

Network-Centric Warfare and sensor fusion

ZSOLT HAIG

Zrínyi Miklós National Defence University, Electronic Warfare Department, Budapest, Hungary

In the information age there are many new operational concepts that deal with significant role of information. One of them is the Network-Centric Warfare. This paper presents the philosophy of Network-Centric Warfare and compares the conventional and Network-Centric grid system. The importance of sensor network and sensor fusion in Network-Centric Warfare is shown.

Introduction

Information superiority is an important factor to enable a new operational concept, that main goal is to achieve full spectrum dominance in military operations. The heart of these concepts is closely couple the capabilities of sensors, command and control (C2), and shooters. The emerging operational concepts can be characterised as network-centric, and the vision of future warfare can be characterised as Network-Centric Warfare.

Concept of the Network-Centric Warfare

The concept of Network-Centric Warfare is a derivative of network-centric computing. The evolution of computing from platform centric computing to network-centric computing has been largely enabled by recent key developments in information technology. Some of the most important developments in information technology include Hyper Text Markup Language (HTML), web-browsers, Transmission Control Protocol/Internet Protocol (TCP/IP), and the Java computing architecture. These developments make it much easier for computers with different operating systems to interact with each other. The concepts of Network-Centric Warfare exploit information superiority to provide a competitive edge in warfare.¹

Information technology has a very significant impact in the concept of Network-Centric Warfare. In current Platform-Centric Warfare, the sensing and engagement capability can be found in the weapon system. There is only a limited capability for the weapon to engage targets because it can only use the situational awareness generated by its own sensor. If a weapon is able to engage a target located by a remote sensor, the

Received: November 10, 2003

Address for correspondence:

ZSOLT HAIG

Zrínyi Miklós National Defence University, Electronic Warfare Department

P.O. Box 15, H-1581 Budapest 146, Hungary

E-mail: haig@zmne.hu

flow of weapon data is normally via communications systems. The single weapon directly connects to the single sensor (Figure 1).

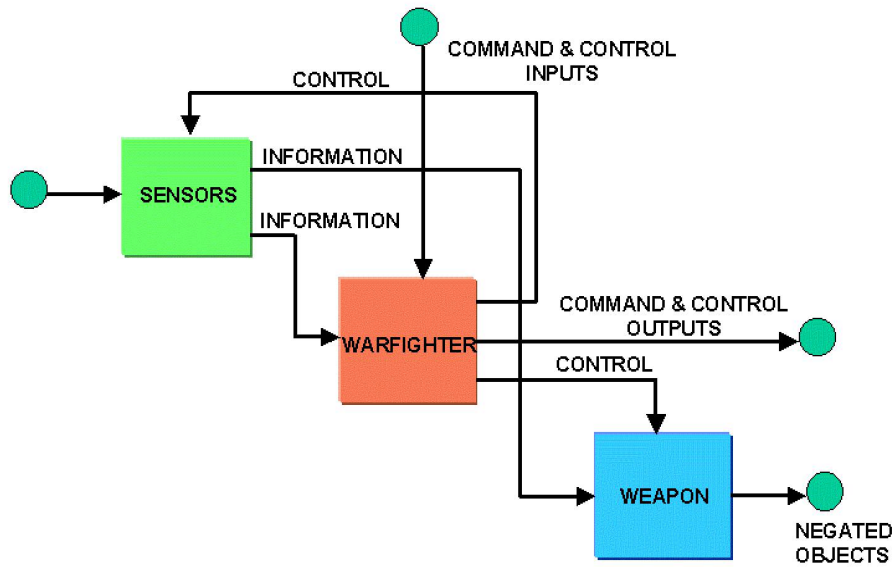


Figure 1. Platform-Centric Warfare²

Network-Centric Warfare is characterised by sensor-to-decision maker-to-shooter information systems that enable superior decision and response within the tactical cycle time, thus achieving the benefits of speed and accuracy of command.

This concept requires network-centric vision in command and control cycle.

Network-centric vision includes:

- real-time communications between sensors, decision makers and shooters;
- the real-time ability to obtain the necessary environmental and tactical data, transmit them to all platforms, and visualize and efficiently utilize the data;
- a decentralized command and control structure which provides that each decision maker can receive and evaluate all applicable data.

