NOKIA

Toward efficient full-IP networks for defense

A new approach to address increasing information needs

Strategic White Paper

Digitization of the battlefield and network-enabled operations are at the heart of the “transformation” processes undertaken by the armed forces. They rely on unified networks of information and communication for which interoperability and information security are of paramount importance. The convergence toward full-IP is a major trend, which is expected to grow faster in order to meet the evolving needs of the armed forces.

ceis

NOKIA

Contents

NOKIA

Executive summary

Digitisation of the battlefield and network-enabled operations are at the heart of the "transformation" processes undertaken by the armed forces. They rely on unified networks of information and communication for which, interoperability and information security are of paramount importance. The convergence towards full-IP is a major trend, which is expected to grow faster in order to meet the evolving needs of the armed forces.

The last ten years have been marked by an evolution of the contexts of engagement of the armed forces, which are now more mobile and independent, but also more scattered. In the framework of multinational coalitions, armed forces intervene into theaters whose configurations greatly vary. These interventions require taking into account a growing number of different sources and different formats. The result is an exponential increase in the quantities of transmitted data, which have to be exploited and stored.

The systematic use of drones, geo-referenced positions, satellite images and telecommunication networks are part of today's operations. These technologies also provide a preview of future operations: Robot-borne multiple sensors on land, air and sea will inform the battle space. The internet of Things will be part of the soldier's uniform and will allow access to the necessary information to conduct a mission. The soldier will be able to communicate with drones in natural language to order fire support on moving targets. The increasing number of exchanges in growing areas (logistics, health, daily life in operations) already involves new means of communication enabling the automation, exploitation and storage of these data. The increasing integration of computing and communication technologies, the worldwide interconnections of data networks and the widespread use of pictures and videos are major developments that have profoundly changed the strategic environment. These developments and the emergence of new threats have led to a process of "transformation" in all modern armies. This endeavor is intended to provide armed forces with the necessary capabilities to maintain and, if possible, to improve their operational superiority.

Current infrastructure networks, especially backbone networks, were built very hierarchically. The lack of a comprehensive approach is causing severe operational constraints, particularly in terms of use, deployment, fluidity, interoperability and security.

In this regard, IP/Multiprotocol Label Switching (MPLS) technologies have the ability to create a suitable environment for the interconnection of networks with different characteristics on the one hand and tying together heterogeneous systems on the other hand. They meet the needs and requirements of the armed forces. The architecture of IP networks provides distributed architectures, both virtualized and decentralized, enabling network

resilience, greater centralization of applications, and bringing broadband infrastructure closer to end users. If the transition to IP technologies is already under way, its deployment remains geographically uneven. This transition also requires an adaptation of governance models to strengthen the overall approach and the scalability of military communications systems. .

Operational requirements

The increasing digitization of the battlefield leads to the transformation of military tools and enables the emergences of new practices.

Indeed, the framework of interventions of the armed forces is now, more often than not, joint, multinational, and under the aegis of diverse organizations. Recent engagements also highlight the changing profile of the adversaries.

These adversaries are now politically motivated or religious armed groups, terrorist networks or mafia. The objective of the armed forces is to achieve the isolation, destabilization or neutralization of targets and the rallying of populations by winning “hearts and minds.” The desired end state is the reintegration of crisis-struck populations within the national and the international community.

New technological means

Communications networks generate profound structural consequences in military organizations. They condition and modify their organization and their operational capacity. They provide the military leader with a wide range of possibilities for action over long distances. Thus they strengthen the capacity of the armed forces to surprise their opponents. For example, the U.S. military demonstration of the use of drones in Afghanistan and Iraq, remotely operated from the Cannon Air Force Base in New Mexico, set new modes of action for operations that followed. The ambush of the French armed forces in the Uzbin Valley in Afghanistan has also shown the fundamental role of unmanned aerial vehicles (UAVs) in the acquisition of information and fire support requests and highlighted this critical capability gap.

