SWEDISH DEFENCE
RESEARCH AGENCY

FOI-R--0490--SE
August 2002
ISSN 1650-1942
Scientific report

Mattias Axelson and E. Anders Eriksson

Towards an Industry for Network Based Defence?

- Creating information age defence systems

FIND
Programme

SWEDISH DEFENCE RESEARCH AGENCY

FOI-R--0490--SE

August 2002

ISSN 1650-1942

Scientific report

Mattias Axelson and E. Anders Eriksson

Towards an Industry for Network Based Defence?

- Creating information age defence systems

Issuing organization FOI – Swedish Defence Research Agency	**Report number, ISRN** FOI-R--0490--SE	**Report type** Scientific report
	Research area code 1. Defence and Security Policy	
	Month year August 2002	**Project no.** A1143
	Customers code 1. Research for the Government	
	Sub area code 11. Defence Research for the Government	
Author/s (editor/s) Mattias Axelson E Anders Eriksson	**Project manager** Martin Lundmark	
	Approved by Jan Foghelin, Head of Division	
	Sponsoring agency Ministry of Defence	
	Scientifically and technically responsible	

Report title

Towards an Industry for Network Based Defence? – Creating information age defence systems

Abstract (not more than 200 words)

Two different schools of thought were found on industry aspects of the shift towards an information age defence – in the report they are labelled ‘reformists’ and ‘revolutionaries’. The ‘reformists’ acknowledge changes to defence induced by technological development, but see these as quantitative, i.e. not qualitatively disrupting the character of conflicts. The ‘revolutionaries’ in contrast foresee significant societal shifts likely to change conflict and defence also qualitatively.

As for the industrial base ‘reformists’ typically stress the role of established defence prime contractors in harnessing commercial ICT developments. From the point of view of ‘revolutionaries’, small and medium sized companies with defence domain expertise could exploit disruptive technologies to develop innovative military applications by being flexible in adapting new technologies and in reconfiguring organisational skills and resources. Based on the findings of this study, governments are advised to improve collaboration with a range of companies from both the defence and commercial sectors in order to take advantage of the innovative potential of current developments in technology and business.

Keywords
Network centric warfare, Revolution in Military Affairs, Revolution in Security Affairs, Defence, Industry, Technology, Innovation, Strategy, and Collaboration.

Further bibliographic information	**Language** English
ISSN 1650-1942	**Pages** p. 49
	Price acc. to pricelist

Utgivare Totalförsvarets Forskningsinstitut - FOI	**Rapportnummer, ISRN** FOI-R--0490--SE	**Klassificering** Vetenskaplig rapport
	Forskningsområde 1. Försvar- och säkerhetspolitik	
	Månad, år Augusti 2002	**Projektnummer** A1143
	Verksamhetsgren 1. Forskning för regeringensbehov	
	Delområde 11. Försvarsforskning för regeringens behov	
Författare/redaktör Mattias Axelson E Anders Eriksson	**Projektledare** Martin Lundmark	
	Godkänd av Jan Foghelin, Avdelningschef	
	Uppdragsgivare/kundbeteckning Försvarsdepartementet	
	Tekniskt och/eller vetenskapligt ansvarig	

Rapportens titel (i översättning)

Mot en industri för nätverksbaserat försvar? – att skapa försvarssystem i informationssamhället

Sammanfattning (högst 200 ord)

Studien identifierar två olika synsätt på skiftet mot informationssamhällets försvar – benämnda ’reformister’ respektive ’revolutionärer’. Reformisterna betraktar förändringar inom försvarsområdet som föranledda av teknologiska utvecklingar. Men de ser dessa förändringar som kvantitativa, och inte som kvalitativa med potential att ändra konflikters karaktär. Revolutionärerna anser däremot att påtagliga skiften i samhället kan förändra konflikter och försvar kvalitativt – dvs att nya aktörer, nya metoder och teknologiska kombinationer kommer att ta plats på konfliktscenen.

Reformisterna ser traditionella försvarsföretag som naturliga utvecklare av framtidens försvarssystem. Revolutionärerna menar att små och medelstora företag med kunskap om försvarssektorn kan exploatera nya innovationer och utveckla innovativa försvarstillämpningar. Utifrån studiens resultat rekommenderas stater att utveckla samverkan med både civila företag och försvarsföretag. Detta kan bidra till förbättrade möjligheter att exploatera den innovationspotential som skapas inom företag och med den teknologiska utvecklingen.

Nyckelord

Network Centric Warfare, Revolution in Military Affairs, Revolution in Security Affairs, nätverksbaserat försvar, försvar, industri, teknologi, innovation, strategi, samverkan

Övriga bibliografiska uppgifter	**Språk** Engelska
ISSN 1650-1942	**Antal sidor:** s. 49
Distribution enligt missiv	**Pris: Enligt prislista**

FOI1004 Utgåva 11 2002.02 www.signon.se Sign On AB

Preface

Since 1990, the FOI Defence Industry Programme, FIND[1], has studied defence industry strategies and the industry's restructuring process for the Swedish Ministry of Defence. The focus has been on European and US defence industry integration and multilateral defence materiel collaboration. In addition, the programme has in recent years included studies on the globalisation of the defence industry and aspects of the shift from manufacturing as the core business of defence contractors to the increased focus on the development of services and solutions.

There is growing interest in Sweden (as well as in other countries) in the concept of network centric warfare, which was introduced in the US during the 1990s. In Sweden this concept is about to materialise in the form of the development of a new command and control system – the Ledsyst. The ambition of Swedish defence policy is to take decisive steps towards a network based defence.

This report contributes to the knowledge regarding industrial prerequisites for harnessing the potential of information and communication technologies for defence systems. It should therefore be useful for Swedish policy and strategy making in developing a network based defence. For industry actors this report may give insights into the defence markets' changing rules of engagement.

We wish to express our gratitude to all those people who have contributed to this study. We are indebted to those in America and Europe who kindly spent hours with us discussing industry aspects of the changing conditions in the defence sector. We also wish to thank Dr Björn Lindkvist of the Stockholm School of Economics and Lt.Col. Göran Pettersson from the Strategic Plans and Policy Directorate of the Swedish Armed Forces Headquarters for their review of this report. In particular we wish to thank Mr Andrew James of the University of Manchester, UK. He contributed excellently to this report with a study on policy and industry development regarding network centric defence issues in the UK.

The authors are obviously responsible for all interpretations and conclusions presented in this report – and for any remaining mistakes.

Stockholm in August 2002

Mattias Axelson and E. Anders Eriksson[2]	Martin Lundmark
Authors	Programme manager

[1] www.foi.se/find

[2] mattias.axelson@foi.se; e.anders.eriksson@foi.se

Executive summary

In Swedish defence policy a shift towards network-based defence has been proclaimed. This is a shift from a defence designed around the capabilities of hardwired platform systems to one where communication networks enable ‘seers’, ‘doers’ and ‘deciders’ to cooperate in a great variety of patterns to perform various tasks. However, so far Swedish activities within this novel defence paradigm have been more about producing PowerPoint slide shows than e.g. building demonstrators or pursuing field experimentation. This study was set against the issue of what industrial base will be needed to provide the systems, and in particular the system of systemssolutions, necessary to develop a network based defence.

Two different schools of thought were found on industry aspects of the shift towards an information age defence – in the report they are labelled ‘revolutionaries’ and ‘reformists’. In the context of the broader RMA (Revolution in Military Affairs) debate, ‘reformists’ can very well be more extravagant in terms of their predictions on imminent technological breakthroughs than ‘revolutionaries’. However, ‘revolutionaries’ tend to stress the potential of technological and broader societal changes to revolutionise not only the way conflicts are fought but also their fundamental nature. In particular they tend to stress the risk that asymmetric adversaries turn out to be more competent users of emerging technological and organisational opportunities than military establishments. We term this position RSA (Revolution in Security Affairs) in contrast to ‘traditional’ RMA.

‘Reformists’ typically stress the role of established defence prime contractors in harnessing commercial ICT developments and are negative with regard to the ability of governments to usefully develop direct links with these technological and business ‘new frontiers’. This outsourcing arrangement requires that military customers are able to specify their requirements early on in the development process. ‘Revolutionaries’, in contrast, argue that a *co-evolutionary development model*, simultaneously involving operational concepts, materiel, training etc., is necessary to harness the power of commercial ICT developments effectively enough to cope with RSA. This in turn requires experimentation in which suppliers and users work closely together. In this co-evolutionary work the ‘revolutionaries’ typically stress the need for the military customer to work directly with innovative small and medium sized enterprises, and not only with traditional defence primes.

