Network-based operational command and control

MISSION ACCOMPLISHED IN A NETWORK THAT FITS CURRENT OPERATIONS

Joint operations involving modern weapon and sensor systems can be conducted all the way up to the front in real time thanks to complex command and control information systems. The prerequisite is that the underlying data network must have a logical, correct structure and be highly available and secure. However, these aspects are precisely where improvements are needed.

by Jahn Koch, Customer Segment Manager Defence

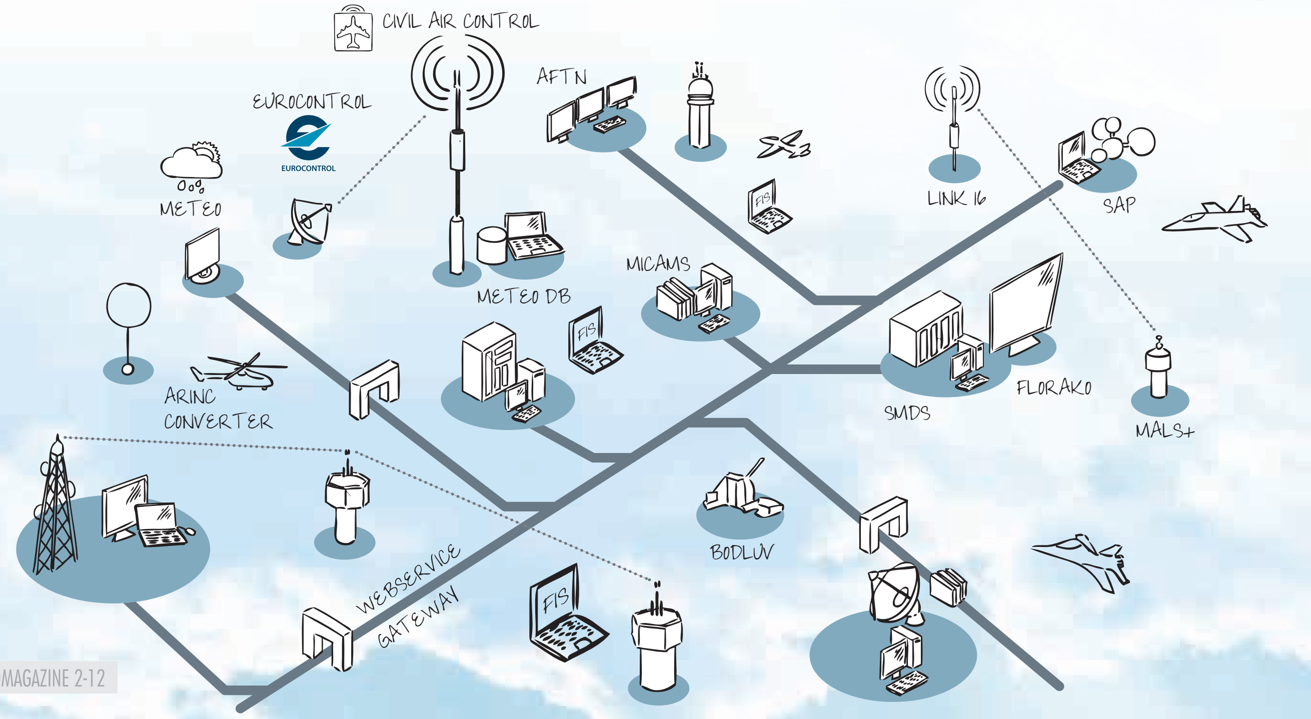
Command and control information systems have been undergoing an extraordinary evolution for years now. They allow large quantities of sensor data to be gathered and compiled in ways that are ever more comprehensive, detailed and, most importantly, reliable and to be converted into a precise operational picture. In addition, there is highly advanced software available today that can give human decision-makers options for action generally within mere seconds using independent concentration and analysis processes. The objective is always to weave together all relevant tactical information to form a common relevant operational picture (CROP) in the medium term whether the data being processed pertains for example to the fuel level of a helicopter, infrared pictures from a reconnaissance drone as a video feed or the health of an infantry platoon advancing on the critical flank in urban terrain. The information is used as a basis for assigning specific tasks to effectors on the ground, in the water and in the air (also in outer space in the foreseeable future) to reach a sub-goal or the final goal of the operation.