This convergence of human and technical networks influences the design, planning and execution of military operations. While most armies are structured around military intervention models, their deployments are based on principles related to the characteristics of the communication networks. Their engagements in the field, require them to control their elongations to ensure the coordination of units and the domination of the cyberspace to face potential opponents.

Networks are present at all levels of intelligence, decision and action, and allow real-time sharing of a global vision of the situation. All actors combine their situation assessments and decisions live, to define and implement, together, the best operational strategy.

Decisional superiority for modern armed forces is thus characterized by this ability to control systems and devices with significant elongations as well as the ability to integrate those with allied command systems.

A surge in operational requirements

The three main types of communication networks are:

- Infrastructure networks, linking together other national networks, allies' networks, other ministries' networks and police forces mobilized in the context of global security or crisis missions
- Elongation networks (mainly satellite-based), allowing the exchange of information among the command structures and the forces deployed in operating theaters
- Tactical networks, providing the deployed forces with the necessary tactical communications

The infrastructure network is the backbone network that has the ability to maximize reliability and performance of large-scale, long-distance data communications. In this respect, it must provide, besides the main features of information processing and information display, the following capabilities:

- Interoperability: Interoperability is defined by the ability of several systems to operate together. The multinational and joint nature of operations, as well as the need to ensure the continuity of information flow from the elementary tactical level to the strategic level (end-to-end concept) reinforces the requirement for interoperability among Communication and Information Systems. The digitization of information, real-time sharing of information, the multitude of user applications (voice, data, video, geolocation, etc.) and the emergence of new norms and standards introduce more and more complexity in communication systems. This complexity requires in turn more expertise.
- Quality of service: Users expect a high level of service related to security tailored both to the needs of their information system (bandwidth, transit times, priority flows, data processing times, etc.) and to the conduct of operations.
- Security: The protection of the communication network must guarantee the confidentiality, authenticity, integrity and availability of information.
- Adaptability and flexibility: The variety of military engagements implies modular, adaptable and reconfigurable network architectures compatible with the rapid deployment criteria.

Faster dissemination of information combined with a greater flow of data (from intelligence sensors such as drones, satellite intelligence, etc.) induces a strong demand in additional networks. In addition to sensors-based communications, exchanges related to logistics and health, as well as living conditions in operating theaters constitute a major evolution, which requires implementing specific means of communication.Information exchanges at the tactical level are following a similar trend toward more automation in order to increase the tempo and efficiency of operations.

Larger volumes of data also require the development of storage capabilities and adequate processing tools (databases, automatic processing tools, aid to exploitation, etc.) in order to extract, exploit and store relevant information in a timely manner.

The need for a new approach

Current infrastructure networks have built in a hierarchical way to carry voice, the main purpose of which was to connect static geographic entities. These networks have gradually been adapted to transport data, but their overall architecture has not been modified. Thus, local networks (LANs) and national networks (WANs) were added to meet these operational needs, but at the expense of a comprehensive approach taking into account human and financial resources and operational constraints.

NATO's allies' communication network infrastructures already rely on intranet networks. These networks are based on technologies stemming from the internet. They should allow easy genuine collaborative work through the exchange of information of all kinds across heterogeneous transit and service networks, and through the provision of standardized common services (security, messaging, directory WEB portal, etc.). However, the different intranets are layered and the logical consistencies as well as technological and organizational homogeneity are not properly addressed. Furthermore, these systems suffer from a compartmentalized organization. Indeed, the need to exchange classified information has been satisfied by the creation of ad hoc networks, often limited to the level of the organization. Thus, exchanges with allies (coalitions, European Union, NATO) are mainly realized through specific links.

This situation has led to strong constraints in terms of:

- Use: Any staff officer must now use multiple intranets daily, and exchanges among intranets require excessive manipulation for users and administrators.
- Deployment: The regulations on classified information exchanges require several separated networks.
- Fluidity and processing of information: These are incompatible with current requirements in the conduct of operations.

