

German Armed Forces' IT System at turning point

Editor's Note

This article comes from the office of the German Signal Allied Liaison at the Signal Center of Excellence. The Canadian Forces, German Army and French Army are represented at the Signal Center with liaison officers. The British liaison Officer is based in Washington, D.C., but visits Fort Gordon regularly. Their mission is to update their countries' armed forces about current and future developments in U.S. Army equipment, doctrine, training and force structure and to keep U.S. Forces abreast of similar operations in their respective forces to ensure seamless mission execution during joint operations.

By LTC Frank Beyer

Until recently, development, procurement and employment of information technology systems were tailored to meet the requirements of a single military service. Coordinated concepts, harmonized structures and procedures designed to produce possible joint solutions were few and far between. So we ended up with so-called island solutions i.e. isolated solutions and a myriad of systems and products.

This situation was further aggravated by long periods of analysis and development that characterized the planned procurement of major IT systems. Additional problems were caused by an attitude that would not accept anything but ideal solutions and functional requirements were often changed during realization due to mission requirements. All of this led to costly adjustment measures and delays or, in the worst of cases, to aborting IT projects.

Thinking and acting in terms of missions!

Keeping our soldiers out of harm's way in theaters of operation may also depend on the continued availability of IT services, that is on the support IT services provide to command and control processes and workflows. While meeting the criteria of efficiency, uniformity, relevance to operations, and quality, it is of paramount importance to take all measures that will ensure uninterrupted and effective availability of required IT services, in particular during operations

when we act together with our allies. We must keep track of the evolving information technology landscape to be able to consistently align the development of German Armed Forces' IT systems to the requirements and priorities of our missions. However, not everything that is technically feasible makes sense.

Prerequisites for further development

In order to guarantee, in the future, a development that evolves along the above criteria, the following prerequisites must be met to determine necessary IT capabilities and possible harmonized solutions to satisfy requirements.

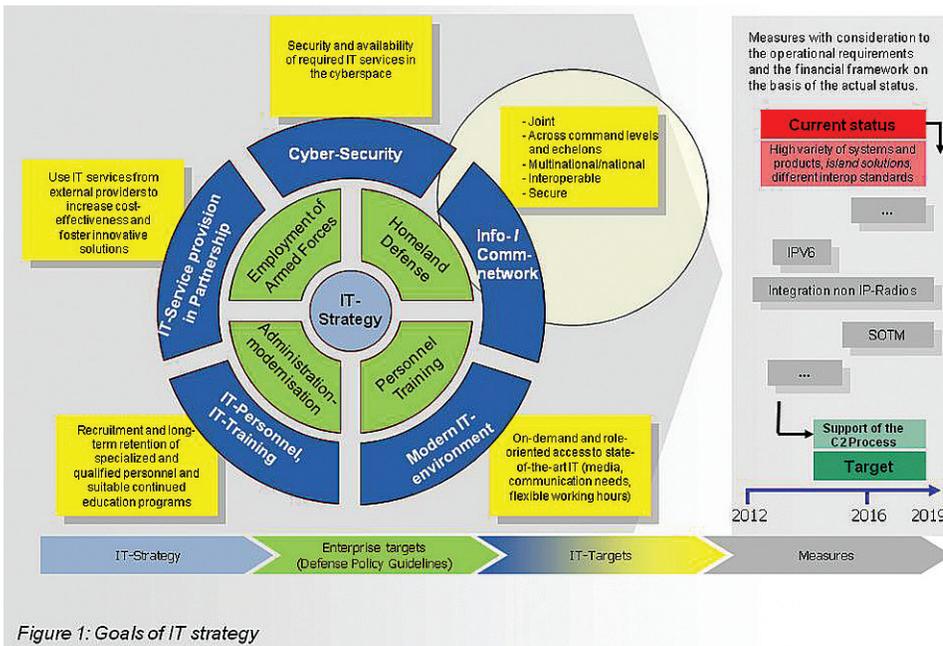
- Commitment of strategic goals defining the long-term alignment of the German Armed Forces' IT system;
- Evaluation and taking into account of operational-level doctrine and lessons learned that will have an impact on the engineering design of the information and communications components of the German Armed Forces' IT system;
- Derivation of capabilities, functionalities and services based on a uniform, architecture-oriented harmonized approach resulting from multinational definitions;
- Creation of a database that can be used for the implementation of this approach.

