

**10<sup>th</sup> International Command and Control Research  
and Technology Symposium  
The Future of C2**

Topic: **Edge Organizations**

Paper's Title: **Towards the Edge and Beyond: The Role of Interoperability**

Author

Name: Dr. Ulrich Schade  
Organization: FGAN/FKIE  
Address: Neuenahrer Straße 20  
53343 Wachtberg-Werthhoven  
Germany

Phon: +49 228 9435 436

Fax: +49 228 9435 685

E-Mail: [schade@fgan.de](mailto:schade@fgan.de)

## Abstract

*Interoperability is a key condition for network centric operations. Therefore, it is necessary to analyze this concept in all details and to discuss it lively. The paper at hand is meant to contribute to this discussion.*

*Interoperability can be examined with respect to systems as well as with respect to forces. Under the NCW-perspective, the force view is focused. With this in mind, in the paper at hand, the degrees of interoperability are discussed, and, for each degree, examples are given in order to illustrate what is missed at the degree under discussion. Finally, it is argued – on the base of what is missing even under maximal interoperability – that the military equivalent of an edge organization still needs a hierarchical structure to ensure cooperation and synchronization of its parts as well as optimal acting.*

### 1. Introduction

Beside agility, interoperability is one of the two key conditions for network centric operations (cf. Alberts & Hayes, 2003, chapter 7). It is defined as the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together. Although this definition seems to be clear enough, there are at least two aspects of interoperability which deserve further discussion. The first of these aspects even can be taken from the definition itself: Interoperability can be examined with respect to forces or with respect to IT-systems. Under a military perspective, the IT-systems in question are of course C2 systems.

Checking the literature about interoperability, one may notice that both, the *Levels of Information Systems Interoperability (LISI)* as well as the *NATO Interoperability Directive (NID)* strongly focus on the system view. In contrast, the NCW-literature points out that it is the interoperability between forces which determines the profit network centric operating offers. The shift towards the force view also underlines the correlation of both views. This correlation manifests in the insight that the more interoperable the systems are the less the burden of the forces' staffs is. If forces are connected via highly interoperable systems their staff members need not devote their time and labor to close interoperability gaps, but can cope with their primal tasks, instead.

The second aspect of interoperability which has to be discussed in detail is its granularity. Interoperability comes in varying degrees which correspond directly to the levels of network-centric capability as given in the NCW maturity model (cf. Alberts & Hayes, 2003, p. 109). Surprisingly, under the system view as well as under the force view, the number of degrees or levels congruently is set to four. Sometimes, a level is added to denote the absence of interoperability. Thus, a document may mention five levels or degrees of interoperability without contradicting the standard count. Of course, the specific meaning of the degrees, but also the labels used depend on the view taken. Especially, the labels used in the NID are misleading, e.g., the missing of interoperability is termed "isolated interoperability," a kind of nominal contradiction. However, the labels used in the NCW-literature are also somewhat misleading as they obviously neglect the system view. Alberts & Hayes (2003) use "interoperability in the physical domain," "interoperability in the information domain," "interoperability in the cognitive domain," and "interoperability in the social domain." With respect to the system view, this labeling may result in useless discussions about attributing

cognitive and social abilities to the systems. Even more, under the force view, a term like “cognitive interoperability” is also questionable as cognitive processes are involved in order to establish interoperability of degree 2, of degree 3, and of degree 4. Fortunately, Alberts & Hayes (2003, chapter 7) also suggest an elegant solution to the labeling problem by connecting their explanations of the degrees 2, 3, and 4 to language processing. Thus, the interoperability degrees might be labeled by linguistic terms, namely “physical interoperability,” “syntactic interoperability,” “semantic interoperability,” and “pragmatic interoperability,” respectively. The usage of the linguistic terms is also in accordance with the use of one of them, namely “semantic interoperability,” in AI. As a consequence, these terms will be used in the following sections of the paper at hand which will discuss the degrees of interoperability in content.