- Human Resources: Administration, service and maintenance of the networks require expert resources, which are in short supply. The superposition of heterogeneous systems is also very costly to maintain.
- Interoperability: The multiplicity of standards has led to an extreme heterogeneity that undermines coherence without leveraging the benefits of internet technologies.
- Security: The multiplicity of entry points is the first weakness.
- Investment: Acquiring, operating and maintaining such a wide diversity of networks implies very high costs in spite of the growing integration of off-the-shelf equipment.

The next step for NATO will be to expand this IP/MPLS transformation to all the member countries of the Alliance, by fostering a global consistency in the architectural and technological choices for these deployments.

A technological response

To overcome these constraints, the architecture of communication networks can and should be completely revised with the advent of IP/MPLS networks. The architecture of IP networks provides virtualized and decentralized distributed architectures, enabling bigger network resilience, greater centralization of applications, and taking broadband infrastructure closer to end users.

These architectures meet the requirements of current and future military engagements.

Within the new tactical environment of today's operations, it is necessary to have an intranet-type network with a strengthened level of security and quality of service (QoS), and compatibility with operational use and/or exchange of classified defense materials. The introduction of IP-based technology answers strategic and technical concerns. The emergence of global standards for the transport and the display of data is linked to a growing need for information sharing among all actors involved. Organizations should now have at their disposal generic communication tools that allow them to better focus on their missions and goals. Although constraints exist in terms of QoS, internet technologies provide a concrete and a sustainable response to these issues.

Indeed, the IP/MPLS protocol creates a suitable environment for the interconnection of networks with different characteristics and in tying together heterogeneous systems. IP/MPLS technology is becoming a de facto standard regardless of the nature of the subscribers.

Development of IP technologies within NATO

> "Moving to IP has one major advantage for us and that is interoperability."
>
> — Malcom Green, Chief of CAT9 Communication Infrastructure Services, NATO, 2009

The engagement of NATO forces in combat operations and the search for greater interoperability accelerate the systematic use of the IP/MPLS to the tactical levels, until recently little concerned with NATO standardization.

The armed forces operate under a joint command structure and most often in a multinational framework. In this context, and in order to hold a joint tactical situation, interoperability requirements are very strong among the command systems on the one hand, but also among the information systems and combat systems on the other hand. This interoperability requires a strong expertise in the fields of norms, standards and software.

The co-existence of heterogeneous systems currently limits interoperability, in particular at the strategic level.

Currently, the exchange of information between NATO and allied nations are made through a combination of systems connected to the backbone of NATO, called NATO SECRET WAN (NSWAN) or linked via a complex network architecture.

In order to improve the efficiency of exchanges, to reduce human and technical costs and to meet the latest safety requirements, NATO launched two lines of work: greater integration of services on its network and an evaluation of the mode of provision of services to its members. The objective is to make its network architecture evolve toward a single classified network, the NSWAN, based on IP/MPLS technologies.

The Alliance has defined a range of secure information exchange gateways (IEGs), allowing the realization of exchanges among NATO systems and other systems (allied nations, member states of the European Union, members of coalitions) while respecting the security guidelines. The Alliance has also moved forward several programs aimed at transforming its communication systems. For example, the objective of the NATO General Communication System (NGCS) is to support the provision of IP communication services to NATO static and deployed users with significantly increased capacity, improved performance and advanced QoS.

The emergence of cloud technologies

Many applications in the field of administration and management have moved to the public service's private cloud. These applications are many and varied: e-learning, human resource management, business planning, travel expenses management, payment simulation, IT maintenance management,

directory, etc. Yet, despite all these applications, cloud computing is for the moment only used for back office tasks and not for the operational aspect of operations.

The United States Army has opted for a strategy to increase the performance of its information systems based on cloud computing. In recent years it has begun a review of its networks, servers and existing equipment, which are numerous, disparate and obsolete. Among the priority modernization programs of the Army, the LandWarNet program is ranked first with an investment of 1.9 billion United States dollars in acquisition and 546 million dollars in research and development. The project will create a common, joint and secure architecture.