Conceptual Reboot

The German Ministry of Defense's IT strategy ties in with this approach and is the conceptual foundation for the design and implementation of the German Armed Forces' IT architecture. This conceptual foundation has been adapted to meet the needs of the new structures and processes geared towards the realignment of the German Armed Forces. It defines IT goals and measures required to implement those goals. It sets standards for subsequent documents. In this context, our focus is on the improvement of our mission capability.

One of the main challenges is the provision of a

(Continued on page 42)



technical solutions that do not depend on a predefined structure or mission when called to implement the standards and measures of the German Ministry of Defense's IT strategy, one analysis used an exemplary, scenario-based and architecture-oriented approach. A reference architecture harmonized among the single military services provides the framework. The taxonomy of the NATO Overarching Architecture was used.

The approach used made it possible to arrive -- based on the interacting system triad of "capabilities, functionalities and services" -- at system engineering conclusions and solutions that enable us to implement measures of IT strategy in a timely manner, while meeting budget constraints (five years plus a three-year allowance). A demonstrated engineering solution that ensured our command and control capability exemplified the capability gain.

Using this approach throughout the German Armed Forces, will make it possible to generate consistent, comparable and traceable documentation in the future -- comprising the process from identifying user requirements to selecting German Armed Forces' IT system products and services. The mandatory use of the NATO Architecture Framework and the Bundeswehr's IT Office updated service taxonomy based on current in-theater user requirements are preconditioned. This precise and multinationally uniform description of capabilities and services will make it also possible to combine partial C2 support capabilities in a coordinated fashion and at multinational level (see Figure #2).

Required information processing capabilities
The command and control

(Continued from page 41)

secure joint information and communications network across all levels of command and its compliance with national and international interoperability standards. This is the only way to provide uninterrupted support to command and control processes and workflows across all levels from the homeland to the mission areas while complying with IT security requirements (See Figure #1).

How can we transform the currently available information and communications systems into a near-term, affordable and structurally independent system that also provides us with a network-enabled operations capability?

With this question the Director of the Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support, aptly

defined the principal challenge. The IT strategy provides us the harmonized implementation planning and evaluation criteria for the production of budgetary documents.

To achieve this end, the IT strategy puts an emphasis on defining, evaluating and improving capabilities, functionalities and IT services and also defines parameters for inferring, evaluating and implementing future user requirements as well. The following rationale will be applied. Capabilities are needed by military commanders and users in the mission areas to perform their tasks. Following NATO standards, tasks are associated with so-called services, which are provided by IT products that feature defined functionalities. A service provides task performance support to a user. The service can be made available through different sources and can be requested by different users in accordance with a role and authorization concept. Thus, necessary capabilities and functions are defined by the user's in-theater requirements and do not causally follow from current technical conditions.

In order to produce transferable

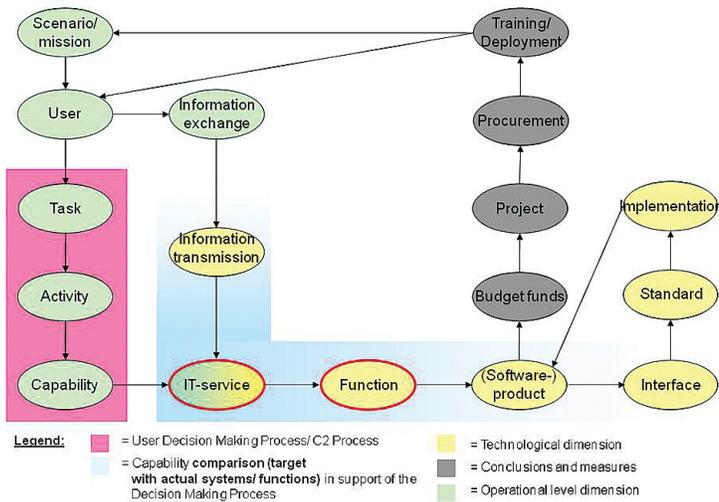


Figure 2: Command and control process capability evaluation

information systems support the user in the application of multinationally aligned command and control processes and workflows for training, exercises, operations and routine-duty activities. It will be crucial to ensure at all times an unlimited capability to work multinationally with allies and partners in mission-specific networks as part of United Nations, NATO, EU or civilian organization efforts while at the same time taking specific military needs into account.

