C4ISR: A COMPREHENSIVE APPROACH

Georges D'HOLLANDER

Abstract: In this keynote speech the NC3A General Manager identifies several key lessons from current operations and ways of developing capabilities, including the lack of agility, coherence and upfront interoperability. In dealing with current operational and capability development challenges, NATO and the member nations need to identify overlaps and redundancies and apply effectively the concept of 'smart defence' under growing financial pressures, while at the same time providing for close interaction with various international organizations, civilian security players, e.g. police forces, and private actors in complex crisis management operations. Among the specific recommendations are the establishment the position of a Chief Technology Officer and the transition from project to programme management.

Keywords: Civil-military interaction, legacy architectures, network enabled capabilities, interoperability, agility, coherence, smart defence.

Ladies and Gentlemen, thank you for the opportunity to address you today on the subject of C4ISR – A Comprehensive Approach.

I intend to present briefly my personal view on this subject, drawing from lessons identified and learned from recent events in Afghanistan, and from my own experience over numerous years operating in this environment. Despite some significant successes – let me say at the outset 'more of the same' will not be good enough!

NATO's new Strategic Concept, agreed in Lisbon last year, emphasised the shift from a pure military focus to the broader mission of security. The intent of the new mission requires a comprehensive political, civilian and military approach – with an increased engagement with international partners and civilian organisations plus greater cooperation in capability development, to minimise duplication and maximise cost-effectiveness.[1]

This intent rolls off the tongue with ease – but we should not underestimate the complexity associated with this strategic shift. Embracing a true Comprehensive Ap-

proach will not be easy and it will exacerbate the challenges we already face in delivering capability with a pure military focus.

Albert Einstein once said that "insanity is doing the same thing over and over again and expecting different results." Well I suggest to you today that – more of the same will *NOT* do - we will need to change the way we do business in order to succeed.

NATO's Consultation, Command and Control Agency is responsible for delivering many of the C4ISR NNEC capabilities into NATO and I believe we can draw lessons from this experience to help us to better deliver on NATO's aspirations in the new Strategic Concept.

NATO has been working towards delivering an effective network enabled capability for several years now. The initial ideas and concepts were in fact socialized at the very first NNEC conference back in 2004? This is strong testament to the foresight of Allied Command Transformation (ACT) that the NNEC vision has stood the test of time. During past NNEC conferences, however, I have on occasions wondered whether we were really making any headway. But in recent times, largely brought about by the imperative of recent NATO operations, we have seen significant advances towards the NNEC dream.

To give you some concrete examples. Currently we are currently working on three major network-enabled programmes. Earlier this year we signed the contract with industry for the Air Command and Control Information Services programme, and we expect to sign contracts later this year for the Intel Functional Services and NATO Common Operational Picture programmes. All three of these programmes are based on a service-orientated paradigm and represent real and tangible progress towards an operational NATO network enabled capability.

In Afghanistan, we are implementing key NNEC solutions. Last year we delivered the initial operational capability of the Afghanistan Mission Network and we have a programme of work this year and next to expand the scope and functionality of this still further. These capabilities provide a single operational network on which all the troop contributing nations and the government of Afghanistan can share information and work together. Initially, the work focused on the construction of the network and the linkage with national networks to provide a seamless infrastructure. This year we are already introducing an enterprise service bus and integrating the majority of the ISAF operational tools in a network enabled fashion. For the first time, we can begin to fight off the same map with common tools and information.

However, I would be misleading you if I told you that delivery of these capabilities has been easy or that we, NATO, have delivered these capabilities in the most effective or efficient way possible.

It is clear to me that we must capture and truly learn the lessons from recent experience and improve; otherwise the opportunities of the comprehensive approach will remain out of reach. So, what are these lessons?

To begin with, we lack *agility*. It still takes far too long between the war fighter requesting a capability and NATO being able to deliver this into theatre. Our acquisition processes remain optimised for the delivery of NATO infrastructure, not supporting urgent war fighter information needs. Our formal acquisition projects have been heavily supplemented with prototype solutions with ad hoc interfaces to national capabilities to meet urgent requirements. We have had to find short term fixes to interoperability challenges and this has led to concerns over resilience, reliability and our ability to sustain and support.

We also lack *coherence*. We still focus on projects rather than programmes or capabilities. We fail to take a 'system of systems' view and recognize that 'end to end' interoperability is the real goal. Our processes and funding structures do not always help! They all too often result in operational stovepipes—or the so called 'cylinders of excellence'—with no single body taking responsibility for coherency and interoperability.

The AMN (Afghanistan Mission Network) project is starting to address this, but many would argue this is too little too late. We still lack an enterprise wide common vision and roadmap for change and we continue to struggle with the challenge of aligning NATO programmes with national capabilities. There is still much room for improvement.