In Network-Centric Warfare, sensors and shooters are connected each others through a network. Weapons can engage targets based on a situational awareness that is shared with other platforms. Combat power can therefore be applied with fewer weapon systems than are currently required. Just because weapons and sensors are interconnected, it does not mean that targets can be engaged randomly or without

authority. Control is essential to ensure that targets are engaged in accordance with the operational plan.

Perhaps the greatest distinction between Platform-Centric Warfare and Network-Centric Warfare involves linkage between sensors, shooters, and decision-makers. Platform-Centric Warfare tightly links all three logically and physically, while network-centric may separate these assets and then link them in different ways.

Therefore on the modern battlefield, the network is a considerable force-multiplier.

The grid system

Figure 2 depicts the three interlocking grids of Network-Centric Warfare - the information or C2 grid, the sensor grid, and the engagement or shooter grid -, and the three major types of participants, such as sensors, command and control elements and shooters.

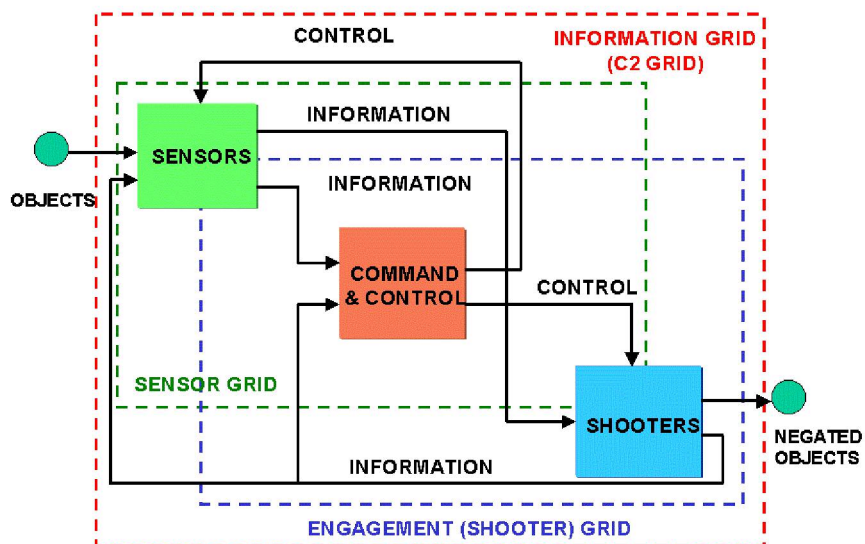


Figure 2. Network-Centric Warfare³

The sensor grid is composed of air, sea, ground, space, and cyberspace based sensors. They are specialised devices mounted on weapon systems, carried by individual soldiers, or embedded into equipment. Sensor grid provides the forces with a

high degree of awareness of friendly forces, enemy forces, and the environment across the battlespace.

The information (C2) grid provides the infrastructure, and gives the overall architecture. This infrastructure provides the facilities and devices to receive, process, transport, store, and protect information. The information grid has embedded capabilities for information assurance prevents intrusive attack and assures commanders that their information will be valid.

The engagement (shooter) grid consists of all available weapon systems. The operational architecture of engagement grid enables the warfighter to achieve the necessary battlefield effect at precise places and time. Figure 3 tries to illustrate the system of grids and their connections.

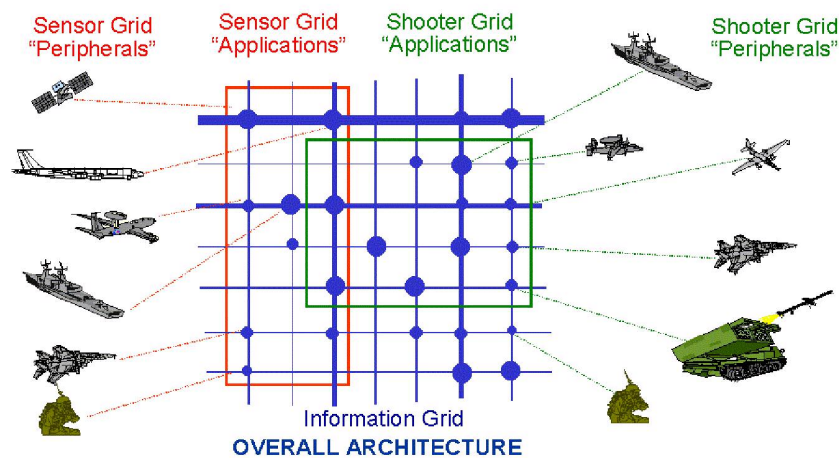


Figure 3. The grid system

The grids function as an interoperability framework. It means that:

