11th International Command and Control Research and Technology Symposium:
Coalition Command and Control in the Networked Era,
September 26-28, 2006, Cambridge, UK

Information Access in Tactical Command and Control Information Systems

Thomas Nitsche

FGAN/FKIE
Research Establishment for Applied Sciences
Research Institute for Communication, Information Technology and Ergonomics
Department of C2IS

Neuenahrer Straße 20
53343 Wachtberg-Werthhoven
Germany

nitsche@fgan.de
Phone: +49 . 228 . 9435 – 505
Fax: +49 . 228 . 9435 - 685

Track: Information Operations/Assurance

Information Access in Tactical Command and Control Information Systems

Thomas Nitsche

FGAN/FKIE
Neuenahrer Straße 20, 53343 Wachtberg-Werthhoven, Germany
nitsche@fgan.de

Abstract

The paradigm of network-centric warfare is a powerful concept to employ the opportunities of modern IT systems. Its aim is to improve military effectiveness by achieving information superiority. In principle, every system or person can communicate with everybody else in the network, where all the information available is shared among the different users.
However, this potentially unlimited amount of information has to be restricted to mission-relevant information in order to achieve a relevant *operational picture. Security regulations and tactical C4ISR systems impose further restriction, due to restricted access to classified information, as well as limitations of bandwidth and local storage in mobile devices.*
Basis, combinable filters are developed to maintain security regulations and support the users of the (tactical) C4ISR system in selecting the appropriate mission-relevant information.

1. Introduction

The paradigm of network-centric warfare is a powerful concept to employ the opportunities of modern IT systems. Its aim is to improve military effectiveness by achieving information superiority [1]. It is based on the global connection of all military systems, ranging from sensors (e.g., reconnaissance systems) over the command and control systems to actors (effect systems). Their combination forms a global information grid (GIG) (Figure 1).

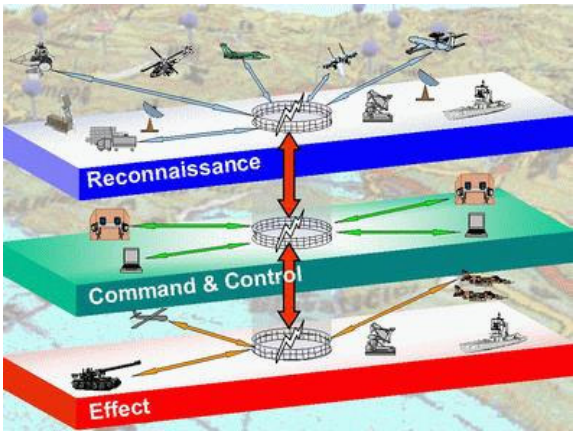

Figure 1 - Combining sensors, actors (effect systems) and command and control systems to form a global information Grid (Figure taken from www.fgan.de)

However, the information available in the information grid can never reflect the full reality. Some information may be incorrect, while other information is still unknown due to limited reconnaissance and intelligence capabilities (Figure 2). It is thus the task of the commanders

to assess the operational (or tactical) picture to give appropriate orders. Similar may hold for the combat units themselves, provided they are allowed to react according to the current situation within the limitations of their mission orders.

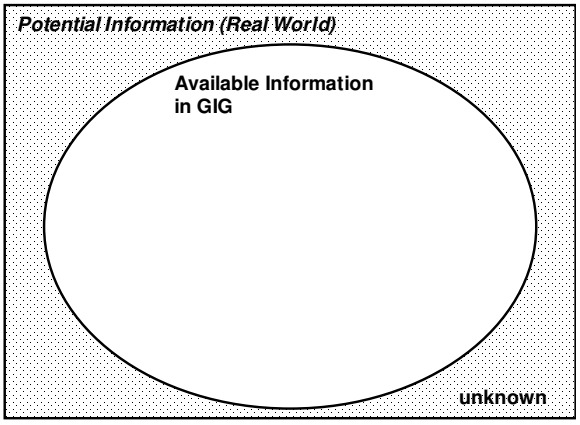

Figure 2 – Available information as part of the potential information space

In the information grid, all available information is shared among the different users. This improves situational awareness and results in information and decision superiority. This improves mission effectiveness and dominating the battlespace [6], because it allows deploying military power more rapidly and effectively.

