REFLECTIONS ON INDUSTRY'S CONTRIBUTIONS TO SMART DEFENCE

Edited by Lisa Aronsson and John Louth

RUSI
www.rusi.org

Royal United Services Institute

OCCASIONAL PAPER

About the Report
This report explores industry's perspectives of Smart Defence in advance of the NATO Industry Day Conference in October 2012. The Royal United Services Institute (RUSI), Allied Command Transformation (ACT) and NATO Defence Investment Division hosted a workshop on this subject in March 2012, and five authors – Trevor Taylor, John Louth, Mike Maiden, Henrik Heidenkamp and Andrew D James – were asked to reflect on the findings of the workshop. The authors were tasked with examining industry's interests and the risks and opportunities associated with Smart Defence. They also considered the ways in which NATO might be able to improve engagement with industry and advance the Smart Defence Initiative.

RUSI would like to express its gratitude to Allied Command Transformation for supporting its efforts to reflect on these important questions, and to Cathy Haenlein and Ashlee Godwin of the RUSI Publications Team for their editorial support.

About RUSI
The Royal United Services Institute (RUSI) is an independent think tank engaged in cutting edge defence and security research. A unique institution, founded in 1831 by the Duke of Wellington, RUSI embodies nearly two centuries of forward thinking, free discussion and careful reflection on defence and security matters.

For more information, please visit: www.rusi.org

Occasional Paper, October 2012

Reflections on Industry's Contributions to Smart Defence

Edited by Lisa Aronsson and John Louth

www.rusi.org

The views expressed in this paper are the authors' own, and do not necessarily reflect those of RUSI or any other institutions with which the authors are associated.

Comments pertaining to this paper are invited and should be forwarded to:
Lisa Aronsson, Research Fellow, Transatlantic Studies, Royal United Services Institute, Whitehall, London, SW1A 2ET, United Kingdom, or via email to lisaa@rusi.org

Published in 2012 by the Royal United Services Institute for Defence and Security Studies.

About RUSI Publications

Director of Publications:	Adrian Johnson
Publications Manager:	Ashlee Godwin
Editorial Assistant:	Cathy Haenlein

Paper or electronic copies of this and other reports are available by contacting publications@rusi.org.

Printed in the UK by Stephen Austin and Sons Ltd.

Contents

Introduction

Lisa Aronsson

Smart Defence, and the initiatives associated with it, constitutes NATO's core strategy for developing and protecting Alliance defence posture and for supporting the industrial base in challenging economic and operational circumstances. It was introduced as a new mindset, set to transform the way NATO does business by promoting specialisation, prioritisation and most importantly for this study, multinational co-operation. In order for Smart Defence to be truly transformative, however, NATO needs to develop new models for engaging both its member states and the defence industry. Above all, it needs to become a 'smarter customer' by harmonising policy, planning processes and structures, by managing information flow among stakeholders, and by demonstrating leadership and effective management.

In advance of NATO's 2012 Industry Day Conference, the Royal United Services Institute commissioned five essays on the topic of the contribution of the defence industry to the implementation of Smart Defence. Each of the authors was asked to address one of five issue areas: first, NATO's interface with industry and opportunities available for rationalising points of contact; second, prospects for assessing and improving information flow between stakeholders; third, the business case and opportunities for industry associated with deeper engagement; fourth, industry's role in generating efficient multinational programme development; and fifth, industry's views on working with NATO and potential means of reducing the uncertainty and complexity associated with multinational programmes. The five papers overlapped in their emphasis on the need to establish clarity and confidence on the demand side, communicate opportunities for industry, and make enduring commitments to programmes with sustainable funding structures.

The authors highlight the numerous challenges that NATO, governments and industry must overcome in this regard. First and foremost, as Trevor Taylor argues, NATO must remember that it is a relatively small defence customer, and its consensual decision-making processes generate costs for industry in the form of uncertainties around intent, timeframes and funding structures. Taylor also argues that NATO must keep the multiple dimensions of defence spending in mind: governments need to balance the sensitive economic and military impacts of defence spending within their own borders and in Europe, particularly in light of current economic and political challenges. In addition to managing relationships among stakeholders, John Louth emphasises the importance of managing information flow at all stages of capability development. At the earliest stages, the Allies must begin to accept the principle of interdependence and real limits on sovereign decision-making.

This is essential if the Allies are to generate stable views of threats and a hierarchy among them, and in order for common requirements to develop.

The industrial landscape – or 'ecosystem' as it is described by John Louth – is also changing, and this has important implications for NATO and Smart Defence. Mike Maiden outlines the emerging landscape, and its changing role in providing the 'non-manpower elements of capability'. Traditional companies and major primes, Maiden notes, are still vitally important to NATO, but global IT companies, high-tech, communications companies and small, niche businesses are becoming increasingly significant, and are 'moving closer to the front line'. NATO can only expect to harness the potential of these companies by improving its coherence as a customer, simplifying its structures and generating confidence in its intent and in the sustainability of its financing. Industry, on the other hand, has its own role to play in integrating new business actors and providing smaller companies with a route to market. It is the visibility and clarity of business opportunities, Henrik Heidenkamp argues, or the existence of an 'addressable market', that can ensure industry is able to contribute to the implementation of Smart Defence. NATO must also find a way to penetrate national defence-planning processes, generate incentives and remove barriers to co-operation and, as Heidenkamp argues, elevate the defence industrial dimension in its discussions with national governments and with industry.

NATO, the nations and industry concur that multinational programmes offer the prospect of greater efficiencies. Andrew D James argues that there is 'little doubt' that NATO and its member states need to find ways to overcome cynicism and promote multinational development and procurement through refreshed structures and processes. NATO also has the potential, he argues, to learn from best practices and past experience. It can transform itself into an information hub, protecting the Alliance's knowledge base, capturing innovation and lessons learned, generating ideas for new business models, and coming up with metrics to measure the efficiencies associated with Smart Defence. The five authors all argue independently that NATO must become a 'smarter customer', by rationalising points of contact, managing information flow and offering clear business opportunities; and that industry will then, for commercial reasons, respond in support of Smart Defence.

