

Information superiority: Enabling the need to share

Information superiority is becoming an ever more important component of warfighting. The armed forces can no longer work in isolation, and there is an increasing desire to move from a restrictive 'need to know' to a more dynamic 'need to share' culture, which recognises that for modern day missions the group of people requiring access to a piece of information is now much broader and diverse than before. This culture shift, however, presents the MOD with a number of complex challenges to solve.

Andrew McDonald, Eleanor Hepworth
Roke Manor Research Ltd



The nature of warfare is changing; coalition working, technology advances and cost drivers are all impacting traditional modes of operation and equipment development

One consequence of this is that traditional approaches to information assurance are no longer adequate. The need to communicate effectively with coalition forces and NGOs places significant emphasis on the ability to securely share information across organisational boundaries. This issue is made more complex by the apparent need to work closely with civil authorities, who may or may not be trusted.

In addition, in order to respond to evolving threats; rapid evolution and roll-out of new technologies is needed to support changing operational requirements. This in turn necessitates solutions for information assurance and accreditation that enable fast deployment and integration of new technologies with existing equipment.

Finally, the MOD is under continual pressure to develop new solutions in as cost-effective a way as possible. This is encouraging the reuse of COTS standards and communications equipment, with their associated security models and architectures built for commercial environments. These do not necessarily translate directly onto military applications.

Why 'Need to Share'?

The benefits of 'need to share' are illustrated in the following close combat scenario. However, it is worth noting that these principles are equally applicable to the entire battlespace, including air, land and maritime.



Figure 1

Figure 1 shows the initial situation (not to scale). A group of insurgents are attempting to set up an ambush along a key supply route.

Unbeknown to them they have been under surveillance by Special Forces for several days. The Special Forces have been gathering intelligence data on command structures and group membership, all of which is classified as Secret. They are under strict instructions not to engage the enemy, or reveal their presence to friendly, neutral or hostile forces.

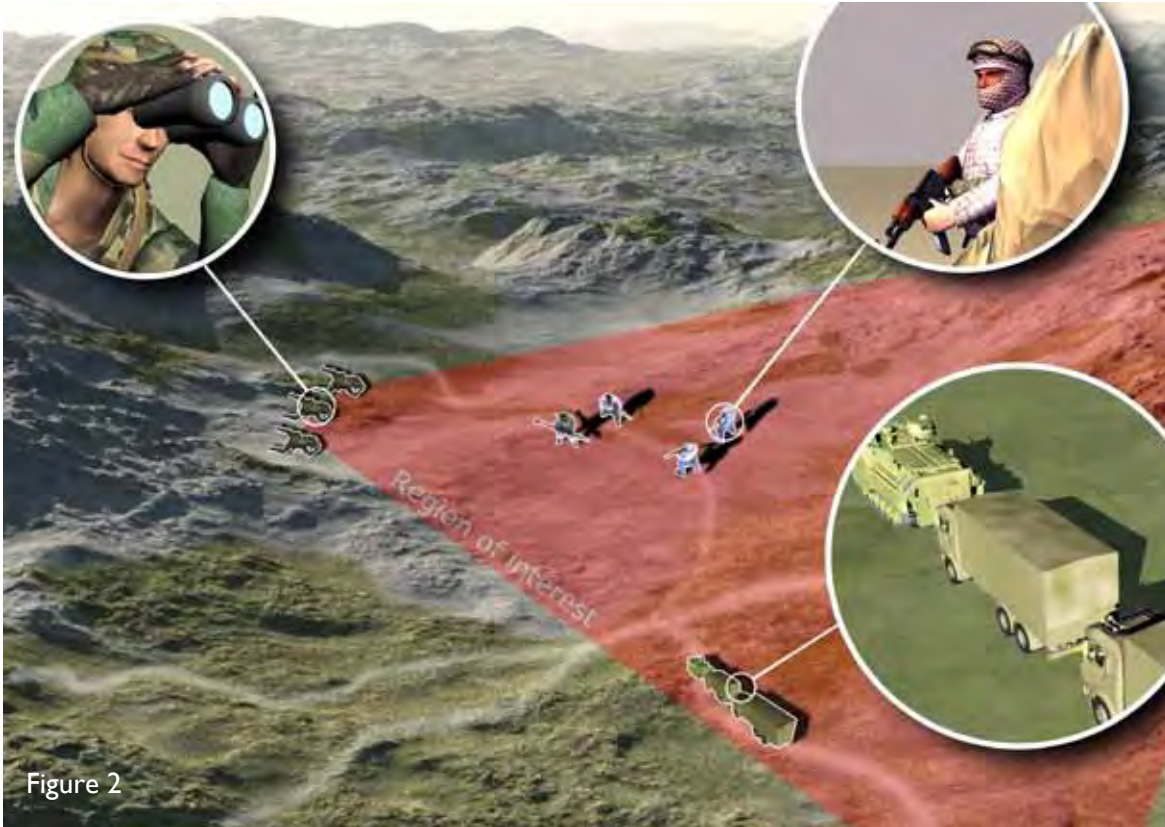


Figure 2

Figure 2 shows the region of interest observed by the Special Forces which includes the insurgents and friendly convoy heading towards the ambush.

