



United States Mission to the OSCE

Remarks to the OSCE Military Doctrine Seminar

General Lance L. Smith
Commander, U.S. Joint Forces Command,
NATO Supreme Allied Commander for Transformation
Vienna, Austria on February 14, 2006

I'm pleased to be here today to discuss the topic of technology and how it impacts the environment that we operate in today.

In my current jobs, this is an issue that we're confronted with every day. Clearly, I think we all view technology as a force multiplier when used right, but the hardest part of managing that top technology, at least for me, is trying to determine when you incorporate it into the commands that work for you and then, at the same time, how to make sure that you keep pace with technology and not create the kinds of problems that Dr. Mey mentioned during his talk.

We live in an era when technology offers incredible potential to increase the collective security within Europe and the rest of the world. It is not new—we've relied successfully on technology to ensure our collective security for many years. Monitoring and enforcement of arms control treaties in the 1960s and '70s (Limited Test Ban Treaty, Strategic Arms Limitation Talks, and Anti-Ballistic Missile Treaty) were all based on "national technical means of verification"—primarily seismic networks and overhead reconnaissance satellites. This limited transparency served the common interests of both sides in preserving stability and preventing conflict. As political and security conditions changed, particularly in the mid-1980s, the scope of transparency increased. In 1992, the Treaty on Open Skies was signed providing a regime for unarmed aerial observation over the entire territory of its participants. The openness of the Open Skies Treaty allowed for a transparency of military forces and activities, including other treaties and other agreements that could be monitored through the same systems. Likewise, the Treaty on Conventional Armed Forces in Europe established the cornerstone of collective security for the European region and continues to be successful in leveraging the concepts of limits, openness, and transparency, resulting in a more secure region spanning from the Atlantic to the Urals. These treaties are successful in large part because of the prudent use of appropriate technology to ensure collective security within a very static and fixed threat environment.

But now we are faced with a variety of very fluid factors much different from years past. These factors run the gamut from increasing sophistication of asymmetric warfare or irregular warfare, and radical ideologies, to failing states and unresolved conflict. These factors will also likely continue to shock our collective security interests for the foreseeable future, particularly as tensions, crises, and conflicts occur with little or no warning.

Furthermore, the impact of regional unrest will be magnified as "information age" networks provide a conduit through which huge amounts of public information can pass instantaneously virtually anywhere in the world. This effect is magnified because this "flattening of the world," as Thomas Friedman puts it in his latest book, also allows our

enemies to connect and collaborate in increasingly sophisticated ways that are very difficult to monitor, detect, or influence. Terrorists and extremist groups will use these networks to foster unrest and discontent through targeted information campaigns, and this unrest will be viewed globally, as we've seen recently. Asymmetric warfare is becoming more and more sophisticated, and—when enabled by access to technology—it can achieve disproportionate strategic effects. This sophistication requires the militaries of the world to become increasingly more aware of thorough review processes when adapting their militaries to meet tomorrow's challenges. Periodic reviews that take into account the changing environment, especially on the technological front, are important for shaping and transforming a country's military. For this reason, the United States' most recently conducted a Quadrennial Defense Review, which emphasizes preparing the forces to meet the challenges of a world becoming increasingly sophisticated in its employment of asymmetric warfare. This has caused us to rethink what tools we should use, how we organize, and the way we operate.

One of the first things we realize is that these new decentralized, amorphous threats make coalitions and partnerships even more important than they've ever been in the past. No nation is so large they can go it alone, and no nation is so small that they cannot contribute strategically. Interoperability is the key to effective multinational operations and hinges on technology. To make technology useful to us, we need to ensure that it is capable of operating in an environment of ever increasing joint multi-national and multi-national interagency operations. Interoperability must not only be the goal within individual security organizations, but also between organizations—something that has not received a great deal of attention in the past. NATO has adopted a holistic approach to dealing with a full range of potential missions—from crisis prevention, to humanitarian operations, to stability and reconstruction. We recognize our forces will operate in the multilateral environment alongside other coalition partners, and in close cooperation with international organizations, national, and non-governmental organizations.

In these working settings, intelligence collection, analysis, dissemination and sharing will be critical to anticipating, preventing, or containing conflicts. Situational awareness of the environment we operate in and a proactive approach in the earliest stages of emerging crises will be required. Having the upper hand in controlling and using information will be a necessity for decision makers in order for them to rapidly analyze the situation and determine the appropriate course of action—and to be able to make the right decisions quickly. Data is not the same as information, and information is not the same as good intelligence—we need systems that can process huge amounts of data into intelligence that we can act on. A secure information network for intelligence sharing and collaboration across militaries and governments in rapidly evolving situations is critical to this end.

