Sharing Data over Challenging Military Networks

Lawrence Poynter
Product Management,
iOra Inc,
New York, USA.

Rear Admiral Philip Wilcocks CB DSC DL
Board Advisor,
iOra Limited,
Fleet, United Kingdom.

***Abstract*—This paper describes the challenges for sharing data in deployed environments and how they are then complicated by the performance of the available military networks in ensuring a consistent and holistic view of data. To mitigate the effect of reduced or unavailable network resources this paper then describes a series of strategies that support information sharing and collaboration.**

I. INTRODUCTION

The use of computers and their networks to support military operations has become a fundamental constituent of modern warfare and planning. All global militaries acknowledge the requirement for embedded computer and network operations at the very core of their campaigns. Not only do these systems support the essential command and control, the means by which military commands become spread to the assigned forces, but also record and disseminate intelligence, circulate and control personnel information and manage logistics. Increasingly these electronic records are also used to forensically record the decision making processes where complex military actions can be later reviewed to recreate the information available to the battlefield commander at the point of action execution. Consequently, for the military commander a key requirement is that any decision that he or she makes has to be made on the latest and most relevant operational data. Ensuring that information is current and consistent across all deployed operational sites, irrespective of location, and what is often called the 'single point of truth' is a fundamental information assurance goal. Providing this assurance is exacerbated by a number of constraining factors that have developed over the years to create what has been labelled *the perfect information access storm*.

II. FACTORS THAT AFFECT DATA ACCESS

A. The Web Generation

The modern soldier, sailor and airman come from the information age where in their civilian lives they are used to interacting with responsive web tools delivering social networking, email and the web. Traditional applications built for the military by risk-averse system integrators take many years to reach operational service and as a result fail to share the same level of usability that an individual may experience on their personal iPhone or Blackberry. Consequently users fail to adopt these older format applications where costly training is required and at worst information is inconsistently updated leading to information inaccuracies.

B. The Emergence of the Information Portals

Since the dawn of the new millennium the collation and distribution of operational content in web portals has rapidly become the de facto method for militaries to share and collaborate on data. A portal is a computer environment that is used to presents diverse information to users using a standard user interface. Typically portals were designed to operate over terrestrial connected Local Area Networks (LANs) and typically struggle when users attempt to access these environments over extended Wide Area Networks (WANs) or as is standard for deployments in remote sandy environment's, high latency networks delivered via satellite. In extreme operationally sensitive deployments the simple process of linking computers together is often just infeasible, leading to isolated deployments.

C. Collaboration and the Need to Share

Operational interoperability is a key focus where nations join forces to address a specific strategic objective. Implementing interoperability is fraught with issues where security of access is top of the list. Ensuring that only your closest allies have access to key material is fundamental. In the days of paper documents it was easier to control and manage the availability and flow of paper within the group of permitted and interested parties. The move to computer based recording has created a security dilemma where whole volumes of data can be accessed or re-directed on the click of a mouse. Additionally, as the use of computers by governments matures, interoperability between nations becomes more difficult as individual nations undergo system updates leading to different platforms, versions and file formats. The mixture of platforms causes havoc for those charged with the responsibility of linking nations together, where the platforms themselves have been built by design as single portal silos. This is illustrated by the use of portal platforms that can vary between Lotus Notes, Oracle and Microsoft SharePoint. Even within SharePoint different

nations have standardized on different versions making interoperability and sharing of data highly problematic at best.

D. Global Deployment

Military deployments can be anywhere on the globe – but typically the most remote environments are where the latest high speed networking is not available. Where some form of network is available, it is a given that this will be disabled by one side or the other to diminish the opponent's operational capability. Consequently mobile networking that is delivered as part of the deployment needs to be provided as the backbone of operations and is provided by satellites, UHF, VHF and other methods. Sadly, all of these methods either suffer from high network latency, meaning that they are unsuitable for modern web based applications, or are low in bandwidth, meaning that they are not capable of transmitting the level of information required between sites. In the worst instances these communication methods suffer from both low bandwidth and high latency.

E. Information Congestion

The availability of network resources are also impacted by the sheer volume of data that needs to be transmitted up the chain. The major network hogs include intelligence feeds from covert cameras and UAV, the ever present requirement for video conference down to the tools of collaboration that includes planning by Microsoft PowerPoint where single files run into the 10's of megabits. A single web based portal application can easily have the impact of consuming all of the available satellite bandwidth for its communication requirements alone. Operators need to analyze in detail the data update profile for each of their deployed applications and architect networks that allow for the efficient distribution of information to all points of the network.