## **2. Degree 0: Missing interoperability**

According to the NID, missing interoperability means: “*The key feature of Level 0 is human intervention to provide interoperability where systems are isolated from each other.*” In short, systems are not connected. No data can be exchanged. Interoperability is missed, totally. The point to be mentioned, however, is that an operator can close the interoperability gap, e.g., by bringing the data from one system to the other system via CD. In some specific cases, this even might be reasonable, e.g., to preserve security. In most cases, however, operator resources are wasted.

Missing interoperability also occurs with respect to forces if the forces in question cannot exchange any data. The result, often, is disastrous due to uncoordinated actions. For example, during the Israeli counterattack on the 8<sup>th</sup> of October 1973 (Yom Kippur War), the commander of the 162<sup>nd</sup> armored division, Mj. General Avraham Adan, did not receive the information that his advance was no longer supported by parts of the 143<sup>rd</sup> armored division which instead were ordered towards the south at 10:45 a.m. At noon, Adan ordered his forces (namely the brigades 600 and 460) to attack the Egyptian positions and to cross the Suez Channel east of Firdan. The Egyptians shattered the attack and counterattacked. At 2 p.m. the Southern (Israeli) Command eventually noticed the difficult situation of the 162<sup>nd</sup> division and ordered the 143<sup>rd</sup> back. Not before 5 p.m., the first battalion of the 143<sup>rd</sup> arrived. But again, coordination failed, and the battalion engaged a unit of the 162<sup>nd</sup>. Eventually, at 7 p.m., the Egyptian counterattack was stopped. In the end, the 162<sup>nd</sup> had fought, intensely, during the whole day, losing 70 of their 170 battle tanks, while the 143<sup>rd</sup> had spent the day marching (cf. Adan, 1980, for details). In this example, missing interoperability results in an uncoordinated action that endangered a whole armored division. An even worse result missing interoperability among forces can evoke is unintentional fratricide (“friendly fire”). To give a prominent example, Lt. General Lesley J. McNair, chief of the U.S. Army Ground Forces, and more than 100 other allied soldiers were killed by an allied air force operation in July 1944 (Johnson, 1996). In sum, missing interoperability forestalls the synchronization of forces, often with disastrous results. Therefore, missing interoperability has to be avoided by all means.

## **3. Degree 1: Physical Interoperability**

Again, with respect to systems, the NID provides a sounding definition: “*The key feature of Degree 1 is physical connectivity providing direct interaction between systems.*” The systems are connected. Thus, they are enabled to exchange data. This does not mean that the receiver system can process the incoming data; it only gets it. Interoperability of Degree 1, for

example, holds if a WINDOWS system receives a text from a UNIX system written in TeX. Processing of the data received (the TeX text) will cause problems as can easily be viewed by opening the text within WORD. Again, an operator can close the interoperability gap, in this case by a cumbersome transformation of the data. Again, operator resources would be wasted.

With respect to forces, the realization of physical interoperability seems to be the most important part. As soon as communication is physically established, the human intellect seems to add all other interoperability degrees. This is correct – sometimes. As Alberts & Hayes (2003) have explained, the main tool to achieve interoperability is language. With respect to forces, interoperability of degree 1 (but not more) is on hand if the forces are connected but do not speak the same language. For example, during operation „Lam Son 719“ (spring 1971), the U.S. Air Force could not support the operation as planned because the Vietnamese air controllers did not speak English and the American pilots did not speak Vietnamese (Kissinger, 1979). A similar remark appears in the U.S. DoD’s final report to Congress about the first Gulf War: “Community-wide shortage of Arabic linguists affected intelligence, counterintelligence, and liaison efforts” (U.S. DoD, 1992, p. 401).

#### **4. Degree 2: Syntactic Interoperability**

With respect to systems, syntactic interoperability means that the receiver system can process the incoming data, syntactically. A simple method to grant such an interoperability is to enforce exchange standards, e.g. to enforce that data exchanged respect a given XML schema. Syntactic interoperability grants the exchange and sharing of information. However, syntactic interoperability does not grant the exchange and sharing of knowledge. The information exchanged might be interpreted, differently. For example, if information about the movement of a howitzer is exchanged, it might be that one system has a (default) representation of howitzers as self-propelled vehicles whereas the other system has a (default) representation saying howitzers are towed. Normally, operators are not aware of these kind of discrepancies in their systems. Thus, the differences may go unnoticed but nevertheless may add up to errors in awareness, beliefs, and decisions.