Allied Command Transformation is currently developing the NATO Network Enabled Capability in an effort to allow information systems to 'talk' to each other – seamlessly and effortlessly. NATO recognizes that our interoperability has been hampered because there is not an effective way for the command and control systems of individual nations to network together. Setting and enforcing standards will be critical to linking the systems together into an effective network. This will require a great deal of collaboration between industry, NATO, and individual nations. In the end, the NATO Network Enabled Capability will define the requirements and establish standards for defense planning within NATO, and will produce an integrated, highly adaptive command and control capability for the NATO Response Force. This does not necessarily mean that the US or NATO have the best standards in the world, but it can provide a baseline from which to start.

This amount of change creates a great deal of angst, and that's understandable. However, I don't believe that this change in itself will leave any nation, no matter the size, out of a coalition or Allied operation if they are dedicated to participating as a full partner. The United States is committed to a strong Trans-Atlantic, European-wide link—we view closer ties and closer integration as critical to peace and stability. Every nation has the ability, or should have, to fill a needed capability. In this respect, coherency and coordination is key. There is still a great deal of capacity that can be filled with respect to very specific, but perhaps routine, missions. We should explore better surveillance of borders to prevent smuggling and trafficking, better use of biometric technology in passport control and travel documents, and better use of detection technology to monitor containerized shipping. All of these contribute to addressing and responding to terrorist actions and destabilization within all of our individual borders. The OSCE has already begun to look at these very important issues, for which you deserve great credit. I know there is the oft-mentioned dilemma between security and privacy, but I'm confident a balance can be struck that ensures collective safety and protects the privacy rights of individuals.

Because technological changes are so quick, we should seek solutions that are non-proprietary and are developed on an open architecture in order to ease technology transfer concerns and facilitate spiral development. With spiral development, we can better control costs and field the system faster, since the product is built in stages with frequent feedback. And, as I've already stressed, we need systems that are interoperable and spiral development demands that. These are big challenges, and we need to work with industry to insure that what they produce for all of us is "born interoperable," which must begin early in the planning cycle. This will allow us to continually upgrade existing systems so that we can apply the efforts of all our partners at a time and place of our choosing. The bottom line is that all systems need to support the vision of transformation.

The United States has worked hard to make capabilities that increase interoperability more available to our Allies and current and future coalition partners. There is also a great amount of commercial, off-the-shelf technology that can lower our costs by bringing economies of scale and efficiency. However, with less and less distinction between technology with strictly military applications, and technology with only civilian applications, we are offered a double-edged sword. Technology with multiple applications— or "dual use" technology— increases standardization and lowers costs, but it also means the opportunity for using sensitive military technology for civilian applications, or even using civilian technology in a harmful way not intended. We all have national interests that present dilemmas such as interoperability versus releasability, and releasability versus security.

Within this context, each of us has a responsibility to defend our technology from misuse by criminals and terrorists. The potential for 21st century dual-use technology falling into the wrong hands remains problematic—no nation is immune from the risk of diverting defense goods and technology into the wrong hands. I believe that we are making progress in the United States to ease the release of technology to our allies and partners. The OSCE should be complimented for the activities it has undertaken in this effort. Decisions taken in 2004 by the Forum for Security Cooperation concerning export controls over MANPADS, end-user certificates for small arms and light weapons, and on brokering controls for small arms and light weapons are all notable efforts to combat this threat. Is everyone happy? No. Is there room for improvement? Of course. Will it require continual discussions and

compromise? Certainly. And it is important to remember that “interoperable” is not synonymous with “identical.”

There will be costs involved, there’s no doubt about it. Five or ten years ago, we might have thought we had a decade or more to retool our forces and security organizations—enough time for rigorous analysis, planning, and budgeting. Many people wanted a peace dividend—and perhaps still do. But as we’re finding out, transformation is not cheap. Every nation needs to determine what their level of effort will be. There isn’t a technological gap between our nations, but there is a capability gap driven primarily by a commitment and funding gap, and this leads to interoperability gaps. We’re not going to solve that here today, but it’s something that will need to be determined sooner rather than later and something that no doubt will come up in the discussion period. Perhaps internationally developed programs such as the Joint Strike Fighter or the Euro-Fighter, with their commitment to design development based on participation of multiple countries from Europe, Asia, and America, can serve as a model for future technology developments.

I don’t want to take up much more time talking. I think that we’ve established the ground work for good discussion afterwards. I would like to say thanks to the OSCE for allowing me to be here today. Just as a final note in closing, I would like to say that all the best technology available will do us no good if we don’t have trained, ready, and motivated people at every level and across the entire spectrum. We must all work as a team not just those in uniform, but also civil servants, contractors, NGOs and industry leaders. We are in a fight together—a fight that will have lasting repercussions for all nations represented here today. Investments in technology for our collective defense are costly, but not doing so will be even costlier. Thank you very much.