Journal homepage: www.jmisci.com
Contact: jmiseditor@gmail.com

Journal of Military and Information Science
Institute of Science

Technical Report

A Short Review on Integrated C2 Systems

Cüneyt Başaran

HAVELSAN Naval Combat Management Systems Department (DSYSTM), 34890 Pendik-İstanbul
E-mail: cbasaran@havelsan.com.tr

Abstract- This report addresses the evolution of C2 systems from platform centric to network centric in the Information Age. It investigates the advantages of information distribution on a through different command grids to build a Force Multiplier. It addresses the standards, challenges and methods to overcome the limitations. Finally HAVELSAN C2 and supporting systems enabling Network Centric Operations are mentioned.

.**Keywords-** Integrated C2 Systems, Network Centric Warfare, NATO Network Enabled Capability, HAVELSAN.

1. Introduction

The level of information technology which has been reached today, has tremendous effects on our lives. Even small children at their first ages are developing motor capabilities and play games on tablet computers. In the following years of their childhood they enjoy playing online games in a networked environment, where game specific information is shared over internet among peers.

We exploit the benefits of the information age as it penetrates our daily lives. Even household appliances are operating in a networked environment nowadays, sharing information with other devices.

This evolution also affects the capability of C2 systems which are built for effective combination of sensors and weapons on those platforms.

In the late 90's, a new concept was introduced described as "translating an information advantage into a decisive war fighting advantage". Since the sharing of information is the core part of this new concept, the "Network" which enabled the data distribution became the central part of the system. The new concept was named as NCW (Network Centric Warfare) in USA (Alberts et al, 2000).

Eventually, NATO recognized that transformation of the military based upon Information Age principles was essential, and pursued a course of transformation denoted as NATO Network-Enabled Capability (NNEC) (Declaration, 2002). NATO adapted this concept by defining NNEC program to build a better Command and Co ntrol among allies, primarily for interoperability. The networking and information infrastructure (NII) is defined as the supporting foundation that enables collaboration and information sharing among users, and reduces the decision-cycle time. The infrastructure enables the connection of existing networks in an agile and seamless manner.

This leads to Information Superiority which is the ability of getting the right information to the right people at the right time. NATO defines information superiority as the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

The NNEC program provides various benefits to all levels of military and civilian actors. Some of these benefits are:

- Improved efficiency
- Drastic increase in interoperability among nations
- Improved and secure way of sharing information

- Better information quality
- Faster decisions and command.

Although NCW and NEC definitions are slightly different, both represent the intent of achieving enhanced military effects through the better use of information systems.

NCW/NEC is envisaged as the coherent integration of sensors, decision-makers, effectors and support capabilities to achieve a more flexible and responsive armed forces. In this vision, commanders will be better aware of the evolving military situation and will be able to react to events through voice and data communications.

It is a long-term transformation program which includes the communications, information systems, operational procedures and people.

2. Implementation Areas

Then, the structural or logical model for network-centric warfare has emerged. But there is a need of high-performance information grid which provides a backplane for computing and communications. This information grid enables the operational architectures of sensor grids and engagement grids. Sensor grids rapidly generate high levels of battlespace awareness and synchronize awareness with military operations. Engagement grids exploit this awareness and translate it into increased combat power.

Although building the key elements of these grids at strategic or operational level is a reachable goal, nevertheless there are still challenges at tactical level.

Several nations and organizations started developing standard architectures to improve interoperability between different nations and organizations.

NATO started developing an architecture framework abbreviated as NAF to assure interoperability at planning, programming, budgeting, acquisition, and Joint capabilities integration and system development process.

2.1. NATO Architecture Framework

The NAF is an Enterprise Architecture framework by the NATO which is derived from the DoDAF (USA Department of Defence Architecture Framework) Enterprise architecture and MoDAF (U.K. Ministry of Defence Architecture Framework)

NAF Goals from the point of Information Sharing:

- providing guidance for developing and describing NATO architectures
- Enabling a paradigm shift from human communication through mass amounts of written text to communication by standardized models of the real world
- Information Accessibility

Another work that NATO achieved is building an Network and Information Infrastructure for the Alliance's cognitive and technical ability to federate the various components of the operational environment, from the strategic level down to the tactical levels which is a formal definition of NATO Network Enabled Capability (NNEC)

2.1.1. NATO Network Enabled Capability

Briefly, NNEC can be considered as the ability to effectively federate capabilities in coalition operations, by addressing not only the networks and systems, but also the information to be shared, the process employed to handle it, and the policy and doctrine that allows sharing information and services.

The need for NNEC is intrinsic to all coalition operations. NNEC supports heterogeneous partners, with different capabilities and needs, to operate under a federate set of "rules" that provide interoperability from the technical to the cognitive domain.

2.1.2. NNEC Roadmap

In order to realize the net centric capabilities in a manner consistent with the development and implementation of the broad spectrum of NATO capabilities, the NNEC Feasibility Study is realized (NNEC FS, 2005).