With respect to forces, the situation is similar. Since language is ambiguous, elliptical, and vague, humans communicating sometimes interpret the information (verbally) exchanged, differently. The result, again, might be an error in awareness, in beliefs, and in decisions. For example, in the Battle of Chesapeake Bay (1781), Admiral Sir Thomas Graves flew “engage the enemy” but (maybe) forgot to lower “line ahead.” The signal was interpreted differently by the British captains. Some ships opened the fire, others kept the line (Tuchman, 1988). In the end, the French fleet under the command of Admiral François Comte de Grasse seized control of the sea and sealed in the British at Yorktown. The Earl of Cornwallis received neither reinforcement nor supply. His surrender to Washington became inevitable.

#### **5. Degree 3: Semantic Interoperability**

Under semantic interoperability, information is interpreted, identically. In principle, with respect to systems, semantic interoperability can be achieved if the systems use the same data model, e.g., the *Command and Control Information Exchange Model (C2IEDM)* or its future successor, the *JC3IEDM*, both propagated by the Multilateral Interoperability Programme (MIP), cf. <http://www.mip-site.org/>. The C2IEDM also forms the base for Battle Management

Language (BML), another approach to achieve semantic interoperability (cf. Hieb, Tolk, Sudnikovich & Pullen, 2004).

However, relevant parts of data models, especially those which express semantic relationships and semantic restrictions, often are not implemented, but exist as business rules or document descriptions. As long as these parts are not implemented they cannot be exploited by the systems. As a consequence, there still is a window for semantic misinterpretation and ambiguity. According to Dorion & Boury-Brisset (2004) the missing parts can be added. An ontology will be the result which can be used to enhance semantic interoperability. In a similar vein, we developed a system which takes reports written in natural language and interprets them by means of Information Extraction and ontology-driven semantic annotation (Hecking, 2003; Schade, 2004). In general, ontological components are promising tools to achieve semantic interoperability for systems.

If forces exchange information and if the receiver interprets the information in the same way as the sender, situational awareness emerges. However, this is not sufficient for self-synchronization. In addition to the meaning of the received information, the receiver has to understand the sender's intention in order to act as the sender expects him to act. In general, by speech acts (Austin, 1962), the sender conveys her intention, but some speech acts are indirect. The literal meaning differs from intention. Semantic interoperability only ensures that the literal meaning of the exchanged information is shared. The intention is not included. The most prominent example illustrating this difference is the Battle of Waterloo (1815, 18<sup>th</sup> of June). Napoleon had beaten the Prussians at Ligny (16<sup>th</sup> of June), and he did not want them to interfere in his struggle against Wellington. Thus, he detached parts of his forces under the command of Marshal Marquis Emmanuel de Grouchy to "pursuit the Prussians" (17<sup>th</sup> of June). In the morning of Waterloo, Grouchy and his forces heard the thundering of the cannons. The Marshal insisted on following his orders (literally) instead of taking Gérard's (General Étienne-Maurice Comte Gérard) advise "*il faut marcher au canon*" which would have been in accordance with Napoleon's intent. As a consequence, not Grouchy's, but Prussian forces arrived on Napoleon's flank to decide the battle.

Grouchy's error at Waterloo is quite prominent. It even appears in literature: *Die Weltminute von Waterloo* by Stefan Zweig (1928). However, errors like this occur, especially if sender and receiver do not share mother tongue or communicative conventions because communicative conventions determine in which cases literal meaning differs from intention. The coordination of joint as well as of combined forces, obviously, suffers under the problem of different communicative conventions most. This partially is reflected in Eisenhower's well-known judgment on alliances (1948, p. 4): "*History testifies to the ineptitude of coalitions in waging war. Allied failures have been so numerous and their inexcusable blunders so common that professional soldiers had long discounted the possibility of effective allied action unless available resources were so great as to assure victory by inundation. Even Napoleon's reputation as a brilliant military leader suffered when students in staff colleges came to realize that he always fought against coalitions – and therefore against divided counsels and diverse political, economic, and military interests.*"

## **6. Degree 4: Pragmatic Interoperability**

Under the NCW-perspective, semantic interoperability can be achieved. This results in shared awareness and thus in a common relevant operational picture. With respect to forces, pragmatic interoperability adds that the receiver of a message recognizes the intent behind it.

