This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL
REPORT

Network-Based Operations for the Swedish Defence Forces

An Assessment Methodology

WALTER PERRY, JOHN GORDON IV,
MICHAEL BOITO, GINA KINGSTON

TR-119-FOI

June 2004

Prepared for the Swedish Defence Research Agency

RAND EUROPE

The research described in this report was prepared for the Swedish Defence Research Agency.

Library of Congress Cataloging-in-Publication Data

Network-based operations for the Swedish defence forces : an assessment methodology / Walter Perry ... [et al.].
p. cm.
"TR-119."
Includes bibliographical references.
ISBN 0-8330-3539-8 (pbk. : alk. paper)
1. Sweden—Armed Forces—Organization. 2. Unified operations (Military science) 3. Sweden—Defenses. 4. Sweden—Military policy. I. Perry, Walt L.

UA790.N397 2004
355.3'09485—dc22

2003025742

Published 2004 by the RAND Corporation
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

Network-centric warfare (NCW), or network-based warfare, is generally thought to be "an information superiority enabled concept of operations that generates increased combat power through the networking of sensors, decision makers and shooters, to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization" (Alberts et al., 2002, p. 2). In contrast to network-based operations or warfare, traditional warfare is considered to be *platform-centric*. The difference between the two is that each weapon system in platform-centric warfare acts independently, so that one must mass force to mass combat effectiveness, whereas, in network-centric warfare, effects are massed rather than forces. For this reason, network-based operations are attractive to the Swedish Defence Forces.

A structural or logical model for network-based operations has emerged. Its fundamental requirement is a high-performance information network that provides the capacity for computing and communications among entities participating in a given operation. This is what we refer to as the *network infrastructure*.

An effort is under way to complete Sweden's military modernisation effort by 2015, focusing on warfare in the 2025 time frame. An early product of this effort, scheduled for completion in 2005, is to be an operational network design. The design will include, among other things, an architecture, a communications infrastructure, and a sensor management plan. The tools to assess the cost and effectiveness of the design must be in place early to assist in that process. The Swedish Defence Research Agency (FOI) is tasked with developing a methodology to identify the costs and benefits of alternative network structures.

Research Objective

The primary objective of this research is to develop a general methodology that can be used to assess the costs of performing a wide range of military functions using alternative network structures: in essence, to define an analytic process. Although we do not address the benefits directly, we address them indirectly through the requirements for an operational network. We recognise that the Swedish military will also require a more direct assessment of the benefits.

This project comprises two basic tasks: (1) Identify the operational functions to be served by a comprehensive network-based defence structure and (2) identify support activities needed to perform these functions and recommend an approach for assessing their costs, as well as the costs of the network infrastructure and the operational infrastructure. The application of the recommended approach to an operational function and illustrative network infrastructures is left for future work.

Sweden's Emerging Defence Policy Options

The 1999 Swedish policy paper *The New Defence—prepared for the next millennium* highlights the magnitude of the changes in international relations that have taken place in recent years. The report states:

> The Swedish defence system is about to undergo necessary renewal and modernization. The reason for this is the security situation in the world at large. We can now create a modern, flexible and versatile defence on the basis of national service. The units and systems that will be needed in the future should be capable of being utilized for both the defence of Sweden and participation in international operations.

The government envisions that, in 2004, important decisions will be made that will guide the future orientation and structure of the Swedish armed forces. Three of the four options under consideration place considerable emphasis on coalition military operations outside Sweden. The decisions will provide guidance to the armed forces on the direction they are to take in the next 10 to 15 years.

Operational Functions

Among the problems facing system architects and analysts are (1) identifying the full spectrum of military operations to be conducted in a network-based structure and (2) understanding just how such operations will be performed and what level of network-based support the operations will require. The operational functions supported by the network are those associated with the selected option for the Swedish Defence Force's future structure. In any case, the functions will have full-spectrum requirements, which fall into four broad categories:

Combat Operations: Functions directly related to combat operations, such as air and missile defense, and joint command and control.

Peacetime Operations: Other functions, such as supply and personnel management, are more applicable to normal peacetime operations.

Interagency Operations: Still other functions relate to interagency operations, for which the military has to exchange information and data with other government departments.

Noncombat Coalition Operations: These include functions such as humanitarian assistance operations and assistance to local civil authorities.

Prioritisation

Given the costs and technological challenges associated with creating a large-scale military network, there is a need to prioritise the effort. The 2004 defence decision should provide important guidance for Swedish military planners and technologists, who can then prioritise which aspects of a military network can receive immediate attention. For example, if it is determined that homeland defence will still be emphasised, then a function such as air and missile defence would probably receive high priority. If, on the other hand, international operations are to be emphasised, other aspects of a military network, such as a joint command system with the ability to interface with selected nations that are likely coalition partners, would assume greater priority in terms of resources.

