Chapter 9 – NATO REQUIREMENTS MATRIX

Referring to the following documents:

- RTO programme and NATO requirements [18];
- DCI (Defense Capabilities Initiative) document [19];
- LTR 0402 (Advanced Intelligence Network System) [20];
- LTR 2940 (Command & Control C2 – Joint C3I) [21];
- LTR 0430 (Rapid Environmental Assessment) [22]; and
- SACEUR 2030.7/SHPRJ/00 and SACLANT HC-02/Ser NC 0012 (Requirements from the Strategic Command) [24].

We present here in a concise form the NATO requirements and respond with the relevant comments as applicable in the context of the wireless technologies discussed in this document.

9.1 COMMAND AND CONTROL: DEPLOYABILITY OF COMMAND, CONTROL, COMMUNICATIONS AND INFORMATION SYSTEMS (C3I) – FLEXIBILITY OF MOBILE FORCES

The technologies described have as prime goal to serve deployability by ensuring the desired communication possibilities in a rapid, flexible and robust way. The ad-hoc features emphasized in this report serve not only the initial setup but also subsequent movement scenarios for forces and command posts.

Main contributions come from:

- Ad-hoc networking;
- Handover inside the same (military) WPAN/WLAN system; and
- Vertical handover between of different kinds of military WPAN/WLAN systems and cellular networks-civilian or military/public authorities.

The last point refers in particular in urban warfare and antiterrorist operations.

Moreover urban operations need additionally:

- Penetrability of the basic radio technologies for operation inside buildings and/or underground (e.g. UWB as discussed);
- Low frequency bands and narrow bandwidth; and/or
- Setting up relaying mechanisms in a very rapid manner (meshed networking and/or handover techniques).

International standards as described will enable connectivity of equipment from different NATO countries.

9.2 COMMAND & CONTROL: RAPID ENVIRONMENTAL ASSESSMENT (e.g.: FOR WARRIORS)

Sensors and sensor networks serving dismounted soldiers are considered as primary equipment to be served by military. The salient characteristics are:

1) Very low power devices and very short distances (UWB and Bluetooth) as part of a PAN (Personal Area Networks) of an individual warrior; and
2) Low power density communication and larger distances for extended sensor networks.

Security considerations and ESM not important for i. because of extremely short range.

Presenting a unified assessment picture to involved warriors are served by the technologies discussed, in particular via:

1) 802.16 (broadcast, multicast);
2) 802.16 and its mobile extension (for roaming); and
3) 802.11a&b if the same WLAN is moving as a whole (without roaming).

Some drawbacks and hence desirable/necessary improvements, additions and adaptations are:

1) Single point failure of the base station possible (802.16, 802.11 infrastructure mode), whereby ad-hoc routing protocols (e.g. MANET) can enable distribution at application level.
2) Privacy considerations can be presently addressed by encryption enhancements for 802.x (in general) in conjunction with security at higher layers (e.g. IPsec, SSL).
3) Improvement of range is desirable, possibly at the cost of bandwidth by moving to a lower frequency.

For time critical (e.g. firing information) real time assessment is important so that latencies caused mainly by routing updates have to respect stringent bounds. Moreover authentication of the target information source becomes the highest security consideration.

9.3 COMMAND & CONTROL: C2 NETWORK ARCHITECTURES

Ad-hoc routing and wireless technologies provide the main support for flexible network architectures. Contra positioned to this, multiple access techniques displace many of the routing characteristics together with their complexities and problems. By advancing the use of state of the art middleware over such networking infrastructures, a whole new range of applications can be offered down to the last warrior with minimal adaptation effort. This opens also the way to new distributed solutions.

Since all technologies discussed are part of the internet related communication stack, application planning, realization and delivery is greatly facilitated by relying on exclusively internet related developments (three tier architectures for database access, browsers with various plug-ins, etc.).

Increased reliability is achieved by:

1) Flexible routing (a network level feature);
2) Duplication of key functionalities (a middleware level feature); and
3) Provision of location transparency of key networking functions (a network level/management plane feature).

For example routing functionality will be increasingly provided in mobile/low end devices, with minimal infrastructure requirements and at a modest cost.