Not only the meaning of the message's content would be clear, but also the reasoning behind sending it. The receiver would perfectly know the sender's intent and her expectations for him to act. However, with respect to forces, this is the end of interoperability. The receiver knows every relevant aspect of the actual situation; the receiver also knows what actions of him are expected, but the receiver need not to act as required. So, the remaining question is what kind of force could make the receiver to act according to the expectation such that self-organization emerges and such that sender and receiver act in concert?

With respect to systems, the answer is much easier. Pragmatic interoperability as well as acting in accordance to the information received can be integrated in the code. It "only" has to be specified how the receiver system has to respond to and to act upon types of information it receives. For example, the receiver system might be programmed that whenever it gets a report saying that own forces or civilians are wounded, it has to respond by alarming a unit which can rescue the wounded. A system programmed in this way would operate and act seamlessly in concert with the other systems it is connected to.

In contrast to systems, forces act on their own will. They are subjective in their judging of situations as well as of information. From a linguist perspective, the sender might use one of two avenues to make the receiver act as intended. She may request the action, politely, or she may order it. Traditionally, in a military context, orders are preferred. Orders are shorter and more precise than polite requests ("*Answer fire!*" vs. "*May I ask you to answer the fire?*"). However, in order to order an action, the sender must have the authorization to do so. Traditionally, this authorization is provided by the hierarchical structure of military organizations. Edge organizations, in contrast, do not come along with hierarchies. They do not provide formal authority to order actions. Leadership is defined by competence, decision making is the job of everyone, and the power resides on the edge. In short, every force, even every single soldier has to decide whether to act according to the intention of someone else or whether to act dissenting according to own subjective situational judgment.

As edge organizations do not back the formal authority necessary for traditional ordering, there is the concern that the transformation of the forces into an edge organization might result in chaos in the battlefield. Alberts & Hayes (2003, pp. 27ff.) argue against this concern. They explain that self-synchronization instead of chaos will emerge if the following assumptions hold:

- "Clear and consistent understanding of command intent;
- High quality information and shared situational awareness;
- Competence at all levels of the force; and
- Trust in the information, subordinates, superiors, peers, and equipment."

Alberts and Hayes also offer an elaborated example to support and to illustrate their argument, the Battle of Trafalgar (1805). However, the example is somewhat misleading because the British navy in the times of Napoleon surely had been an hierarchical organization. Admiral Lord Nelson changed the way to fight naval fleet battles (inspired by Rodney's victory at The Saints, 1782) but he did not change the hierarchical structure of the navy. As Alberts and Hayes described in detail, Lord Nelson even made use of the hierarchical structure in order to prepare the battle, painstakingly. He exposed and explained his intent to Admiral Collingwood and the captains of his ships. Thereby he ordered to put it into action.

A much better example to illustrate self-synchronization is provided by the Battle of Cynoscephalai (197 BC) where the Romans commanded by T. Quinctius Flaminius defeated

the Macedonians under their king, Philipp V. The Macedonian king commanded the right wing of his phalanges and let attack them with confidence and haste. The Romans as well as the Macedonian left wing under Nikanor were surprised, As a consequence, they had no battle plan. As the left Roman wing faltered under the strong attack, the right one annihilated the Macedonian's left with ease. This was the situation when an unknown Roman tribune – without any explicit order – synchronized the efforts of the Roman forces. He took 20 maniples out of the victorious right wing and led them into the rear of the Macedonian right one. This maneuver ended the battle instantly (Mommsen, 1854; Gilliver, 1999). The tribune had to act without knowing of any command intent (other than “let us win!”). He had to judge the situation and he had to act, accordingly. This had not been as simple as it may look like as the battle of Naseby (1645) proofed. Here, Prince Rupert's cavalry after crushing the right wing of the Parliamentary forces went too far in pursuit and thus could not assist the Royalists' right wing and centre.

