OFFPRINT FROM *STRATEGIC OUTLOOK 8*

Total defence, information sharing and new interfaces

Ann Ödlund and Matilda Olsson

Serious shortcomings in information sharing between the actors in the total defence can lead to the creation of isolated 'islands' in different parts of the total defence and in different geographical areas, instead of coherent planning and coordination. If information sharing does not work, it will be difficult to answer certain questions from a national perspective, such as 'What do we have?', 'What can we do?' and 'How do we prioritise?' - regardless of whether it concerns planning or action in an actual crisis. Well-functioning information sharing within and between the actors in the total defence is a prerequisite for total defence planning and civil-military coordination.

Information sharing: The glue in the total defence

To be able to plan and make informed decisions, decision makers at different levels are dependent on both specific information and common operating pictures that provide an overview of a particular area, situation or sequence of events. Operating pictures are used in the crisis management system and in military defence, and are based on information gathering, analysis of information, compilations and intelligence. Operating pictures are essentially developed specifically by authorities and other actors in order to understand and obtain an overview of an unfolding crisis or event. This is in order to notify other authorities of the information requested or to provide a basis for common operating pictures at higher levels. Operating pictures are context dependent. Recognised Maritime Picture (RMP) is one such example.

Authorities with specific responsibilities in the crisis management system have an obligation to share information and operating pictures with each other. In turn, these obligations lead to the formation of a network in which information can be shared between actors and administrative or hierarchical levels in peacetime as well as in war. In the case of information for the government in peacetime, each authority, upon request from the Government Offices or the Swedish Civil Contingencies Agency (MSB), must provide the information that is needed for common operating pictures. During a heightened state of alert, the authorities must keep the government informed about the current situation and the development of events within each of their areas of responsibility, as well as about action taken and planned. The Swedish Armed Forces must also receive the data that it needs from the authorities, such as the National Board of Health and Welfare and the Swedish Energy Agency, as well as from other defence authorities, such as the Swedish Defence Materiel Administration and the National Defence Radio Establishment, in order to be able to fulfil its obligation to provide information to the government in the event of a heightened state of alert.

Information sharing and common operating pictures processing can be problematic even in the context of peacetime, as observed during the storms Gudrun (2005) and Per (2007), the forest fire in Västmanland (2014), the terrorist attack on Drottninggatan on 7 April 2017, and the forest fires in the summer of 2018. The problems were technical, due to shortcomings in procedures and uncertainties over how information should be shared within organisations and between actors.

FOI Memo 6862
Project Nr I181103
Approved by Mike Winnerstig

October 2019

The perspectives of grey zone and heightened state of alert place additional demands on actors. In the case of grey zone, there is considerable uncertainty as to whether disruptions or other events are caused by a foreign power, terrorism, sabotage or accident. This uncertainty implies that those responsible for information sharing and for compiling and interpreting common operating pictures are faced with situations that are difficult to assess, where misjudgement risks giving a potential opponent an advantage. Even in the event of a heightened state of alert, where there is a known opponent in the form of a foreign power, uncertainty will remain for decision makers. In addition, there is the case of a war situation or threat of war as a basis for decision making, which means that focus and priorities shift from peacetime crisis management to an activation of the total defence. Information sharing both in a grey zone and during a heightened state of alert, as well as in the transition from peacetime to war, needs to be planned and practised.

What is normal, what is different – and for whom?

In terms of the future conflict environment, an Armed Forces long-term perspective study (2016-2018) states that the year 2035 will encompass a wide range of threats. These hostile activities will include significant elements of non-linear warfare, where the boundary between peacetime and war is blurred and where cyber and influence operations may be included. In the grey zone, attacks need to be detected at an early stage, which in turn requires an overview of both civil and military incidents. The question is, firstly, over which actors should collect such information and compile it; and secondly, how it should be communicated. In the grey zone, it is perhaps primarily a question of the possibility of early warning and the detection of hidden attacks. The study of anomalies, i.e. significant changes in the normal situation, is fundamental here. Intelligence and knowledge about the normal picture in different areas are therefore central to being able to assess events, to create an accurate basis for decision making and to take the most appropriate action. An additional question will be over who has the skills and resources to assess and communicate what is normal in different areas.

