

The Dutch Approach of ISTAR concept during NRF-4

The tempo of both the decision making and the execution of current operations is high and will only increase as a result of technological developments. This increases the importance of timely and relevant intelligence and information, in which the emphasis will lie on digitisation and management of all available information. This form of information warfare (*Network Centric Warfare*) will take place at all command levels. The struggle for superiority in the collection and the use of information will become of greater importance in the planning and execution of operations. In this respect efforts must be directed at achieving a balance between the capability for information collection and the possibilities for using the information in question. **The ability to have the right information quickly available is of vital importance to the success of the fast paced operations.**

The only way to have information rapidly available at each level is to make maximum use of technological support (communications, hardware and software for situational awareness, night vision, etc.) and to ensure that the operational decision-making process including the connected sub-processes are kept clear and unambiguous. Conversely, the fact that deployment will usually take place in an international coalition will, in turn, slow down the tempo. **Consequently, the setting of the intelligence requirement and the direction of the collecting agencies must take place as closely together as possible.**

According to the Netherlands Armed Forces policy, The NATO ISTAR LAND concept creates the conditions to this end and the Netherlands Minister of Defence decided in 2001 that **all collecting agencies of the Royal Netherlands Army would be placed under a single leadership within an “Intelligence-Surveillance-Target Acquisition and Reconnaissance”- unit (ISTAR).** This battalion was to be operational by mid-2006.

The first serious deployment of 103 (NL) ISTAR Battalion took place within the Land Component of the **NATO Response Force 4 (NRF-4).**

In this article we will present two major lessons learned of this new unit during a six months participation within NATO's rapid reaction capabilities. The first lessons learned topic will demonstrate the importance of “Intelligence Fusion”. The second topic elaborates on the Network Enabled capabilities. Before doing so, we will first have a short look at the characteristics of the ISTAR system, the tasks and organisation of 103 (NL) ISTAR Battalion and the role of the battalion within *NRF-4*.

The ISTAR concept

ISTAR is a system of systems. It consists of **separate systems, units, headquarters and formations that become more effective and efficient by means of interfaces and central coordination of their information and activities**, without adversely affecting the responsibility of the various levels. From the manoeuvre battalion upwards, each level has its own basic ISTAR capabilities (unit/assets) that complement each other and partially overlaps in the area of responsibility. All systems, units, headquarters and formations at the various levels are linked. This gives intelligence staffs and other authorised users access to the collected information and recorded intelligence.

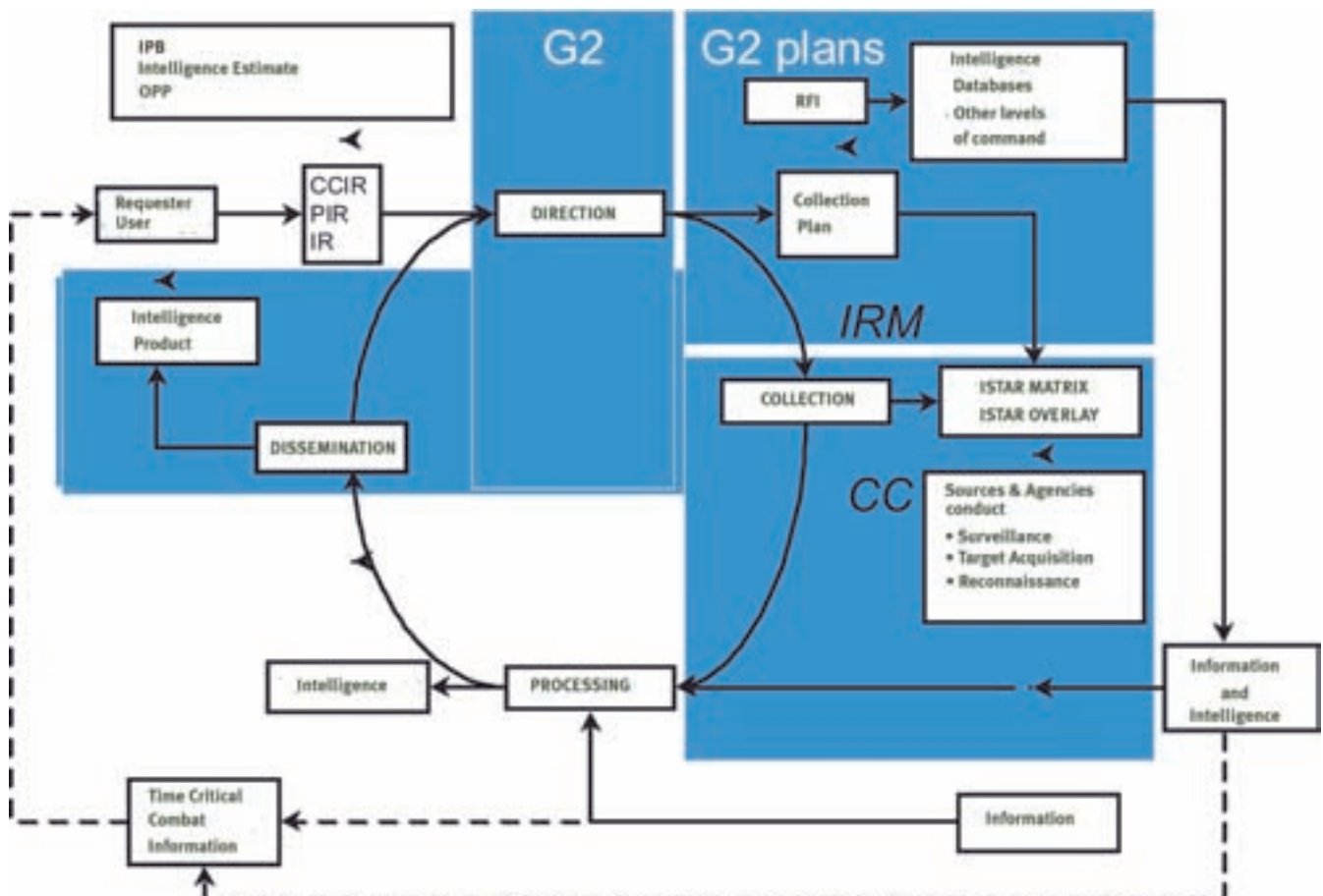
Intelligence in the ISTAR “system of systems” **gives direction to surveillance, target acquisition and reconnaissance in the area of (intelligence) responsibility.**