The example of Cynoscephalai suggests that situational awareness, competence, and trust are necessary to the emergence of a self-synchronization of forces. Command intent, however, may not. If players are of equal level and share interests they can self-synchronize their efforts under a quite general specification like “let us win!” But command intent can counteract the fragmentation of efforts which might occur if the understanding of the situation or the respective self-interests differ among the players. Understanding of the situation normally is blurred by subjective motivations, or even by hubris or excessive caution. The following examples will illustrate the influences of these forces.

In the Battle of Arausio (105 BC), the Romans suffered a terrible defeat against the Cimbres and Teutons. Main reason for this defeat had been the hubris of Proconsul Q. Servilius Caepio. Consul Cn. Mallius Maximus had been sent by the senate to deal with the invasion of the tribes. The consul entered negotiations, but Caepio, formally inferior, of higher birth, and of equal incompetence (Mommsen, 1854) thought that Maximus would gain all the honor and to prevent this ordered his own forces to attack. Both Roman armies were annihilated as result (according to T. Livius [Livy], 80,000 Roman soldiers and 40,000 servants and camp followers were killed).

Not hubris, but excessive caution is attributed to Mj. General George B. McClellan who – although more successful than Mj. General Henry Halleck before as well as Mj. General Ambrose E. Burnside after him – missed the chance to end the U.S. Civil War in 1862 on the fields of Antietam. After the confederate victory at Manassas, General Robert E. Lee started his first attempt to carry the war into the North. There, he detached part of his forces under the command of Mj. General Thomas J. “Stonewall” Jackson to capture Harpers Ferry and its supplies and tried to delay the Union forces himself. McClellan succeeded in reorganizing the Union forces quicker than Lee had expected. His forces followed the Confederates into Maryland where McClellan engaged and defeated Lee at South Mountain and Crampton's Gap (14<sup>th</sup> of September), forcing the Confederates back to Antietam Creek near the town of Sharpsburg. McClellan did not attack on the 16<sup>th</sup> of September such that most of Jackson's forces could reunite with Lee's. Harpers Ferry had surrendered the day before. During the battle (17<sup>th</sup> of September), Lee committed every soldier but McClellan held back his reserves which again might be attributed to his caution. However, it is the southern most part of the battle field which is of interest here. McClellan's plan was a simple one: Burnside's corps had to cross a bridge over the creek (or the creek itself) to outflank Lee. The corps, however, was delayed by some 450 Georgians from 9:30 a.m. to 1 p.m. Finally, the bridge was taken. After another 2-hour delay to reform the lines, Burnside's corps advanced to Sharpsburg, threatening to cut off the line of retreat for Lee's decimated Confederates. But then, about 4

p.m., Mj. General Ambrose P. Hill's light division arrived on the field coming all the way down from Harpers Ferry where they heard the thunder of the battle in the morning. (Hill avoided Grouchy's error.) Burnside's troops were driven back. The Battle of Antietam was over. On the next day, Lee began to withdraw his forces to the South.

Hubris as well as excessive caution mean incompetence. Thus, it can be argued that the examples do not form an argument against an edge force. "Competence at all levels of the force" is after all a condition for self-synchronization. There are, however, situations in which caution is self-preservation. The question is what would happen if an edge force of corps size is in the situation of Burnside's corps? The creek has to be crossed. But, crossing the creek under the fire of 450 snipers spells death, at least for those who try first. Self-synchronization votes for a fierce assault, self-preservation forbids it. How could self-synchronization emerge in such a situation?

Even worse, competence is a fleeting property. Grouchy, for example, had a fine record before Waterloo. Thus, competence cannot be granted in advance. It may fail, and hubris as well as excessive caution may show up unexpectedly with negative results to the force's ability to generate self-synchronization.

In short, in situations in which self-preservation might prevent the execution of actions necessary for success the actions must be enforced. Besides, in situations in which parts of the force reveal incompetence this has to be countered. Command is the tool. But, in these kinds of situations, command has to come along with responsibility. It has to be firmed by formal authority. And the authority and the burden of responsibility has to be assigned beforehand such that every member of the force knows about it. Thus, the force must have a (flat) hierarchical structure.