The technological further development of systems must not limit itself to single scenarios or current missions since quite a number of mission scenarios can be envisaged which, given their specific requirements, would go beyond today's missions. Systems tailored to address special tasks and with strictly defined information relationships are not suited to timely react to changed requirements.

Future information processing must meet six core requirements.

- The processing of information must be designed in such a way that it can be integrated into a multinational environment. Thus flexibly providing a network-enabled capability to the most varied constellations of forces, without having to rely on structure-dependent solutions. The latter includes the capability to offer partners our own functionalities and conversely to use their services. This implies that EU and NATO requirements, too, have to be considered.
- IT support must be ensured to assist in accomplishing missions -- and this includes command and control processes and workflows at the operational and tactical levels -- both in a national and multina-

tional setting. This includes the already established services providing support to current missions.

- The provision of user-friendly, state-of-the-art web-based and portal-based platforms (IT hardware and software) to integrate information and collaboration.
- The provision of mission-relevant equipment for defined users in the homeland and the "extension" of the "in-theater" information space into Germany. This includes the possibility to exchange data between information spaces of different security classifications as well as the user's option to retrieve databases already established during routine-duty activities -- and all this must be doable even when on operations.
- The realization of a network-enabled operations capability essentially depends on the technological ability to generate, visualize and access a situation picture that is tailored to the respective levels.
- The realization of the "one-system philosophy" makes it possible for the user to have only one designated point-of-contact for troubleshooting (operation) and requirements (analysis, development and procurement).

Conclusions for further technological development of the C2I systems

The above core requirements encourage a service-oriented alignment of the harmonization and continued technological development efforts.

As far as possible, platform components, services and functions will be established only once. The number of services and service-related interfaces necessary for information exchange must be reduced to a minimum.

(Continued on page 44)

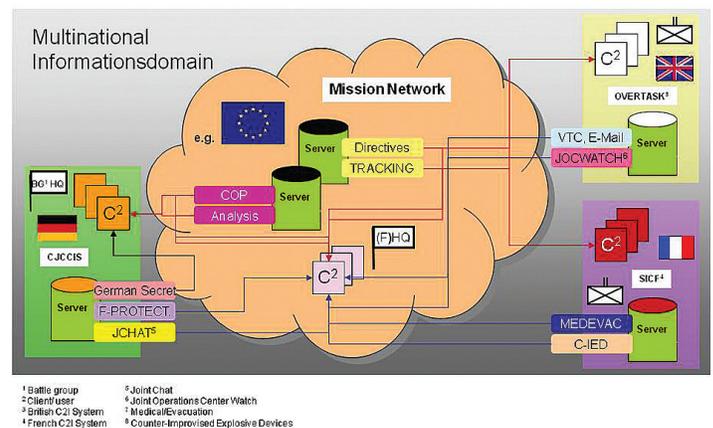


Figure 3: Service-oriented structures

(Continued from page 43)

military organizations must be provided as specific services on the standard platform which also includes the standardized platform services (see Figure #3).

This requires a classification and systematization of the services (including those already implemented) based on a predefined scheme, that is to say, based on the harmonization of taxonomy resulting from the MoD IT-strategy and its reference architecture.

Bridging the gap between mission requirements and tight financial constraints must be accomplished through suitable measures that cover activities in the areas of development, in-service use, training and operation. This includes decoupling of hardware and software components by means of server virtualization and provision of overarching functions and technologies -- already known to the user from private applications or stipulated by NATO and EU regulations. The variety of products must be limited and the GAF will mainly use military off-the-shelf or commercial off-the-shelf products. A holistic operational-level IT service management and standardized German Armed Forces' test activities as well as a centrally controlled training of administrators and users are required.

With the MoD IT-strategy and its related Reference Architecture and Taxonomy, we came also up with possible solutions for implementing the identified necessary measures. The possible solutions comprise an updatable concept for the realization of services and the subsequent migration plan. This is geared towards moving from the

current military service specific command and control information systems to a joint C2I system for the armed forces.

The "Development Plan" from 2012 to 2019

The goal is to provide standardized hardware and software components that work in a joint service environment and across all levels of command and control. The target system will comprise, besides common platform components and joint service applications, functions for specific user groups in terms of engineering (see Figure #4).