Thus, from the point of view of the revolutionaries, small and medium sized companies with defence domain expertise could exploit disruptive technologies to develop innovative military applications by being flexible in adapting new technologies and in reconfiguring organisational skills and resources. This challenges the notion that only traditional defence contractors could manage integration of competencies and resources to develop innovative defence systems for network centric warfare. Therefore, traditional defence contractors should consider how to develop flexible and adaptive capabilities in order to harness the innovation potential of ICT in defence settings. Based on the findings of this study, governments are advised to improve collaboration with a range of companies from both the defence and commercial sectors in order to take advantage of the innovative potential of current developments in technology and business.

1 Introduction

This report is inspired by the adoption of RMA ('Revolution in Military Affairs') and network centric defence thinking by Swedish policy makers. This Swedish process was set in motion by a series of studies commissioned by the Swedish Armed Forces (SwAF) to US systems integrator SAIC starting in 1998. These ideas quickly gained strong high-level backing most recently confirmed by the central role given to what is now termed Network Based Defence in the defence bill submitted by Government to Parliament in December 2001 (Prop. 2001/02:10).

It is acknowledged within the defence establishment in Sweden that, so far, Swedish activities within this novel defence paradigm have been more about producing PowerPoint slide shows than, e.g. building demonstrators and pursuing field experimentation. However, this is now intended to change with the so-called Ledsyst projects addressing novel C3I (Command, Control, Communication and Intelligence; sometimes SR is added to denote Surveillance and Reconnaissance) systems from the vantage point of technology, methods, personnel and organisation.[3]

The purpose of the present report is to explore, for the benefit of the Swedish MoD, defence industry policy aspects of this emerging, novel defence paradigm. Thus, while most of the RMA literature focuses on general strategic and technological aspects, this study aims to fill a gap regarding the industry aspects of a shift towards information age defence systems.

The research reported here consists of two steps preceding final analyses and documentation: The first step included reading literature within the network centric paradigm and interviewing experts in the Swedish defence establishment. This lead us to views on network centric defence similar to those outlined under the heading of the 'revolutionary' standpoint below, and to the following three research questions:

- What business models should defence organisations adopt to exploit the potential of ICT (Information and Communication Technologies) developments – in particular for network centric defence solutions?

[3] These projects are referred to, respectively, as LedsystT, M, P, and O.

- Given the leading role of civil firms in cutting edge ICT, how should defence organisations tap the competencies of leading commercial sector suppliers?
- What scope is there for international cooperation on network centric defence solutions?

The second step consisted of interviewing industry and defence establishment representatives in four leading countries –United States, United Kingdom, France and Germany – to shed light on these research questions. Interviews with Swedish industry representatives can also be included in this part of the study.

Outline of report

The chapter following this introduction deals with methodology, primarily the semi-structured interviews performed in the five countries mentioned above. Then follows a review of the general RMA literature highlighting in particular the difference between, on the one hand, schools of thought that foresee a possible dramatic technical and tactical change, but in a relatively stable general security setting ('traditional RMA'), and on the other hand those who also stress the potential for new forms of conflict and security challenges (here termed 'Revolution in Security Affairs', RSA).

The key conceptual part of the report consists of two chapters devoted to analysing conflicting perspectives on network oriented defence acquisition and qualitative vs. quantitative innovation.

The interview findings are reported in two chapters: one organised by country, the other thematically.

Finally, two chapters are dedicated to conclusions. One draws general conclusions on industry aspects of the shift towards information age defence systems, and one is more specifically geared to Swedish policy challenges.

2 Methodology

This is an exploratory study intended to capture the industrial change processes involved in the creation of network centric defence capabilities. The report relies on interviews with people in Europe and the US working with issues on future defence systems and relevant industries. In all, 35 interviews were performed with one or several individuals from defence companies, commercial sector companies and government agencies in France, Germany, Sweden, the UK, and the US. In several interviews, more than one respondent was present. Consequently, more than 50 people were interviewed.

The interviews were conducted during the summer, autumn and winter of 2001/02.

The experienced defence industry researcher Mr Andrew James of the University of Manchester conducted the UK interviews on behalf of this research project. His contribution provides this report with valuable insights on current network defence related industry and procurement developments in the UK and in general. A thorough presentation and analysis of the UK study, by Mr James, will be published in a forthcoming FOI report.

Most of the non-UK interviews were conducted by Dr Eriksson and Mr Axelson jointly, a significant share by Mr Axelson alone, and one by Dr Eriksson only.

All respondents are, to some extent, involved in the process of developing defence systems for the future. They hold positions such as senior vice president, director of strategy, and senior analyst. The vast majority of interviews lasted for a couple of hours or more. The character of the interviews was open conversation around a set of broad questions. As discussed below, not all respondents were prepared to discuss network centric solutions and the like in explicit terms. Consequently rather lengthy discussions were sometimes needed in order to reach common ground. Aspects particularly in focus were collaborative patterns within the industry, future business prospects and changes in acquisition policies.

In addition, literature on Network Centric Warfare (NCW), the Revolution in Military Affairs (RMA), and other central concepts is reviewed in the following chapter.

3 Perspectives on general trends in defence and security in the 21st century

A literature review is needed to position this study in relation to previous research on current changes in military affairs due in particular to the rapid advancements in ICT. Whereas most previous literature focuses on general strategic and technological aspects, this study aims to fill a gap regarding the industry aspects of a shift towards information age defence systems.

The RMA debate: a revolution in military or in security affairs?

The US debate on an ongoing or imminent Revolution in Military Affairs (RMA) was sparked by the equally spectacular American successes in military terms in the Gulf War 1991, and in economic terms during the IT led long boom of the 90's. Key RMA publications include the US strategy document Joint Vision 2010, Nye and Owens (1996), and Owens (2000).

In fact, the RMA movement is in no way uniform. In a critical assessment of it, O'Hanlon (2000, pp 11-18) usefully distinguishes several RMA schools of thought. First come three schools, according to O'Hanlon progressively more ambitious, then three schools defined in more disparate (and non-exclusive) terms:

The **system of systems** school focuses on the potential of rapidly improving computers, communication, and networking to make existing systems – weapons, sensors, C3I components, etc. – function in a much more integrated fashion.

The **dominant battlespace knowledge** school goes beyond the above by also assuming radical improvements in sensors, rendering the battlespace 'transparent'.

The **global reach, global power** school goes even further in envisioning the development of new, far more precise, lethal, agile and deployable weapons.

The **vulnerability** school instead stresses the opportunities arguably opened to asymmetric threat actors by the technological and organisational developments that RMA is intended to exploit.

The **visionary** school is a mixed bag of thinkers who, according to O'Hanlon, argue for an even more significant military revolution ahead than the global reach, global power school. Among cited manifestations are The Third Wave (Toffler and Toffler, 1993), and NCW (Cebrowski and Garstka, 1998), but also those positing huge energy sources or new sensors making oceans completely transparent.[4]

The **cautionary** school also believes that major security changes may be in stock for us but cautions against rash conclusions as to the nature of these, and consequently on what action to take.

O'Hanlon in our understanding subscribes to the system of systems school based on the unequivocal advances in ICT. Regarding dominant battlespace knowledge and global reach, global power, O'Hanlon argues that physical limitations, slower progress in mechanical technologies than in ICT, and countermeasures and adaptations available to an adversary interact to make them much less convincing. Further, O'Hanlon is sympathetic towards the vulnerability and cautionary schools, arguing for R&D and experimentation rather than major RMA procurement programmes.

We find O'Hanlon convincing on these counts. As for the visionary school, however, we have some problems with his position. In simple terms we argue that NCW would be better placed in the system of systems – and/or cautionary – school. In fact we think that O'Hanlon, in conceiving the visionary school, mistakenly juxtaposes one position that is extreme in the traditional RMA position, combining extravagant assumptions on technological developments with a lack of dynamism in the realm of character of conflicts, with one that stresses the tendency of societal change to co-evolve with the character of conflicts. The latter position has more kinship with the vulnerability and cautionary schools than with global reach, global power or dominant battlespace knowledge.