Emerging U.S. Vision

From the dawn of organised conflict, military strategists have used communications and information to beat the enemy. The ancient Greeks dispatched runners over long distances to deliver military messages. European infantries used drummers to communicate common battle orders to soldiers fighting together who did not speak the same language. Network-centric warfare sprang from a need, dramatised in World War II and Vietnam, to use information technology to create a more lethal fighting force, as well as to avoid casualties from friendly fire. Although currently most widely used within the U.S. Navy, where it was first developed, NCW is emerging as a key operational concept to support the U.S. military's force transformation. The nature of NCW is such that large weapon systems, such as ships, can take advantage of its benefits more readily than can the more dispersed Army formations.

Methodology

The methodology proposed in this report assumes that the operational functions have been prioritised and networks have been proposed to support theoperational functions. The operational functions are then grouped intointeraction categories according to their requirements. These categories support the identification of common subnetworks and of analogous systems or components in the cost-estimation process.

Categories of Interaction

Although it may be a theoretical ideal to have all military functions available on a single federated network that all military users can access, the reality is that there will be a stratification of users according to their need to have access to the data, their function, hardware and software costs, and security concerns. In most cases, the subnetwork will dictate access requirements. We refer to this stratification of users as the *categories of network interaction.*

The categories are distinguished in three ways: the degree of access required, including both the number of participants in the operational function and the variety of data required; the security requirements; and the timeliness, or time criticality, of the information needed to support the operational function. Each of the operational functions falls into one of the four categories of network interaction illustrated in Figure S.1.

Category 1—Specialised Interaction. In this category, the requirements are not as extreme as for those of the categories that follow. The requirements for access to information vary with participants' roles and the structure of the supporting subnetwork. The requirement for near-real-time access to information varies by participant. And although some security may be required, it is not a driving factor. The requirements for access, timeliness, and security may each range from medium to low, requirements that cover a wide range of networks, many of them not suitable for defence needs. For example, as the level of access, timeliness, and security approaches zero, the need for any form of network disappears.

Category 2—Ubiquitous Interaction. Functions that require this degree of network accessibility generally affect large numbers of organisations—for example, subnetworks that support personnel management activities, payroll, and supply functions, along with certain joint operations requiring several units from all services. In general, the several participants in the supported activity

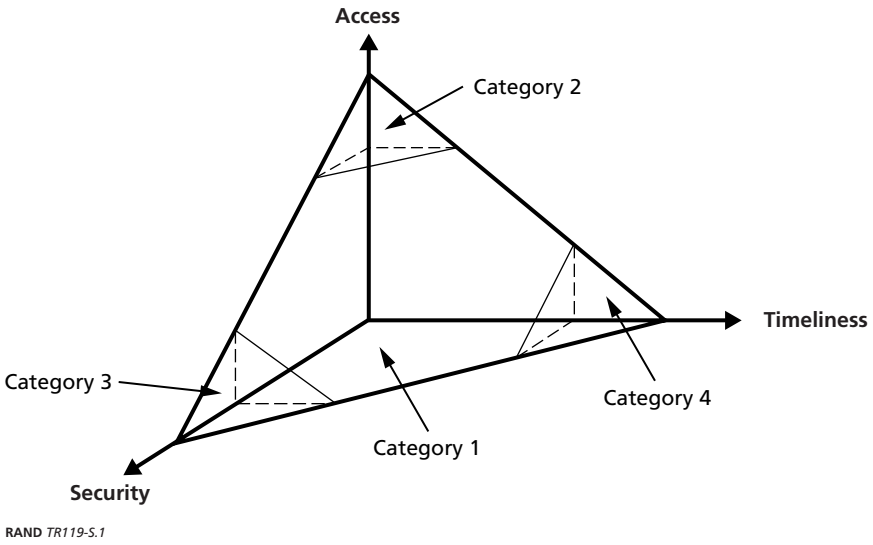

Figure S.1—Interaction Categories

will require similar access to data and information on all aspects of the operation available on the federated network.

Category 3—Secure Interaction. Several operational functions require that both operations and information be secure, placing unique demands on the network for interactions among participants and the information exchanged to be secured both physically and electronically. Most intelligence operations, covert activities, and Special Forces operations are of this nature.

Category 4—Real-Time Interaction. Operations requiring this level of support are usually extremely time-sensitive combat actions that require that very few participants have access to critical real-time data and are able to share that data among all participants, even when network connections and nodes have failed. They are highly restrictive (few participants), intense operations, such as cruise and ballistic missile defence.

Deciding on an Interaction Category

One of the early tasks in assessing the costs and benefits of network-based operations is determining the category of network interaction each operational function requires. To make this task easier, it is helpful to establish measures that can assess the broad interaction requirements needed to support each operational function. The degree of interaction available from the federated network is clearly a function of the structure of the underlying information

network available; therefore, the measures selected are designed to assess the federated network's ability to supply the full range of information services, on demand, to the entities participating in operational functions. These measures are defined in Chapter 3. In Table S.1, the measures that are used to determine which category an operation's function falls into are listed on the left; the categories of interaction are shown along the top.