- define objective network-centric operations with
 - time-sensitive targeting;
 - collaborative operations;
- define the linkages within each grid, so they
 - increase performance;
 - provide robustness;
 - synchronize operations;
 - enable network-centric behaviour and virtual assets;

- define the linkages between grids, so they
 - enable flexible mission-tailored operational threads;
 - provide multiple paths for robust architecture;
- provide links between existing and emerging systems.

The information (C2) grid is a fundamental building block of information superiority. The information grid is a “network of networks” consisting of communications paths, computational nodes, operating systems, and information management applications that enables network-centric computing and communications across the battlespace. The information grid provides dial tone, web tone, and data tone. The connectivity and computing capabilities of the information grid enable the sensor grid to generate battlespace awareness.

The information grid consists of both military and commercial communication capabilities and transmits multiple information types in multiple modes at multiple data rates. Voice, data, and video can be transmitted via point-to-point or direct broadcast.¹

Comparing the conventional and network centric information (C2) grids, the conclusions are the following:

- Conventional information (C2) grid has:
 - ineffective linkages across services’ C2 systems;
 - lack of timely and flexible tasking of sensor grid;
 - conventional C2 sensor stovepipes confuse C2 and sensor grids progress.
- Network-centric information (C2) grid provides:
 - distributed synchronization and interoperability across C2 grid;
 - mission tasking (commander’s intent) to sensor and shooter grids;
 - C2 reviews nominations from sensor grid and assign actions to shooters. Information (C2) grid accepts target, assigns to shooter, and creates time sensitive targeting sensor-to-shooter data channel (Figure 4).

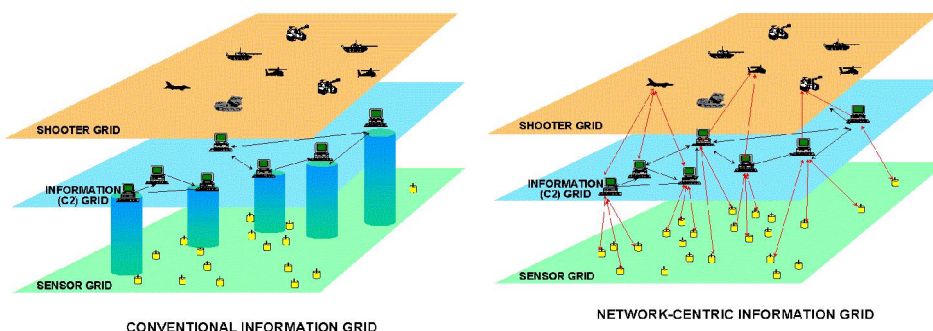


Figure 4. Comparison of conventional- and network-centric information grid

Sensor grids provide the commander with the operational capabilities necessary for achieving awareness across the battlespace. Abstractly, sensor grids are sets of sensor peripherals and sensor applications that are installed on the information (C2) grid. The sensor peripherals – as I mentioned above – consist of space, air, ground, sea, and cyberspace based sensors. These sensors can be based on dedicated sensor platforms, weapons platforms, or deployed by individual soldiers. The sensor grid applications consist of the software applications associated with specific sensor peripherals, as well as the software applications that enable multi-mode sensor tasking and data fusion.¹

Main features of the conventional and network-centric sensor grids are:

- In conventional sensor grid:
 - sensor connected with dedicated C2 node, and
 - it provides only one way broadcast.
- Network-centric sensor grid:
 - correlates and fuses wide range of disparate sensors and data;
 - manages uncertainty, transforms data into information, nominates to C2. Therefore the conventional sensor grids give overlapped and fragmented sensor pictures at the C2 grid. Opposite this, network-centric sensor grids provide a real-time integrated sensor picture for warfighters (Figure 5).

