CIVIL-MILITARY INTEROPERABILITY IN SUPPORT OF NATO EMERGING SECURITY CHALLENGES

Jamie SHEA

Abstract: A speech by the Deputy Assistant Secretary General, Emerging Security Challenges Division, NATO International Staff, to the Second Workshop on Multinational Cooperation in Civil-Military Interoperability in Sofia, underlining the importance of civil-military interaction and multinational approaches in various frameworks, as well as their important contribution to allied and national capabilities to deal with new threats and challenges.

Keywords: Counter-terrorism, cyber security, energy security, non-proliferation, defence against terrorism, CIED.

Dear participants,

First of all, thanks for inviting me to speak at your workshop. Your objectives are certainly on a par with the goals of the Emerging Security Challenge Division which are mainly to ensure that military and civilian worlds can better understand themselves, find some areas of common interest and finally cooperate in a comprehensive manner.

It is also in line with the comprehensive approach and the Strategic Concept. Nevertheless to succeed we need to act in a rigorous framework:

- What is our NATO expertise, what is our NATO add-value?
- Who are the stakeholders we would like to work with?
- What kind of complementary projects, cooperation would we like to promote (keeping for each part our specificity)?
- What do we want to achieve?
- What will be the benefits? The scale of economy?

Jamie Shea 23

Having said that, the 'Multinational Approach' is exactly what NATO should promote now, in line with the multinational capability approach under the lead of Allied Command Transformation, the Voluntary Multinational Fund under the Conference of National Armaments Directors (CNAD) and with the support from the Defence Against Terrorism Programme of Work (DAT POW).

You would like to focus on interoperability: absolutely right because it is the core of the mission of NATO (which makes it possible to have 28—or more—nations working together and succeeding). The technical and capability dimension is essential.

You want to focus your future projects also on crisis management and disaster relief: these are the most appropriate domains in which NATO can provide its expertise. I know that you involved the Operation Division in your 1st workshop which is the Division strongly devoted to these activities.

The Emerging Security Challenges Division (ESCD) is also very involved in these kind of activities because our 'portfolio' has been created with a cross-cutting approach: counter-terrorism, cyber, energy security, non-proliferation.

Firstly, all these activities are linked together and we try to enhance a joint approach. Secondly, all these activities have a military and civilian dimension.

To take the Counter Terrorism, we have under our responsibility the Defence Against Terrorism Programme of Work (DAT POW) with several initiatives. Let me give you three examples: Counter Improvised Explosive Device (C-IED), Chemical, Biological, Radiological, Nuclear (CBRN) Defence, Harbour Protection.

C-IED is the main reason for casualties. We are developing capabilities to face this threat such as stand-off detection, biometrics tools, and a route clearance package. All these capabilities can be used in a military or civilian environment.

Fighting the CBRN threat is also of interest of military and civilians alike. It is also an opportunity for the division to ensure greater cooperation between the Counter Terrorism Service (CTS) and the Weapon of Mass Destruction (WMD) directorate.

The purpose of Harbour Protection is to develop a deployable architecture of systems. It fits the military requirements in particular the Force Protection ones and also it could be a useful capability to propose to the civilian maritime authorities. It is also an opportunity for the Counter Terrorism Service to work closely with the Energy security section.

I will say more than that. They fit perfectly in the crisis management domains or disaster relief situation: the prevention, the protection of infrastructures and populations, the security of supply are expertise that NATO can easily export outside.

Regarding your C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), I would like to mention that the Cyber Defence section should be one of your main customers or partners. We have a robust team in SHAPE working on the military dimension but we have a section in ESCD which is capturing the political dimension. This section also has the objective to be supportive to the nations and help them to better protect their national systems. The work with industry and with civilian sensitive organisations is essential.

Due to the growing inter-action between the civilian and military worlds and the economical constraints it is essential to support the kind of approach and projects which you would like to promote.

I can tell you that ESCD will be with you 100 percent and we will provide all the support we can.

I take wish you a good meeting waiting for your outputs and see how we can cooperate and support.



Dr. JAMIE SHEA is Deputy Assistant Secretary General, Emerging Security Challenges, NATO. Prior to taking up this position he was Director of Policy Planning in the Private Office of the Secretary General from 2005 to 2010. He was Director of the Office of Information and Press of NATO from 2000-2003, and in May 2003 was appointed to the position of Deputy Assistant Secretary General for External Relations in the new Public Diplomacy Division. He was also NATO Spokesman from 1993 to 2000.

In addition to his NATO responsibilities, Jamie Shea also holds a number of academic positions, most notably with the

Collège d'Europe, Bruges, the Brussels School of International Studies of the University of Kent, Canterbury, and Sussex University where he is a visiting lecturer. Jamie Shea completed his doctoral studies in Philosophy at Oxford University in 1981. He also holds a Bachelor of Art from Sussex University in History and French.