Network requirements can be determined from the categorisation of the operational functions. The network architectures that will support those functions can be assessed from the network requirements directly, and the benefits of network-based operations can be assessed indirectly. The method used to analyse the architecture will depend on the requirements and the novelty of the architecture.[1] The categories also group similar networks for costing.

Table S.1

Determining Interaction-Category Thresholds

Measure	Category 1 Specialised	Category 2 Ubiquitous	Category 3 Secure	Category 4 Real-Time
Intensity	Medium	High	Medium	Low
Capacity	Medium	High	Medium	Low
Richness	Medium	High	Medium	Low
Reach	Medium	High	Low	Low
Monitoring	Medium	Low	High	High
Robustness	Medium	Low	High	High
Security	Medium	Low	High	Medium
Timeliness	Medium	Low	Medium	High

Illustrative Operational Functions

In theory, all relevant information needed to support operations is available for users to access in support of all operational functions. Under ideal circumstances, all participants in the network could gain access to and use any function in the network. In reality, the number of users for a particular function will be limited according to need-to-know, cost constraints, and other considerations.

[1] Assessment approaches are not discussed in detail; however, they may include analysis of both the network and the network components, using simulation, throughput-analysis tools, or comparison with existing networks or components.

The Swedish military should consider what operational functions it requires for inclusion in a network or federation of networks. Of the several operational functions that could be included in a network, three have been singled out for more detailed analysis: air and missile defence, joint air-land-sea battle command, and joint targeting. Examples of other operational functions that could be included in a Swedish military network include disaster relief, mass casualty response, supply management, and training status of individuals and units.

An additional important consideration for Sweden is the degree of international interoperability that should be included in its military networks. With emphasis being placed on multinational operations, the Swedish military must consider the degree to which its military networks should be interoperable with similar systems being developed by other nations.

Costing

Although our objective here is not to actually assess the costs associated with performing the operational functions in a network-based structure, we suggest a *general methodology* that can be applied to any operational function executed within any network-based structure. For a general methodology, we identify cost categories that encompass the network itself; its development, management, and maintenance; and the possible costs associated with performing operational functions in a network-based environment.

The following is a summary of cost-estimating practices, followed by a broad range of general approaches available to estimate network-based operations for Swedish Defence Forces. Next, we consider the lessons learned from the U.S. Navy's Cooperative Engagement Capability (CEC).[2] We conclude with a suggested methodology for estimating the cost of network-based operations in the Swedish Defence Forces.

Cost-Estimating Approaches

There are three basic approaches to cost estimating: bottom-up, analogy, and parametric. The following paragraphs provide an overview of the three approaches and their advantages and disadvantages.

[2] The CEC system links U.S. Navy ships and aircraft operating in a particular area into a single, integrated, air-defence network, in which radar data collected by each platform are transmitted on a real-time (i.e., instantaneous) basis to the other units in the network.

Bottom-Up: The bottom-up approach relies on detailed engineering analysis and calculation to estimate costs. Details the analyst needs are design and configuration information for all parts of the system being estimated, including material, equipment, and labour. The detailed design and cost estimate has the advantages of addressing many issues so that the effect of each issue is well understood.

Analogy: With the analogy approach, an analyst selects a similar or related system and makes adjustments for differences. This approach works well for derivative systems or evolutionary improvements to existing systems. Its main advantage over the bottom-up approach is that only the changes or differences must be estimated, which saves time and expense. However, a good starting baseline must exist for this method to be applied. For radical changes or new technologies, the bottom-up approach is more appropriate.

Parametric: A third approach uses parametric methods to forecast outcomes. *Parametric methods* attempt to explain cost as a function of other physical or technical characteristics, such as software lines of code, data throughput, and size or weight. This approach has as its principal advantage that its application is straightforward once the basic relationship has been defined. Unlike the first two approaches, a detailed conceptual design is not necessary to apply the method, although a method of determining the relevant input characteristics is required. Another, more subtle, advantage of parametric relationships generated using regression analysis is that one can also generate information on uncertainty of the forecasted value. In other words, one obtains a result of $y \pm e$, where e is related to the error terms of the regression. This uncertainty value can be just as informative as the predicted value.

A Methodology for Estimating Costs of Network-Based Operations

Assessing the costs and benefits of converting to a network-based defence structure requires a sound methodology that can help analysts to objectively compare alternative structures. The problem is to identify all costs and to adopt an accepted costing method to apply to each. The costs associated with implementing network-based operations derive from two broad categories: those associated with the network infrastructure and those associated with the operational functions to be supported by the network. The appropriate cost methodology should be able to estimate the costs of different networks that perform different operations at different support levels so that decisionmakers will have an idea of what kind and how many networks they can afford. The

methodology should also be capable of comparing the cost of performing a given operation without a network with the cost of performing the operation in a network, thus allowing for a comparison of costs and benefits of a network for each operation.

