OFFPRINT FROM *STRATEGIC OUTLOOK 8*

Sharing sensor data improves management of crises, terrorism and heightened state of alert

Maria Andersson, David Lindgren, Peter Nilsson, Åsa Berglund and Ola Svenonius[1]

In addition to the worsening international security situation, Sweden is at risk of terrorist attacks and an increase in serious crime. Total defence capabilities and crisis management need to be strengthened. Inter-authority cooperation and cooperation with rescue services and the Armed Forces regarding technical sensors and sensor data can contribute to strengthened total defence capabilities and crisis management. However, to accomplish this, the procedures of the authorities need to change.

Strengthening total defence through cooperation

The terrorist attack on Drottninggatan, Stockholm, in 2017, and the forest fires in northern Sweden of 2018, are examples of serious incidents where it became evident that inter-authority cooperation, between various government agencies, is of great importance to ensure an effective crisis response. For example, cooperation makes it possible to create a shared situation awareness, that is, a compilation of critical information provided by several authorities. Shared situation awareness enhances comprehension of the extent of a crisis.

Sensors and the data provided by sensors make important contributions to situation awareness. Surveillance cameras are an example of sensors frequently used by authorities. Sensor data include images captured by surveillance cameras and detection of objects, such as vehicles or number plates. Cameras are positioned around town squares, in underground stations and along roads and railways. In the event of a serious crisis, the rescue services, the Swedish Transport Administration and the police can cooperate in response to camera images and rapidly gain information about the extent of the crisis. Absence of a prearranged procedure for cooperation can delay information sharing, which may lead to the crisis becoming more serious.

Developing a predetermined cooperation procedure regarding the use of sensors and sensor data is an important step towards improved total defence capability. Cooperation regarding sensors can be crucial in ongoing crises or social disruptions, where current, accurate and continuously updated situation awareness is required to avert an event.

Currently, there is no formal cooperation plan involving sensors and sensor data. Rather, cooperation takes place on an ad hoc basis when emergencies arise. When cooperation does take place, it is often based on personal contacts between individual officials at the authorities. There is a great risk that important personal contacts are missing and that the system is vulnerable to staff changes. The consequences of such an ad hoc system is an inefficient use of society's assets, as well as a lack of time and resources to manage any legal or organisational issues that may arise. Efficient total defence capability requires established routines for the exchange of sensor data and a preparedness to share and receive sensor resources from other authorities. Cooperation and collaboration have to function in everyday life in order to function in the event of a crisis.

Government agencies have specific tasks during crisis management and heightened states of alert. They are responsible for the planning of their own crisis and security management. If they have little or no access to sensors, they become particularly dependent on cooperation between authorities in a crisis.

[1] The article is based on research performed in collaboration with the police.

FOI Memo 6863
Project Nr I181103
Approved by Mike Winnerstig

October 2019

FOI

In order for cooperation regarding sensors to be successful, it is of key importance for government agencies, rescue services and the Armed Forces to provide one another with more knowledge about each other's sensors, how they are used and what type of information they can provide. It is also of great value to provide more knowledge about how situational awareness can be improved by using sensor data. For instance, various types of data processing services can facilitate analysis of large data sets or provide a clearer image of an area. Unmanned flying vehicles with mounted cameras, known as Unmanned Aerial Vehicles (UAVs) or Unmanned Aerial Systems (UASs), can be used to collect information about areas that would otherwise be impossible to reach or hazardous to operate in. It is also possible to obtain a quick overview from the air, which is often crucial in a crisis.

The effects of a serious societal crisis are often felt for a long time after the event and far from the location where it occurred – for instance, this was the case after the terrorist attack in Stockholm. Therefore, there is a desire for integrated cameras in railway stations and underground stations, as well as along roads, railways and underground tracks. These types of cameras provide information on how the flow of people and vehicles are affected during a crisis.

> "The effects of a serious societal crisis are often felt for a long time after the event and far from the location where it occurred – for instance, this was the case after the terrorist attack in Stockholm."

Working together on the procurement of new sensors is another form of cooperation that could be of interest to government agencies. A joint procurement process could benefit standardisation, which in turn could facilitate sensor operation and sensor data management. In addition, this might lead to more favourable purchasing agreements, as authorities could use each other's competencies for the specifications about what sensor requirement to require.

Legal challenges

Swedish crisis management is largely based on inter-authority cooperation and cooperation between actors on the local, regional and central levels, as well as between various sectors. The regulations that apply in everyday life also apply in a crisis. The administration of Swedish government agencies is based on authorities having defined tasks and being independent of the ministries and each other. According to various legal regulations, authorities are required to cooperate, but there are no indications as to how. Consequently, situations requiring cooperation could arise, where legal regulations that are applicable to the everyday operations of authorities could hamper effective cooperation.

Another aspect of inter-authority dependency is that authorities are generally bound by confidentiality. Confidentiality protects the information assets of an organisation and the individuals connected to its operations, and confidentiality is transferred to other authorities to a varying extent. The fact that one authority has access to a particular type of sensor or sensor data may constitute sensitive information from a security perspective, as it reveals the capabilities of the authority and thereby the country. Together, this means that confidentiality regulations limit the possibilities for authorities to cooperate.