NATO's Customer and Facilitator Roles in Defence Equipment Co-operation

Trevor Taylor

This paper argues that NATO has two roles relevant to its industrial relationships. In one it is a customer, seeking to procure goods and services which it uses to support its purposes and those of its members. In the other, it is a facilitator and a forum for discussion, helping governments to recognise that they could gain access to otherwise unaffordable capabilities by buying and operating them on a collective basis. As a customer, NATO has almost insurmountable limitations, but as a facilitator, its potential is much stronger.

In looking to improve its relationships with the defence industry, NATO needs to take account of the attributes of a 'good' defence customer and to assess itself in the light of the pertinent factors.

The Good Customer

It is not difficult to articulate what constitutes a good customer for any business. Such a client knows what it wants, has a realistic budget and resources to pay promptly for what it wants, and has a capacity to make (and stick to) timely decisions. (Insofar as competitive tendering is involved, the preparation of bids is in general an expensive activity, especially if a requirement is complicated. When teams have been put together to enable the prompt delivery of a project, their maintenance over a protracted period while final commitments are made is also expensive.) Finally, a good customer is one that spends a lot, enabling it to make a marked contribution to a company's turnover and profit.

In the specific context of defence, a good customer is also one that is ready to fund development costs over a period of years, and to bear many of the technical and financial risks associated with the development and production of complicated systems that often have only one reliable customer: the sponsor. This is the reason that BAE Systems and other companies from Europe have sought to invest in the United States and to secure access to the US defence market. With this in mind, NATO is clearly facing a series of challenges that cannot be ignored.

A Small Customer

First, unless some commitment is made to a specific, large new project, NATO is a small customer. NATO's total military budget is about $2 billion a year and the budget for its Security Investment Programme is about $1 billion. Even with a civil budget of around $500 million, NATO's total spend, most of which goes on personnel, is around the same as that of

Portugal's defence budget. It is a sad but almost inevitable fact that small customers receive less attention from companies than large ones.

Clearly, should the pooled capabilities dimension of Smart Defence take off, this could change, and the finally agreed Alliance Ground Surveillance (AGS) programme will have an impact, but it is significant that even the costs of the envisaged missile defence programmes amount to only $1.3 billion over a fourteen-year period.[1] Compared with the UK aircraft carrier programme or the British contribution to the Joint Strike Fighter, this is at most a middle-sized commitment.

NATO Challenges: Decision-Making, Free-Riding and the Pressure for US Solutions

The defence industry, and certainly the European defence industry, can have little affection for NATO's decision-making processes, which in turn reflect the fundamental nature of the Alliance. NATO's primary purpose is to protect the sovereignty of its members, which rules out the possibility of decisions by majority vote, and renders problematic elements of supranationality, certainly during peacetime. Even though the Alliance has long practised decision-making by consensus rather than requiring unanimity, the fact that the Alliance is a collection of sovereign entities can disrupt decision-making.

At least measured decision-making is likely on Smart Defence matters. The 'pooling' aspect of Smart Defence must involve especially the smaller members contributing to equipment-based capabilities that they could not possibly afford (or even envisage) on a national basis. These are capabilities for which they might not have planned to have to pay anything, and it is likely that, when it comes to the allocation of payment shares, they will be drawn towards a 'free-riding' strategy and almost certainly to the embrace of prolonged discussions about precisely how much they should pay. They will be very wary of what, in Sven Biscop's words, would look like 'a pooling and charging' arrangement, especially when there is no obvious formula for settling how much each should pay.[2] According to a 1998 US Government Accountability Office report, at least five variables are relevant to cost-shares with regard to security investments: members' capacity to pay; the benefits of the use of projects; the economic benefits of the construction of projects; the non-infrastructure contributions of individual states; and various political and economic factors.[3] Reconciling all of these considerations can take time.

Moreover, if the Alliance is drawn to low-risk technical solutions for major capabilities, the obvious answer is always likely to be a US-origin system, of little benefit to the economies of Western Europe. As the debates in Germany and France about the possible merger of BAE Systems and EADS have exposed, governments in Europe are concerned about the economic, as well as the military, impact of defence spending. The NATO air surveillance

and command-and-control solution was, after all, a fleet of Boeing E-3A aircraft, and the AGS solution started with the E-8 JSTARS (Joint Surveillance and Target Attack Radar System) in pole position until European preferences for a significant contribution led to the advance of a potential solution based on the Airbus A321 and a European radar. In the summer of 2012, on a programme that had begun its formal life with Atlantic Council approval some seventeen years earlier, it finally proved possible to sign a $1.7 billion contract for the supply of five Block 40 Global Hawk aircraft equipped with an American radar system, but with Europeans contributing to the equipment on the ground and communications technology.

François Heisbourg has already referred to 'attempts to turn NATO into a procurement agency for US systems' as part of efforts to find new markets for American industry when the US defence budget is falling.[4] That Smart Defence might generate such a perception clearly hinders its capacity to attract tangible support, but, in any event, getting workshare into Europe from US systems (as occurred also with the purchase of AWACS – the Airborne Warning and Control System) or getting Europeans to buy completely from a US production line involves discussions that take time and clearly mitigates against quick decisions.

What Can Be Done?