Furthermore, the system converts data, information and/or intelligence from many different sources and collecting agencies into intelligence. This intelligence is aimed at the assessment of capabilities and the expected intentions of the adversary or groups as well as the weather and terrain situation in the (future) area of operations. The ISTAR system integrates activities between intelligence staffs and collection agencies at the same level and co-ordinates between the various levels. It achieves central monitoring and constant systematic implementation of collecting activities, target acquisition,

information processing and intelligence reports with all available assets within the entire operational framework.

Furthermore it ensures **robust and uninterrupted coverage of the area of (intelligence) responsibility** and is able **to respond quickly to the needs of the commander and his units.** It provides timely, relevant, objective information and intelligence for the command and control and/or target combating. To make the system accessible, the G2 of a formation has access to (parts of) the ISTAR Battalion.

The slide below details the main ISTAR activities and the corresponding G2 task organization.



103 (NL) ISTAR Battalion

The main task of the battalion is **to collect and process data and information to produce usable intelligence for the commander.**

He indicates the “total intelligence requirement” and provides directives and orders for its acquisition.

He also provides directives for he use and dissemination of the intelligence. It is therefore essential that parts of the ISTAR battalion

headquarters are in direct contact or even co-located with the G2 of the supported headquarters.

Other tasks of the battalion are:

- support of the units to be deployed, by providing information on the deployment area,
- provision of intelligence support to headquarters and units for the duration of a deployment.