This highlights a dimension other than fast vs. slow technological progress, viz. stable vs. changing character of conflicts. The positions stressing changing character of conflicts, i.e. the vulnerability school, the cautionary school, and the NCW part of the visionary school, could be tentatively summarised under the heading of revolution in security affairs (RSA) in contrast to the traditional RMA schools.

As developed elsewhere, we tend to agree with the RSA position – that a fairly major societal change may be in the making, and that it is likely to have profound security consequences. Indeed the post-cold war security environment could be seen as the beginning of these. The Third Industrial Revolution is a good heading for this general societal transformation, indicating that it is possible to argue for the imminence of such a change without adhering to the apocalyptic perspective of the Tofflers. After all, the third major structural change since ca 1800 is a lot less extravagant than the third since the dawn of man. (Eriksson, 1999 and 2002)

It is very significant for this report that while global reach, global power and dominant battlespace knowledge very much build on traditional RMA (i.e., non-RSA) assumptions, the system of systems school is compatible with both RMA and RSA assumptions. However,

[4] According to O'Hanlon, the first four entries represent 'major RMA schools' while the subsequent two have been extracted by us from a cursory section on 'Other RMA Schools of Thought' (O'Hanlon, 2000, pp 17-18).

RSA assumptions – allowing significant uncertainty as to the character of future conflicts – imply tougher challenges on system of systems integration activities since a wider scope of defence tasks have to be considered and prepared for, at least in the form of options. As we will see below, RSA and RMA assumptions tend to lead to different positions on industry and acquisition issues.

In our understanding the NCW school of thought with Cebrowski and Garstka (1998) and Alberts et al. (2000) as key publications, is open to the broader RSA view. In particular the section on NCW myths in Alberts et al. (2000, 5-13) is informative in this regard. This is why we find O'Hanlon mistaken in lumping NCW together with a set of particularly technologically and scientifically adventurous thoughts.

A final remark on O'Hanlon's categorisation is that while dominant battlespace knowledge is relevant only to quite resource-rich actors – and global reach, global power essentially only to the US, a system of systems approach may be quite useful also to a security actor of modest resources – even to an asymmetric threat actor.

System of systems integration and network oriented thinking

The combination of defence industry globalisation, increasing importance of new technologies and changes in demand, drives transformations of the defence industry forward. In no other segment of the defence industry is this transformation as significant and important for future defence capabilities as in Command, Control, Communication, and Intelligence (C3I). Innovations in information and communication technologies (ICT) are improving capabilities of collecting and distributing information. There is a view that defence systems integrated into networks have the potential to significantly improve the capabilities of armed forces and the efficiency of military operations. Therefore, there is a growing demand for integration of C3I systems, sensors and weapons (sometimes called 'shooters') into systems of systems. (Nye and Owens, 1996; Cebrowsi and Garstka, 1998; Alberts, et al, 2000; Owens, 2000)

The development of information technologies is expected to have far-reaching consequences for capabilities of defence systems and on how warfare is conducted. Such improvements may be both at the level of individual systems – such as integrated platforms – and at superordinate levels due to the capacity to share information and communicate in a network. It is the latter that is referred to as system of systems or, more or less alternatively, Network Centric Warfare (NCW). Network Centric Warfare has been defined as *'an information superiority-enabled concept of operations that generates increased combat power by networking 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-synchronisation'* (Alberts, et al., 2000, p 2).

There is no commonly accepted definition of system of systems. In this report, a system of systems is understood as *'a set of different systems so connected or related as to produce results unachievable by the individual systems alone*' (Krygiel, 1999, p 33). Of course, according to this definition a combat force in the 17th century consisting of infantry, cavalry and artillery could count as a system of systems. The interwar development of new combat systems, e.g., mechanised warfare and air defence, meant that system of systems integration became a much more complex and abstract undertaking, which is exemplified by the major role played by civilian scientists in the UK air defence case (e.g. Burns and Stalker, 1994). In these and other 20th century cases, system of systems integration was very much about finding the 'right' package of operations concept, technology, training etc. and then retaining it with only minor adjustments until the advent of some significantly new piece of equipment requiring a period of equally radical innovation.

To proponents of the traditional RMA school, the situation today should not be that different from the 20th century cases. Owens (2000, pp 98-102) argues for 'the' system of systems comprising dominant battlespace knowledge, immediate/complete battle assessment, and near-perfect mission assignment. From this point of view it seems likely that, just as for air defence or mechanised warfare – or for the car as a mobility or lifestyle concept (cf. below) – the truly fundamental system of systems integration should happen in an early, formative period leaving us locked-in with a dominant design for the foreseeable future.

The RSA school, in contrast, tends to see system of system integration as a much more continuous process where old and new sensors, decision-makers and shooters are combined in ever new ways to achieve new types of objectives coupled to new types of conflict, adversarial behaviour, etc. This network-oriented notion of a system of systems is that one system – or component – should be able to tactically interact in combination with a great variety of other systems and components based on the task at hand and the availability of other assets. In the most visionary network-centric views, platforms are reduced to commodities carrying different ad hoc combinations of components for seeing, telling, and acting.

The important role of commercial technologies

Even though the Internet in its origin was a defence-funded project, the rapid development during the last decade or so has been driven by commercial sector companies and by non-profit-seeking individuals – organised around computer networks. Innovations in the ICT sector are often initially developed by small start-up companies. The IT industry has the shape of a network of smaller and larger companies and individuals who collaborate and compete depending on what capabilities are needed for a certain project. Characteristically, technology life cycles are short and it is therefore a challenge to take advantage of any innovations in advance of competitors.

It is recognised within the defence establishment in the US as well as in other countries that these developments bring the consequence that potential adversaries could have access to the same technology and thus the same potential technological capabilities as the US. Consequently, it is increasingly difficult to predict what military capabilities other states might have (DSB, 1999, pp 8-9; DoD, 2001, pp 6-7).

Obviously, this is not uniquely a US condition. In Sweden the recent Defence Bill (MoD. 2001/02:10) recognises the difficulties of predicting technological developments and consequently the rise of new potential threats. Therefore, as a consequence of the globalisation of commercial technologies with potential military use, no country or company could expect to have an assured long term defence technological advantage. Instead, the capability to develop military applications from commercial technologies is considered as essential to remaining on the cutting edge of defence solutions. (DSB, 1999; Axelson and James, 2000)

4 Conflicting perspectives on network oriented defence acquisition

Interviewing industry and defence establishments about the industrial ramifications of Network Centric Warfare (Cebrowski and Garstka, 1998; Alberts et al., 2000) turned out to be an interesting, but sometimes frustrating, experience. We believed this US DoD sponsored concept to be an internationally well-known version of new network oriented defence and security thinking, but found a range of responses hardly consistent with this view.[5] Briefly there were three groups of respondents:

1. those unfamiliar with the concept of NCW;
2. those demonstrating an understanding of NCW rather different from the one we started with and more akin to traditional RMA; and
3. those understanding NCW roughly the way we did.

Interestingly enough, the third group was the smallest. It did, however, include the two offices we visited in the Pentagon along with some other key actors. Therefore, a simple misunderstanding of NCW on our part is not a credible explanation of this outcome. Instead we believe these mixed perceptions to be very informative and, at least partially, possible to analyse based on the interviews and the literature review.

Further, we found no dramatic difference between most adherents of group 1 and group 2. In some countries like the US and UK, not to mention Sweden, NCW is a well-publicised concept; in Germany and France this does not seem to be the case. When, for the benefit of group 1 we reformulated our questions in terms of commercially driven ICT developments and C3I systems more generally, their responses tended to be akin to those of group 2. In some cases, in fact, there were considerable similarities to group 3. Thus familiarity with network centric terminology is neither a guarantee nor a necessity for adhering to this type of thinking.

In what follows we will refer to group 2 as *'reformists'* and group 3 as '*revolutionaries'*. As discussed above group 1 are typically reformists, although in some cases with significant 'revolutionary' traits. This also exemplifies the obvious fact that there are many positions in between the two ideal types we have chosen to develop.

[5] One major explanation for our mistake is that in the Swedish defence debate of the last couple of years, network oriented terminology – e.g. network centric, network based – has almost replaced RMA.

	View on changing security affairs	View on innovation	View on industrial base
Reformists	RMA • Focus on the impact of technology	Quantitative • Focus on faster cheaper, better etc. of established products	Tier structure • Traditional defence contractors • IT firms as subcontractors
Revolutionaries	RSA • Focus on the interaction between technology and societal change	Qualitative • Novel combinations • Technology and business models co-evolve	Industrial Networks • Collaboration in networks • Focus on non-traditional defence firms, e.g. innovative SMEs

Figure 1. Perspectives of 'Reformists' and 'Revolutionaries'. The matrix illustrates the different points of view of reformists and revolutionaries.