In recognition of the fact that NATO as a customer is inevitably constrained by the limited resources that states put at its disposal, as well as by its decision-making processes, more attention should be paid to NATO's potential to act as an intermediary between its member governments and industry, particularly with regard to capabilities unavailable on a national basis to most member states. It could serve as a forum where governments and industry seriously come together to discuss the equipment-based capabilities of tomorrow, as well as what is available today. With a fair wind, some of these discussions could lead to two or more members coming together to procure (or develop and procure) novel systems which would then become available to NATO states in future operations of the willing. Whether such systems would be given some kind of NATO badge, as were the Tornado and Typhoon, would be a secondary matter for the consideration of the governments involved. What would matter would be that the stock of capabilities available to NATO's European members would have been significantly enhanced. This implies review, reorganisation and reinvigoration of the Conference of National Armaments Directors and the NATO Industrial Advisory Group, with a particular need to move away from sub-structures based on the land, sea and air domains and towards a capability-based approach. It also implies working together with the European Defence Agency, with both Canada and the United States provided with a voice in this forum by their membership of NATO. Many of these issues are discussed more extensively in Henrik Heidenkamp's paper in this volume.

Insofar as NATO might emerge in some areas as the procurement authority, it should adopt a process whereby companies would not be expected to invest much in marketing and the preparation of bids until the largest capabilities, and also the financing and the procurement strategies, had been agreed. In short, significant time needs to be devoted to the preparation of projects in order to facilitate their rapid implementation.

Notes and References

1. Active Layered Theatre Ballistic Missile Defence plus an element of territorial defence capability.

2. Cited in H Breitenbach and B Giegerich, 'A "Smart" Opportunity: Industry Can Benefit From NATO Strategy', *Defense News*, 20 May 2012.

3. Cited in Carl Ek, 'NATO Common Funds Burdensharing: Background and Current Issues', Congressional Research Service Report for Congress, 15 February 2012.

4. François Heisbourg, 'A third quest for the holy grail of defence', *Financial Times*, 16 September 2012.

Smart Defence and the Critical Flow of Information: A Single Version of the Truth

John Louth

The Smart Defence Initiative, introduced by NATO Secretary-General Anders Fogh Rasmussen in February 2011, has, at its core, the quest for a more effective economic relationship between those who demand and exercise military capabilities in NATO and those within the defence industry who design, develop, manufacture, maintain and modify essential defence equipment and services.[1]

Consequently, the *relationship* between NATO, its member states and industry and the management of *information* between these stakeholders comprise the vital enabling components of the entire initiative. Recognition that success rests on these pillars is, of course, both comforting and challenging: comforting in that this key outcome of the annual Allied Command Transformation (ACT) Industry Day held in September 2011, and of the subsequent multinational workshop held at the Royal United Services Institute (RUSI) in London in March 2012, constitutes progress; but challenging in that both officials and industrialists now have to 'make good' on this insight.

This paper explores the dynamic interface between the key components of relationship and information management in the context of Smart Defence. It is far from exhaustive, and is designed as an immediate and provocative 'think piece', rather than presenting the conclusions of comprehensive, evidence-based research. Nonetheless, its themes echo those that were deemed important at both the September 2011 Industry Day and the March 2012 workshop. The paper ends with a set of short recommendations.

Smart Information for Smart Defence

The concept of Smart Defence rests on a simple conceptual ladder of structures and activities that is summarised in Figure 1. At the very top of the model, from which all other steps derive, is the critical task of horizon scanning to capture, understand and prioritise systemically the hazards, threats, risks and opportunities faced by NATO and its members within the geopolitical system. Of course, not all nation-states view the world in the same manner, but a NATO-derived perspective and hierarchy of threats is essential if common NATO requirements are to develop. The NATO Defence Planning Process (NDPP) provides the overall framework for capability development within the Alliance, but a much more robust 'requirements capture' process may be necessary as NATO develops its role as a facilitator of collective capability targets and design specialisation.

Figure 1: A conceptual framework for Smart Defence.

Source: John Louth, 2012.

Consequently, the second step within the conceptual model – the establishment of NATO user and system requirements – could enable pooling and sharing initiatives, and the joint procurement and development of capabilities. This, in time, could deliver the ambition embodied in Smart Defence: the provision of capabilities that are shared between states, economically acquired and affordable to use and maintain over decades, and that may be defined by North American and European narratives of relative fiscal austerity. Respective national defence budgets and individual national requirements can and should inform this partnered requirements process. Information, therefore, will need to flow in both a dynamic and systematic manner between nations and NATO that will inevitably challenge long-held notions of national autonomy and independence. Accepting this new and real emphasis on interdependence will require a subtle change of behaviour and values amongst partners, while the political and cultural threats to this transformation should not be underestimated.

Inevitably, the organisational development of Smart Defence will involve traditional concepts of negotiation – at the intra-state level and between governments, NATO and industry (no matter where the latter is based or listed) – as well as trade-offs between common partnered needs and national ambitions, and an element of competition to ensure the best possible contribution from the defence industry. This means that industry must have:

- Visibility of the process within a NATO procurement framework for partnered solutions

- Clarity of the forward plan
- Assurance of the flow of money
- An understanding of the contracting mechanisms
- The confidence to engage, especially where corporate intellectual property is to be shared across a number of nations.

Once more, the difficulties should not be underestimated.

As an aside, it is important to recognise that NATO is, first and foremost, a political alliance, albeit one associated with the active projection of military capabilities for the assurance of its member states' security. The aim of the Smart Defence Initiative is to ensure that efficient, and joint, procurement processes and structures are in place, and will be followed, instead of narrow national alternatives, regardless of the political climate. Emphasising effective management over politics is a key feature of the initiative, and nowhere is this more critical than in the generation and use of information.

First, information relating to all aspects of Smart Defence must be accessible to all stakeholders, both within the member states and industry. Consequently, a group or function within NATO must be allocated responsibility for the management of information, and for keeping it current, useful and readily available. This may, in part, contradict the 'Lead Nation' concept, but information, to be effective, has to be managed as an active portfolio from the centre, rather than as a set of disparate elements from within nationally led programmes and projects. Moreover, whilst individual procurement projects will necessarily safeguard sensitive commercial and operational information and data, the preference must be to share information as quickly and widely as possible, whilst being cognisant of sensible project management protocols. This is not easy to achieve, and will require leadership, goodwill and a certain amount of trial and error to capture the right balance between a collective need for openness and appropriate information security.