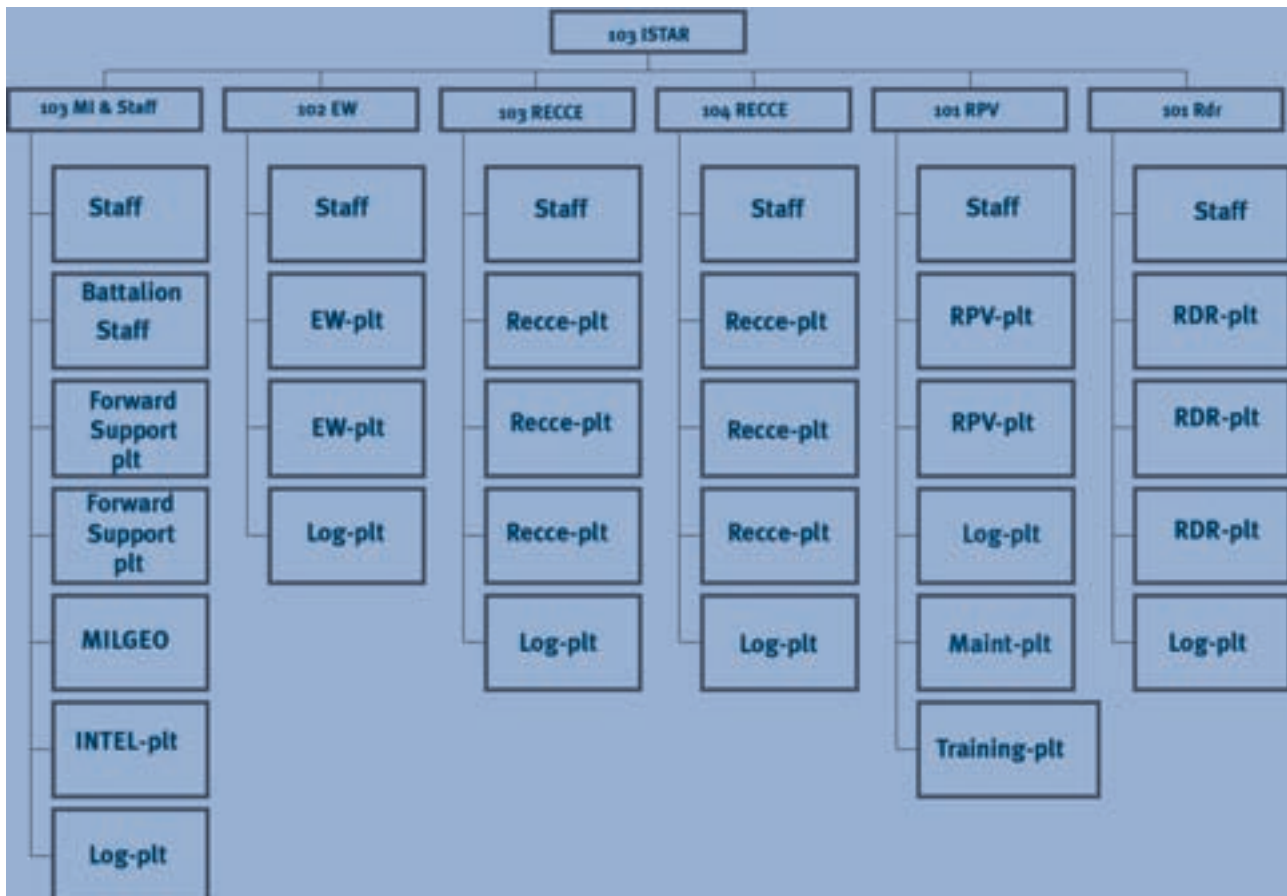
The sub-units and/or the system platoons are tasked with the acquisition of intelligence/collection

of information. The reports do not follow the hierarchical route, but the shortest possible route.

The battalion can be **deployed within the strategic/operational environment:**

- as a battalion-sized ISTAR unit for any multinational HQ at the level of Land Component or Combined Joint Task Force (CCP/CJTF),
- parts of the battalion can be deployed for a multinational headquarters or brigade-sized units or an independently operating battalion.

Generic organizational charts is as follows:



The units earmarked to participate within a High Readiness Forces (HRF) asset must be operationally ready within 5-20 days at a maximum and must be capable to operate in non-article 5 Crisis Response Operations (CRO) as well as in “foreseeable” Article 5 operations. In other words, operations at the high end of the spectrum of force!

The ISTAR battalion must be **capable of cooperating with the intelligence processing capability and collecting agencies of other nationalities.**

Additionally the ISTAR battalion must be able to provide and process information/intelligence from/to the Air Component Commander, Maritime Component Commander and the Special Forces Component Commander.

NATO Response Force 4

The NRF is NATO's quick reaction force. It consists of a Land-, Air, Maritime- and Special Forces component, that are built every six months by different NATO members. The force is capable of deploying within five to thirty days and can perform missions worldwide across the whole spectrum of operations.

From January 15th until July 1st 2005, the **Netherlands** contributed the largest part of the Land Component of *NRF-4*. Together with a large number of allies and under command of the 1st German-Netherlands Corps (*1GNC*), a considerable contingency (approximately 5000 pax) of **Netherlands armed forces** was on stand-by for deployment.

The *NRF*-participation can be divided into two periods.

The first period (Jan-Dec 2004) consisted of training and certification, followed by the "stand-by" period (Jan-June 2005). The operational capabilities were trained during five major exercises, including "NOBLE JAVELIN" (April 2005) on the Canary islands and "*IRON SWORD*" (June 2005) in Norway.