Harmonization of the currently existing individual systems will be accomplished in four migration steps from 2012 until 2020. Migration of the existing systems will be accomplished in a low risk mode with short-time parallel operation of single components. To achieve this goal, an overall system approach with a common reference architecture and a common IT service management will be established.

As part of the first migration step, the so-called migration segment sets the starting point for the stationary component of the future C2I system. This segment consists of hardware, operating system and common application software. It provides all users with selected functionalities from the current C2I systems via a portal that supports a harmonized role and authorization concept. The latter concept defines the rules for the access to the data available in the system. Additionally, services

for classified material accounting will be integrated. This requires mechanisms for searching and calling up the services while complying with IT security requirements. At first, the main focus will be on the provision of stationary joint-service functionalities. However, right from the start requirements defining deployable mobile or maritime components and the interoperability of IT services will be considered. We part from the premise that components used in stationary elements will also provide the basis for developments and regeneration measures affecting non-stationary elements. The components will be provided in such a fashion that mission-related changes of user requirements can be responded to quickly and cost-effectively without straining

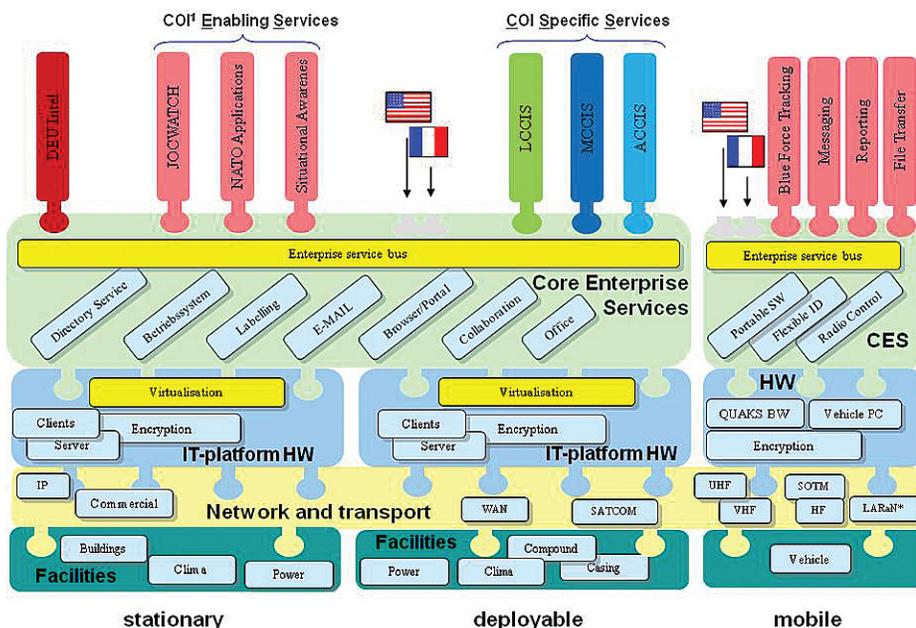


Figure 4: (Layer-)Architecture

¹ Community of interests

development resources. The provision and use of functions across all levels of command and single military services will release financial and personnel resources that can be employed to implement previously nonexistent capabilities.

Migration steps 2 through 4 are aimed at harmonizing deployable (IT in service containers), mobile (vehicle-mounted IT) and maritime (IT on ships) platform components. Wherever it makes sense in terms of engineering and cost-effectiveness, applications will be modularized and supplemented or replaced by standard software and services (see Figure #5).

The following measures are required for migrating the C2I systems:

- Consolidation of requirements of current C2I systems while applying the approach described above;
- Definition of the performance specifications for the first common components of the future C2I system;
- Organizational pooling of Bundeswehr IT Office personnel to provide support during planning and in-service use of the C2I system;
- Organizational pooling of personnel to support and operate the system;
- Establishment of the German Armed Forces' capability during the immediate project phase to set architecture-related and service-oriented standards and guarantee quality assurance.

These measures are the foundation of the specific configurations of a common, modular, flexible, scalable and configurable future C2I system.