Even if the command decision takes only a small portion of the overall time of a mission and thus the operation speed cannot be increased drastically, using NCW tools still provides additional advantages. In [8], Kruse et al. describe findings from the execution of air-strike missions in Afghanistan during Operation Enduring Freedom (OEF). Here the time "to fuel, arm, maintain and fly combat missions" was significantly longer than the time for command. But the time gained from using NCW capabilities was used for contingency planning. The enhanced situational awareness thus allowed the staff officers "to do more tactical and strategic thinking" ([8], page 6).

In principle, every system or person may be able to communicate with everybody else in the network. Using an edge-centric approach, it is not always the creator of information who determines in advance whom this information is sent to. While orders obviously have to reach the subordinate units, for other kinds of information each user itself can (and has to) fetch any information he considers useful.

Such a system can be implemented using a publish-subscribe architecture, where the creator of data informs the other participants about its existence (publish). Then the interested users can subscribe the corresponding data elements and can thus download the data. They may even get informed about updated versions of the data elements, e.g., that a specific unit has changed its position.

In this paper we describe how the potentially unlimited amount of information within an NCW information grid can and has to be restricted. Our target application domain is mobile devices used on the tactical level. In Section 2 general rules for gaining a relevant operational picture are given. Section 3 deals with requirements imposed by assuring information security. Additional challenges imposed by tactical C4ISR systems are discussed in Section 4, while Section 5 sketches a possible implementation. Finally, Section 6 concludes.

2. Mission-Relevant Information

Sharing all available information is, however, not sufficient for successfully accomplishing a mission. From the information point of view, using *all* available data leads to an explosion of the information space, which cannot be handled appropriately by humans and computers. Information sharing leads to a common operational picture (COP), which has to be restricted to a common *relevant* operational picture. Such a reduced view of the available information showing only the mission-relevant data with the warfighter needs is a prerequisite for gaining the proper situational awareness and thus for taking proper actions [3].

There are even some situations in which full information provided to the local entities might prevent the execution of actions necessary for successfully completing the mission. In such situations, the actions must be enforced by command authority. Cf., e.g., the discussion in [13] on self-synchronization and the case of Mj. General Ambrose E. Burnside's corps having to cross a bridge under the fire of 450 snipers (Battle of Antietam, 17th of September 1862). In this example, the information about the enemy troops should to be given to the subordinate units such that they can prepare themselves for the ambush.

However, in other situations, the commander may decide to restrict information access. An example may be the case where a unit has to defend its position as long as possible against a superior enemy. Here, the real size of the enemy forces may be concealed from the own troops to prevent desertion or other undesired actions.

The available information is thus restricted to those data relevant for the current mission, where the restrictions may be defined by the subordinate units themselves and/or their commanders (Figure 3).

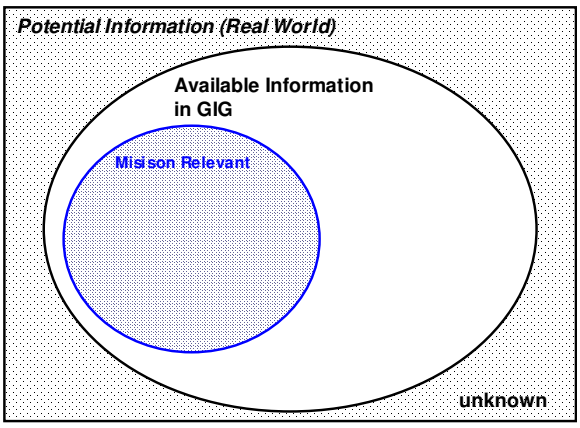

Figure 3 – Mission-relevant data as part of the available information

Criteria for selecting the mission-relevant information include:

- Information category
- The locality of information
- Parts of the command-and-control hierarchy
- Temporal criteria

2.1. Information Category

A first step in restricting the pool of information is to categorize the data. Then the user can select which categories he is interested in and can subscribe to these categories of interest instead of to all available objects.

Information categories include information about own troops (blue forces), enemy troops (red forces), orders, weather data, maps, geo-referenced objects like streets, bridges etc. including their current condition, the political situation, and others.

