Det talte ord gælder

Thank you for the invitation. I'm pleased to be given this opportunity to speak to you about Homeland Security, seen from my point of view.

Homeland Security is a concept we've all grown very familiar with during the last couple of years. In face of the rising threat from terrorism, the protection of society has thus become an imminent focus for politicians, the media and society at large.

The threats and risks of today

The threat we face is diffuse and enormously varied. The possible targets are basically infinite, and the list of potential tools or weapons is close to endless as well. So, let there be no doubt – terrorism is a potent challenge.

Yet terrorism is by no means the only threat, we are faced with. Industrial accidents – such as the accident in fireworks storehouse in Kolding last year, natural disasters such as hurricanes, and unintentional breakdowns of one sort or the other are other very realistic and potentially just as harmful threats, which we need to be able to deal with.

As minister with responsibility for not just the military defence but also the rescue preparedness – and to top it off a coordinating role with regard to general preparedness in the civil sector in Denmark, I can assure you that Homeland Security and society's general resilience are items high on my agenda.

The vulnerability assessment

In January 2004 we issued a national vulnerability assessment. The report offers an analysis of the balance between - on the one hand risks and vulnerabilities, - and on the other hand the preparedness in place in a number of crucial sectors of society. The analysis, for instance, looks into the areas of

IT- and energy supply, transportation, the health sector and the emergency and crisis management structures.

The conclusion of the analysis is that Denmark has a well-functioning preparedness; yet it also concludes that the threat- and risk-landscape is radically different than earlier - and that it is in constant development.

As a result of the globalised and open society of today, the rapid technological development, the specialisation of services and the interdependencies between central sectors and systems – for instance the financial sectors dependency on the electricity sector –society's resilience to day depends on much more than just robust rescue preparedness, police and defence forces.

The various civil sectors and systems need their own preparedness structures, and we need an overview over the way the sectors depend on one another.

Furthermore, it is a fact that many risks and threats are today international in nature. The amount and speed of global internet exchange, and the amount of physical transportation of goods, services and people exemplify, why for instance the break-out of illnesses, the transportation of oil or the spreading of cyber viruses are international safety problems - rather than national or regional ones.

With regard to security treats, it is likewise a fact that they are international. Terrorism is for instance a general threat to the western world – and to the publics feeling of security all over the world.

This internationalisation of these security and safety issues underscores that the interdependency is not just between sectors in Denmark but indeed a cross- border dependency. This means that the factors, which secure the robustness of our society, are much more complex to day than earlier. It also means that the solutions are also in many instances international.

Det talte ord gælder

With regard to homeland security issues, I want to mention that the EU Commission is for example working on creating a programme for the protection of cross border critical infrastructure. Cross border critical infrastructure is for instance transportation routes, electricity supply and the like. We have not yet seen the actual proposal, but it serves as an example of how international cooperation may be instrumental in elevating national safety.

The conclusion of the vulnerability assessment from 2004 led to a series of recommendations, which we are now in the process of implementing. A central one is that we need to enable ourselves to monitor the development of risks and vulnerabilities facing the civil sectors much closer and what is more; we need a central overview over the cross sector risk-landscape.

The traditional intelligence services are useful and crucial, yet they need to be supplemented with information on other sorts of risks, and we thus need a capacity to gather these types of information.

So far, we've established a capacity in the Danish Emergency Management Agency. The tasks will be monitoring, assessment and counselling. The out-put will be yearly cross-sector vulnerability reports and focused counselling of specific actors.

One of the other central recommendations in the vulnerability assessment from January 2004 is that the cross-sector coordination needs to be better. This we've tried to accomplish by creating various forums. Firstly, we've set up a national coordinating forum, where all the central authorities will meet and coordinate the operative response to a given crisis or catastrophe.

Secondly, we've created a number of sector forums, where associated authorities and actors meet to be informed and inform each other on matters regarding preparedness and resilience.

Thirdly, I will mention that we've gathered both the civil emergency management and the military defence under one ministry - the ministry of Defence. This is meant to create more coordination and synergy. The transfer happened about a year ago, and the preliminary results are good. With regard to both operative and strategic cooperation we've seen a positive development.

As an example, I could mention the huge amount of support and assistance from the military defence to the rescue preparedness during the accident in Kolding last year. I'm sure that the fact that the two systems are now under one ministry has helped pave the way for this joint effort, where the rescue preparedness received extensive assistance from the military and the home guard.

As minister, I'm pleased to see that both the military defence and the rescue preparedness have decided to engage in making the most of the new partnership. Needless to say, we expect much more from the partnership in the coming years. A strong partnership combined with a close cooperation with the other central actors – not least the police – is definitely needed in order to successfully meet the challenges of the present and the future.

Now naturally, the good will and the organisational set-up help to promote cooperation and coordination, yet we also want to ensure a suitable technical platform for cooperation.

Technical challenges

Technically, there are demanding challenges ahead with regard to Homeland Security, which we have to address in order to create more cross-sector coordination, full situation awareness etc. Fortunately, however, technology is not only a problem; it is in many instances also part of the solution.