Wireless (802.11 and 802.16) is expected to replace or to serve as back up to fixed (mainly optically based) interconnection possibilities through ease of installation and reduced costs (as long as bandwidth limitations is not an issue). Approaches of this kind have to be taken into account into any new C2 network architecture design. A concrete and realized case is contained in this report.

9.4 COMMAND & CONTROL: INTEROPERABILITY OF C3I SYSTEMS (ALLIED FORCES / MARITIME, AIR AND LAND OPERATIONS)

9.4.1 Maritime, Air Operations Serving Land Operations

Land operations can initially benefit from an air or ship based command post by employing some of the discussed technologies (e.g. 802.16). Deployability scenarios (as above) can include sea or air based platforms.

Otherwise the discussed wireless technologies do not primarily apply.

9.4.2 Interoperability of Allied Forces

For the benefit of land based operations and the need of common standards, see 9.1 to 9.3.

9.5 COMMAND & CONTROL: CAPACITY OF COMMUNICATION CHANNELS (BANDWIDTH, FREQUENCY SPECTRUM)

The described technologies present an impressive increase in data rates (broadband), and thus open up a whole new range of applications and/or the delivery of existing applications on a much wider and more flexible scale.

This can happen at a relatively low price considering the fact that civilian applications have been the driving force advancing in economic terms the basic technology as well as the available COTS systems and components. This brings also increased need for militarization as each particular application requires. Main additional requirements over and above to what the plain COTS systems can offer concern security improvement, increased range and, low detectability.

Partial military/civilian systems coexistence in the frequency spectrum is a major concern in a several ways:

1) Interoperability with civilian networks, especially in NATO peace keeping operations (positive);
2) Intentional and unintentional interference problems reducing capacity and availability (negative); and
3) Detectability and traffic analysis of wireless traffic pose security risks and open up new terrorist threats.

9.6 COMMAND & CONTROL: SECURITY OF WIRELESS COMMUNICATIONS

Radio and broadcast aspect (monitoring) are the main characteristics differentiating the wireless case from any other fixed and wired environment.

As in other (wired) multiple access systems, **authentication** has to be seen in combination with addressing, low level identification mechanisms and encryption keys (see also additional aspects).

The succession of WEP series of standards improves communication security. In this direction 802.11i deals with dynamic passwords, employs stronger encryption (longer keys) and improved authentication. However management related threats on layer two are poorly covered in the infrastructure node. Denial of service attacks cannot be excluded. Particular protection has to be foreseen to ensure SNMP connections. Additionally the use of secure SNMP should be adopted (rather than the simple versions) to offset the vulnerability of wireless on the physical layer.

Encryption at the lowest layer possible should be the desirable goal, but this would bring new challenges to modify procedures for late entry and actual communication in multiple access systems, beyond that which is nowadays envisaged in the relevant standards. This will conceal headers and will prevent threats based on packet and traffic analysis.

9.7 IMPROVEMENTS OF COMMUNICATIONS AND CONSULTATIONS BETWEEN MILITARY AND CIVIL ORGANIZATIONS (PEACE SUPPORT OPERATIONS)

This calls for a dual approach, i.e. having equipment which is interoperable with civilian systems and in addition contain the enhancements and modifications required to meet military requirements. Hence ideas like software radio could be a long term solution in order to be able to cope with both kinds of waveforms. Handover aspects between different technologies are also crucial.

Another approach is the exploit the ease and flexibility of setting up WLAN islands of restricted radius (even with reduced security characteristics) in combination with ad-hoc networking.

9.8 IMPROVEMENTS IN THE CAPACITY TO OPERATE IN EXTREME WEATHER CONDITIONS (PEACE SUPPORT OPERATIONS)

Mesh structured networks and flexible routing (reducing hop length in case of increased path loss due to precipitation) can solve some of the problems.

Routers have also to be produced in more rugged versions as is customary with more traditional military telecom equipment. The same holds for COTS products (PDAs, Notebooks, antennas, etc.)

9.9 SUSTAINABILITY & LOGISTICS

Enhancement of interoperability through increased standardization and implementation of common communication standards is promoted by the awareness in civilian protocols and relevant products and by identifying their key deficiencies for military use.

9.10 SURVIVABILITY OF FORCES AND INFRASTRUCTURE

This report has reviewed (Chapter 8) the vulnerability of wireless communication and information systems (identification of deficiencies in their resistance to interference and unauthorised access). It has also given some directions to most immediate needs.