## **7. Summary**

In order to execute network-centric operations forces have to be integrated in the network. Within the network there has to be a high level of interoperability. The discussions on NCW, prominently Alberts & Hayes (2003), point out that it is the interoperability among the (robustly networked) forces what counts. The military equivalent of an edge organization (the edge force) provides pragmatic interoperability for its parts in order to grant the flow of high quality information as well as shared situational awareness. Given competence and trust, the edge force operates under mission command (Storr, 2003) with sparse control (Builder, Banks & Nordin, 1999). In addition, the paper at hand argued that the edge force nevertheless has to have a (flat) hierarchical structure to provide formal authority for command and for bearing the responsibility. Only this offers a tool for dealing with those cases in which self-preservation might cancel necessary actions as well as with the inevitable flashes of incompetence.

## **8. References**

Adan, A. (1980). *On the Banks of the Suez: An Israeli General's Personal Account of the Yom Kippur War*. San Rafael, CA: Presidio.

Alberts, D.S. & Hayes, R.E. (2003). *Power to the Edge: Command ... Control ... in the Information Age*. Washington, DC: CCRP.

- Austin, J.L. (1962). *How to Do Things with Words*. Oxford, UK: Clarendon.
- Builder, C.H., Bankes, S.C. & Nordin, R. (1999). *Command Concepts: A Theory Derived from the Practice of Command and Control*. Santa Monica, CA: Rand.
- Dorion, E. & Boury-Brisset, A.-C. (2004). Information engineering in support of multilateral joint operational interoperability. *Proceedings of the 2004 C2 Research and Technology Symposium (CCRTS) in San Diego, CA*. Washington, DC: CCRP.
- Eisenhower, D.D. (1948). *Crusade in Europe*. New York: Doubleday.
- Gilliver, K. (1999). *The Roman Art of War*. The Mill, UK: Tempus.
- Hecking, M. (2003). Information Extraction from battlefield reports. *Proceedings of the 8th International C2 Research and Technology Symposium (ICCRTS) in Washington, DC*. Washington, DC: CCRP.
- Hieb, M.R., Tolk, A., Sudnikovich, W.P. & Pullen, J.M. (2004). Extensible Battle Management Language (XBML): A methodology for web enabling Command and Control for Network Centric Warfare. *Proceedings of the 2004 C2 Research and Technology Symposium (CCRTS) in San Diego, CA*. Washington, DC: CCRP.
- Johnson, C. (1996). Fratricide. In: Margiotta, F.D. (Ed.), *Brassey's Encyclopedia of Land Forces and Warfare*. Washington, DC: Brassey.
- Kissinger, H.A. (1979). *The White House Years*. Boston, MA: Little, Brown & Co.
- Livius, T. *Ab Urbe Condita (Römische Geschichte – Antike Inhaltsangaben und Fragmente der Bücher XLVI – CXLII)*. Edited by Hillen, H.J.; Darmstadt: Wissenschaftliche Buchgesellschaft, 2000.
- Mommsen, T. (1854). *Römische Geschichte*. München: DTV, 2001.
- NATO Interoperability Directive (AC322-SC/2-WG/4 WP(2003)0015-REV2).
- Schade, U. (2004). Automatic report processing. *Proceedings of the 9th International C2 Research and Technology Symposium (ICCRTS) in Copenhagen, Denmark*. Washington, DC: CCRP.
- Storr, J. (2003). A command philosophy for the information age: The continuing relevance of mission command. In: Potts, D. (Ed.), *The Big Issue*. Washington, DC: CCRP.
- Tuchman, B.W. (1988). *The First Salute*. New York: Knopf.
- U.S. Department of Defence (1992). *Conduct of the Persian Gulf War: Final Report to Congress*. Washington, DC.
- Zweig, S. (1928). Die Weltminute von Waterloo. In: Zweig, S., *Sternstunden der Menschheit*. Frankfurt a.M.: Fischer, 1964.