One of the most obvious technological challenges is the speed with which technology is developing. Today, technical performance is doubled every 18 months. Advances in communication technology are even faster. Even though the technology to process and disperse information in many cases will be available where needed, it takes a lot of effort to keep up with the speed of the development of especially communications technology.

Most nations tend to develop their own Command and Communication Information Systems (CCIS) using national industry. These projects are very often complicated and time consuming. Before the system meets the users, it is in many cases already technologically out of date. Therefore, I find it appropriate henceforward to use “Commercial off the shelf products” to a greater extent - simply to be able to keep track with the technological development. These products may form a cost effective alternative to expensive, from scratch developed systems.

Furthermore, transmission capacity will in few, but important, cases remain an obstacle for many years. This is particularly true in situations such as responses to humanitarian crises, natural catastrophes, and of course military operations. For mobile communications another obstacle is the supply of electrical energy. Battery capacity does not increase nearly at the same rate as information and communications technology, but advances in the so-called “fuel cell technology” may change that in a foreseeable future.

Networks and Network Based Operations

Another big technological challenge is to create and maintain networks that match the demands of today.

Networks have always been important for society. Think of railways, roads, pipelines, power grids and the like. But now they are perhaps more important than ever. In fact the technology based infrastructures are today so important for our lives and our safety that in stead of talking about an information

society, or a post industrial society, we might just as well speak of a network society.

The fast development of information and communication technology leads to new vulnerabilities in society as a whole, and especially in the communication and IT infrastructure. As the infrastructure networks extend far beyond national borders, many of the networks of today are vulnerable to a knowledgeable, resourceful and determined opponent, and this is one of the challenges we have to address in the near future. However, by utilising progress in our understanding of these complex structures, and our knowledge of countermeasures it is possible in a foreseeable future to build robust, secure and flexible infrastructure networks that will serve as the backbone for security both nationally and internationally.

The military concept of “Network Based Operations” that is focus on information and network centricity may be seen as a military response to the technological development in our societies. It is simply the application of information technology to increase mission effectiveness and efficiency. The whole idea is to create an information infrastructure that in principle allows all relevant parties to be connected to a network of networks. This allows for sharing of timely, relevant and trustworthy information. This same concept is of course also applicable to Homeland Security.

Presently, we are in the Danish Defence working on extending the concept of “Network Centric Warfare” to the Danish concept of Homeland security”. We are also in the process of considering how to form a Homeland Security network of networks, that includes emergency services (police, ambulance, fire fighting etc.) and military services.

Architecture and security

When talking about networks it is important to make sure that info-structure investments are not wasted. This could be done by creating and maintaining

an architecture which identifies components and interfaces, and which allows us to acquire communications equipment that at a certain level is interoperable. To achieve this interoperability Command and Communication Information Systems (CCIS) must be based on “plug and play” modules, which can easily be incorporated in the architecture. An increased cooperation with other nations must be established. It is in my opinion not necessary to reinvent the wheel, as other nations or companies have already developed an CCIS architecture and other communication solutions.

When connected to the network one may serve as a service provider - that is to put information at the disposal of other participants, or as a service consumer, the ultimate user of information or other services. Even though this service orientation is more flexible than the usual rigid “push technology” used in many military and emergency communication setups, it never the less creates new vulnerabilities. First and foremost, because communications networks must be accessible to all the different players with relations to Homeland Security.

The safe transmittal of sensitive, and, in some cases, classified, information among a variety of parties requires the development and implementation of communication networks with adequate security.

This leaves us with one tough challenge: Can our desire for privacy and the needs of National Security be mutually satisfied, and is it possible to have a free exchange of information, while still maintaining the balance of secrecy required for National Security? It is in my opinion merely a question of time, before this is technical possible – if it isn’t already possible today?

Interoperability

Different technological standards among operating systems, technical architecture, etc. for computers and within information technology make for big challenges with regard to interoperability.

The physical interoperability of radios has always been a problem, simply because different incompatible technologies serve different purposes. In Denmark we are working hard on solving this problem. We have for example recently formed a cross-sector Committee on radio communication whose main task is to come up with a draft to a technical solution on radio communication for the actors in the preparedness in Denmark. The Committee must look at the new technology to find and investigate true multirole, multiband radios which are mutually compatible. In the future these software radios may be a host for many waveforms and frequencies and thus be an effective bridge between otherwise incompatible networks.

It is, however important to bear in mind, that the problem of interoperability is much more than a technological issue. It has also something to do with political will, resource allocation etc.

Way ahead

The technological challenges presented by Homeland Security are vast, multi-disciplined and multi-dimensional. Some of these tough challenges we are already addressing and have for some time, while others we are just starting to address.

However, we have - as I mentioned earlier - taken the first steps to being "Net Centric", we are presently considering how to solve the problems of security and we are working on improving our ability to communicate by providing a new radio communications system to the actors of the preparedness in Denmark. So all in all, we are trying to meet the different challenges to the best of our ability and will keep on doing this in the foreseeable future.

These were some of my thoughts on homeland security issues.

I'm sure that homeland security will continue to be an area of development and focus is the coming years. I do, however, feel that we've taken some very

important steps, and that we will be able to match the challenges of the future with appropriate solutions.

Thank you.