The U.S. Army was motivated by the provision of a wide range of tools and services as well as guaranteed access to information by users at any time and any place, and finally, by the streamlining of information systems.

NATO also has launched a vast program of IT modernization. Within this modernization program, cloud technology is one of the priorities. The goal is to simplify and streamline their cost structure through a few big private data centers and an upgrade of the network capacity and robustness to interconnect its main sites with these data centers. It will build upon existing NATO services such as its communication infrastructure, the NATO cyber incident response center and public internet access gateways. Indeed, in military operations, the cloud can serve as a vital resource for increased cooperation.

The cloud will bring new developments to operational users and can be an answer to new needs. It allows access to remote services, consultation of databases and access to analyses located and stored far from operating theaters. This ability to move stored and archived information and to share data of different natures contributes to leveraging knowledge (video conferencing, podcasts, streaming, blogs, wikis, etc.). But it requires a high-capacity network able to guarantee the required bandwidth for critical applications.

Security is also of paramount importance and can be guaranteed through a sovereign or private cloud via data encryption to enhance the security of shared classified documents. Another possibility is the use of an “internal private cloud” whose administration is managed by internal human resources.

Thus, cloud computing can enable the interconnection of multiple applications. The systematic use of such a technology will lead toward greater interoperability among the different defense information systems. The proliferation of such architecture is giving the communications network an even more critical role, as it needs to guarantee the proper interconnection between the end user and the data centers. It means a network able to

manage on demand the bandwidth, the priorities and the security of the different requests. Software-defined control of IP/MPLS networks is emerging as the most relevant solution, both from a performance and cost perspective, to provide the network with the required flexibility and thus get the most benefit from these cloud architectures.

An adequate solution based on civil technologies

The needs in data transmission (mainly video streams) are constantly growing. The improvement of existing means (radio, lines and satellites) is not sufficient.

In a time of budget constraints, the armed forces must reply on technology developed for civil communications. But military communication networks must also retain the following characteristics:

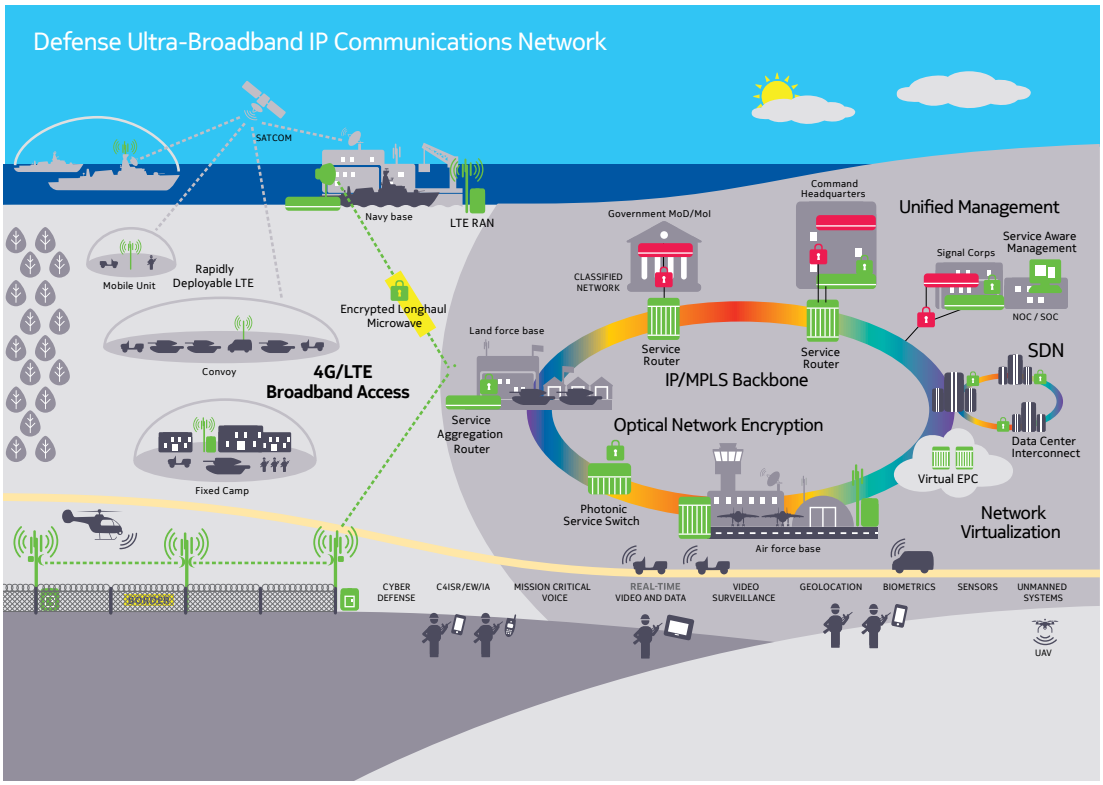
- Electromagnetic discretion
- Mobility management
- Real time
- Resistance to mechanical and weather conditions