There is also a convoy of friendly coalition forces many miles away. They are moving along the road towards the ambush, but may or may not actually go down that specific road. They are currently unaware of either the potential ambush or the Special Forces presence.

Observing the ambush preparations, the Special Forces would clearly like to pass on this information to other friendly forces in the area. However, it is difficult for Special Forces to directly alert anyone to the danger without compromising their mission. Currently, analysts back at HQ identify the danger, declassify it, identify all other friendly forces in the area and propagate the information out to them. In real-time tactical situations such processes can be cumbersome.

The scenario described above illustrates how the ability to dynamically determine the rules related to who can receive information and the enforcement of these rules to control information dissemination are the fundamental pillars for enabling information sharing.

This is vital to the protection of coalition forces and to the success of missions.

Key enablers

The MOD has already recognised the need for a single security architecture that can be used to incorporate disparate security solutions into an overall information assurance capability. To support this, a number of research objectives associated with flexible approaches to information assurance have been identified within the Defence Technology Plan (DTP).

Key to supporting these objectives will be a pragmatic engineering approach that is able to address sub-parts of the problem space and deliver capability over the short term. However, these need to be considered in the context of an overall co-ordinated design activity to ensure that solutions developed near term can be extended and evolved to meet future operational requirements, and that these solutions are cost effective.

For controlled sharing of information, two fundamental enablers can be identified as follows:

- 1) Definition of rules: specifying who can access what information under which conditions.
- 2) Enforcement of rules: ensuring that information dissemination conforms to the rules.

Definition of rules

Information access rules are derived from a combination of factors including mission, nationality, and situation. In environments where coalition forces (as well as NGOs and civil authorities) are working together, the definition of these rules (or policies) in a way that can be rapidly adapted to on-going situations is difficult. Issues include inconsistent definitions of impact levels and protective markings, variations in clearance levels, and how to dynamically assess the risks and benefits associated with the sharing of a piece of information.

Currently, static rule sets are defined that control the sharing of information, and these can be assessed in advance to understand and manage risks. However, in order to allow more adaptive information sharing, these need to be augmented with dynamic rule sets that can be identified and assessed against risks 'on demand'. Two key innovations for this style of operation are semantic labelling of data, and policies that define how labelled data can be combined and transformed. In order to determine how this data can subsequently be shared, new techniques for assessing risks are needed based on a set of rules that define how transformed/combined data can be disseminated. For example, downgrading of image resolution might mean that the image can be shared with an NGO, or providing less precise location information about a sighting of insurgents might allow this information to be shared more widely.

Enforcement of rules

Once a decision to share information has been taken, it is essential that the dissemination of the information is appropriately controlled. This enforcement will have to be conducted at both a procedural and equipment level to prevent unauthorised propagation of sensitive information, as well as providing the underlying encryption needed to retain the confidentiality and integrity of the information in transit.

Issues associated with implementing the above are related to varying equipment capabilities across the coalition, NGO and civil authorities, and the difficulty in proving system behaviour to achieve the required accreditation before system deployment. The changing environment has new threats and vulnerabilities, and although better connected systems offer increased information sharing, they also increase the potential attack surface.

The exploitation of COTS technologies is one way to enable the faster roll-out of new solutions to counter new threats as and when they become apparent. These technologies could potentially include new air interfaces and new security techniques. For example, lightweight solutions to 'bootstapping' encrypted connections, without the overhead of an authentication infrastructure, might provide a 'better than nothing' approach to reducing eavesdropping on communications with an NGO, or cooperative approaches to determining key revocation might allow deployment of networks without the need for on-line, centralised key management systems. However, accreditation of such systems will be difficult without new techniques that can prove system behaviour is as expected. An example of such a technique would be the ability to 'smoke test' the network to ensure data remains where expected.

In addition, more sophisticated network planning and management tools could potentially enable better reasoning about security pre-deployment of a network. This is supported by realtime verification and validation to monitor and enforce policies once the network goes live. A layered approach to risk management can enable 'defence in depth' whereby each layer monitors actual risk and adapts system behaviour to maintain an overall level of acceptable risk.

Conclusion

This paper has discussed some of the challenges facing information assurance as operational requirements evolve and the nature of warfare changes. One of the key capabilities that needs to be supported is more dynamic sharing of information across security boundaries, and the ability to assess the risks associated with dissemination of a piece of information. Whilst a number of research activities are in progress (both within commercial and defence communities), the outputs of these activities need to be analysed, subdivided and roadmapped in order to provide a feasible migration strategy towards future information assurance capabilities.