2.2. Locality of Information

On the tactical level, in general only the near surrounding is relevant for the warfighter. Thus we can in general omit own or foreign forces as well as other geo-referenced objects that are outside, e.g. a *n*-kilometre radius of oneself or outside a certain region.

In the terminology of the C2 Information Exchange Data Model (C2IEDM) defined by the Multilateral Interoperability Program (MIP) [11], data entities with a position attribute like units can thus be omitted if they are outside the selected area.

2.3. Command-and-Control Hierarchy

In general, to execute a certain mission we do not need the full command-and-control hierarchy graph of our own forces including those of our coalition partners and the full hierarchy of enemy forces (as far as they are known). Instead, we can restrict this graph to the relevant parts, which at least include (direct) subordinate units and the commander.

In the case of multinational operations, we also need information about the participating partner units. Such operations require information sharing to a certain degree between the different nations. At least blue-force/red-force tracking, i.e. position information (cf. Section 2.2), are required here. Example missions include combined special-forces anti-terror operations or international coalition forces like in OIF (Operation Iraqi Freedom).

Note, however, that this restriction does not apply to capability lists of vehicles, equipment, weapons or uniforms of own and foreign forces. Although we could omit unnecessary equipment data like, e.g., information about ships on a mission far away from the sea, a (complex) database is still useful as a reference for identifying combatants to avoid fratricide.

2.4. Temporal Information

In a MIP-based data model, no data elements are removed from the database but only marked as invalid by some reporting-data entry which includes time and person who submitted the change. Thus the whole history can be available in the database.

While in the case of mission planning previous operational pictures may be taken into account in order to analyse movements and plans of enemy forces, in a warfighter's mission in general only the current situation is relevant. We can thus also omit out-dated information, like positions of units in the past, and deliver only their current values on the tactical information level.

3. Information Assurance

Security regulations restrict information access to a "need-to-know" basis. A user is not granted access to all information which is available, but only to what is explicitly necessary for accomplishing his mission. This especially holds for classified information. Depending on the classification level, certain requirements regarding the storage and transmission of information apply [5].

Similarly, sharing of information in multinational environments is also restricted by legal regulations (e.g., information classified as "for own nation only") and directives which require special contract agreements between individual coalition partners (cf. [4]). In Operation Iraqi Freedom (OIF), for instance, "coalition forces were often locked out of planning and execution" ([15], page 24) and had to operate as separate entities, since most information was accessible to U.S. forces only.

This further restricts the available mission data as shown in Figure 4.

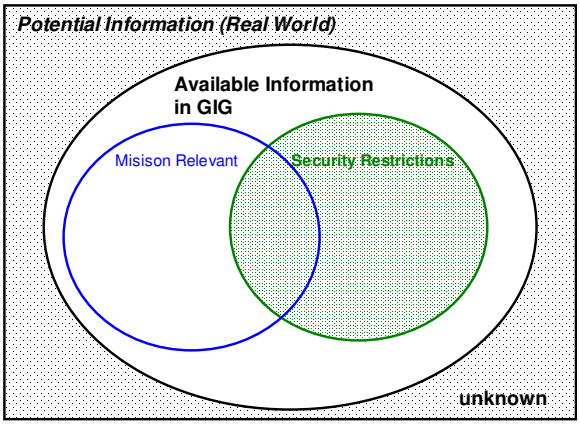

Figure 4 - Security regulations further restrict the mission data

This means that we have to trade the theoretically unlimited access to information within the information grid against the requirements of security restrictions. The broader we allow users to have information access, the more knowledge about the operational picture they may gain which in general improves their situational awareness and mission effectiveness. But such free information access also increases the risk that confidentiality is violated. Thus we have to evaluate the chance of better accomplishing a mission by using better information against the risk of mission failures due to security violations.

3.1. Security Criteria

According to the current DoD directive [5], the five criteria for information assurance are (see also [7]):

- **Confidentiality**: "Assurance that information is not disclosed to unauthorized entities or processes." [1]

[1] Processes within a C4ISR system that retrieve information obviously have to obey the same security restrictions as their accompanying (human) users.

This means that besides information that is releasable to the public, all sensitive and classified data can only be provided to those persons that are allowed to access it. In the case of classified information, this requires a specific security clearance level in order to be keeping such information secret from the enemy.