Second, information must be comparable and credible, which means that it has to be codified and systematised.[2] This requires effective and proactive information managers possessing some degree of subject-matter expertise. Such people can be difficult to identify, recruit, develop and retain, and must be assured of a career structure in order to be individually and collectively effective. The organisational position of a Smart Defence secretariat within NATO, funded for the long-term, requires clarification and prioritisation.

Third, there is often a cultural hesitancy to publish and share information until all facts and interpretations have been captured and properly thought through. Whilst the desire to address all nuances of data and information management is laudable, the best intentions can often be the enemy of the good. To be effective, information must be timely and incremental, especially

as it informs multiple stakeholders with complicated and contested agendas.[3] It takes a confident and secure organisation to act in this manner, so, once more, the organisational position and standing of a Smart Defence secretariat seems critical to success. The key point, of course, is that information is man-made and at the heart of the decision-making process. Consequently, it needs proper husbandry to be organisationally effective.[4]

Today's Challenge, Tomorrow's Opportunity

The challenge is, in many ways, easy to capture, though harder to resolve. How do the sponsors of Smart Defence generate a single, definitive version of the truth of its purpose and features whilst, concurrently, ensuring that tomorrow's business is conducted through its protocols and constructs? There is no short answer, but there is an opportunity today to design a process and culture that is profoundly fit for the purpose, and which is *joint*, *shared*, *economic* and *affordable* – characteristics that will underscore tomorrow's understanding of effective capability and joint security.

Recommendations

It is important for all stakeholders and exponents of Smart Defence to be able to visualise and explain the relationship between its key components. Moreover, a coherent taxonomy and standardised documentary formats and templates would ease the initiative's development. It is recommended that:

- A short and highly visual management model be developed along the lines of that presented in Figure 1. This will demonstrate in a simple manner the necessary flow of information against which programme and project activities can be tested as Smart Defence develops
- Standardised templates (especially for the articulation of requirements) be developed both for NATO and for national utilisation. These should be developed in consultation with industry, underpinned by a common pan-national taxonomy, and kept as simple and functional as possible
- A Joint NATO-industry Smart Defence secretariat be established to implement the above, and other, recommendations as necessary.

Notes and References

1. NATO Secretary-General Anders Fogh Rasmussen reported to the Permanent Representative Council on 24 January 2012 that Smart Defence was progressing in terms of its supporting principles of affordability, availability and alignment between national and NATO programmes and policies.

2. See Jacques S Gansler, *Democracy's Arsenal: Creating a Twenty-First Century Defense Industry* (Cambridge, MA: The MIT Press, 2011), pp. 216–17.

3. See Kenichi Ohmae, *The Borderless World: Power and Strategy in the Global Marketplace* (London: Harper Collins, 1994).

4. See Robin M Rowley and Joseph J Roevens, *Organize With Chaos* (Kemble: Management Books 2000, 2007).

Opportunities for Industry

Mike Maiden

The British government's February 2012 White Paper 'National Security Through Technology' explicitly recognised that 'a healthy and competitive industry in the UK makes a significant contribution to developing and sustaining key defence and security capabilities'.[1] The White Paper acknowledged that companies in the defence and security sector also bring benefits in terms of their contribution to national wealth, to employment and to the range and level of skills in the economy. However, the key issue, and the one that the British government continues to stress, is that the essential focus for defence expenditure in the UK – including for its defence industry – is the acquisition, support and successful delivery of military capability.

At the same time, as the nature of military operations evolves in response to changing geopolitical scenarios, and with the appearance of new state and non-state actors and the onward march of technology, the role that industry plays in providing the non-manpower elements of defence capability is changing. While significant parts of the industry still play an important and traditional role in the design, development, manufacture and through-life support of equipment used by the armed forces, these and many other companies that may not be immediately thought of as part of the defence industrial base – including global IT and communications technology companies – are becoming ever more closely integrated into the complex business of modern warfare, with this involvement extending ever closer to the front line. These trends are impacting upon national thinking about concepts, doctrine, rules of engagement and, of course, acquisition policies. They also have implications for the NATO Alliance.

In the NATO context, the industry dimension, on the one hand, adds another potential layer of complication to the challenge of optimising co-operation between member states to generate and sustain the Alliance's capacity to influence and respond to security challenges. On the other hand, the global defence and security industry, which demonstrates on a daily basis its ability to both compete and co-operate at the same time, can play a significant role, in partnership with national governments and the Alliance, in leveraging technology, industrial capacity and defence investment to deliver desired outcomes. The challenge for NATO, as for national governments, is to define the policy and procedural constructs that will achieve this, whilst at the same time recognising and, where appropriate, preserving the discrete interests and responsibilities of the Alliance, national governments and industry. The Smart Defence Initiative, if it is to deliver meaningful change, will have to square this circle.

Yet what do we mean by 'industry' in this context? Major primes such as Lockheed Martin, BAE Systems, Finmeccanica and Thales are obviously key players. However, as already mentioned, the technology imperative that underpins most aspects of modern military operations means that, in areas such as C4ISTAR (command, control, communication, computers, intelligence, surveillance, target acquisition and reconnaissance), the source of potential military advantage may lie outside the traditional 'defence' industry. Solutions may instead be found, for example, in international corporations such as Hewlett Packard or, as is increasingly the case, in small, niche companies comprised of a few clever people and limited financial resources.

In 2010, there were 4.5 million such private-sector small- and medium-sized enterprises (SMEs) in the UK alone. These accounted for 99.9 per cent of all UK enterprises, 59.1 per cent of private-sector employment and 48.6 per cent of private-sector industry turnover. Only a fraction of these would describe themselves as 'defence' or 'security' companies, but a far greater proportion have skills, capabilities and technologies that could be relevant to the defence and security market. While the numbers will vary between Alliance partners, harnessing the potential that exists within the broader industrial base, including SMEs, represents a common challenge.