The General Data Protection Regulation (GDPR), which protects individuals' privacy and personal information, could further complicate inter-authority cooperation. Sensors often register personal information, but according to GDPR, this is only allowed for specific purposes that are determined by the authority in charge of the camera. If personal information is shared, it will be used for a different purpose than originally intended, which may be prohibited. GDPR also forms the basis for the new camera surveillance act, which requires that most authorities apply for a permit to set up sensors.

In summary, inter-authority cooperation regarding sensors is legally complicated, but not impossible. It is therefore important that legal advisors take part in the early stages of the development of cooperation methods and technology, that is, in the planning phase at each respective authority. At this early stage, technology and methods can still be adapted to ensure that cooperation takes place in a successful and legally correct manner. The planning for inter-authority cooperation regarding sensors should take place before the need arises.

Organisational challenges

Cooperation regarding sensors and sensor data is a complex task, and several perspectives need to be considered. These include technical compatibility, legislation, information security, and, not least, harmonising processes. Not all authorities need to work identically, but their interaction and performance of joint activities should be carried out in a manner similar to each other.

Cooperation regarding sensors fundamentally involves an exchange of technology, leaving little room for improvisation. Cooperation regarding technology also requires planning. However, preparing for cooperation regarding sensors is difficult, as no part of the government has overall responsibility. Nonetheless, all government agencies are required to support each other.

Communication and an understanding of each other's operations are prerequisites for cooperation between authorities. Consequently, a joint conceptual framework is required and joint activities need to be continuously performed. Descriptions of sensors and sensor data varies between authorities, which is natural, as their operations and purpose for using sensors differ. One example is what the police and other civil authorities refer to as surveillance systems. In the Armed Forces, these are known as intelligence systems. Another example is unmanned flying vehicles, such as UAS or UAV, also referred to as Remotely Piloted Aircraft Systems (RPAS), or drones in general. These designations are used both between and within authorities. Semantic differences can easily result in confusion and misunderstanding.

Knowing what support can be obtained and by whom is a central challenge. For various reasons, many authorities do not reveal information about their sensors or the performance of them. It is therefore not practical to compile information about them. However, through continuous dialogue and joint exercises between authorities, knowledge about each other's capabilities will gradually increase. Moreover, authorities will become increasingly confident in each other, which facilitates cooperation. Yet, there will probably always be surveillance resources that are too sensitive to share.

By designing common guidelines, the differences between authorities could be bridged and the risk of misunderstandings reduced. These guidelines should include a classification (taxonomy) for various types of sensors and applicable standards, as well as an overall method of cooperation regarding sensors, describing the issues to be addressed and considered. Discussing types of sensors in principle is not as sensitive as discussing real, specific sensors, as performance or weaknesses do not need to be revealed.

Technical challenges

Sensors often generate large data sets. Analysing sensor data manually and identifying critical information in such large data sets is complicated. It is also difficult for a human operator to maintain concentration for the required period of time. Data processing services could therefore be used to support the operator by automatically distinguishing critical information.

Modern sensors are becoming more and more advanced, frequently demanding specially trained operators to manage them correctly and interpret sensor data. It is likely that this will become even more problematic as new and more advanced sensors are introduced. In the future, it will probably not be meaningful to supply the sensor alone, but specially trained staff will also be required. Cooperation regarding sensors thus entails sharing both technical and human resources.

The way forward

Successful cooperation regarding sensors will require a change in the work procedures of authorities. Inter-authority cooperation also requires cooperation between functions within and between the authorities, and on different levels within them. This applies to an exchange of information as well as development of new methods and tools for cooperation. Besides involving legal advisors in the early planning stages of the technical aspects of information sharing, there is also a close connection to the authorities' security functions.

Over time, rapid technological development will provide authorities with new capabilities and challenges, both in terms of technological systems and legally. This will raise questions such as how authorities should manage sensor data sets, how the sensor data should be used and by whom, who owns the information, and when and how it should be visualised.

For cooperation regarding sensors to be successful under pressure, it needs to be developed in an orderly fashion, prior to a potential crisis. Authorities that could reasonably be expected to send and receive sensor data need opportunities to practise. All the cooperation steps to be taken in a crisis must also function in everyday life.

In order to progress, it is necessary for authorities to prioritise the development of cooperation and engage in activities to strengthen crisis management organised by the Swedish Civil Contingencies Agency (Myndigheten för Samhällsskydd och Beredskap, MSB). It is also necessary for authorities to develop a climate of cooperation, where exchange of sensor data and connected resources is regarded as natural and as enriching each party's area of responsibility. To achieve this, it is important that operative units receive sufficient support so that they can immediately start developing ways to cooperate regarding sensors. As a result, in the event of a crisis, established routines would already be in place. If this could be ensured in Sweden, total defence capabilities and crisis management would be considerably strengthened – without major investments.