure A1-22: Workflow Execution Process.

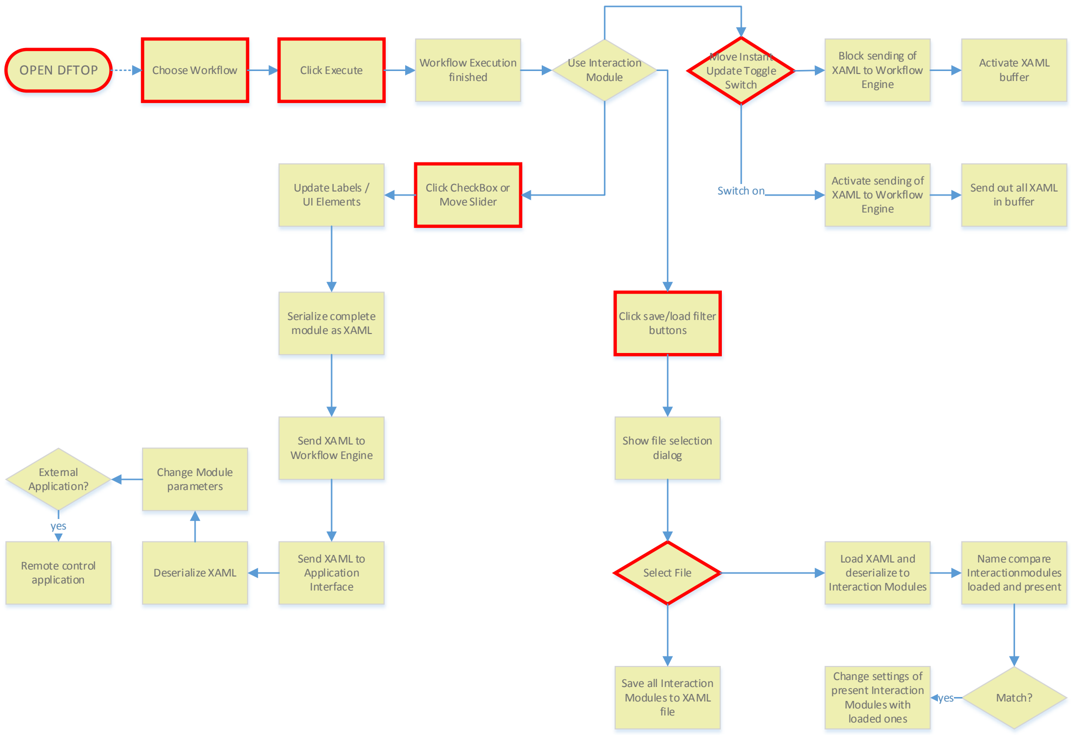

OPEN DFTOP
Choose Workflow
Click Execute
Workflow Execution finished
Use Interaction Module
Move Instant Update Toggle Switch
Block sending of XAML to Workflow Engine
Activate XAML buffer
Update Labels / UI Elements
Click CheckBox or Move Slider
Switch on
Activate sending of XAML to Workflow Engine
Send out all XAML in buffer
Serialize complete module as XAML
Click save/load filter buttons
Send XAML to Workflow Engine
Show file selection dialog
External Application?
Change Module parameters
yes
Remote control application
Deserialize XAML
Send XAML to Application Interface
Select File
Load XAML and deserialize to Interaction Modules
Name compare Interactionmodules loaded and present
Save all Interaction Modules to XAML file
Change settings of present Interaction Modules with loaded ones
yes
Match?

Figure A1-23: Interaction Module Use Process.

A1.2 CONVERSION OF PREFERENCE RANKING TO WEIGHTS

The following procedure is used to translate from preference ranking to relative weights that can be used in an objective function. The procedure is based on [1].

For each preference we sum the total number of assigned preferences by all decision makers:

$$c_{AB}\left(\{MOE_i\}_{i\in A} \succcurlyeq \{MOE_j\}_{j\in B}\right), \tag{1}$$

where $\emptyset \neq A, B \subseteq \{i\}_{i=1}^{|\Theta|} = I$, i.e., A and B are subsets of an index set I of indices corresponding to the set of all MOE, $\Theta = \{MOE_i\}_i$. Any number of these c_{AB} may be equal to zero, due to a lack of assigned preferences regarding some subsets of MOE.