The Royal United Services Institute's Defence, Industries and Societies Programme has developed the concept of a 'defence industry ecosystem' with a number of moving and interdependent parts or stakeholders.[2] This model also applies in the NATO context, with the additional dimension of the Alliance's political and organisational overlay. In such ecosystems, there are no simple solutions to the challenges of achieving the desired level of military capability, value for money for the public purse, and a sustainable defence and security industrial base. Indeed, this is evidenced by successive British governments' changing attitudes to the nature of the relationship between the defence customer and its suppliers, on a continuum between outright market-force-driven competition and various flavours of 'partnering' or 'partnership'.

Such decisions will always be for national governments to make as they spend their taxpayers' money and enact the defence and security policies and programmes for which they have a mandate. It is arguable, however, that the overlaying of national economic and industrial interests onto the search for effective Alliance capability development makes the latter more difficult to achieve. So, in this interdependent defence ecosystem, what are the levers available to NATO to optimise Alliance capabilities, and where should it focus its efforts?

First, NATO should concentrate on improving the demand side of the relationship with the international defence and security supplier base. In the past, some institutions have spent too much time and effort trying to design and manage how industry should work together. If governments come together under the auspices of the Alliance with common or shared requirements, industry will, for sound commercial reasons, organise itself in the most appropriate transnational industrial arrangements to service these requirements. Indeed, industry also has a valuable role to play in the definition of programme requirements and the evaluation of options based both on their knowledge of what is technologically possible and on cost drivers. Conversely, experience suggests that mandated overlays of industrial constructs or work share arrangements have a negative effect on both the efficiency and success of programmes.

Second, there needs to be greater clarity about what is meant by the 'proactive partnership with Industry' mentioned in the implementation section of the conceptual food for thought paper contained within the Secretary-General's Progress Report on Smart Defence.[3] 'Partnership' is a word that conjures up different constructs and expectations. The ambition is to elaborate a definition to which industry would subscribe but, as always, the devil is in the detail.

Third, industry – particularly the lower tiers of the international industrial base – will need to be persuaded that it has a part to play in achieving the objectives of the Smart Defence Initiative. Currently, for most SMEs in the UK, the bureaucracy of the domestic market and the costs involved in bidding are daunting enough. The processes, timescales and contractual terms involved in participating in international competitions and programmes – or seeking to be part of the supply chains of those companies that do – are a disincentive to many companies, including larger ones. The Smart Defence Initiative should therefore seek to reduce bureaucracy and complexity, and increase visibility and approachability.

Fourth, there is the challenge of capturing innovation. Small companies can represent a significant – albeit not the only – source of innovation in terms of new technology, new ways of working and new business models. Much of this innovation remains untapped because small businesses do not themselves have the financial capital, the management bandwidth or the luxury of medium-to-long-term business horizons to be able to realise their potential. Primes and higher-tier companies can make an important contribution in this regard by providing routes to market and, possibly, investment support. Nevertheless, national governments, and NATO itself, also need to consider ways in which sources of innovation, wherever they may be located, can be encouraged, and allowed to realise their innate potential.

Notes and References

1. Ministry of Defence, *National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security*, Cm 8278 (London: The Stationery Office, February 2012).

2. Henrik Heidenkamp, John Louth and Trevor Taylor, 'The Defence Industrial Ecosystem: Delivering Security in an Uncertain World', RUSI Whitehall Report 2-11, June 2011.

3. NATO (PO(2012)0026), The Secretary-General's Progress Report on Smart Defence, Annex 1, 24 January 2012.

Working with NATO: Identifying and Supporting the Creation of an 'Addressable' Market

Henrik Heidenkamp

The fundamental business rationale in the defence market is quite straightforward: companies must demonstrate the long-term commercial viability of their business models to their shareholders, especially in comparison with investment opportunities in other commercial sectors.

Accordingly, the core issue driving industry's working relationship with NATO is the latter's role in supporting the identification and creation of an 'addressable market' for industry's products and services. However, industry is highly sceptical, at best, as to how efficiently NATO can take on and advance this role. Arguably, NATO will have to address various challenges in terms of its structures, processes and levels of ambition in order to mitigate existing uncertainties and present itself as a relevant and reliable partner to industry.

NATO's ability to assume this role is essential for the successful implementation of its Smart Defence Initiative, as a healthy defence industrial base is the foundation of the Alliance's defence efforts. The industry-NATO relationship is, therefore, a crucial component of what could be labelled the 'Smart Defence Nexus', consisting of the interdependent dimensions of the Smart Defence Initiative, with 'Smart NATO' at its core (see Figure 1). Mike Maiden correctly emphasises in his paper in this volume that 'the industry dimension ... adds another potential layer of complication to the challenge of optimising co-operation between member states', not only in its own regard, but particularly in its interaction with other dimensions of the Smart Defence Initiative. Making this multi-dimensional construct work is indeed the 'circle' that NATO will have to 'square'.[1]

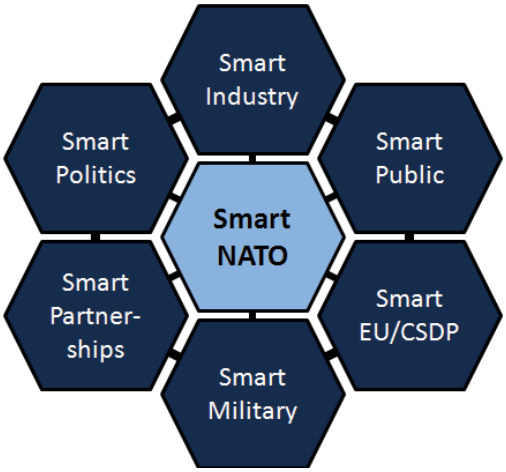
NATO, as an organisation, has to prove how 'smart' it can be, proactively engaging industry, and seeking new lines of communication and influence beyond its walls in Brussels.