Required information transmission capabilities

A feasible networking of information processing systems is always based on a high-performance transmission medium. In

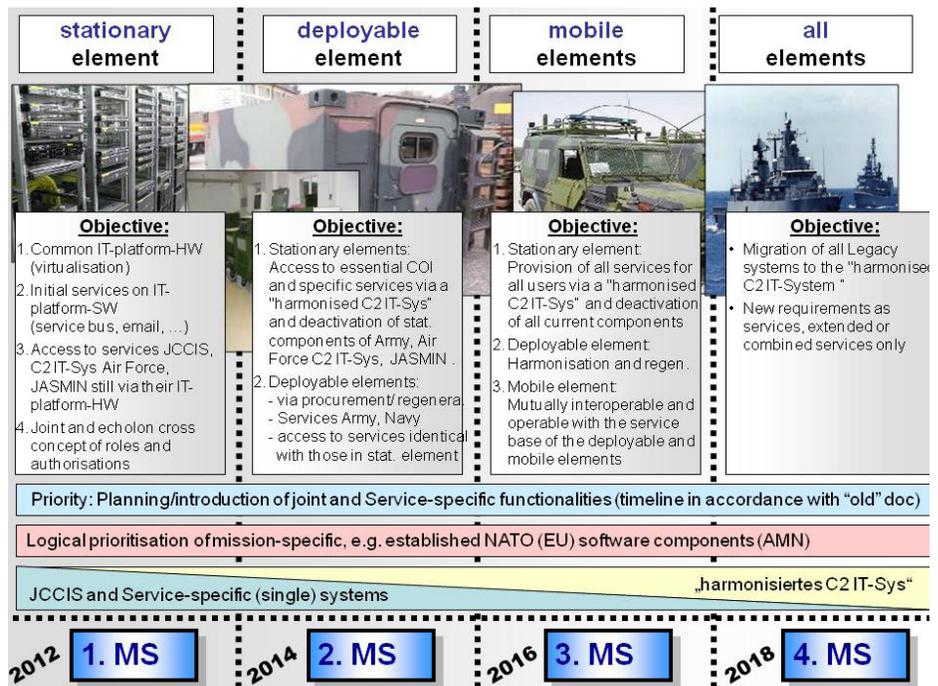


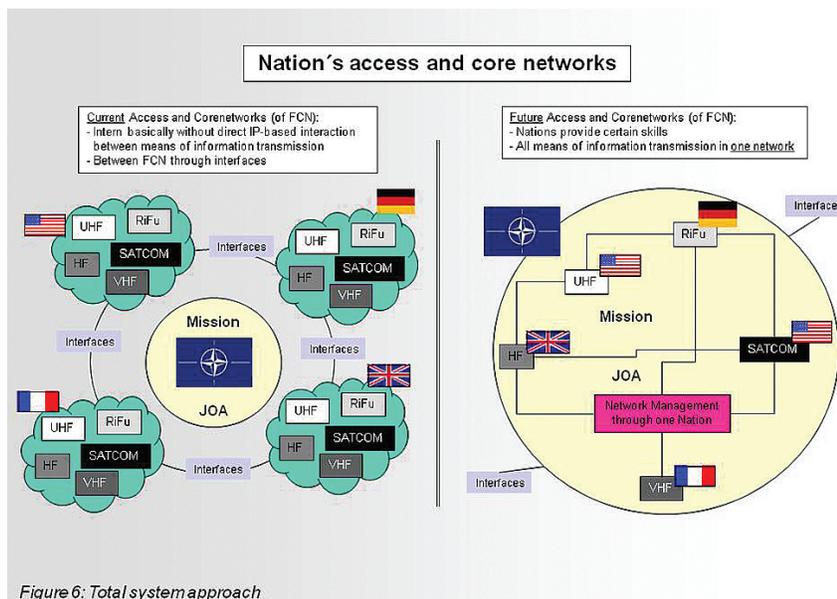
Figure 5: C2I System Migration Steps

conclusion, the information transmission components of the Bundeswehr IT system must ensure the availability of a high-performance, secure and interoperable communications network. This includes the capability to uninterruptedly transmit information by means of tactically mobile and network-capable transmission means. This enables the user to access -- in accordance with the established role and authorization policies -- throughout the communications network the required services via the command and control information systems, support information systems (formerly management information systems) and C2I and weapons control systems.

The network-oriented design requires three core capabilities.