The preferences assigned between *subsets* of measures can be simplified to a set of preferences among *single* measures [2]. We have:

$$\{MOE_i\}_{i\in A} \succcurlyeq \{MOE_j\}_{j\in B} = \{MOE_i \succcurlyeq MOE_j\}_{i\in A, j\in B}. \tag{2}$$

From the counts of assigned preferences in (1) we derive a basic belief assignment within belief function theory [3], [4]. In this setting of our problem representation, the frame of discernment (i.e., the set of all possible elementary preferences) is:

$$\Omega = 2^{\{MOE_i \succcurlyeq MOE_j\}_{i,j\in I}}. \tag{3}$$

We have the following basic belief assignment:

$$m_{AB}\left(\{MOE_i \succcurlyeq MOE_j\}_{i\in A, j\in B}\right) = \frac{1}{N} c_{AB}\left(\{MOE_i \succcurlyeq MOE_j\}_{i\in A, j\in B}\right) \tag{4}$$

where N is the total sum of all counts:

$$N = \sum_{AB} c_{AB}\left(\{MOE_i \succcurlyeq MOE_j\}_{i\in A, j\in B}\right). \tag{5}$$

While it is possible to change the representation in (4) using (2), it is not possible to divide the basic belief mass among the different preferences in $\{MOE_i \succcurlyeq MOE_j\}_{i\in A, j\in B}$ as we have no information on how to divide it among the different preferences. Instead the entire mass must remain on the whole set.

From the basic belief assignments in (4) we can calculate belief and plausibility for any subset of the frame of discernment. However, our interest is limited to analyse the support received by all preferences regarding single measures of performance such as:

$$\{MOE_i\} \succcurlyeq \Theta, \forall i \tag{6}$$

where $|\{MOE_i\}| = 1$. These preferences are what we need, to make a full preference based ranking of all MOE.

We have belief of the preference of MOE:

$$Bel_{\{i\}\Theta}(\{MOE_i\} \succcurlyeq \Theta) = Bel_{\{i\}\Theta}\left(\left\{MOE_i \succcurlyeq MOE_j\right\}_{j\in I}\right) = \sum_{X\subseteq\left\{MOE_i \succcurlyeq MOE_j\right\}_{j\in I}} m_{\{i\}B}(X) \tag{7}$$

and plausibility:

$$Pls_{\{i\}\Theta}(\{MOE_i\} \succcurlyeq \Theta) = Pls_{\{i\}\Theta}\left(\left\{MOE_i \succcurlyeq MOE_j\right\}_{j\in I}\right) = \sum_{X\cap\left\{MOE_i \succcurlyeq MOE_j\right\}_{j\in I}\neq\emptyset} m_{\{i\}B}(X). \tag{8}$$

We can sort all preferences based on the belief and plausibility for each preference $\{MOE_i\} \succcurlyeq \Theta$.

When both:

$$Bel_{\{i\}\Theta}(\{MOE_i\} \succcurlyeq \Theta) > Bel_{\{j\}\Theta}\left(\left\{MOE_j\right\} \succcurlyeq \Theta\right) \tag{9}$$

and:

$$Pls_{\{i\}\Theta}(\{MOE_i\} \succcurlyeq \Theta) > Pls_{\{j\}\Theta}\left(\left\{MOE_j\right\} \succcurlyeq \Theta\right) \tag{10}$$

then $MOE_i \succcurlyeq MOE_j$.

When an interval $\left[Bel_{\{j\}\Theta}, Pls_{\{j\}\Theta}\right]$ is included in an interval $\left[Bel_{\{i\}\Theta}, Pls_{\{i\}\Theta}\right]$ it is not immediately clear which is the preferred measure; MOE_i or MOE_j. We can interpolate with a parameter $\rho \in [0,1]$ in each belief-plausibility interval in order to find the preferred measure [5]. However, we have no information regarding the value of ρ, and any assumption about ρ will be unwarranted.

Instead we may calculate the point ρ_{ij} where the two measures MOE_i and MOE_j are equally preferred. When:

$$\left[Bel_{\{i\}\Theta}, Pls_{\{i\}\Theta}\right] \supset \left[Bel_{\{j\}\Theta}, Pls_{\{j\}\Theta}\right] \tag{11}$$

we have:

$$\rho_{ij} = \frac{Bel_{\{j\}\Theta} - Bel_{\{i\}\Theta}}{\left(Pls_{\{i\}\Theta} - Bel_{\{i\}\Theta}\right) - \left(Pls_{\{j\}\Theta} - Bel_{\{j\}\Theta}\right)} \tag{12}$$

where each belief and plausibility function is taken for $\{MOE_i\} \succcurlyeq \Theta$ and $\left\{MOE_j\right\} \succcurlyeq \Theta$, respectively. If $\rho_{ij} < 0.5$ then $MOE_i \succcurlyeq MOE_j$.