The coexistence of civil systems with military systems should be organized. It is necessary to define an architecture and host structures that allow users to benefit from civilian technologies without compromising the overall coherence.

A network architecture combining civil and military technology

A global architecture based on five types of networks is needed. Some can rely on most recent civil technology innovations adapted to the military needs (Strategic and tactical fixed networks), while others have to be pure military technology (tactical mobile networks) or for cost and efficiency reasons are combining both civil and military technologies (satellite network).

Figure 1. Defense ultra-broadband IP communication network

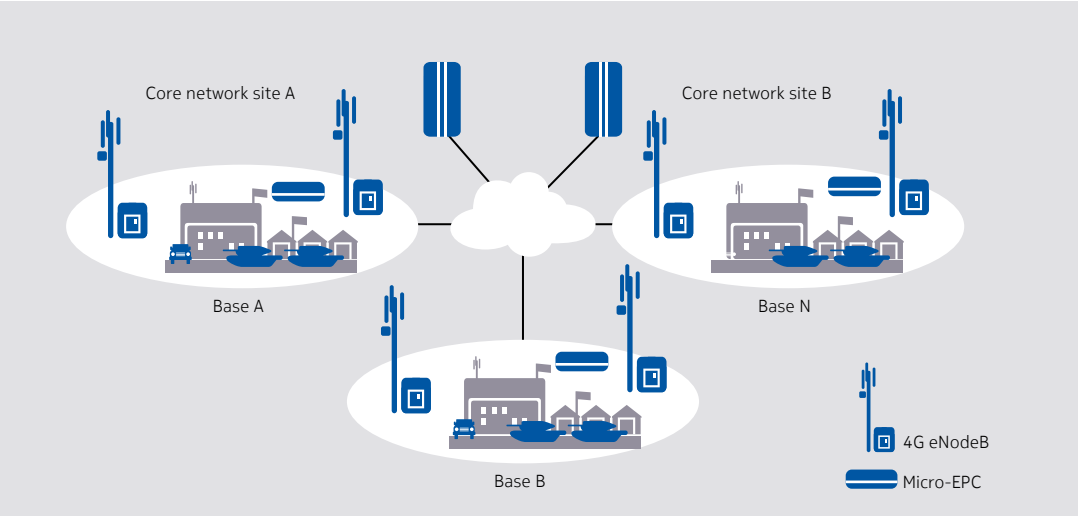


- Strategic infrastructure networks link together other national networks, allies' networks, other ministries' networks and police forces mobilized in the context of global security or crisis missions. They are based on IP/MPLS technology, which provides a scalable infrastructure hosting multiple applications on a single converged network, thanks to throughputs above 100 Gb/s, and solve the interoperability issues. Due to high resilience, they ensure the convergence of video and voice stream and process the operational data in real time. They also help with cloud computing techniques to move centrally an increasing number of business and functional IT applications.
- Deployed tactical networks based on mobile technologies and applications (Wi-Fi®, WiMAX and 3G/4G LTE) provide low security tactical communications necessary to the deployed forces:
  - Radio networks increasingly need high-speed broadband (up to 20 Mb/s), with full-IP and the need to access everything, right away, anywhere.
  - Long Term Evolution (LTE) technology meets the needs of operators (ease and lower cost of deployment, compatibility with IP networks) and those of users (high speed, with throughputs above 100 Mb/s).