A key difference between 'revolutionaries' and 'reformists' is that the latter group stresses the role of established defence prime contractors in harnessing commercial ICT developments. This group tends to be quite negative with regard to the ability of governments to develop direct links with these technological and business 'new frontiers'. In line with this, the 'reformists' tend to see *outsourcing* and the like as a useful business model, even deep into what would traditionally be regarded as defence core competencies – one case in point could be the project Deepwater, cf. below. The 'revolutionaries' take, in fact, a more conservative position with regard to outsourcing, restricting it to non-core activities.

When it comes to the relationship between systems developers and war-fighters the 'revolutionaries' argue that a *co-evolutionary development model*, simultaneously involving operational concepts, materiel, training etc. is necessary to effectively harness the power of commercial ICT developments. This in turn requires experimentation where suppliers and users work closely together. In this co-evolutionary work the 'revolutionaries' typically stress the role of innovative Small and Medium-Sized Enterprises in contrast to traditional defence primes. How to set up this co-operation in commercial terms is no easy question. In particular the 'reformists' stress these difficulties and argue that the practical way to do it is via a prime contractor or outsourcing agent. Of course some degree of experimentation involving the end user may also be included in the outsourcing and prime contractor business models advocated by this group. In such an arrangement, however, it is an activity auxiliary to, and building on, a preceding linear, requirements-driven development process.

We provide our interpretation of these key disagreements on *business and development model* in the subsequent chapter, qualitative vs. quantitative innovation.

A third area where 'reformists' and 'revolutionaries' tend to disagree is what sectors of war fighting are likely to be affected by network orientation. According to 'reformists' network orientation should primarily be expected in traditionally high-tech areas. For example, one respondent suggested Ballistic Missile Defence (BMD) as the best example of a network centric concept. ‘Revolutionaries’ in contrast stress the usefulness of network centricity across the conflict spectrum – without having to predefine systemic and organisational settings as is the case with e.g. BMD, and not least in Peace Support Operations, asymmetric conflicts, etc. (Alberts et al., 2000).

The latest two areas of disagreement suggest that there are significant links between taking an RSA position in the general RMA debate, and thus stressing both *task and technological uncertainties*, and being a ‘revolutionary’ with regard to development of network centric solutions. Conversely, an adherent of traditional RMA is likely to see the building of dominant battlespace knowledge or global reach, global power systems as possible to manage on a requirements-driven basis, these tasks being of a relatively stable nature. Hence, according to this school of thought, the only significant uncertainty to manage is the technological one.

5 Qualitative vs. quantitative innovation

As mentioned in the previous chapter, for group 3 – the 'revolutionaries' – continuous experimentation pursued by the defence organisation itself in cooperation with a wide array of suppliers, including innovative Small and Medium-Sized Enterprises, is key to the successful exploitation of ICT developments for defence. The 'reformists', in contrast, tend to argue for long-range outsourcing arrangements whereby a supplier – typically a consortium – takes care of this exploitation on behalf of the defence organisation. Obviously this requires the defence organisation to specify its requirements and to agree with the contractor on metrics for measuring performance.

As suggested in the previous section, this is indicative of a very interesting contention as to how deep an impact on conflict and warfare is expected from modern ICTs and related institutional and cultural changes – i.e., from the emerging Network Economy, the Third Industrial Revolution or whatever label is chosen (Eriksson, 1999; and 2001).

The network economy and national security

What basically everybody agrees on is that, increasingly, successful defence solutions require effective and efficient exploitation of commercial ICT developments. This is a result of a general network economy feature, viz. increased importance of generic technologies. In the traditional industrial economy, generic technologies existed primarily at the bottom of the value chain, e.g., in materials processing. Higher-level solutions were typically sector specific. Industrially, this corresponded to vertically integrated firms, striving to keep all technologies that were not of a commodity nature in-house. This situation was broken up by what has been termed 'Wintelism' (From *Win*dows and In*tel*; Borrus and Zysman, 1997). Here 'horizontally integrated' generic solution suppliers managed to create strong economies of scale and scope by aggressively marketing their solutions to all domains of application. Particularly when they succeeded in entering (or co-creating) mass consumer markets such as PC's, this led to an incredibly rapid growth in performance-to-price ratios compared to the previous situation where the corresponding technologies were locked-in by high-level systems integrators (prime contractors or commercial OEM suppliers). Of course, 'Moore's law' for integrated circuit performance is the most famous example of this new business logic.

These developments constitute a formidable challenge to traditional public sector business practices, e.g., in defence, where the emphasis has been on cooperating with – and controlling – vertically integrated suppliers. As networks of horizontally integrated suppliers catering to the needs of many types of users become more effective in creating value than dedicated vertical hierarchies, public sector organisations, with legal and administrative restrictions hindering effective use of networks, face a dilemma. In the case of defence this could have serious impact if other, perhaps non-state, actors turned out to be better than the Western democracies at harnessing the network economy for purposes of waging conflict – of course taking account of the pertinent, situation-specific asymmetric success criteria.

Innovation in the network economy

The difference between 'revolutionaries' and 'reformists' can be understood based on the classical dichotomy *product vs. process innovation* and, in particular, the related dichotomy *qualitative vs. quantitative innovation*. What we mean by a qualitative innovation is an artefact or a service offering that combines features in a non-trivially novel way (this, of course, includes the case of completely new features). A quantitative innovation, in contrast, is an already established combination of features achieved at a better performance-to-price ratio. This means that a classical process innovation – a new way of making an existing product – and an incremental product innovation are quantitative innovations whereas a radical product innovation is a qualitative innovation.

According to innovation research, radically new products typically require clusters of related innovations such as new service offerings and business models (among others see Utterback, 1994). The car – supported by sales outlets, repair shops, fuelling infrastructure, driving schools, financing and insurance schemes, etc. – is a classic case in point. The interesting qualitative innovation is this entire 'mobility concept', co-evolving with an even broader 'lifestyle concept' including suburban living, commuting to work, leisure activities requiring car, etc. – i.e. systemic innovation.

In the military domain, the development of mechanised and air warfare in the interwar years provides good arguments for the position that it is the complete package rather than the new product itself that counts. For example, France had more, and in most ways better, tanks than Germany in 1940, yet it was Germany that conquered France with its package of operational concept, equipment, and training (see e.g. Posen, 1984).

We see from the examples above that a major product innovation is typically only one part of a major qualitative innovation. It is also possible to conceive of qualitative innovations that are not centred on a single major product innovation, but rather on a novel concept supported by a multitude of largely pre-existing products and services brought together in a novel way. This type of *combinatorial innovation* is particularly relevant in a network economy setting with the economy-wide interoperability ascertained by the de facto standards induced by 'Wintelist' firms operating as suppliers to all sectors of society.

Therefore, the network economy has great scope for qualitative innovation. Also, there is evidence that qualitative innovation, in order to be effectively pursued, requires intense dialogue between users and suppliers (von Hippel, 1988). Typically experimentation based on e.g. demonstrators is a key forum for such dialogue. In this type of setting, a requirements-driven development process is not effective. Instead technology push and demand pull must interact closely and continuously, i.e. supplier and customer have to interact constantly (Abernathy and Chakravarthy, 1979).

Military innovation in the network economy

The dichotomy *co-evolutionary vs. requirements-driven development* model is where we see the main divide between 'reformists' and 'revolutionaries'. The latter school very much stresses experimentation and the need for military users and advanced technology suppliers to come together around such activities.

The 'reformists', on the other hand, seem to take a position that could be summarised as: 'my supplier's qualitative innovation will only have quantitative consequences for me'. This is often a perfectly correct point. For example, going from steel to plastic requires qualitative changes in the production process, while from a user perspective it may be a perfectly quantitative matter, say same function at lower cost and weight.

In the network centric setting, the typical 'reformist' position is that defence organisations, with all their rigidity and inertia, cannot be expected to become high performing innovators themselves. Instead innovation should be outsourced to suppliers operating under long-term contract with some type of performance clauses. But for this to make sense from the user perspective, innovation must be seen as quantitative – measurable in money and capacity terms.