Identifying the 'Addressable' Market

The visibility of business opportunities is key in any commercial sector, and it is the starting point for the industry-NATO working relationship. NATO headquarters must contribute to industry's awareness and understanding of the relevant stakeholders on the demand side, their requirements, contracting methods, investment budgets, timelines and decision-making procedures. This knowledge will enable industry to better orientate itself in the market, align its product portfolios, make sensible investment decisions and deliver high-quality products and services on time and on-budget. Essentially, NATO has

to help industry answer two questions: 'what is going on?' and 'what is in it for us?'.

Figure 1: The 'Smart Defence Nexus'.



Source: Henrik Heidenkamp, 2012.

In order to do this, duplications or even contradictions in NATO's efforts to communicate with industry – which generate confusion and uncertainty for both NATO and industry – must be avoided. NATO needs to speak with one voice, streamlining the work of its various departments and the views of its member states. A single point of entry for all interactions – both formal and informal – between industry, NATO and its member states would be highly valued by all stakeholders. Ideally placed within the structures of NATO's procurement agency, such a central defence industrial dialogue and decision-making hub would serve four key functions in NATO's efforts to help industry identify an 'addressable' market.

First, it could act as a 'clearing house' for the determination of the capabilities required and the methods for their procurement. So far, NATO has experienced limited success in pressing member states to clearly state which capabilities, both bilateral and multinational, they want to acquire, which capabilities they are willing to abandon, and in which capabilities they stand ready to specialise. Particularly with regard to specialisation, member states are reluctant to take a position due to issues of sovereignty and a lack of trust among Alliance members. The hub could provide an institutionalised mechanism for co-ordination among member states, and could increase industry's awareness of the proceedings, main obstacles and business potential. The Alliance and its member states would also benefit from industry's perspective and expertise.

Second, NATO is a customer – albeit 'a small customer' compared to its member states, as Trevor Taylor points out[2] – of the defence industry in its own right, acquiring various products and services through its procurement agency. The hub could therefore improve industry's understanding of NATO's own procurement role, including the actual amount of money that passes through its procurement structures (and especially the conceivable amount of collective funding); the elements of its procurement portfolio; and the demands and specifics of its tendering, contracting and requirements management procedures. The transparent communication of these aspects is of particular relevance to small- and medium-sized enterprises (SMEs), which represent a significant part of the wider defence industrial base, but which usually do not have the resources to effectively penetrate NATO's procurement system.[3]

Third, it could further integrate industry into NATO's and its member states' requirements-setting and management processes at an early stage.[4] A better understanding of the requirements, and an open dialogue about their industrial implications would significantly de-risk future programmes, and thereby de-conflict the supply-and-demand relationship. Of course, the actual practicalities of industry involvement in a process that addresses key components of future contract designs – and may therefore generate problems of conflicting interests – are highly complex from a legal point of view. However, a balance must be found between the need to involve industry and compliance with the legal regulations of an open tendering process. To this end, the commissioning of 'risk-reduction studies' from industry by NATO or its member states via NATO's procurement agency in the early stages of the acquisition's analysis phase – preferably financed through additional common funding – seems to be a sensible approach.

Fourth, in a constantly evolving strategic context, with changing operational requirements and highly volatile market conditions, the identification, timely communication and effective exploitation of 'lessons learned' is a strategic imperative for both industry and NATO.[5] Through its institutionalised structure, a hub could help maintain the body of knowledge developed through collaboration between industry, NATO, member states and the military user.[6] The repetition of previously identified problems could thereby be partly avoided, and more attention could be paid to the generation of implementable solutions.

Supporting the Creation of an 'Addressable' Market

It is important to be clear that NATO cannot and should not act as an 'industry agent'. Instead, its prime task is to get the demand side right at the national and Alliance level. However, not all demand will be sufficient to drive the creation of an 'addressable' market. As an industry representative convincingly stressed during an ADS roundtable discussion at the Royal United Services Institute in August 2012, only 'deployable forces' will be able to do so.

Accordingly, NATO has to ensure that its defence planning process – and those of its member states – adequately reflect this market demand, not for the sake of company revenues *per se*, but in order to sustain a healthy defence industrial base as a core component of the Alliance's defence effort. To this end, it appears necessary to advance the integration of industry into the national and Alliance defence-planning process. Further, industry, whose standard-setting is at any time arguably ahead of that of both NATO and its member states, would benefit significantly from an acceleration in NATO's capability-planning cycles and a more substantial role for NATO in the research and technology domain.

More fundamentally, in its general efforts to instil in member states the notion that 'defence matters', NATO must substantially advance its influence – both direct and indirect – over national defence industrial policy discourses. Engaging member states solely in capability planning, requirements setting and harmonisation of standards is not enough; in order to generate actual value for industry and the Alliance's defence efforts, the Smart Defence Initiative must be pursued in the context of the rough realities of national defence industrial policy discourses. The defence industrial dimension must therefore be prioritised more highly in the dialogue between NATO, its member states and industry.

Of course, adding a multinational Alliance layer to the various national defence industrial discourses is a highly sensitive topic, as it affects wider perceptions of economic interest, including employment and intellectual property rights. However, in line with the Smart Defence Initiative mandate issued at the May 2012 Chicago Summit, NATO as an organisation must not leave national defence industrial policy discourses unaddressed, as these play a significant role in framing Alliance decision-making, thereby affecting its efforts to support the creation of an 'addressable' market.

Taking into account the Smart Defence Initiative's 'smart EU/Common Security and Defence Policy' dimension, NATO may, in this regard, also consider joining forces with the European Defence Agency and the European Commission's Directorate-General for Enterprise and Industry, both of which play an influential role in European defence industrial discourse. As Trevor Taylor aptly argues in this volume, NATO could thereby give Canada and the United States a voice, through their membership of the Alliance, in the European Union's discourse.