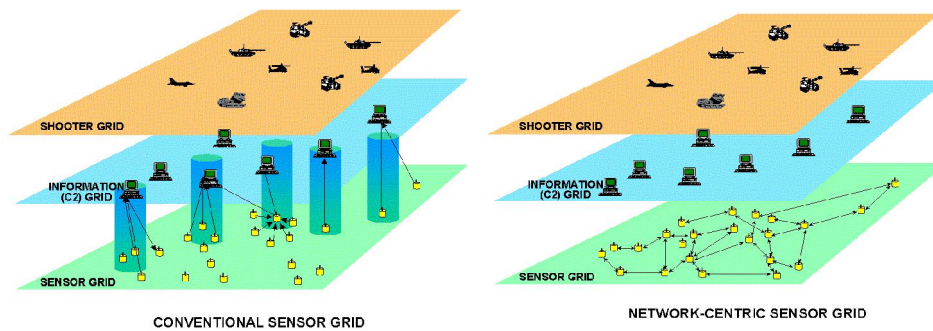


Figure 5. Comparison of conventional- and network-centric sensor grid

The operational architecture of the sensor grid increases battlespace awareness and synchronizes battlespace awareness with military operations. These improvements in operational performance are achieved through a combination of dynamic sensor tasking, data fusion, and effective distribution of information over the information grid. A representation of the sensor tasking and data fusion processes performed with a sensor grid is portrayed in Figure 6.

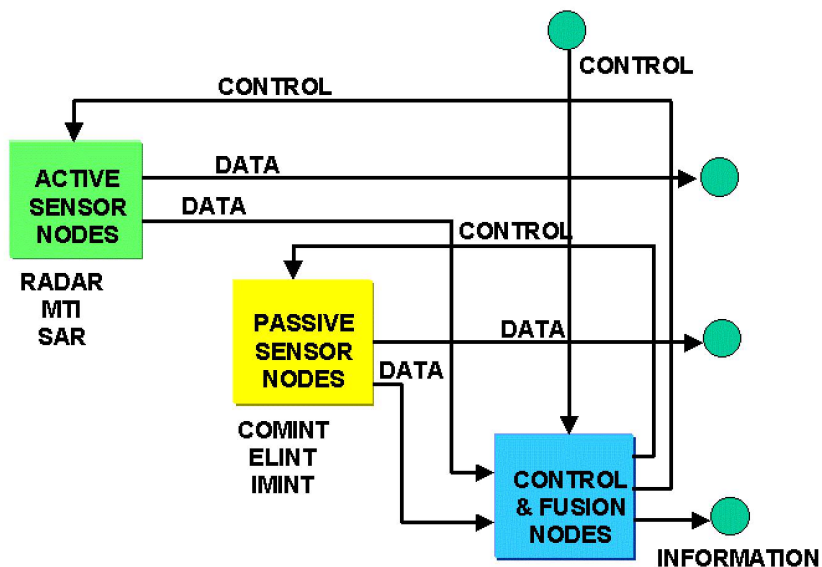


Figure 6. Sensor tasking and data fusion processes¹

The engagement (shooter) grids effectively exploit battlespace awareness to enable new operational capabilities, such as precision engagement, dominant manoeuvre, and full-dimensional protection.

The conventional engagement grids have some disadvantages, for example:

- limited networking between shooters;
- limited networking between C2 and shooters;
- lack-off real-time precision targeting data. Opposite this, the network-centric engagement grids provide:
- platform/weapon-specific response to C2 tasking;
- guaranteed (deterministic, accurate, precise) effects;
- real-time sensor-to-shooter data (via C2 grid) for time sensitive targeting (Figure 7).

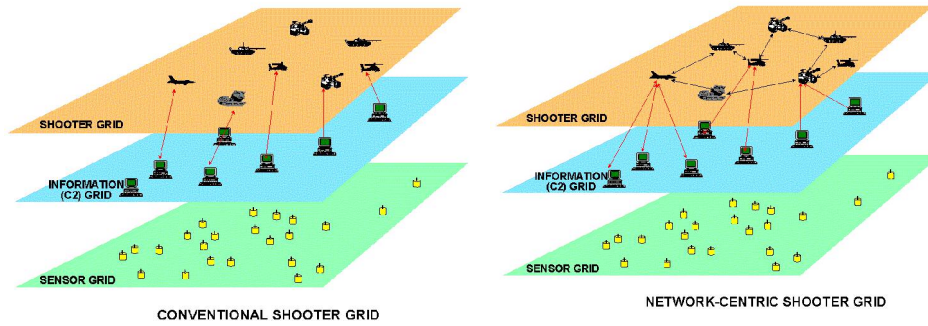


Figure 7. Comparison of conventional- and network-centric shooter grid

This architecture of the three grids provides network-centric interoperability that is flexible and robust (via multiple links) and enables real-time sensor-to-shooter data for time sensitive targeting (Figure 8).