The 'revolutionary' counter-argument to this is that if established defence organisations fail to build the institutional infrastructure, to continuously develop innovative capability packages, they are likely to fall prey to non-conventional actors who exploit the innovation potential of the network economy better.

Evolutionary development

It is widely recognised that the complexity of networked defence systems requires an evolutionary approach to development. In fact, such a development approach is considered increasingly necessary for most – if not all – defence materiel areas. Thus the companies in the market of developing capabilities for network centric defence systems are increasingly asked to conduct step-wise developments. Demonstrators and other experimentation sites are identified by many as key tools for accomplishing this.

There is, however, a significant difference between 'revolutionary' and 'reformist' evolutionary development. To an ideal-typical 'reformist', tasks are not particularly uncertain, thus allowing performance specifications to be formulated. The role of the evolutionary development process is then to manage the technological uncertainties stemming from the fact that commercial forces today drive important technologies for any major defence system. This means that it is no longer meaningful to specify in detail how a new defence system should be designed, instead systems should be specified in terms of performance. Thus system developers are allowed to make use of the technological solutions developed by the commercial sector, which turn out to be the most favourable for achieving the requested performance.[6]

However, according to the 'revolutionaries' – or perhaps more correctly the RSA adherents, technology is not the only uncertain domain with regard to defence systems. Also task uncertainty is claimed to increase through the combination of the general post cold war security environment and the general availability of commercial technologies – also to potential adversaries. Thus technological uncertainty adds to task uncertainty via the technological and organisational solutions chosen by potential future opponents. Future demands from defence customers are, therefore, difficult to predict. In order to allow continual change to keep up with new technological developments and changing tasks, it is necessary to develop new defence solutions – largely based on existing systems – in an evolutionary fashion.

In particular the 'revolutionary' stance with regard to evolutionary development should have fundamental impact on the strategies of companies developing and manufacturing defence materiel. As technologies become generic, competition between corporations tends to move from developing and distributing products to *innovation of unique customised solutions*. This means that the ability to design innovative solutions for customers' specific needs becomes the crucial competitive advantage. This requires the capability of finding and using new technologies and knowledge of how to integrate them with other, pre-existing technologies. One consequence of this is that defence companies are facing the challenge of responding to the rapid cycle time of commercial technologies.[7] This is due to the complexity and pace of change within these commercial technology areas, which make it too expensive for defence companies to develop the bulk of relevant military technologies in-house (Hayward, 2000, pp 119-122). This diffusion of military technology is blurring the border between defence companies and commercial sector firms. How these roles develop should have significant impact on the potential of new defence systems and system of systems.

Conclusion

We began this project pretty much from a 'revolutionary' standpoint and assumed this view to be much more common than we subsequently found. We still believe the 'revolutionary' argument to be very strong indeed, but the dominance of requirement-oriented 'reformist' thinking is an important fact of life to be respected in all defence modernisation efforts.

[6] Some distinguish between evolutionary development (striving to manage technological *and* task uncertainty) and incremental development (striving to manage technological *but not* task uncertainty). Using this terminology the 'reformists' acknowledge the need for incremental but not evolutionary development.

[7] Cycle time refers to the speed of product development and organisational change, which, in many industries, is speeding up. Of course, there are differences in the cycle time between industry segments, for example, the lifetime of a fighter aircraft is several decades, while electronics and software have lifetimes of only a few years. (See Fine, 1998)

6 Developments towards network centric defence by country

This chapter presents findings about development towards network centric defence in each of the countries studied i.e. US, France, Germany, UK and Sweden. The presented picture is an aggregated view of the authors' impressions from each country. It does not claim to cover all relevant aspects or capture all the interconnected processes involved. Nevertheless this chapter could help to give the reader a bird's eye view of current developments towards network centric defence. Most of the information in this chapter is repeated in the following, which is organised by theme. Also, the discussions provided in the thematic chapter go deeper into the subject matter.

United States

The US was the initiator of the concepts of network centric warfare and is ahead of all the other countries in implementing these visions. Several programmes are underway, e.g. the concept and technology development of the Future Combat Systems Programme (FCS). This programme is lead by Boeing and Science Applications International Corp. (SAIC). Another example is the Coast Guard Deepwater programme. The industry involved in the US network centric warfare programmes are chiefly the traditional US based defence contractors such as Boeing, Lockheed Martin, Northrop Grumman and Raytheon. However, commercial firms within the IT sector such as Sun Microsystems are also showing considerable interest in this evolving field.[8]

The US is dedicated to taking military advantage of advancements in the ICT area. In strategy documents such as Joint Vision 2010, Joint Vision 2020 and the Quadrennial Defense Review Report (QDR) from 2001 there is a clear focus on moving on with the creation of a networked defence. Nevertheless, there is widespread frustration within the defence administration and the defence industry concerning the fact that the process of transforming cold war defence is going too slowly. Defence bureaucracy and the lack of coordination between the services inherent in the US politico-military system are strong inhibitors to implementation of a new defence system. There are also different views on how to move forward. These differences partly correspond to the 'reformist' vs. 'revolutionary' positions outlined in the report.

[8] It should be noted that our US interviews were conducted prior to September 11, 2001. Thus the effects of increasing defence expenditure in the wake of the War Against Terrorism have not been caught by our study.

France

Within both government and industry in France, it is believed that the development of ICT will transform defence. The industry – in particular Thales and EADS are active in this field – is involved in demonstrator programmes with the Air Force and the Navy with the purpose of taking advantage of commercial ICT development. Currently there is a program on developing a network centric command and control system for the French Air Force. The programme, which is lead by EADS, goes under the name SCCOA. There seems to be openness to collaboration with commercial companies – both within the government and the defence industry – and it is emphasised that no company could develop suitable networked systems by themselves. Close collaboration between the armed forces and the industry is considered necessary in this development process. Overall, the French development of networked defence systems uses a bottom up approach i.e. focus is on integration at the tactical level rather than designing new network concepts for the entire force.

Germany

Germany is beginning to take advantage of the development of commercial ICT innovations in their defence forces. This is emphasised by the establishment of an IT directorate within the MoD. The purpose is to co-ordinate and lead the development of new ICT based systems. Overall, the current aim is to develop modern information and communications systems and also to focus on issues of IT security. Germany has launched a number of so-called pilot projects aimed at developing and testing a wide range of potential solutions in areas such as IT security and interoperability. Currently, there is a prototype programme to develop a new strategic level C3I system for the Bundeswehr. We found no parallel work network systems of systems programmes for tactical, i.e. real time, systems. However, the ambition is to create interfaces between strategic systems and tactical systems. The industries involved in German activities related to ICT exploitation are for example EADS, ESG and the US owned firm Computer Science Corporations (CSC) as well as Deutsche Telecom.

United Kingdom

The armed forces of the UK are being transformed with the intention of developing enhanced capability in intelligence, surveillance, target acquisition and reconnaissance (ISTAR). At the centre of this endeavour is development of improved command, control and communication capabilities (C3). Thus it seems the UK intention is to transform in the direction of network centric defence capabilities. The UK approach includes the Joint Battlespace Digitisation initiative (JBD), which aims to integrate operational information systems across the land, sea and air environments to enhance military capability in joint operations. To accomplish this, considerable investments are planned in programmes such as Cooperative Engagement Capability (CEC) and Integrated Ground-Based Air Defence (IGBAD). There is considerable concern within the UK government about the potentially considerable costs and technological risks in developing a network centric defence. In response, the UK is likely to pursue an incremental development focused on a limited number of selected areas. A number of companies are interested in, and to some extent involved in, UK efforts to develop network centric defence systems. The major programmes are lead by traditional defence contractors e.g. BAE Systems, Thales and Raytheon. However, due to complexity of these programmes no one company could manage all their aspects. Thus, teaming with other firms, both defence and commercial, is considered necessary to accomplish the assignments involved in developing network centric systems. (James, forthcoming)

Sweden

The Swedish defence is under transformation from a cold war force designed to meet a major Soviet invasion to a flexible, network centric defence for a wide range of tasks. The current focus of this transformation is the development of a network based command and control system – the Ledsyst. From an industry perspective most attention is paid to the technological parts of the new system – labelled LedsystT. Currently the Ledsyst activities are geared to a demonstrator programme. Based on experience from this programme, the process of developing a networked based defence is expected to continue well into the next decade. The Swedish based defence contractors Saab, Ericsson Microwave Systems and Kockums are the main industrial actors involved during the first development phase of LedsystT. The forthcoming phases could, however, include also other firms.