- Combined missions with allied armed forces require a total system approach of multinational interoperability, providing the user with services that feature necessary connectivity, transmission, quality assurance and IT security capacities. A central network

(Continued on page 46)



(Continued from page 45)

management system integrates individual transmission systems into a total system. This makes it possible for the different nations to provide partial capabilities as a service (See Figure #6).

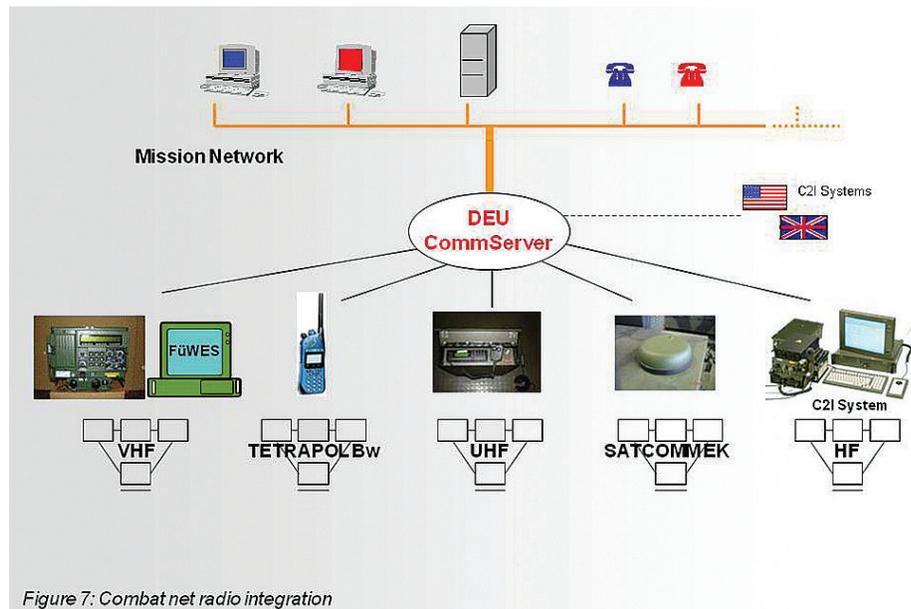
- In the future, we will additionally need transmission means of varying mobility levels without, as far as possible, sacrificing performance.
- The third capability required is the ability to provide uninterrupted, automated transmission between different physical means of transmission. In this context, we must ensure the integration of the combat net radio into a network-oriented communications network (See Figure #7).

Conclusions for further technological development

The possibility of interconnecting all transmission systems -- in particular the inclusion of radio systems -- is the most important capability gain with regard to information transmission. So we can fill capability gaps (e. g. limited VHF radio ranges) or compensate for individual transmission means that are down. Whereas information processing is in its fledgling stage in this respect, some of the required transmission products and systems are already in use or being procured.

The future core network will feature readily available commercial router technology combined with transmission means that ensure adequate data transmission rates. This enables performance of network management, data transfer rate management, quality-of-service mechanisms, control and monitoring functions.

When it comes, however, to access networks, and particularly



to the integration of radio systems, special measures have to be taken for some of them. Successful integration of networks and transmission systems depends on the Bundeswehr's Mobile Communications System and the jointly used components of the Bundeswehr's communications server, which are in the projecting phase. The Bundeswehr's Mobile Communications System is a crucial component of the core network for missions to come. While offering performance features of commercial provider networks, it enables us, in connection with other transmission systems (e. g. Bundeswehr's satellite communications and radio relay systems), to federate all access networks. Access networks are, for instance, subordinate local networks to be federated in a higher-level communications network. Additionally, the system provides -- besides comprehensive quality-of-service mechanisms -- gateways to networks of other nations and organizations as well as to public networks. It enables access to the in-theater information space via

connected C2I and weapons control systems, C2I systems and tactical data links.

A significant capability gap that affects all currently fielded military radio equipment is the missing IP and network capability of these sets. This gap will be definitely closed by the future VHF C2 radio sets -- to be used as part of the Enhanced Future Infantryman System -- and joint networkable radio equipment, in combination with the common share of the Bundeswehr's communications server. New radio sets, such as the joint networkable radio equipment, and the planned procurement of commercially available tactical VHF radio equipment will increase the currently low data transfer rate. All services required by the subscriber, including the simultaneous transmission of speech and data, will be provided in adequate quality. Usability of the joint networkable radio equipment and other IP-capable radio sets also requires the routing functionality and protocol conversion capability of the common share of the Bundeswehr's communications server.