In this study, it is suggested that design of a program management approach based on a description of NNEC Maturity Levels, to handle the complex development and integration necessary to realize NNEC across NATO.

The NNEC roadmap milestones as explained in (ACT ICT, 2009) were chosen based on operational capabilities required between 2009 and

Başaran, C.. (2014). A Review on Integrated C2 Systems, Journal of Military and Information Science, 2(3), 77-83.

2020. Each milestone is initially associated with a specific target date, as well as a long term goal made up of the specific milestone objectives.

- Milestone 1: Generalized Information Sharing

Milestone 1 aimed to "Achieve a Federation of NATO and Alliance Forces Capable of Sharing Information Services". The intent of this milestone is to improve both inter- organization and inter-agency (non-military government agencies, International Organizations) information sharing which result in limited federation of processes.

- Milestone 2: Federated Processes

The aim of milestone 2 is to "Achieve a Federation of NATO and Alliance Forces Capable of Federating Processes and Services in Addition to Information". This milestone concentrates on federating processes, both Alliance and national, as well as improving collaboration with the inter-agency.

- Milestone 3: Better Decision Support

The aim of milestone 3 is to "Achieve a Federation of NATO and Alliance Forces sharing a Majority of Services and Information". This milestone is characterized primarily by improvements in the supporting tools arena although additional improvements will also be realized in both information sharing and federation of processes.

Most of the systems will be interoperable enabling the seamless sharing of information across the functional areas. Command and Control capabilities will be more mobile and less dependent on location. Battle-space management and situational awareness will both be fused and capable of providing real-time pictures including force protection and logistics information. Logistics decision support tools will be shared or interoperable across all stakeholders. The initial role-dependent situational awareness capability will be introduced. This milestone will require a high degree of data/information fusion.

- Milestone 4: Continued Refinement increment

This milestone represents a state in which services shared and integrated, there exists dynamic integrated information access; high use of collaboration; and embedded reach-back with ad-hoc capability to extend or reconfigure on the fly. Future iterations of the Roadmap may include additional packages of milestones, providing the ability to concentrate on multiple threads of development within the same dataset.

Based on these roadmaps several C2 systems are developed and integrated with strategic and planning level. Existence of high capacity networks and SOA expedite this process

2.2. Integration of C2 Systems at Operational and Tactical Level

Based on the roadmaps, there is a wide range of applications at operational and tactical levels which includes management of sensors, weapons and communication systems.

2.2.1. Sensor Management within Battle Force

One application of NCW is Sensor Integration and Management at Multilevel Information Grids Common Operational (COP), Tactical (CTP) and Fire Control Picture (FCP) which are illustrated in Fig.1.

This concept is elaborated in (Johnson and Green, 2002) in detail. The COP consists of non-real-time tactical information used for mission planning and force management. The CTP consists of near-real-time tactical data and information used for cueing and managing BF resources. The FCP is the collection of real-time fire control quality data/measurements used to support weapons during launch and in-flight.

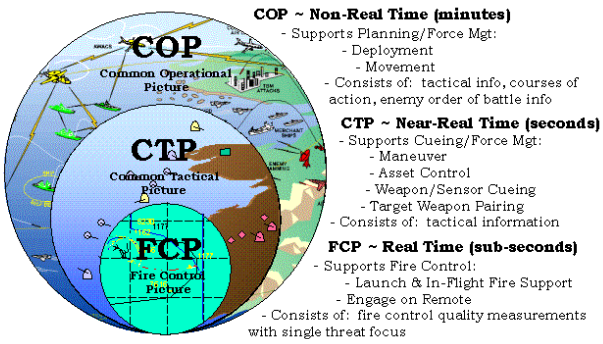

Fig. 1. Managing Resources in Battle Force

In this configuration all information is shared across BF platforms over a synchronized common database. Information superiority is achieved in the Naval Battle Force (BF) by establishing and maintaining shared and consistent battle space awareness across the BF in this concept. Information from all three categories are relevant to the effective and efficient management of BF resources as well as for addressing BF threats and operations.

The information superiority originates from taking full advantage of the capabilities of the distributed sensors and communication resources to best fulfil the dynamically changing needs of the distributed information users.

Utilizing resources in a platform-centric perspective, limits their utility to the BF at large. Additionally, both the sensors and communication links are constrained with physics-based bounds that limit their area of coverage and accuracy.

In order to achieve information superiority, the BF must ensure consistency between the three information grids. Thus, collapsing the information realms is both an enabler of resource management as well as a result of resource management.

An important enabler of network-centric sensor management is the automated control of data distribution throughout the BF. Major bandwidth constraints exist due to the physical limitations of the BF's communication devices. These limitations prevent the paradigm of wasteful transmission, or the sending and receiving of all data and information among the BF platforms or decisions nodes. To most effectively utilize the bandwidth, the BF must intelligently distribute data and information between decision nodes based on the needs of the BF information users, which dynamically change as the operations and missions unfold.