There is also scope to do more for less. In these times of fiscal constraint, we need to do much better at delivering more 'bang for the buck.' There is scope for driving cost out of the business by identifying overlap and redundancy in the programmes we deliver and seeking opportunities for rationalising existing capabilities and making more effective use of outsourcing of capabilities that today could be regarded as commodities.

The Secretary General recently discussed the challenge of building security in an age of austerity at his speech to the Munich Security Conference.[2] He spoke of the concept of 'Smart Defence' and the role of NATO in setting strategic direction, identifying areas of cooperation and sharing best practices. He emphasised the need for better coherence and the need to "get greater security for the money we invest in defence: pool and share capabilities, prioritise and coordinate better."[3]

In recent months, in my Agency, we have been taking the necessary steps to address some of these issues. I would like to think that in some areas, we are already delivering at least Smart¬*er* Defence.

Let me pick up on two key initiatives:

The first one is the establishment (or revitalisation) of the role of a Chief Technology Officer, or CTO, to lead the coherency drive. This, for me, is a key step which is beginning to bear fruit!

Secondly, the ongoing role that we have played for some time, but which we look to expand in facilitating a number of multinational programmes to encourage better co-operation between nations in key areas of NNEC implementation. Our work in multi-national engagement will marry well with the ACT Task Force initiative seeking opportunities to increase multi-national activity.

Through the CTO, we are adopting an enterprise wide approach, assessing and analyzing the C4ISR landscape across NATO to find to bring about improvements to achieve greater:

- Effectiveness in support of the war fighter;
- Efficiency in reducing costs; and
- Improvements in interoperability.

We are engaging with project and programme managers across NATO and the Nations working closely with ACT. We begin with a strategic audit of legacy and planned programmes and are in the process of engaging with National CTOs and CIOs, Industry and other bodies to address architectural coherence. We are beginning to strengthen governance structures at a Programme rather than Project level.

So why are these activities so important at this time? It is well worth briefly exploring the context.

The experience of Afghanistan is that, when we bring coalition forces together, we immediately encounter *serious interoperability challenges*. I suggest it is difficult (if not impossible) to add-in interoperability on or after the event. It has to be designed in at the outset. And here I am not just talking about technical interoperability but this also relates to people, process or ways of working. We often talk about the importance of using architecture to ensure that we can plug and play, but the reality—only too often—is that we plug and pray.

The *financial climate* is driving behaviours that seek more efficient ways to deliver capabilities through economies of scale, i.e. doing things once rather than multiple times. So we see multi-national programmes emerging: such as MAJIIC, multi-national CIED, multi-national cyber defence and multi-national ICC. The Agency plays a positive role in facilitating these projects with the nations and we see a real role for partner countries, such as Finland, in these projects. Partner countries can be espe-

cially beneficial in helping NATO strengthen its relationship with our civilian colleagues, such as the EU.

Additionally, internal to NATO, there is major *organisational reform programme* underway which seeks to reduce 14 agencies down to three. This should not be viewed as just about driving efficiencies but rather about streamlining processes and delivering greater coherence across multiple programmes often with greater agility. It is up to us all to steer and guide this reform, to bring about tangible benefits in the way we deliver capability.

Keeping pace with technology has always been a challenge both to NATO and nations – at a time when the talent pool is being drawn to more lucrative areas.

And finally, our *legacy*. We have inherited what we might call an accidental architecture. One that has grown organically over many years but at the enterprise level does not provide the required level of interoperability. If we were designing from scratch we would no doubt have been more efficient by avoiding overlaps.

So we begin to see the scale of the challenge. In my view it has less to do with technology but more about the need for transformation of our systems. This becomes a *Management of Change* challenge. John Kotter—the guru of change—lays down the key attributes required for successful change programmes. The first is recognition of the imperative for change – the '*burning platform*'; the second is a '*coalition of the willing*.'[4]

In ISAF today, the rate of change is driven by the Taliban. So, if we were ever in any doubt about our responsibilities, let us remember our troops on the front line. I think it was Mario Andretti—the F1 racing driver—who once said "if I am in control, I am not going fast enough." Well maybe this is the situation we find ourselves in today. Change is not always comfortable and we are not always in control, but we must embrace it.

The Comprehensive Approach will broaden our engagement outside traditional areas. The enterprise will expand and evolve and this will create new opportunities and new risks. Cyberspace is already part of that operational environment and, more importantly, the populations that we seek to secure are operators in the same environment. Don't think for one moment that cell phones are foreign to people in Afghanistan. In fact they are key enablers to their offensive effort.