F. Limited/Intermittent Networks

Mobile networks provide a unique opportunity for linking globally distributed assets, but their limited bandwidth, high latency and, often for commercial reasons, intermittent availability make them a communication channel that is highly restrictive. This is at its most extreme for many of the forward deployed positions needing to operate in an environment where they have long periods of network disconnection. In these instances updates to operation plans and intelligence need to be synchronised up and down the command chain on a schedule that is dictated by the availability of satellite network connection time. This is a major risk factor in the maintenance of information consistency and requires active management in verifying the accuracy of data.

III STRATEGIES FOR OVERCOMING NETWORK LIMITATIONS

What this means for those responsible for information management is that they fight their own daily battle to ensure that information is consistent across all deployed sites and command posts with guaranteed availability. This is complicated further where deployment-wide network governance is typically non-existent meaning that users often have to speculate on the availability of a network to support their specific operational requirement.

The commercial world has evolved to provide some technology solutions to ease difficult networking environments that include the following:

A. Network Accelerators

Network accelerators are positioned at either end of a network and have the effect of speeding up communication between two points in that network. In general these devices 'intelligently' store repeated network calls issues by the computer so that in effect less data is required to be sent over the network. Most accelerator devices are installed as hardware appliances at each end of the network, although there are some providers that implement a software-only install. These appliances have the effect of typically speeding up network traffic 6 to 10 times. A significant drawback of these devices is that they require a continual network connection to operate and do not proactively forward deploy complete content replica's in the event of network disruption or complete disconnection.

B. Data Compression

Reducing the quantity of data that is required to be sent over the network has a direct impact of the bandwidth usage and commercially the cost of delivery. Various compression tools are commercially available that provide mechanisms for reducing the data footprint of updates so that better use can be made of the available mobile network. The best compression techniques involve extracting redundant data that does not need to be transmitted from the complete dataset as a whole. This is in comparison with far less effective techniques that analyze delta changes to single files in isolation. The effect of compression can be quite dramatic where files, typically based on Microsoft PowerPoint, are being updated, saved as new instances and then propagated over the network. Where content revisions are limited the level of file transmission reduction can reduce from 10's of megabits to the 10's of kilobits, that in turn has a dramatic effect on the requirements of available network when transmitted onto 100 forward units.

C. Content Distribution

To remove the requirement for the deployed user to reach back over the battlefield network to access data, content distribution is used to proactively deploy key data closer to the user so that they do not need to rely on an external network connection. In this way, for example, an operator would replicate updates to the mission plan on a schedule to the forward operating base, so that when required by the commander, they have a local store of information and do not have to reach back to access the necessary data. These local

data replica are either based on the same HQ infrastructure or more increasingly implemented using virtualization technology that reduce the administration overhead for both setting up and maintain the backend portal infrastructure. These virtual platforms can quickly be deployed and re-deployed as and when required.

D. IP Networks over Radio

Extending the use of radio to transmit data in addition to voice has become particularly achievable as part of global deployments. However, although presenting a new communication data channel, the bandwidth available is often too restrictive in terms of its ability to adequately provide a network service for a host of web based applications. Pre-processing and post processing in the form of compression and de-compression is required to expand the set of data applications that can be used over the radio network. One significant bonus of radio communication is the perceived cost savings that can be achieved by transmitted data over radio as opposed to costly satellite based networks.

E. Least Cost Routing

When a force has access to multiple communication routes actively switching between providers of bandwidth using least cost routing is often favored by militaries as a smart way of reducing bandwidth costs and ensuring network availability. This approach has traditionally been used by Navies where the typical scenario is for vessel communication to switch from satellite based delivery whilst operating offshore blue waters, to more cost effective VHF delivery of the same data when in range of shore (typically 50 to 70 miles). The intention with these programs is that the bearer switch be performed seamlessly by the intelligent bearer hub to ensure both cost savings and network consistency.

F. Hybrid

Typically most militaries use a hybrid of the options described above to ensure that content is consistently available to all interested users are their point of need. A common infrastructure is the use of network acceleration devices alongside deployed replica's, where the acceleration provides optimized access during times of network connection and the deployed replica can either provide LAN speed access at the remote end of the network or fulfill a local replica or COOP (Continuation of Operation) server capability in the event of network disconnection.

IV CONCLUSIONS

Significant research and development investment is being expended in all forms of wireless networks to support remote military deployments. The transmission of data both up and down the battlefield chain of deployed command will continue to be a core requirement for global militaries. In parallel the ability for data production at all nodes of the network will increase of the burden on the deployed network and we will continue to require techniques for ensuring that access to key data is provided whatever the location and that information consistency and the single point of truth are ensured.