7 New rules of engagement – changes in the defence industry in the wake of the information age

The following chapter presents findings from the interviews on industry aspects related to the development of network centric defence systems. Firstly, defence industry issues are addressed. Examples of new business models of defence procurement are presented in the second section. The third section contains aspects of international collaboration in development of network centric systems. The findings presented in here are from the studies in France, Germany, the UK and the US. There are few references to Swedish cases, however, and then related to early phase development of network centric defence systems, since few, if any, particular industry consequences could yet be observed.

Defence industry structure in change

Traditional defence companies are the prime contractors in current defence programmes on integration of Command, Control, Communication and Intelligence (C3I) systems. General Dynamics UK is leading the British BOWMAN programme, Raytheon has developed the CEC systems and Saab has lead in the first phase of the Swedish command and control programme LedsystT. However, no individual company has the wide range of capabilities necessary to successfully manage such advanced network integration programmes. This is being recognised by defence companies and there is a growing openness to collaboration. Therefore teams of companies are involved in most programmes in the field of advanced integration of C3I systems.

Managing the differences in cycle times between the IT sector and the defence industry is a major challenge for defence companies. Despite the examples of inter-industry collaboration, defence contractors – with the bulk of their revenues in platform systems – are often reluctant to change their business models in order to take full advantage of the potential of collaboration with non-defence companies. This is often referred to as a consequence of organisational and managerial conservatism and also a lack of incentives. The business models of the defence industry and defence procurement agencies are designed to manage major programmes lasting for several years and sometimes even several decades. With the increasing importance of commercial technologies, these business models between industry and government have to change in order to promote transparent collaboration with industries operating with short cycle periods. Such processes are underway, both in the US and Europe, but progress is often slow.

It is not surprising that traditional defence contractors are primes in the development of network centric defence systems as there are several obstacles to commercial sector companies wishing to enter the defence market. Defence acquisition polices are characterised by long lead times and cumbersome bureaucracy. Developing such systems requires defence specific knowledge and experience. This is considered to be the main barrier to entering the defence market and it is thus the major advantage enjoyed by the current defence companies. The security standards for defence materiel and requirements for documentation in development and production are major hurdles to entering the defence market. Furthermore, the appreciated size of the defence market is only a small fraction of what companies such as Sun Microsystems or Cisco see in their commercial sector markets. The combination of difficulties of entry and bleak opportunities to make considerable profits are often referred to as indications that IT and telecommunication companies are not likely to challenge defence companies in the market for defence specific applications and systems integration. This is also due to the fact that defence system requirements often are extremely specialised regarding security and survivability.

However, despite the often repeated difficulties of inciting leading commercial ICT firms to work for defence, we have come across numerous examples in our interviews. Companies such as Sun Microsystems, Cap Gemini and Cisco are, for example, providing technologies and services to the C3I area as well as network solutions. The French defence electronics company Thales has a number of commercial sector companies as partners in network integration projects. The French procurement authority DGA has found commercial sector companies very competent in developing demonstrators of new systems. Another example is the collaboration between Sun Microsystems and Raytheon, where Sun develops the system architecture and Raytheon is making the applications, for example user interfaces. In both Germany and the UK commercial companies are involved in the endeavours to create network centric systems. Such examples indicate that commercial sector companies are entering the defence market not only as suppliers of commodities but also as collaborative partners for both defence companies and government authorities.

As the increasing number of partnerships with traditional defence contractors implies, commercial sector companies are becoming established in niches as both suppliers and partners to defence companies. There is evidence that these developments will intensify not least because commercial sector firms are gaining experience in the defence market that could prove valuable in their core markets. It is argued by respondents that experience from system of systems integration for military customers will teach commercial firms lessons valuable for coping with the challenges they that are likely to face in the commercial sector in forthcoming years.

Naturally the new role of commercial firms is most pronounced in the least defence specific applications, typically communication other than at tactical level. However, even in the field of real time systems some respondents see scope for a new role-play between traditional defence companies and their commercial counterparts. Defence companies have long experience of developing real time systems in hard-wired settings. It is now being debated whether advancements within open systems should be applicable to systems with real time requirements. To date there are no open systems that could solve the real time issue but, for example, Sun Microsystems is working on this challenge. This is driven by the real time requirements of financial systems, which are creating incentives for developing open systems with real time capacity.

These findings show that the industry structure evolving to harness the advanced network centric defence systems market is in change. There is a strong dominance of traditional defence contractors, but commercial sector companies are entering the market. Nevertheless, networked defence systems are, by and large, still being developed within the traditional defence industry structures. This should indicate that innovation is likely to take place within established frames of thought and practice.

Emerging novel business models

The increasing importance of advanced IT based systems is beginning to impact on procurement models. This study came across several interesting cases where companies take on strategic roles in development and management of defence systems.

The German armed forces are in the process of developing a joint C3I system. The purpose of the new system is to achieve joint interoperability at the strategic level. In the process of acquiring this system, an evolutionary development approach with commercial competition is used. Initially, there were eight competing proposals, out of which three received an order to go ahead and develop a demonstrator. The German MoD and each consortium financed these demonstrators on a 50/50 basis. A consortium led by the German subsidiary of Computer Science Corporation (CSC) won the competition between the demonstrators. This consortium was then awarded the contract to develop a prototype C3I system. When this prototype is ready there will be a new round of competition in the development phase. It is also interesting that the winning consortium received access to knowledge and technology from the other two demonstrators.

In France the aerospace company Aérospatiale (now part of the EADS group) has since long been contracted to support the government in the development of C3I systems for the Air Force. To avoid a conflict of interest regarding the role of Aérospatiale, the company had no other commercial interests in the programme.[9] The roles played by company and government are close in the development of C3I systems and collaboration between the Air Force and EADS takes place on an experiment site located on a French air base, Mont-de-Marsan.

In Germany as well as in the UK, defence communication functions are being outsourced to commercial sector companies. In Germany the MoD is setting up a so-called IT company to run the armed forces' communications networks. Presently, two consortia are competing for partnership with the government in this IT company. One consortium consists of Siemens, IBM and Deutsche Telecom, the other of CSC, EADS and Mobilecom.

[9] Aérospatiale now being part of EADS means that this role-play does not hold anymore, a pre-EADS contract is, however, still in force.

In the US, the business model of the Deepwater project is an interesting case. The Coast Guard is planning to outsource, among other things, the development of its C3I system. The main reason for doing this is perceived lack of competence within the Coast Guard to lead such system integration. The three contenders for the project are a Lockheed Martin led team, a Boeing led team and a SAIC led team. The winning consortium would be responsible for both the development and maintenance of the system over a 5-year period – then the contract could be renegotiated. One interesting issue is, of course, how good mechanisms can be designed to allow the transfer of this contract to another supplier at a later date. The overall duration of project Deepwater is planned for at least 20 years, but even after that, in all likelihood there would be a considerable legacy.[10]

In terms of quantitative and qualitative innovation the development of information systems discussed here provides examples of both approaches. Based on a long-term contract with limited customer participation in development activities, the Deepwater project seems predicated on far-reaching assumptions as to the possibility of specifying necessary Coast Guard activities well in advance, i.e. a quantitative approach. The role of the German IT Company is also an example of a quantitative approach to development. A qualitative approach, on the other hand, would include continuing experimentation to exploit new opportunities in order to create new novel functionalities. The German C3I programme, in contrast, is embracing more of a qualitative approach with step-wise development and integration of knowledge and technologies from the different demonstrators. The C3I system development in close collaboration between the French Air Force and EADS indicates a qualitative innovation strategy. In the US, qualitatively oriented force experimentation is conducted at a significant scale.

International collaboration in network centric defence programmes

The findings of this study indicate that programmes related to defence network integration tend to be relatively nationally bound. Yet there are several examples of foreign defence contracts being invited and playing significant roles. The differences between countries in this regard reflect general differences to what extent they allow the entrance of foreign defence contractors. In the present climate of international integration of defence companies and collaboration on multinational defence programmes, integration within the field of networked systems is expected to increase. Not least the call for interoperability is expected to be a driving force for pursuing international collaboration.