Much has changed in recent years when it comes to who owns or operates vital societal functions and critical infrastructure. Skills have been transferred from the public sector to the private sector and there are many new entrants. A clear example of where such a transfer has taken place is in the field of telecommunications. This development implies the need for a fundamental analysis regarding which areas and actors are relevant to the total defence in today's context. In other words, there is a need to take stock of which actors have the knowledge and thereby the opportunity to communicate information about what is normal and what deviates from a total defence perspective.

"Research has shown that there are limitations in national conditions for sharing confidential information, such as between intelligence and security services and the broad circle of authorities responsible for emergency preparedness, for example."

Aside from the particular characteristics of the grey zone, there are two factors that may potentially complicate information sharing. One is private ownership, which may create commercial barriers to sharing certain information, for example. The other concerns the need to maintain confidentiality in the distribution of information. Information sharing and coordination take place in the interfaces within and between authorities and actors. Research has shown that there are limitations in national conditions for sharing confidential information, such as between intelligence and security services and the broad circle of authorities responsible for emergency preparedness, for example. In this case, there are shortcomings in the technical systems for information transfer, cultural differences, limited resources, ill-defined mandates, as well as a lack of a clear boundary between the intelligence system and other authorities. Barriers and lack of trust between authorities or, in this case, sectors are examples of some of the problems.

Building new and changing old

An adequate function for sharing information and processing operating pictures is important for decision making in peacetime, grey zone and war, and its inclusion in the design of the total defence should therefore be ensured. The civil-military interface is central to everything from planning and supporting mobilisation, the supply of essentials such as food, fuel, and electricity, to healthcare and transport. An analysis is required of how civil-military coordination should be directed strategically, effected between central and regional levels, and realised between the Swedish Armed Forces and various civil actors. There is a need to organise a total defence that can provide the conditions for this to be possible.

On the basis of the need for efficient structures for the total defence, the government issued a directive in 2018 for an inquiry into roles, mandates and coordination within civil defence, in order to create clearer conditions of responsibility. This inquiry will analyse and propose a structure for civil defence at central, regional and local level. According to the directive, the proposals should be based on the Swedish Defence Commission's report *Resilience* from 2017, which, amongst other things, proposes a division of governmental authorities into societal sectors, each with a sector-responsible authority. This and other forthcoming inquiries are likely to lead to new responsibility relationships and interfaces between actors, both civil-civil and civil-military. Building new means a chance to design the structures and the allocation of responsibilities according to the needs that exist within the total defence. All in all, the total defence is now being given opportunities for strengthening and improvement, which include not least a basic capability for sharing information.

Functioning information sharing is in everyone's interest

Common operating pictures are created through the compilation of information based on a specific purpose in a particular context, and constitute planning or decision data for both long-term deliberations and operational decisions. If actors lack relevant organisational structures, technology, training and understanding of the purpose and of their own role, information sharing risks being deprioritised. In turn, this may result in important information being omitted from planning or decision data. If the obligation to share information to meet a particular need is one side of the coin, the right to access information represents the other. One side of the coin cannot work without the other. The right to information is discussed less often than is the obligation to share it. The ability to handle confidentiality, cultural differences and a lack of understanding of different needs can constitute barriers.

It should be in everyone's interest to create the best possible conditions for decision makers to carry out their duties, both in planning and in operations. Each actor taking responsibility for their part in a chain of information sharing can ultimately determine what decisions are made. In a situation where time is scarce and the pressure great, decision makers need quick access to relevant information. For information sharing to work effectively in crisis and in war, functioning structures for both peacetime crises and a heightened state of alert must be in place. The design of these structures needs to be preceded by analyses and planning concerning similarities and differences between peacetime and wartime needs. Ultimately, this is a balancing act between the use of known peacetime procedures and structures and a transition to an organisation adapted to the requirements of total defence.

Over the past few years, the total defence concept has changed from being a largely unwelcome guest, both in the crisis management system and in the defence policy arena, to becoming an increasingly central activity whose presence cannot be neglected. Today, there is a greater interest in and commitment to total defence issues, politically as well as among authorities and other actors. This may mean the renewal and improvement of the total defence, where the possibility of information sharing between authorities and private actors would be high on the agenda.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Telephone: +46 8 5550 3000
www.foi.se