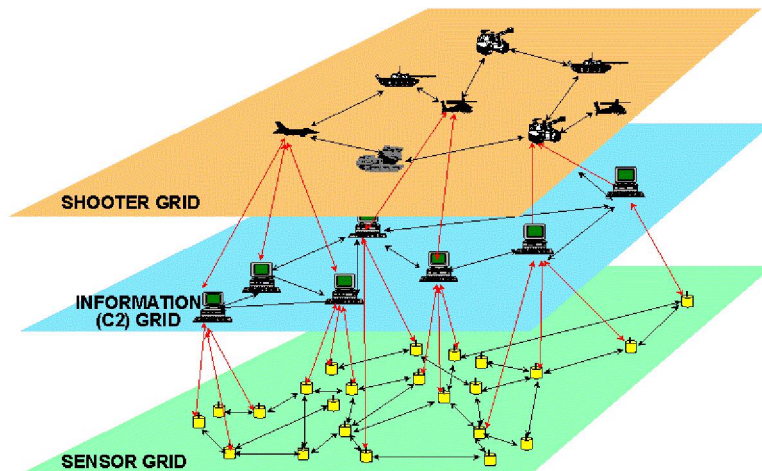


Figure 8. Network-centric grid system

Sensor network and sensor fusion

The final part of the paper attempts to focus on the sensor fusion. Why sensor fusion is important?

A single sensor hasn't the ability to direct the application of precision weapons, therefore data must be integrated from a number of sensors and databases. The sensor grid's capability to perform data fusion is critical to its capability to rapidly generate high levels of awareness. Data fusion increases battlespace awareness in several ways. Multi-spectral data fusion increases battlespace awareness by increasing the probability of object detection and object identification. In addition, sensor fusion which combines the output of multiple sensors can increase awareness of moving targets in the battlespace by increasing the probability of track initiation as well as decreasing the time required to develop engagement quality tracks of moving targets.

Let see some reasons why we should apply sensor network and data fusion.

Sensor networks decrease system costs. Using commercial network technologies (Asynchronous Transfer Mode/ATM/, ETHERNET, Fibre channel) in traditional sensor systems to reduce total cost of ownership and increase performance. Creating common network-centric sensor interfaces across programs.

Sensor networks enable detection of low-signature targets. Low signature targets are difficult to detect, classify, and engage, because of low radar cross-sections, low radiated noise, low radiated infrared or heat, etc. Combining sensors and sources in numbers, types, and locations to sense and illuminate low signature targets.

Sensor networks reduce error. Combining sensors from different positions or with different frequency ranges to improve measurement accuracy. It requires precise synchronization and position of sensors.

Sensor network and data fusion improves targeting. Employment of sensor networks allows us to solve line-of-sight problem by terrain, or environmental constraints imposed by weather. The combination of sensor tasking and data fusion enables multiple sensors, based in space, the air, or on the ground, to effectively increase the amount and quality of information available.

Certain classes of objects cannot be tracked, located, or identified with sufficient accuracy using a single type of sensor. This deficiency can sometimes be overcome by linking sensors of different types to achieve an all source capability. Figure 9 portrays the significant reduction in position uncertainty that is possible with sensor fusion.