This ensures a transparent gateway for the entire operational communications system of the German Armed Forces.

However, even cutting-edge network technology has its limitations. The failure of single transmission means or signal teams, or even of different systems, can be offset by network technology. However we will not be able to compensate for the failure of a complete system or project (e. g. the common share of the Bundeswehr's communications server). Therefore it is absolutely necessary to develop and field the common share of the

Bundeswehr's communications server and to make the Bundeswehr's Mobile Communications System available in operations abroad.

Future developments and evolutions must be aligned to build a transmission platform that can be used transparently by services and that meets mobility requirements in all mission scenarios.

Conclusion

The German Ministry of Defense's IT strategy is the conceptual basis for the realization of the German Armed Forces' IT. This IT

strategy has been developed along the lines of the new structures and processes that are geared towards the realignment of the German Armed Forces. The IT strategy defines IT goals, necessary technological capabilities and the measures required to realize them. Additionally, uniform standards for future user requirements were defined.

Information processing is improved through a service-oriented alignment, standardized hardware and software and timely and uninterrupted provision of a situation picture. To achieve this goal, current systems must be migrated to a joint C2I system (See Figure #8).

In the field of information transmission, the capability gain is obtained by networking of all transmission networks, in particular by integrating the area of radio communications into the overall communications network. Major milestones have already been reached. Some of the projects, however, currently have risks to their realization due to engineering, contractual and financial constraints.

LTC Frank Beyer has been Chief of the German Liaison Team to the U.S. Army Signal Center of Excellence since January 1, 2013. He previously served as Desk Officer for Plans, Policy and Concepts in the Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support.

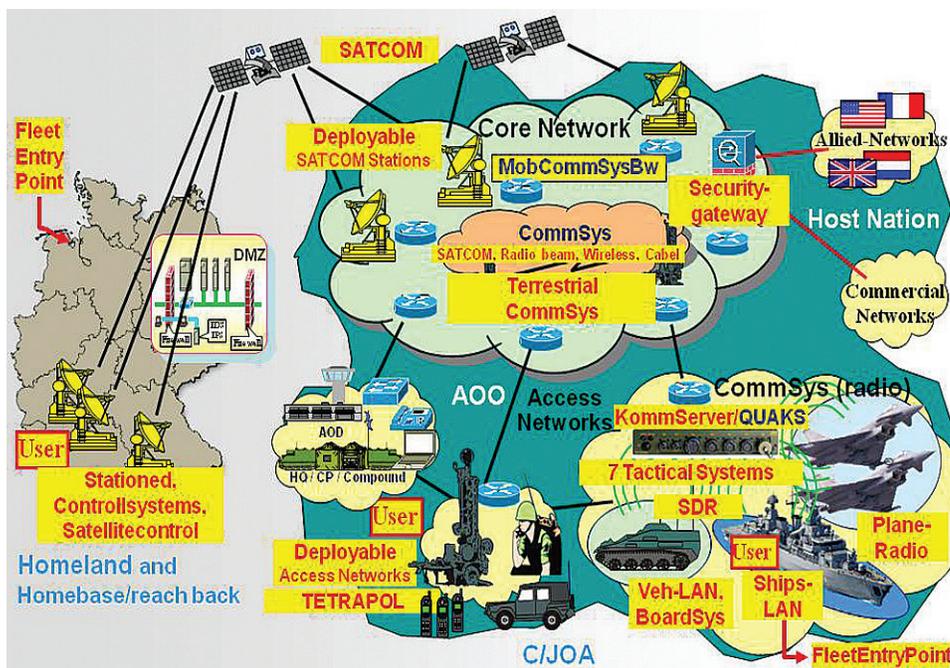


Figure 8: Gains in information transmission capability

ACRONYM QuickScan

AOO - Area of Operations
C2I - Command and Control Information
COTS - Commercial off-the-shelf products
DMZ - Demilitarized Zone
GAF - German Armed Forces
IT - Information Technology
JOA - Joint Operation Area
MOTS - Military off-the-shelf products

MoD - German Ministry of Defense
MS - Migration Step
NATO - North Atlantic Treaty Organization
RiFu - Point-to-Point Radio System i.e. LOS - Line of Sight
SDR - Shortwave Defined Radio
VHF - Very High Frequency