Confidentiality is ensured by encrypting classified data if transmitted or stored outside a well-protected security area such as in mobile devices used in the field. All communication connections, be they point-to-point, point-to-multipoint (broadcast) or multipoint-to-multipoint (conferencing) connections transmitting data, voice or both or them, have to be secured with appropriate protocols like the Secure Communications Interoperability Protocols (SCIP) [2].

- **Authentication**: "Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information."

  The user authentication in an IT system normally requires some user-identifier and password, but may include more advanced protection schemes using biometrics.

- **Integrity**: "Protection against unauthorized modification or destruction of information."[2]

  Integrity ensures that the data seen by a user is actually the value that was stored or transmitted, i.e. an intruder cannot interfere with the communication and provide some wrong data. Changes of data elements are only allowed by authorized users or processes. To keep track of the changes they should be logged.

- **Non-repudiation**: "Assurance the sender of data is provided with proof of delivery and the recipient is provided proof of the sender's identity, so neither can later deny having processed the data."

  In its strong sense this requires that exchange of and access to (classified) data is logged, such that we can track who has received and/or seen what information.

- **Availability**: "Timely, reliable access to data and information for authorized users."

  While the other criteria above ensure that only authorized users can access any information, and that the data they get is in fact valid, availability ensures that (authorized) users get the requested information if they need it. Otherwise we could hide all information from all users and not deliver any data at all. This would obviously satisfy the first four criteria, but would also prevent the users from successfully accomplishing their missions, hence making the C4ISR system useless.

3.2. Objectives of Information Assurance

The objectives behind the information assurance measures are to keep information advantages or even information superiority, to enable the successful execution of the current and future missions, and to reduce the risk of losses of man, material and (human) sources. Satisfying

[2] See enclosure E2.1.23 in [5] for a wider definition of integrity.

confidentiality, i.e. keeping (classified) information secret from the enemy, is one of the important points here.

However, information assurance is not dealt with for its own purposes but to support combat mission effectiveness. If the security restrictions are too hard to enable an appropriate mission accomplishment, i.e. if the overlapping area in Figure 4 between the mission-relevant data and the accessible data is too small, the decision commander has to compare the value of the information for his forces against the potential value for the enemy if discovered. The aim is to restrict access to the information that is mission-relevant and not "too sensitive" if disclosed.

Besides the criteria already discussed in Section 2, the sensitiveness of the information can also be evaluated according to

- The temporal relevance of information. Here we ask how long is this information important. Positions of own troops are, for example, outdated in hours or days, if the units are moving.

- The locality of adversary counter-operations. If, e.g., the mission orders of a local attack, counter-terrorism operation or rescue mission are revealed to the adversary, this mission may fail. As long as this has only local influence, this is less relevant than revealing whole strategic or operational plans.

- The source of information. This criteria takes, besides the classification level, its source into account, i.e. if it is derived from signal intelligence (SIGINT), HUMINT, ELINT, etc. For example, weather information, although sensitive, can also be derived by the enemy.

4. Challenges of Tactical C4ISR Systems

Tactical C4ISR systems introduce further challenges, as shown in Figure 5.

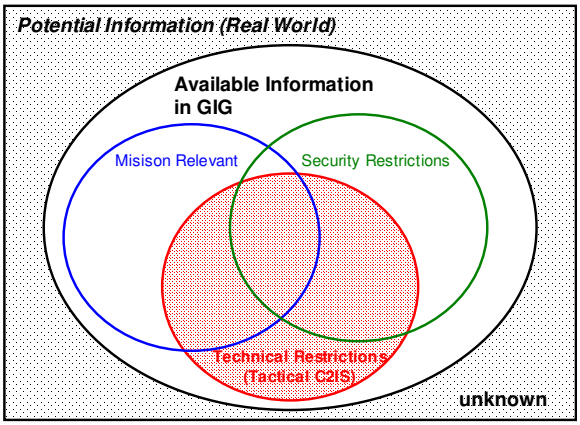

Figure 5 - Further restrictions in tactical C4ISR

4.1. Communication Restrictions

Since the units on the tactical level are in general mobile, they cannot rely on fibre line communication but have to use satellite or radio communication. Here the available bandwidth is

orders of magnitudes smaller the one that is available in higher-level command posts or head quarters. Software-defined radio (SDR) devices used for tactical radio communication only offers a bandwidth in the magnitude of kilobits.[3] Satellite connections offer some more bandwidth, but the long distances impose higher latencies.