A fundamental precondition for NATO's successful contribution to the identification and creation of an 'addressable' market, as described above, is the issue of obtaining a comprehensive mandate from the member states' political leaderships, which in turn must be reflected in the influence of the hub's members and its personnel. If the hub is not to become a 'meet and greet' exercise without any real impact, senior decision-makers with real

influence in NATO and its member states must, with the backing of enough highly qualified personnel, support and drive the hub's work as part of the Smart Defence Initiative's 'smart politics' domain.[7]

Making Bold Decisions

The Smart Defence Initiative requires NATO member states to make bold decisions. It requires the same of NATO as a whole, which will have to adopt an open mindset if it is to work constructively with industry, and benefit from its best practice and expertise. Further, NATO must engage with national political discourse on defence industrial policy and should hold member states publicly accountable for any ongoing lack of commitment to the various dimensions of the Smart Defence Initiative.

It is not the primary task of industry to make 'smart defence' work, but it stands ready to provide its share of the burden, if NATO proves to be a reliable and relevant partner. However, NATO – and its member states – must acknowledge that if it does not get the demand side right, then industry will inevitably move away.

Making the industry-NATO working relationship flourish will therefore require leadership from both senior NATO officials and senior policy-makers in NATO member states, both of whom will have to accept and advance NATO's widened role in 'smart defence'. Since NATO's roles as a relevant partner for the defence industry and an effective acquisition stakeholder for its member states represent two sides of the same coin, these must be conceptualised and realised in parallel, and it is this challenge that lies at the heart of the 'Smart Defence Nexus'.

Notes and References

1. See Mike Maiden, 'Opportunities for Industry', in this volume.

2. Trevor Taylor, 'NATO's Customer and Facilitator Roles in Defence Equipment Co-operation', in this volume.

3. See Mike Maiden, 'Opportunities for Industry'.

4. See John Louth, 'Smart Defence and the Critical Flow of Information: A Single Version of the Truth', in this volume.

5. For an assessment of NATO's information-management capacity, see John Louth, 'Smart Defence and the Critical Flow of Information'.

6. Lisa Aronsson and Molly O'Donnell, 'Smart Defense and the Future of NATO: Can the Alliance Meet the Challenges of the Twenty-First Century?', Conference Report and Expert Papers,

presented by The Chicago Council on Global Affairs, 28–30 March 2012, p. 10, <http://www.thechicagocouncil.org/userfiles/file/NATO/Conference_Report.pdf>, accessed 2 October 2012.

7. In his paper, John Louth recommends the establishment of a joint NATO-industry Smart Defence secretariat. See John Louth, 'Smart Defence and the Critical Flow of Information'.

Smart Business Models: Industry's Role in Efficient Multinational Development and Procurement

Andrew D James

In a time of budget austerity, Smart Defence aims to make NATO forces more effective and efficient through deeper international co-operation, prioritisation and specialisation. An important – although somewhat overlooked – element of the Smart Defence agenda is the issue of how smarter multinational development and procurement could be promoted. Multinational programmes offer the prospect of greater efficiencies – it is argued – through the economies of scale that may be generated by pooling national requirements into a single programme. There is little doubt that NATO governments should work together to identify programmes suitable for joint development and procurement with other member states, and potentially through NATO co-operative frameworks. This raises important questions for the defence industry. What can industry do to facilitate multinational development and procurement? What new business models can be applied to multinational programmes to enhance their effectiveness and efficiency?

'Old Wine in New Bottles'?

Cynics may argue that Smart Defence is little more than 'old wine in new bottles', not least because since the 1970s, NATO countries have sought to promote multinational co-operation on defence programmes. There have been successes: the NATO Sea Sparrow missile programme is one such success story, built on a solid foundation of agreed operational requirements between participating governments, support from senior defence officials in the US and Europe, and strong leadership at the project level. However, there have also been many high-profile failures that have left industry actors frustrated and disillusioned. The story of NATO's Alliance Ground Surveillance programme is well known: a programme characterised by delays, disagreements and budget cuts. Unfortunately, it is not the only example of the challenges posed by multinational programmes.

Defence economists have long been sceptical about the economic case for multinational programmes, arguing that barriers to efficient transatlantic programmes have added costs, which have in turn been passed on in contract prices. National procurement officials and industry personnel know from experience that the co-ordination costs of such programmes can be high, and that programme management complexity and problems increase in a non-linear fashion as the number of partner countries increase. *Juste retour* has too often been the order of the day, distorting markets and increasing

costs. At the same time, there exists the paradox that multinational programmes designed to promote co-operation have often been the source of tensions within the Alliance, characterised by some as a Trojan horse to sell US technologies to Europe. Equally, they have sometimes been seen as a means for countries with large defence industries to impose their solutions on smaller NATO members.

In part, this cynicism is justified given the record of many multinational programmes; but it needs to be addressed head-on by advocates of Smart Defence if their aspirations are to be met and industry is to be fully engaged. There is little doubt that effectively structured and well managed multinational programmes may generate considerable economic benefits. Lessons can be learned from good practice and past experience to develop new business models for multinational programmes. In an environment of steeply declining defence budgets, the opportunities they offer for efficiency gains must be grasped with both hands.

Increasing Efficiencies in Multinational Development and Procurement

What Can NATO and National Governments Do?
The industry response to Smart Defence will be 'show us the money!' Indeed, industry engagement in multinational programmes under Smart Defence will only occur if industry can see concrete business opportunities in the form of specific and funded programmes. If industry is not convinced of the business case for engaging in programmes in the NATO market, then it will likely turn its attention – even more so than it already has – to the growing markets of Asia, the Middle East and South America.

Sceptics wonder whether 'Smart Defence' might just be a fancy label for justifying further defence cuts. As such, NATO needs to aggressively communicate the fact that Smart Defence is about reducing inefficiencies and frictions in the acquisition process, and that this has the potential to increase the resources available for delivering capabilities. Furthermore, advocates of Smart Defence are right to argue that it could potentially create new market opportunities which might not otherwise exist.