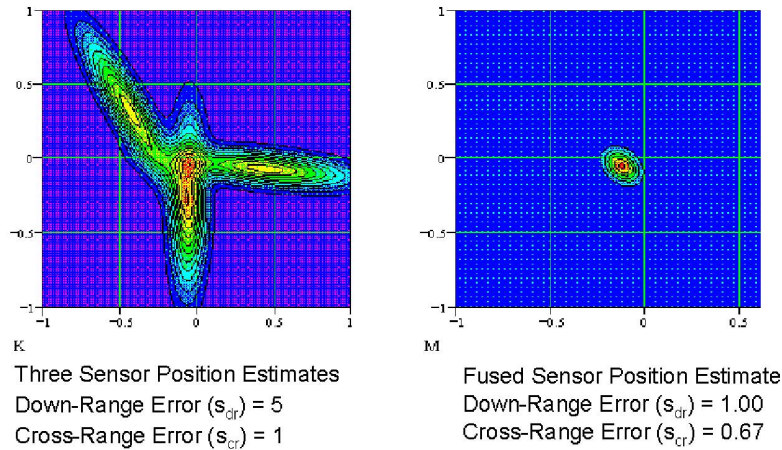


Figure 9. Payoff of sensor fusion²

This increased performance is of particular value in detecting, locating, and identifying high-value targets, such as mobile surface-to-air or surface-to-surface missile launchers, as well as surface-to-surface missiles in flight. For example, information collected by a wide-area surveillance sensor, such as a radar MTI located on sensor platform, can be used to cue other sensor entities with different characteristics or capabilities such as imaging sensors, ELINT sensors, or manned reconnaissance teams.

Sensor network and data fusion improves tracking. The U.S. Navy's Cooperative Engagement Capability (CEC) generates increased battlespace awareness by fusing data from multiple sensors and enabling quantum improvements in track accuracy, continuity, and identification over the information that could be achieved by using standalone sensors. The performance in tracking improvement associated with the embedded CEC sensor network is portrayed in Figure 10.

The results of sensor fusion are:

- decreased time to engagement;
- improved track accuracy and continuity;
- improved target detection and identification;
- extended detection ranges.

The main requirements of sensor network are:

- assure information, reduce susceptibility to countermeasures;
- provide accurate sensor node georegistration and synchronization;
- fuse data and coordinate sensors within network;

- reducing information overload;
- simplify queries and user interfaces;
- provide target recognition;
- simplify network deployment, set-up, and management;
- reduce sensor node power;
- reduce sensor node size and detectability (micro sensors, Micro-Electromechanical Sensors /MEMS/, microbots, micro vehicles, Unmanned Aerial Vehicles/UAV/etc.);
- enhanced communications technology between sensor nodes, such as ATM and Bluetooth technology.

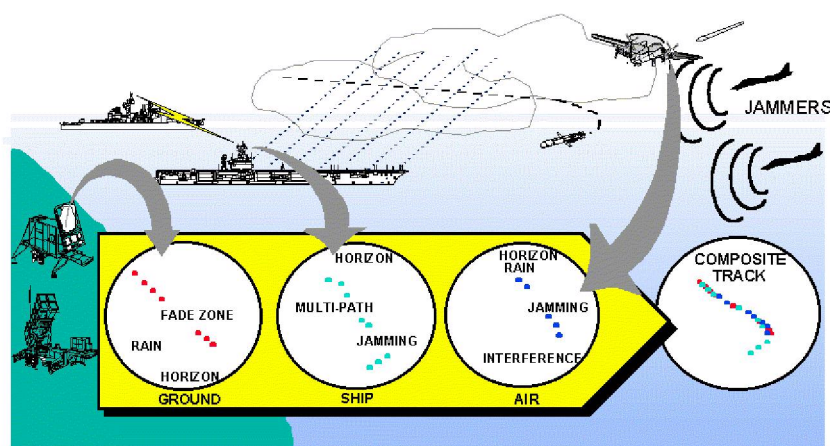


Figure 10. The U.S. Navy's Cooperative Engagement Capability (CEC) sensor network²

Conclusion

Network-Centric Warfare is the emerging military response to the information age. Sensor networks enable new applications such as sniper detection and localization. Sensor networks will improve operational pictures and engagement through more accurate detection, identification, and tracking. Emerging software technologies such as spatial routing, sensor fusion, distributed collaborative computing, and declarative queries will enable smart sensor networks that improve performance and use. Emerging hardware technologies such as MEMS, wireless links, and node miniaturization will enable large distributed sensor networks.

References

1. *Observations on the Emergence of Network-Centric Warfare*
<http://www.dtic.mil/jcs/j6/education/warfare.html>
2. D. S. ALBERTS, J. J. GARSTKA, F. P. STEIN: *Network Centric Warfare: Developing and Leveraging Information Superiority*, CCRP Publication Series, 1999.
3. M. R. FRATER, M. RYAN: *Electronic Warfare for the Digitized Battlefield*. Artech House, Boston, London. 2001.