As previously mentioned, the US owned corporation General Dynamics UK is leading the UK's BOWMAN project. One Raytheon and one Lockheed Martin team are competing for the British CEC system order. In Germany the US owned Computer Science Corporation won the competition for a prototype of a new C3I system for the German defence forces. Ultimately, the issue of whether foreign based defence contractors could be trusted

[10] This contract has now been awarded: 'On June 25, 2002, U.S. Deputy Secretary of Transportation Michael Jackson, joined by U.S. Coast Guard Commandant Thomas H. Collins announced the award of the largest acquisition in the history of the Coast Guard. The Integrated Deepwater System (IDS) contract valued at approximately $17 billion was awarded to Integrated Coast Guard Systems (ICGS), a joint venture established by Lockheed Martin and Northrop Grumman.' See www.uscg.mil/Deepwater/Welcome.htm.

to influence system of systems will, of course, depend on the general policy climate regarding defence industry and materiel. In the UK, strong bonds with the US are reflected by the acquisition of the CEC system. The creation of EADS means that competencies from Germany and France[11] are co-ordinated in e.g. the French Air Force C3I programme. Obviously, if the consolidation of the defence industry continues there will only be a handful traditional defence contractors left possessing substantial capability for system of systems integration. Then relying on foreign-based defence contractors should be expected to become increasingly common.

Political processes to reform the defence materiel market are underway and this will have great impact on international defence industry and defence materiel collaboration. The current situation with the Framework Agreement between the six leading defence industry countries in Europe is one such process. Another is the ongoing Defence Trade and Security Initiative (DTSI) and Declaration of Principles (DoP) with the purpose of liberalising bilateral defence materiel regulations between some European (and other) countries and the US. Respondents considered these processes as indicators that international collaboration related to system of systems is likely to intensify. Furthermore, integration of defence systems into a network could be rather expensive and few – if any – countries would wish to bear the financial burden by themselves. It is also likely that a vast part of system of systems integration would be included in various defence materiel programmes where international participation is already becoming common.

As long as the capability of accomplishing coalition operations remains a political goal, industry collaboration could be valuable in order to improve efficiency of interoperability creation. From that perspective, both industry collaboration and interoperability per se would benefit from a common international architecture for system of systems. It remains to be seen whether there would be enough political commitment to make such a standard real.

[11] Spain is, of course, also a partner in EADS, but less visible in C3I activities.

8 General conclusions

The findings presented in this report show that the defence market for network centric solutions is indeed under evolution – the defence industry structure of today might be challenged tomorrow. It will, however, take time before the industry structures for networked defence systems integration are well established. Given this and based on the observed roles played by the actors entering this evolving market niche, what conclusions can be drawn? After exploring drivers and barriers to change we turn to the three research questions posed at the outset.

Drivers of change

It appears that the development of the business practices of procurement agencies will shape how the industry evolves to the greatest degree. The business practices are likely to reflect the fact that no country should be expected to be willing to bear the financial burdens of having all the necessary competencies domestically. Furthermore, improving the capability of managing coalition warfare should be a driving force behind the development of international standards for the architecture of system of systems. At present, however, there are few international partnerships in network integration projects. Overall, the domination of national defence contractors is still the main feature. This is due to traditions of supporting the domestic defence industry and reluctance within companies to pursue international integration. However, internationalisation of the defence industry is underway. As a consequence there might be increased international collaboration in the development of network centric defence solutions. In addition, there are examples from Germany and the UK that indicate some modification of traditional acquisition practices with their strong bias towards favouring domestic companies.

There is a growing importance of, and use of, commercial technologies as the creation of networked defence systems evolves. The roles played by traditional defence contractors and newcomers from the commercial sector are characterised by combinations of competition and collaboration – not head-on competition.Since competition for programmes takes place between teams of several companies, partners in one competition are competitors in another – an example of so called co-opetition, often cited as a key feature of the network economy. Traditional defence contractors are often the prime contractors for programmes on networking defence systems into an integrated system of systems. In addition, they develop products and services in areas where defence domain knowledge is considered crucial. However, exactly what these areas are could change over time and commercial companies could learn the requirements of the defence market – which is a natural consequence of collaboration in consortia.

Towards a new industrial landscape?

The new feature emerging in the market for integrated system of systems is the changing industrial relationship between primes and partners and suppliers concerned with developing new defence solutions. It is the network of different companies – both defence and commercial sector firms – that forms the competence base necessary to create the technological prerequisites for networked defence forces. As a consequence, the rules of engagement are changing for traditional defence contractors.

Current trends, even though embryonic, indicate that commercial sector companies will, in all likelihood, dominate component and network technologies at the general infrastructure level. In addition, commercial sector companies could be expected to be able to provide services based on Internet-based commercial services e.g. in logistics. Furthermore, integration of information system of systems and to some extent sensor system of systems are possible niches for commercial sector companies. These areas do not require the same domain knowledge as sensors to shooters integration and they are built extensively on commercial technologies and systems. Integration of the three system levels – information systems, sensors, and weapons and platforms – would, based on the present situation, seem likely to remain a unique defence industry competence due to the required defence domain experience and knowledge of weapons systems.

But must the domain knowledge, alluded to in the previous paragraph, reside within an integrated prime contractor firm? Arguably, in a network economy setting, small and medium sized companies with defence domain expertise and capability of co-ordinating networks of commercial sector firms could be able to bring together competencies for integration of the entire range of defence systems. Companies working with such an approach would basically use qualitative innovation as their business idea. Thus they would exploit disruptive technologies to develop innovative military applications by being flexible in adapting new technologies and in reconfiguring organisational skills and resources. The entrance of such new actors to the defence systems market could seriously challenge traditional defence contractors. First, the defence companies' advantage of domain knowledge would vanish. Secondly, this would happen as their difficulties in embracing the potential of ICT developments are being exploited by the newcomers' efficient use of disruptive technologies.

Reluctance to change

While collaboration in networks is certainly viewed as important – even if the actual implementation of network strategies is proceeding slowly – there are few signs of appreciation of the type of implications outlined in the previous section. Commonly there is a notion that the solutions developed for network centric defence systems are a minor development on how previous defence solutions were designed and constructed, i.e. a quantitative view on innovation. As discussed above, this is likely to be an understatement of the potential impact innovations in ICT might have on defence systems.

Established defence companies have few incentives to change their way of working unless their customers, governments, are willing to support and ultimately finance new endeavours. If newcomers are successful in challenging traditional defence firms, this in itself creates incentives for change. But obviously this to requires action on the governments' part.

New business model to harness innovation

In this section we address the first two, intertwined research questions:

- What business models should defence organisations adopt to exploit the potential of ICT (Information and Communication Technologies) developments – in particular for network centric defence solutions?
- Given the leading role of civil firms in cutting edge ICT, how should defence organisations tap the competencies of leading commercial sector suppliers?

We have found two main candidate business models for dealing with the fact that crucial technology innovation takes place in a global market and within other industries than defence.

The first one is relevant primarily for situations of quantitative innovation where it is conceivable for government to define relevant requirements and metrics such that a performance contract can be agreed with the suppliers. In sectors where new services are innovated in a routinised fashion, e.g., telecom, such a performance contract could also deal to some extent with qualitative innovation through benchmarking with best industry practice. Such outsourcing arrangements mean that the task of transforming business models so as to harness the innovation potential in the commercial sector is delegated to the prime contractors. Yet there are considerable challenges also for the outsourcer. In addition to getting performance requirements and metrics right, their business model must also allow a substitution of incumbent contractors falling short of contractual obligations or losing out in the bidding for a subsequent period. This complex of problems was not in focus for the present study. Nevertheless, it is applicable for a wide domain of non-core organisational tasks.

When it comes to qualitative innovation, however, we contend that the outsourcing business model is not adequate. Here it is key that the business relationships between government and industry should be able to cope with the fact that not all potential problems facing modern defence forces are possible to foresee and that the potential of new innovations is difficult to predict (task and technological uncertainty, respectively). This can be accomplished if defence forces develop operational concepts through experimentation in close collaboration with industry based on demonstrators. Here government itself must take an active part in managing the interface with new types of suppliers. Governments need to use their bargaining power as customers and create financial incentives as well as a demand structure that helps defence companies pursue network-oriented business strategies. This could include business models that allow firms to make reasonable profits on developing continuous flows of ideas and demonstrations of alternative solutions to problems, either currently experienced by states or possible in the future. Failing to embrace the potential of qualitative innovation poses a threat not only to companies that may lose their competitive advantages, but also to governments who risk not possessing sufficient capabilities to meet potential threats derived from novel use of commercial technologies on adversaries' side.