If national governments allocate money to multinational programmes then industry will follow, but without such programmes there will be no business case and little industry engagement. Industry will also need to gain confidence that NATO members will be able to agree on capability requirements and stick to them throughout a programme. Above all, industry engagement requires stability of intent on the part of national governments: long-term programmes require confidence that governments will maintain funding for such programmes once they are agreed. Budget uncertainties, delays

and cuts are bad for programmes and undermine industry's willingness to engage.

NATO's use of multiple agencies with different contracting processes also poses challenges to industry: a consistent NATO approach to procurement is overdue and would facilitate industry engagement. At the same time, transatlantic industry co-operation is also hamstrung by US export control regulations. The International Traffic in Arms Regulations (ITAR) generate security of supply concerns on the part of European allies. Even when things are going well, ITAR can introduce delays into programmes. Time is money in defence contracting, and so these delays can add to programme costs. ITAR is being reformed, but this needs to happen quickly to increase efficiencies in transatlantic programmes.

What Can Industry Do?
If the efficiency of co-operative programmes is to be enhanced, then NATO and national governments need to work with industry to develop and implement new business models for such programmes. There are a number of best practices and success stories to build on that offer an alternative to the traditional and troubled approach of many multinational programmes.

The F-35 Joint Strike Fighter – despite its escalating costs and the challenges posed to the programme by ITAR – provides a model of how to allocate work within a programme that is based on competition and competence rather than *juste retour*. Similarly, the European Neuron UCAV (unmanned combat air vehicle) programme is based on a work allocation model that has moved away from *juste retour* to emphasise the strengths and capabilities of participating companies, thereby creating a truly European value chain. Such models stress that participation in multinational development teams should be based on the ability of industry partners to contribute some combination of money, technology and market access, rather than on the scale of their national government's budget contribution.

Similarly, although not a co-operative programme, the example of weapon systems user clubs such as that for Leopard main battle tanks (MBTs) also provides a potential model for the future. As an integral part of its customer relationship management strategy, the manufacturer of the Leopard MBT, Krauss-Maffei Wegmann, has defined and devised common supply concepts, further developments and plans for adaptions, offering not only the equipment, but also related training and logistic services. Such user clubs may offer economies of scale, share user learning and reduce life-cycle operating costs.[1]

At the same time, industry should not necessarily wait for NATO national governments to formulate ideas for new programmes. Industry could be

proactive here – as Bastian Giegerich has argued – by focusing strategic marketing efforts on developing products and projects that embrace Smart Defence. This means conceiving and proposing concrete capability projects that include partners from two or more allied nations. National governments may well respond positively to such ideas as they seek to balance their capability ambitions against budget realities.[2]

Learning from Experience

Industry has a crucial role to play in the implementation of NATO's Smart Defence vision. Multinational programmes have had a troubled past, but there is much good practice and past experience to draw upon and cynicism needs to be tackled head on. NATO, national governments and industry need to work together to develop new business models for multinational programmes. This needs to go beyond the NATO Industrial Advisory Group to promote broader engagement between industry and NATO, including at the highest levels on both sides. In an environment of steep declines in national defence budgets, the opportunities that new business models offer for efficiency gains must be seized. A first – small – step should be a 'Learning from Experience' exercise bringing together the best and the brightest from industry, national governments, NATO, think tanks and academia to identify and diffuse best practice. NATO can act as a central information repository, working with national governments and industry to identify what works and what does not – and why. This should be backed up by the use of metrics to assess Smart Defence outcomes. Those tasked with implementing Smart Defence need to learn from the best – and learn from the past – to create efficient and effective multinational procurement processes for the future.

Notes and References

1. 'Five Questions on Pooling & Consolidating Demand: An Interview with Frank Haun, Chief Executive Officer of German Krauss-Maffei Wegmann', 3 September 2012, <http://www.eda.europa.eu/news/topstories/12-09-03/Five_Questions_on_Pooling_Consolidating_Demand>, accessed 1 October 2012.

2. Bastian Giegerich, 'NATO's Smart Defence: Who's Buying?', *Survival: Global Politics and Strategy* (Vol. 54, No. 3, June–July 2012), pp. 69–77.

About the Authors

Lisa Aronsson
Lisa Aronsson is a research fellow in Transatlantic Security Studies at RUSI, responsible for leading research projects, hosting seminars, conferences and commenting on matters related to US foreign policy and transatlantic security co-operation. She is also an advisory board member of the Transatlantic Project at the IDEAS Centre for Strategy and Diplomacy at the London School of Economics.

Henrik Heidenkamp
Henrik Heidenkamp is a research fellow with RUSI's Defence, Industries and Society Programme. Prior to joining RUSI, he was a post-doctoral fellow with Queen's University's Centre for International Relations in Canada and worked for the military policy branch of the German Ministry of Defence (Fü S III 2) in Berlin.

Andrew D James
Andrew D James is a senior lecturer at Manchester Business School in the United Kingdom where he focuses on innovation strategy and public policy questions in the defence, security and aerospace sectors. He has held a number of international advisory positions, including for the European Commission and the European Defence Agency, and was an external expert on defence matters and rapporteur to the European Union Research Advisory Board.

John Louth
John Louth is deputy head of the Defence, Industries and Society Programme at the Royal United Services Institute. He has worked as a consultant and programme director throughout the defence sector, including for the BMT Group and QinetiQ, and as an adviser to the European Defence Agency on the development of pan-European procurement policies and practices.

Mike Maiden
Mike Maiden is chairman of NDI Ltd, a membership-based business development organisation working with SMEs operating in the defence, aerospace, space and security sectors. He previously worked at the Ministry of Defence, and in 2010 established his own defence and security consultancy. He is a trustee and council member of the Royal United Services Institute, a senior adviser to Renaissance Strategic Management and a defence expert member of the UK Innovation Forum.

Trevor Taylor
Trevor Taylor is professorial research fellow in defence management at the Royal United Services Institute, where he heads the Defence, Industries and Society Programme, and is a member of the Acquisition Focus Group. He is also professor emeritus at Cranfield University and is an adjunct faculty member of the Naval Postgraduate School in Monterey.