Moreover, the bandwidth has to be shared among the different units, so delays for a free communication channel may occur (cf. [15], page 23). Thus we have to limit the amount of communication to higher priority messages and cannot have access to all information we might wish of.

In addition to that, network connections may not be available at all temporarily due to non-cooperative environments. Reasons for that can be shielding effects, e.g. in urban operations, or radio interference by enemy forces. We may even require radio silence in order to hide the own location.

4.2. Storing Information on Mobile Devices

The bandwidth limitations and the (temporary) unavailability of network connections have a negative effect on the availability of services and information. We therefore cannot rely on a C4ISR architecture where all information is stored on (central) servers in the network, since their availability cannot be guaranteed at any time.

Instead of that we have to keep some services and data locally on our mobile devices (see [10] for an example implementation). Examples may include maps, locations of own and enemy forces as well as mission targets. In order to guarantee the availability of mission-relevant information, we have to replicate some of the data.

Unfortunately this affects confidentiality, since parts of the information to be held on the local device may be classified. Such mobile devices may range from PCs installed within a tank or car to PDAs or head-mounted displays carried by the soldier. These devices do not have the same level of protection as those servers installed in head-quarters. Potential security threats include compromising radiation or even capturing the device by enemy forces. This implies that information stored locally might become available to the enemy. However, strong encryption schemes shall give sufficient security in practice for information that is relevant in a certain limited period of time, such that later disclosure does not result in any major security problems.

The risk of revealing information by radiation can be reduced by special harnessed devices. However, we cannot achieve the same level of protection as in securely constructed and checked buildings. If tanks or soldiers are operating in the field and fighting in close proximity to the enemy, distances which prevent radiation signals to be intercepted cannot always be ensured.

In order to limit its consequences we shall restrict the locally stored information such that it is not “too sensitive” if disclosed. Some security directives even do not allow (classified) information to be kept locally at all, but this requirement is actually hard (or even impossible) to satisfy in tactical networks.

[3] Weiss et al. describe a SDR testbed implementation that is capable of transmitting up to 256 kbit/s [14], while a Finish SDR demonstrator only achieves less than 10 kbit/s running in anti jam mode [12].

Storing information locally also affects non-repudiation and integrity, since access to local data should be logged, and changes to data should only be allowed if the user is authorized to do so. In a distributed system using mobile devices that are allowed to work in an off-line mode, we have to design the system such that the soldiers can operate fully locally without having network access all the time. This requires that logging of data access can be done locally. Unfortunately, this may lead to so much data that the local storage capabilities are exceeded. In this case we have to reduce the amount of logging. This can be done by the worst-case assumption that all the data downloaded to the local device may have been potentially accessed by the user. We therefore do not need to explicitly log the access to each data element separately, but consider the whole local database as a single unity.

Similarly, memory and storage limitations restrict the amount of data we can download to the mobile device. While storing data and/or code locally is necessary to be able to work in an off-line mode in the case of unavailable network connections, the available local memory may not be sufficient for storing all the desired information. In this case we have to prioritize data, thus possibly omitting lower priority information.

5. Implementation: Applying Information Filters

We thus have to restrict information access on mobile devices to only mission-relevant and non-critical information by proper filters. According to the "need to know" principle, the unit at least has to know its mission task. For situational understanding and reducing the risk of friendly fire, the positions of the own forces shall also be known. However, to limit the security risks and the bandwidth/storage requirements, this information can be limited to those forces located in the surrounding area of only a specific size. The same holds for the restriction of the command and control hierarchy graph. Other information like reconnaissance results on enemy forces or even strategic plans or human intelligence reports have to be handled with more care.

Basic filters shall be developed to maintain consistent security regulations and support the users of the C4ISR system to select only mission-relevant information.

As discussed before, such basic filters include, among others,

- Category filters deliver data elements of a certain category, e.g. blue-force/red-force.
- Locality filters filter data elements outside certain geographical areas.
- Time filters restrict the data elements to the status of a certain time point, which is either a certain time in the past or the current time, i.e. all data elements will be constantly updated if their value changes.
- Access restriction filters handle security related access control, and omit non-authorized data elements.