All *NRF-4* elements were trained in a "three-block warfare" scenario. In future Crisis Response operations, NATO units will deal with a combination of humanitarian aid, reconstruction operations and combat operations, including counter insurgency.

This combination, mostly conducted in difficult and dangerous terrain, is an enormous challenge for every commander on all levels. To support these commanders with validated and relevant intelligence is of great interest.

Looking at on-going military missions in Iraq and Afghanistan, we can conclude that "*three-block warfare*" is more than a futuristic development. It is already reality.

The first ISTAR lessons learned

During the *NRF-4* period, **103 (NL) ISTAR Battalion was reinforced with Romanian, Norwegian and Portuguese assets**. From an intelligence point of view, the battalion consisted of human intelligence (humint) assets, electrical warfare and signal intelligence assets (EW/Sigint), unmanned aerial vehicles (UAV), weapons location radar and long-range reconnaissance sensors. For Command and Control (C2) and for All Source Intelligence Process (ASIC), a multinational staff element was created. 103 (NL) ISTAR Battalion was directly **attached to the Land Component Commander (1 GE/NL Corps)**.

In the "three-block warfare" scenario's used in the *NRF-4* exercises, the area of special interest for intelligence personnel had mainly shifted from capabilities oriented analyses, to more and more intentions oriented analyses.

For many intelligence specialists this has meant a **change of mindset**. Force Protection issues like intelligence gathering on anti-force activities, remain key. Nevertheless, the analysis of the intentions of key players in the area of operations has gained importance. Relations between the formal and the informal leadership must be fathomed. We need to know what the possible consequences are if we deny the informal leadership or what could happen if we do business with them.

Very real in today's Crisis Response operations are the Prioritised Intelligence Requests (PIR's) regarding **intentions and capabilities of irregular- or even terrorist organisations**. Conducting intelligence operations on this issue is, at least, very challenging. Depending on the operation there is a last group of possible intelligence requirements. **Organised crime** is an important factor in almost every Crisis Response Operation.

One of the most important lessons learned during all the *NRF-4* exercises is that we have to improve the operating procedures on the information overflow and intelligence fusion. The amount of information that is gathered in a "three-block warfare" scenario is difficult to manage with the danger of becoming meaningless information. Instead of creating a history book, annalists should use the information for predictions. It is the job of an analyst to find patterns in the divers quantity of information, using different kinds of techniques. We can, for example, regroup incidents according to similarity (mortar attacks), or according to intensity. We can make the incidents visible over time, but we should do more than plot the incidents. All kinds of information, such as human Intelligence, signal intelligence, reconnaissance, etc, must be fused in order **to build up a common intelligence picture**.

Challenges ASIC

In the intelligence fusion concept of the 103 (NL) ISTAR Battalion, all information is put together and made visible within time-space factors. The next step is the most important, namely to compare all the rough information and demonstrate connections. By using different kinds of analyst techniques and software programs, the battalion is able **to create a predictive ability** instead of writing a history book. With the so-called Recognised Environmental Picture Concept we will have a better possibility in discovering the *Modus Operandi* of irregular forces in a specific Joint Operation Area. The question that remains is what level is best equipped for the intelligence fusion process, or should every level execute its proper intelligence fusion?

In the 21st century, **the concept of transferring information is becoming network-based, supported by the latest ICT-technology.** This enables command & control systems in which sensors, analysts, decision-makers and shooters are all connected together, resulting in an enhanced Situational Awareness and capability to act immediately upon targets of opportunities. The C4I-concept of 103 (NL) ISTAR Battalion is based upon this network structure on the way to Network Centric Warfare.

In order to contribute to and benefit from the **“Information Age”**, special attention should be given to **interoperability.** Almost all recent operations are conducted in a joint and/or combined environment. To achieve the maximum results, both the technical solutions and the accompanying doctrines need to be synchronised. This needs effort from all participants.

Especially, during the NRF exercise “IRON SWORD”, we have learned that in a Network Centric environment there is a **need for additional Standing Operating Procedures.** On the other hand, without a network system there is a risk that essential information will not be in time at the right place.

Some important questions are still to be answered:

- What kind of information do we want to make available on the network?
- Do we need to disseminate information at once to a certain level?
- If so, at what level should it be disseminated?
- How should it be made visible in the system?

A well thought-out ISTAR and intelligence fusion system, enabled in a Network Centric environment, will be a force multiplier for operational and tactical commanders in future operations.