We notice that in the special case when we are only comparing MOE pairwise one-by-one the situation is simplified. The requirement that we must have $\rho_{ij} < 0.5$ in order for $MOE_i \succcurlyeq MOE_j$ is equivalent to having:

$$Bel_{\{i\}\Theta} + \frac{1}{2}\left(Pls_{\{i\}\Theta} - Bel_{\{i\}\Theta}\right) > Bel_{\{j\}\Theta} + \frac{1}{2}\left(Pls_{\{j\}\Theta} - Bel_{\{j\}\Theta}\right), \tag{13}$$

i.e., that the mid-point in the belief-plausibility interval MOE_i is higher than for MOE_j.

This implies that we can obtain an exact preference order of all MOE using a standard sorting algorithm based on the belief-plausibility interval mid-points have $\rho_{ij} = 0.5$ for each MOE.

We assigning weight the formal requirement is that the weight w_i is larger than w_j when $MOE_i \succcurlyeq MOE_j$. One possible approach that uses the preferences as carrying additional information regarding the actual weight (and not only the preferences) is to assign weight in proportion the mid-points.

We first calculate:

$$w_i^* = \frac{1}{2}\left(Bel_{\{i\}\Theta} + Pls_{\{i\}\Theta}\right) \tag{14}$$

and then assign weights as:

$$w_i = \frac{w_i^*}{\sum_{j=1}^{n} w_j^*} \tag{15}$$

where $n = \left|\{MOE_j\}\right|$.

A1.3 REFERENCES

[1] Schubert, J. and Hörling, P. (2014). Preference-based Monte Carlo weight assignment for multiple-criteria decision making in defense planning, in Proceedings of the 17th International Conference on Information Fusion, Salamanca, Spain, 7-10 July 2014, paper 189, pp. 1-8.

[2] Utkin, L.V. (2009). A new ranking procedure by incomplete pairwise comparisons using preference subsets. *Intelligent Data Analysis* **13**(2):229-241.

[3] Dempster, A.P. (1968). A generalization of Bayesian inference, *Journal of the Royal Statistical Society: Series B* **30**(2):205-247.

[4] Shafer, G. (1976). *A Mathematical Theory of Evidence*. Princeton, NJ: Princeton University Press.

[5] Schubert, J. (1995). On ρ in a decision-theoretic apparatus of Dempster-Shafer theory. *International Journal of Approximate Reasoning* **13**(3):185-200.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-MSG-124 AC/323(MSG-124)TP/825	ISBN 978-92-837-2151-2	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Developing Actionable Data Farming Decision Support for NATO

7. Presented at/Sponsored by

Final Report of MSG-124.

8. Author(s)/Editor(s)	9. Date
Multiple	July 2018

10. Author's/Editor's Address	11. Pages
Multiple	160

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Actionable	Data analysis	Modelling and simulation
CWIX	Data farming	NATO
Cyber defence	Decision support	Operation planning
DACDAM	DFTOP	Visualization

14. Abstract

Data Farming is a process that supports decision makers. The essence of data farming is that it is a question-based approach. The basic question repeatedly asked in different forms is: *What if?* The core objective of this task group was to apply actionable data farming that could contribute to the development of improved decision making of relevance to NATO forces.

The *Operation Planning Syndicate* addressed the question on how to provide actionable support to decision makers in operation planning. We developed the *Data Farming Tool for Operation Planning* (DFTOP) to support decision makers and analysts. Initial validation efforts have concluded that DFTOP meets the need of the military planner, and successfully brings Data Farming into the actionable decision support domain.

The main goal of the *Cyber Defence Syndicate* was to explore possible scenarios through data farming that could facilitate the understanding of some aspects of cyber defence. The syndicate members developed the *Data-farmable Agent-based Cyber Defence Assessment Model* (DACDAM) to support decision-making.

The overall conclusion and recommendation to military leaders is that data farming is feasible for NATO and nations, and should be used as a methodology for actionable decision support in operation planning and cyber defence.

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

DIFFUSION DES PUBLICATIONS

STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research
for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DGSlST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

DANEMARK
Danish Acquisition and Logistics Organization
(DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72
92322 Châtillon Cedex

GRECE (Correspondant)
Defence Industry & Research General
Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALIE
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research
Establishment
Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military
Academy Library
P.O. Box 90.002
4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

REPUBLIQUE TCHEQUE
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

ROUMANIE
Romanian National Distribution
Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a
informačné stredisko STO
Demänová 393
031 06 Liptovský Mikuláš 6

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi
Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

**The British Library Document
Supply Centre**
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

**Canada Institute for Scientific and
Technical Information (CISTI)**
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

NATO
OTAN

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

S&T organization

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30
1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2
1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECH REPUBLIC
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18
197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5
2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12
Tartu 51013

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7
D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25
H-1885 Budapest

ITALY
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301
00175, Rome

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002
4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25
NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide
P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 06 Liptovský Mikuláš 6

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SPAIN
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down, Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2
CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-2151-2