International cooperation in network centric defence

The third research question read:

- What scope is there for international cooperation in network centric defence solutions?

We found above that such cooperation is relatively limited in scope. However, we also found that the case for international cooperation is quite strong. One key problem is that also countries differ considerably with respect to the financial resources they can invest in network based defence. Therefore, interoperability requires a 'scalable' architecture such that less resourceful countries are able to make their full contribution in coalition operations rather than being effectively excluded due to lack of network interoperability. Adhering to generic industry standards as far as possible is a key methodology for achieving this.

9 Implications for the Swedish government

Arguably we live in a revolutionary era. Sweden is embracing this revolution – whether it is labelled RMA, NCW or NBF. In the forthcoming years Sweden will develop its first demonstrators on the road towards a network centric defence. This should be interesting to many other countries. In the Swedish debate it is often stated that European defence industries lag behind as concerns NCW. These views were aired by several of our Swedish respondents. In fact, this study shows that this is not quite true. There are still good reasons for Trans-Atlantic – in addition to European – cooperation, but lack of competent European partners when it comes to harnessing modern ICT for defence is not one.

In the US, both conceptual development and practical improvements of network centric systems is taking place. Collaborating with the US on the development of network centric defence solutions is crucial in order to keep up with rapid developments. However, developments in Europe should also be followed closely. European countries may lag behind the US – and perhaps Sweden – in the development of conceptual thinking about the impact of ICT in the defence context. But this does not necessarily mean that European countries lag behind Sweden in actually developing networked systems. In fact, the findings from this study indicate that France and UK are ahead of Sweden in developing and fielding networked systems and using evolutionary development strategies. Also Germany can present highly relevant case experience. When it comes to outsourcing and the like, all studied countries have useful lessons to teach Sweden.

Our European study was confined to the three major countries in addition to Sweden. The argument on 'scalability' of network architecture developed above indicates that also technologically advanced countries of more comparable size to Sweden might constitute useful partners.

Collaboration with European partners should reduce the risk of re-inventing the wheel and serve as a benchmark for the capabilities developed in Sweden. In addition, this would benchmark competencies within the defence industry in Sweden in areas relevant to the development of a network centric defence. This would be valuable in the process of developing niches of competitive advantage for defence relevant industry in Sweden. However, it is crucial to consider that the semantics may be different. People who barely know the term network centric warfare could, in fact, be in charge of advanced network integration. In sum, both the Swedish government and the defence industry in Sweden would benefit from collaboration within Europe. This said, collaboration with US – both bilateral and multilateral – remains important since no country or group of countries will be able to match the capabilities developed there.

Therefore, we propose that the Swedish government should:

- Apply a qualitative approach to innovation of network centric defence capabilities, including experimentation with a broad range of solutions.
- Collaborate with a wide range of commercial suppliers to take advantage of the rapid development in commercial ICT. This could entail:
  - inviting commercial sector companies to participate in the development of demonstrators.
  - using its bargaining power as customer to increase collaboration between traditional defence suppliers and commercial sector companies.
  - beginning to actively place orders with a large number of mainly small commercial sector companies in order to create an environment for innovative military use of ICT developments.
  - studying, which, if any, activities related to the operation of network solutions, could be outsourced.
- Consider how collaboration with other European countries and European defence industry could be developed for mutual learning from ongoing system of systems programmes.
- Strive for large-scale partnerships with European countries and between the defence industry in Sweden and its European counterparts in the development of a network centric defence. This could entail:
  - taking initiatives to create a common architecture – based on commercial standards – for C3I systems in Europe.
  - striving for partnerships in areas where the defence industry in Sweden could develop a competitive advantage.
- Strive for close collaboration between US defence contractors and niches in the defence industry in Sweden in the development of a network centric defence. This could entail:
  - supporting the development of niches where the defence industry in Sweden possesses the potential to become valuable and preferred partners to US counterparts.
  - inviting US companies with interesting competencies, which complement those in Sweden, to participate in the development of, e.g., LedsystT.

List of acronyms

BMD	Ballistic Missile Defence
DGA	Délegation Géneral pour L´Armement
DoD	Department of Defence (US)
C3I (SR)	Command, Control, Communication, and Intelligence (Surveillance, Reconnaissance)
FCS	Future Combat Systems Programme
ICT	Information and Communication Technologies
IT	Information Technology
MoD	Ministry of Defence (GE, FR, SE, UK, etc.)
NBF	Nätverksbaserat försvar (Network Based Defence)
NCW	Network Centric Warfare
RMA	Revolution in Military Affairs
RSA	Revolution in Security Affairs
SME	Small and Medium-sized Enterprises

List of references

Alberts D. S., Garstka J. J., and Frederick P. S., (2000) *Network Centric Warfare: Developing and Leveraging Information Superiority*, Washington DC: DoD C3ISR Cooperative Research Program

Abernathy W.J., and Chakravarthy, W.J., (1979) Government Intervention and Innovation in Industry: A policy Framework, *Sloan Management Review*, 20(3)

Axelson M. and James A.D., (2000) The Defence Industry and Globalisation - Challenging Traditional Structures, FOA User Report, FOA Defence Research Establishment, Stockholm

Borrus, M., and Zysman, J., (1997) Globalisation with Borders: The Rise of Wintelism as the Future of Industrial Competition, *Industry and Innovation* 4 (2), December

Burns T., and Stalker, G.M., (1994) *Management of Innovation*, Oxford Univ. Press, Oxford

Cebrowski A. K., and Garstka, J. J., (1998) *Network-Centric Warfare: Its Origin and Future*, U.S. Naval Institute, Annapolis, MD.

DSB (Defense Science Board), (1999) Final Report of the Defense Science Board Task Force on Globalization and Security, December: Office of the Under Secretary of Defense for Acquisition and Technology: Washington DC.

DoD (Department of Defense, US), (2001) *Quadrennial Defense Review Report* (QDR)

Eriksson, E. A., (1999) Information Warfare: Hype or Reality? *The Nonproliferation Review* 6 (3), pp 57-64

_____,(2002) Who will harness the power of the network? Forthcoming in *Cambridge Review of International Affairs*

Fine, C.H., (1998) *Clock Speed, Winning Industry control in the Age of Temporary Advantages*. Perseus Books, Reading, Massachusetts

Hayward, K., (2000) The Globalisation of Defence Industries, *Survival* **42** (2) Summer

James, A (forthcoming) *The system-of-systems industry – UK case study,* FOI Swedish Defence Research Agency, Stockholm

Joint Vision 2010, Chairman of the Joint Chiefs of Staff, May 1997

Joint Vision 2020 Chairman of the Joint Chiefs of Staff, June 2000

Krygiel, A., (1999) *Behind the Wizards Curtain*, DoD C3ISR Cooperative Research Program,

MoD (Ministry of Defence, Sweden), Prop (*Bill) 2001/02:10*

Nye Jr, J.S., Owens, W., (1996) America's Information Edge, *Foreign Affairs* 75 (2)

O'Hanlon, M., (2000) *Technological Change and the Future of Warfare*, Brookings Institution Press, Washington, DC

Owens, W., (2000) *Lifting the Fog of War*, Farras, Straus and Ginoux, New York

Posen, B.R., (1984) *The Sources of Military Doctrine: France, Britain and Germany between the World Wars*, Cornell University Press

Utterback, J.D., (1994) *Managing the Dynamics of Innovation*, Harvard Business School Press, Boston

von Hippel, E., (1988) *The Sources of Innovation*, Oxford Univ. Press, New York

List of interviews

BAE Systems, UK

Boeing, US

Cap Gemini Ernest & Young, SE

Cisco, SE

Department of Defense, OSD, US

- AT&L
- C3I

DGA (Délegation Géneral pour L´Armement), FR

EADS (European Aeronautic Defence and Space Company), FR

ESG, DE

Ericsson, SE

Ericsson Microwave Systems, SE

FMV (Defence Materiel Administration), SE

FOI (Swedish Defence Research Agency)

IABG, DE

Ministry of Defence, UK

Ministry of Defence, DE

MITRE, US

Northrop Grumman, US

Raytheon, UK

Raytheon, US

Rheinmetall, DE

Saab AB, SE

SAIC (Science Application International Corporation), US

SEI (Systems Engineering Institute), US

Sun Microsystems, US

Thales communication, FR

Thales Racal, UK