I therefore see cyberspace as an operational capability to be exploited in our effort to secure the physical and intellectual freedoms of the population. Yes, I know, the minute you mention cyberspace in a military setting, we immediately think of the challenges of cyber defence; but let us first agree that cyberspace represents operational

opportunities as well as challenges. We must recognize that the opportunities go far beyond the traditional scope of either psyops or information operations.

Exploiting this capability to complement or replace kinetic actions is something we do not yet fully understand. The same can be said for intelligence led operations. Remember that the battleground is the human terrain. It is the intelligence on the perceptions, attitudes and actions in the human terrain that we need more than anything else; and where better to get that intelligence than from the population directly.

The quid pro quo is the establishment of the information infrastructure to support the needs of the population and administration for education, healthcare, business, dialog and engagement. It is clear that our operational art has not yet fully embraced the new capability. Integrating cyberspace into our operational repertoire is no longer a technical issue, but remains an intellectual challenge. We understand why when we read that the experts in the field now define cyberspace more in terms of the social interactions rather than the technical; and we all know that social interactions are infinitely more complex than technical ones.

So finally, to come back to the *comprehensive approach*.

The challenge before us is to address the needs and requirements of, not only, our Ministries of Defence but the larger integrated security sector of the Nations. The extent of civilian involvement in NATO Expeditionary Operations and the involvement of NATO in non-military missions (for example disaster relief operations) is a good reason for NATO to address the integrated security sector which includes not only the Armed Forces and the Ministries of Defence, but also the civil police forces, ministries of interior, emergency management services and intelligence agencies.

Through such an approach, all the stakeholders can leverage the diverse sources of NATO and National funding mechanisms to achieve greater efficiencies and more importantly, operational capability. True bang for the buck!

Ladies and gentlemen, I suggest that the complexity of our task has risen at least 10 fold and as I said at the outset – more of the same will not be good enough!

Within my Agency, we have begun the journey: the CTO function represents a strategic step forward and the associated concepts and ideas, that I have outlined, are quickly gaining traction but now need to be consolidated and embedded into the culture of the new Agencies. This will not be easy. It will require strategic leadership and commitment.

We cannot ignore the financial context. Economies of scale can be achieved by joining complex projects into multinational efforts through a coalition of the willing. Such programmes not only provide an opportunity for nations to share costs, but

more importantly they allow NATO and nations to work from the outset to achieve greater effectiveness and interoperability. One could say – *Born Interoperable*.

So in summary, since those early heady days of developing the NNEC foundation document and conceiving an intellectual plan for transformation, real world events have conspired and required accelerated solutions. We have come a long way and I think we can be justifiably proud of recent progress. But there is still much to do. Now is the time to take a strategic look at our aspirations, strengths and weaknesses.

The fertile ground for exploitation is 'On the Edge' as Admiral Cebrowski might have said – that is between NATO and Nations. It is here that NATO needs to step up to the plate and drive coherency and open opportunities for greater collaboration through effective use of architectures and standards.

The next operation is already upon us in Libya. We must capitalize upon the wealth of experience sitting in this conference today and address the 'Lessons Identified' from recent operations and from our combined experiences and take the difficult decisions now.

More of the same will not be good enough!

Thank you and I am more than happy to take questions.

Notes:

[1] *Active Engagement, Modern Defence*, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, adopted by Heads of State and Government in Lisbon, 19 November 2010, <www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>.

[2] Anders Fogh Rasmussen, "Building security in an age of austerity," Keynote speech at the 2011 Munich Security Conference, 4 February 2011, <www.nato.int/cps/en/natolive/opinions_70400.htm>.

[3] Rasmussen, "Building security in an age of austerity."

[4] John P. Kotter, *Leading Change* (Boston, MA: Harvard Business School Press, 1996).

GEORGES D'HOLLANDER is General Manager of the NATO C3 Agency since 1 July 2009. On 1 December 2004, then Major General D'hollander took up the post of Director of the NATO Headquarters C3 Staff, a position he held until 30 June 2009. Prior to that appointment, he was the Head of the CIS Division within the Belgian Armed Forces, and he also acted as Chairman of the NATO Army Armaments Group at NATO Headquarters from early 2002 until November of 2004. His military service was split between duties performed in operational units as a staff officer and appointments as a commanding officer within both Belgian Army and Defence Staff. He served for more than eight years in the former German Bundesrepublik.

Mr. D'hollander was born in 1950 and was commissioned into the Signal Corps of the Belgian Army after completing a five-year course at the Royal Academy in Brussels, where he graduated as an Engineer in Telecommunications and Electronics. In 1981, Captain D'hollander studied at Brussels University and gained a Special Licence in Informatics with great distinction. He is also an Ancien of the NATO Defence College (1996, Course 88) and in January 2001, he stayed in London as a Member of the Royal College of Defence Studies.

E-mail: info@nc3a.nato.int.