Estimating Network Infrastructure Costs. The methodology to estimate network infrastructure costs requires that specific operational functions and networks have been selected for costing.

The first step in the methodology is to define an appropriate cost-element structure for the network. Network infrastructure (information network) costs include the investment costs of exploring and defining the network concept; costs of developing the system, including system design and specification, software development, and test and evaluation; and the costs of procuring and deploying facilities, hardware, and software. Network infrastructure costs will also include ongoing costs to operate and maintain the network and are generally driven by the costs of personnel and software maintenance.

There is no set or prescribed answer to the question: What is the appropriate level at which to define a cost-element structure and estimate costs? At the planning stage, when little detailed information is available about the system, it may not be possible to estimate at an expanded level of detail. Similarly, when detailed information on analogous systems is not available, it may not be possible to estimate in great detail. Yet, if the system to be estimated is very similar to an analogous system, it may be sufficient to estimate without much detail by drawing on the significant similarities.

However, it may be necessary to estimate at a detailed level when the system to be estimated is unique, and the estimator must look at many small components of the system for which cost methodologies are available to build up to the cost of the total system. Finally, when high resolution is required, and sufficient data, time, and money are available, a more detailed estimate may be appropriate.

The second step is to determine the interaction category appropriate for the selected operational functions. This means applying the measures and metrics described in Chapter 3.

The third step in the methodology is to link the capabilities and metrics of the network to elements of the infrastructure cost. The use of the metrics for assessing categories of interaction can assist in determining at least ordinal levels of cost differences for each cost element. Linking the capabilities and metrics of the network to the cost element then guides the choice of an appropriate estimating methodology, the next step.

The fourth step is to choose an appropriate cost-estimation methodology. Ideally, we would like to link each cost element with its capabilities and metrics and select a cost-estimating methodology that is sensitive to the key metrics. We may use analogies to other elements in the same interaction category, or perhaps a parametric cost-estimating relationship that used the metrics as inputs, or to formulate new cost-estimation relationships between metrics of the network and estimated costs.

Difficulties in Estimating Software-Intensive Systems. One of the most difficult areas of network infrastructure to cost is the software. Software-intensive systems have proven notoriously difficult to estimate in the United States. Many U.S. weapon systems have experienced cost growth and schedule delays because of problems in software development, which include frequent changes by the user, overlooked tasks, lack of coordination among functions during development, and poor estimating methodologies.

Methodology for Estimating Network Operations Costs. The cost methodology must also assess the costs of performing the military operation in terms of personnel, equipment, and consumable items, such as fuel or repair items. For example, it is conceivable that additional personnel would be required to interpret or use the additional information a network provides for a given operation. It is just as conceivable that fewer personnel would be required to synthesise or process data in a networked operation, if the network did the processing. It is also conceivable that networking will allow some participants in the network to have fewer sensors of their own because they benefit from the information provided by the entire network. In these ways, networking would reduce some equipment costs. In any event, the cost methodology should assess how the network will change the way an operation will be performed and estimate the resulting differences in personnel, equipment, and other relevant costs.

Identifying which operations are affordable to network and which operations have the highest ratio of benefits to costs, when the cost methodology is combined with a methodology for assessing benefits, provides decisionmakers the information they will need.

Conclusions

Developing a common reference for discussing network-based operations will be important as the Swedish military moves increasingly in the direction of this new way of commanding, controlling, and executing military operations.

The operational functions we discuss are examples of what could be included in a series of federated military networks. Some functions would have applicability in normal peacetime operations as well as during an actual military operation. Other functions are more directly related to actual operations. The major defence policy decisions that Sweden will make in the coming years will help guide the prioritisation of these functions. Fiscal and technology realities will mean that networking will gradually enter the Swedish military; therefore, priority should be given to first introducing functions that relate to the types of operations the Swedish military is most likely to undertake.

We devoted considerable attention to the costing of military networks—a still-imprecise art, much less a science. Since the concept of network-based operations is still being introduced into the more technologically advanced militaries of the world, there are few lessons and past experiences that provide guidance on how to approach costing of new systems. The report provides insights on what are likely to be major cost drivers in military networks, one of the most critical, and most difficult to predict, being software development. Early definition of requirements can help in this area. Since the Swedish military is still developing its concepts of network-based operations, it is still too early to predict with any accuracy the eventual costs of a network. However, those involved in the networking effort in Sweden should be aware of the major issues associated with network development costs, which we have highlighted in this report.

A next step is to apply the approach to an operational function and illustrative network infrastructures.