- These cellular technologies already allow users from the public security, transport or energy sectors to optimize the performance of existing broadband communication systems. These cellular technologies will provide additional solutions needed in mobile tactical communication. They also optimize the software radio technologies used at the lowest levels

- Military and civilian satellite networks allow the exchange of information between the command structures and the forces deployed in operating theaters. The military satellite network will be secure and resistant to interference. The civil satellite network will be less secure and less resistant to interference, but it will enable the transport of higher volume of data streams.
- A highly secure tactical deployable network resistant to frequency jamming and managing mobility, provides tactical communications necessary to the forces deployed in the field by using the software-defined radio technologies.
- One or more surveillance networks based on civil technologies preserve human resources assigned to the custody and control tasks.

Figure 2. Architecture



NOKIA

A suitable governance

Digitization is at the heart of the transformation process of the armed forces communication networks and evolves with information technology (capacity and speed of treatment, bulk storage capabilities) and communications (cloud software radio), as well as sensor technologies.

However, dual technologies fail to meet all the military requirements because some areas are not covered by civil technologies and require specific studies. Communication networks also evolve according to new uses, resulting in a complex mechanism that requires both monitoring of developments in the civil sector and discerning the specific needs of the military. The systems used by the armed forces can suffer from a discrepancy or obsolescence compared to the ones available in the civil market and can not only jeopardize the operational superiority of the armed forces, but also complicate the appropriation of the systems by future users.

The future of the defense communication networks is therefore subject to the need to streamline and control the overall consistency of IT resources and networks available across all the armed forces. Following NATO's IT and Communication and Information Systems modernization programs, allied nations have also undertaken endeavors to streamline their existing systems into a simplified model.

As such, the definition of future communication networks and their acquisition strategy should take into account the following requirements:

- Streamline existing and future systems through a comprehensive approach at the top political level
- Optimize cost vs. effectiveness of communication systems
- Provide real added value not only to the end user but also to those who are in charge of exploiting and deploying the systems. Thus it should lead toward simplification, openness and flexibility.
- Manage in a progressive and pragmatic way the transition from existing systems to a new generation of systems
- Keep better control of information and of the communication systems, including use of a reliable and sustainable industrial base of vendors and service providers

This is requiring regular analysis to reconcile operational constraints of deploying new technologies, needs for training of network operations team and military forces, as well as budget resources.

NOKIA

Conclusion

Digitization and network-enabled operations are at the heart of transformation processes of the armed forces. They rely on unified communication and information networks, for which interoperability and information security are of paramount importance. The convergence toward full-IP is a major trend, which is expected to grow faster in order to meet the evolving needs of the armed forces. On the technical level, the IP/MPLS protocol creates a suitable environment for the interconnection of networks with different characteristics and in tying together heterogeneous systems. IP/MPLS technology is thus becoming a standard regardless of the nature of the subscribers. The architecture of communication networks can and should be completely revised with the advent of IP/MPLS networks. The architecture of IP networks provides distributed architectures, virtualized and decentralized, enabling bigger network resilience, greater centralization of applications, and extending broadband infrastructure closer to end users.

This strategic white paper was done in collaboration with CEIS

Acronyms

IEG	information exchange gateway
LTE	Long Term Evolution
MPLS	Multiprotocol Label Switching
NATO	North Atlantic Treaty Organization
NGCS	NATO General Communication System
NSWAN	NATO SECRET WAN
QoS	quality of service
UAV	unmanned aerial vehicle
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access

NOKIA

For more information please contact:

Nokia
148/152 Route de la Reine
92100 Boulogne-Billancourt France
'Click here to find out more'
CEIS
280 boulevard Saint Germain
75007 Paris France
http://www.ceis.eu

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: PR1507012672EN