These filters operate between the global information grid and the mobile units. They can be applied by either the user itself in order to select the mission-relevant information, by the commander to hide certain information, or by the underlying system itself to enforce the observation of information assurance requirements.

By combining different filters, we achieve complex selection operations. A simple example is shown in Figure 6.

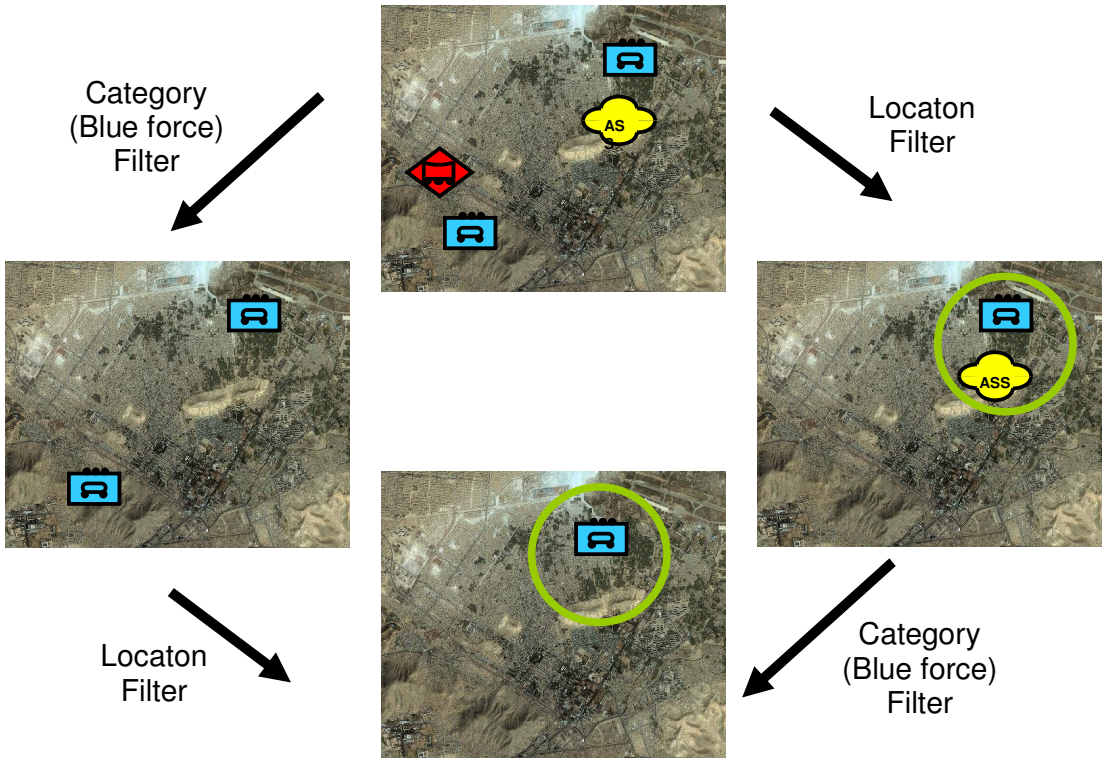

Figure 6 - Combining multiple information filters

Semantically, sequential application of filters as shown above corresponds to their conjunction, i.e. only those elements are passed that satisfy all of the corresponding filter requirements:

$$f_n(\ldots (f_2(f_1(X)) \ldots) = (f_1 \wedge f_2 \wedge \ldots \wedge f_n)(X)$$

Parallel application of filters corresponds to their disjunction:

$$f_1 (X) \parallel \ldots \parallel f_n (X) = (f_1 \vee \ldots \vee f_n)(X)$$

Here the results of the different filters have to be combined to fill the final information pool.

We are currently implementing parts of these information filters into a demonstrational system aimed at evaluating the command process in tactical C4ISR systems [10].