This is the theoretical aspiration of today's armies in the national (combined forces) and international (joint forces) environment of large alliances. The reality right now is still more modest in many places. There is a worldwide trend towards network-centric warfare, however. This approach allows the progressive merger of formerly separate branches of the service to forge highly effective task and response forces.

Operational networks: highly available and broadband if possible

At present, network-centric operational command and control posts (also known as war rooms) need one small data centre with a corresponding local network environment for their work from brigade size onwards plus a contemporary command and control information system. The subordinate units and platforms usually have to make do with more meagre data capacities. The smaller the unit and the larger the geographic distance to operational command and control, the more modest the channels for constant information exchange usually are. This is particularly true if the operation takes place on foreign territory, where it is impossible to connect the front with one's own existing fixed-line network infrastructures. The same applies to airspace and the high seas.

The more services and functions are required at an existing low throughput rate and the more information that is fed back in return to operational command and control, the better it is.



The general availability of a connection is indispensable if one has to accept less bandwidth than desired and can use only the most urgently needed interactive services over long-range channels (such as low-bit-rate HF messaging and analogue radio telephony). As a rule, smaller units are connected to operational command and control over highly mobile radio networks. Temporarily "dismounted" staffs of larger units and combat groups are frequently connected over partially mobile microwave link networks. If the operation takes place in one's own territory, one can often resort to existing backbone networks. From an operational standpoint, they are particularly suitable for connecting high-performance systems such as tactical radar stations and fire control systems. The rule of thumb for modern communication and command and control resources at the front (access level) is this: the more services and functions are required at an existing low throughput rate and the more information that is fed back in return to operational command and control, the better it is.

Lurking dangers of electronic warfare

Operational networks are highly mobile at the tactical level (at the edge) of combat units. Whenever possible, they connect seamlessly to the operational level with their own resources, generally employing radio integration. They are secure to the extent that they move in a way that keeps them sealed off from other networks and have only a small number of defined transitional points into larger networks of the same military operator. Effective cryptologic protection and additional electronic hardening measures such as frequency hopping, for example, are required as well as a transmission capacity adjustable to tactical needs (field strength superiority versus detectability). Otherwise, they are at the mercy of blows from opponents waging electronic warfare (EWF). It is relatively easy to locate transmissions with physical means, to disrupt them or to put them in to disarray. Or the transmitted contents can be captured and compromised – with fatal consequences for one's own troops and mission success.

Radio equipment commonly used today has standardised cryptographic protection (generally software-based). This fact does not enhance security, however, because the products of different manufacturers are not fully compatible with each other. The situation is further exacerbated by political regulations on exporting and handling encryptions in various regions of the world. The same risk exposure exists analogously wherever an opponent can gain access to one's transmission media, i.e. also to fibre-optic and wire connections. Operational networks at the lower tactical level, for their part, are rarely exposed to the frequently evoked danger of cyber attacks as long as they have no other network transition points than the ones provided for. The associated principle is as follows: "Protected and only to the next highest operational level".

Connected to the top command over the data highway

Certain powerful sensors, weapon systems and platforms that generate a high data volume must be connected directly to the core, i.e. to the broadband strategic command and control network. Like the radio integration points, they are generally connected through temporary microwave links or are directly connected electronically or optically as part of the permanent military infrastructure (especially in the case of permanently installed sensors such as radar stations). If the operational network also has permanent command and control network infrastructures – often referred to as the backbone – the war rooms are also connected to them. This is the case throughout most developed countries. If there is no permanent fixed-line network, the partially mobile "dismounted" level of the operational network (often microwave in this case) forms the top and most powerful conclusion of the operational network.

The people with operational responsibilities and battle commanders are connected through the backbone to their superiors in the strategic and political command of an army or multinational combat force. This top command does not control the course of the operation directly but instead by specifying targets and goals. As part of the military administration, the top command typically operates on its own conventional fixed-line network structures. However, these structures are usually independent sub-networks separated from the civilian portion of the network and protected with additional hardening and logical zone transitions. Cyber attacks can sometimes inflict severe damage to this part of the combined network, commonly called the standby network, without protection guaranteed to be at the highest security level. The standby network is therefore amongst the critical infrastructures of every nation regardless of its civilian or military users. ■