6. Conclusions

The paradigm of network-centric warfare is a powerful concept to employ the opportunities of modern IT systems to improve military effectiveness by achieving information superiority. In principle, every system or person can communicate with everybody else in the network, where all the information available is shared among the different users.
However, this potentially unlimited amount of information has to be restricted to only mission-relevant information in order to achieve a relevant operational picture. Security regulations and tactical C4ISR systems impose further restrictions, due to restricted access to classified information and limitations of bandwidth and local storage in mobile devices.
Standard filters are developed to maintain security regulations and support the users of the (tactical) C4ISR system to select the appropriate mission-relevant information. These simple filters can be combined to more complex selection operations.

Acknowledgements

The author would like to thank Ret. Col. Gerd Dürr, Michael Wunder, Marc Spielmann, Michael Gerz and Sylvia Käthner for providing valuable inspirations and comments.

References

[1] David S. Alberts and Richard E. Hayes. Power to the Edge: Command and Control in the Information Age. CCRP Publication Series, Washington, DC, 2003.

[2] John S. Collura: Secure Communications Interoperability Protocols, SCIP. In *7th NATO Regional Conference on Military Communications and Information Systems (RCMCIS'2005)*, pp. 15-22, October 4-5 2005.

[3] Edward Dawidowicz, Vairzora Jackson, Thomas E. Bryant and Martin Adams. The Right Information … and Intelligent Nodes. In *8th International Command and Control Research and Technology Symposium (ICCRTS)*, Fort McNair – National Defense University, Washington, DC, 17-19 June 2003.

[4] U.S. Department of Defence. DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organisations". http://www.dtic.mil/whs/directives/corres/pdf/d523011_061692/d523011p.pdf, June 16, 1992.

[5] U.S. Department of Defence. DoD Directive 8500.1, "Information Assurance", http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf, October 24, 2002.

[6] U.S. Government Accountability Office. Defense Acquisition – The Global Information Grid and Challenges Facing Its Implementation. GAO-04-858, Report to Subcommittee on Terrorism, Unconventional Threads, and Capabilities, Committee on Armed Services, House of Representatives. July 2004.

[7] Jeff Hughes and Martin R. Stytz. Advancing Software Security – The Software Protection Initiative. In *8th International Command and Control Research and Technology Symposium (ICCRTS)*, Fort McNair – National Defense University, Washington, DC, 17-19 June 2003.

[8] John Kruse, Mark Adkins and Kimberly A. Holloman. Network Centric Warfare in the U.S. Navy's Fifth Fleet – Web-Supported Operational Level Command and Control in Operation Enduring Freedom. In *Proceedings of the 38rd Hawaii International Conference on Systems Sciences (HICSS)*, IEEE Computer Society, January 2005.

[9] John Kruse. Improving Situational Awareness with Collaborative Technologies. In *Proceedings of the 33rd Hawaii International Conference on Systems Sciences (HICSS-33)*, IEEE Computer Society, January 2000.

[10] Sylvia Käthner and Marc Spielmann. A Base Component for Network-Based Service-Oriented C4ISR Systems. In *Coalition C4ISR Architectures and Information Exchange Capabilities (RSO-IST-042-RSY-014)*, The Hague, The Netherlands, 27-29 September 2004.

[11] Multilateral Interoperability Programme. The C2 Information Exchange Data Model (C2IEDM Main), Edition 6.15. http://www.mip-site.org, 2004.

[12] Topi Tuukkanen, Ari Pouttu, Pentti Leppänen (Eds.): Finish Defense Forces. Finish Software Radio Programme. Telecommunication Laboratory/ Centre for Wireless Communications, ISBN 951-42-7187-4, http://www.mil.fi/paaesikunta/materiaaliosasto/liitteet/finnish_software_radio_programme.pdf, 2003.

[13] Ulrich Schade. Towards the Edge and Beyond: The Role of Interoperability. In *10th International Command and Control Research and Technology Symposium (ICCRTS) – The Future of C2*, McLean, Virginia. 13-16 June 2005.

[14] Stephan Weiss, A. Shligersky, S. Abendroth, Jeff Reeve, Luc Moreau, T.E. Dodgson and D. Babb: A Software Defined Radio Testbed Implementation. In *R. W. Steward and D. Garcia-Alis (Eds.), Proceedings of IEE Colloquium on DSP Enabled Radios*, pp. 268-274, Livingston, Scotland, UK, 2003.

[15] Clay Wilson. Network Centric Warfare: Background and Oversight Issues for Congress. *CRS Report for Congress RL32411*, June 2004.