The BF's tactical information users consist of human operators and decision-makers as well as automated C4ISR, combat, and resource (i.e., sensor) management systems that have tactical roles. As missions change in priority and existence during the course of operations, the needs of such BF tactical information users change.

Automating the exchange of BF information to meet the dynamically changing user needs is a key factor in addressing this challenge. Since the timeframes required supporting the distribution of COP, CTP, and FCP are too fast and the amount of data and information is too large to permit a manual solution, the establishment of an intelligent data distribution capability relies on automation,

The intelligent data distribution concept is based on an automated, distributed link resource management system that places a smart processor at each decision node or participating platform. Each link manager should:

- determine the needs of the information-recipient users or decision nodes;
- keep track of what data and information is available;
- determine the feasibility of transmission
- send commands to other link managers within the BF to control and manage transmissions and transmission modes,
- transmit data and information as required.

A possible solution for managing links under such a paradigm would be to establish transmission modes such as one based on the three information grids (COP/CTP/ FCP). As platforms information needs change, the transmission modes change in response. For example, a platform in the middle of an engagement might invoke the "FCP" transmission mode that tailors the information update rate, bandwidth usage, and transmission direction on all remote links that can contribute to the engagement.

Once the Information Data Link between the platforms is established, the following goals can be reached.

- Effective Use of Limited Sensor Resources
- Effective Use of Limited Operator Resources
- Track Picture Advances
- Sensor Fusion and Synergism
- Situation Assessment Improvements
- Fire Control Support will be elaborated

A sample multisensory fusion application is depicted in Fig. 2. In this concept; track or plot information is collected from surveillance sensor of different platforms to build a coherent tracking and improve situation assessment.

Başaran, C.. (2014). A Review on Integrated C2 Systems, Journal of Military and Information Science, 2(3), 77-83.

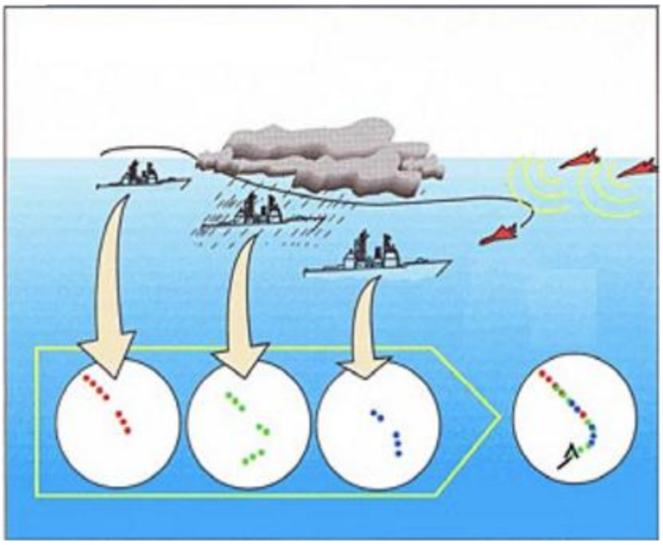

Fig. 2. Multi Platform Multi Sensor Fusion

Another example is presented in Fig.3 by managing sensors to improve precise tracking capability.

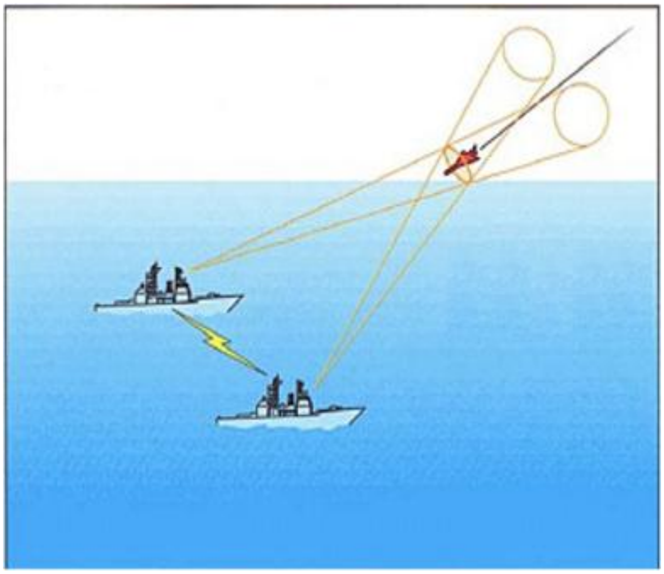

Fig. 3. Precise Tracking

2.2.2. *Fire Control Integration*

Another capability is optimizing the Fire power and effectiveness by the participation and coordination of multiple non-collocated warfare assets in tactical engagements. Possible integration approaches at fire control grids are analyzed in detail in (Young, 2005).

Integrated Fire Control (IFC) is the ability of a weapon system to develop fire control solutions from information provided by one or more non-organic sensor sources; conduct engagements based on these fire control solutions. IFC enables expansion of a weapon's battlespace to the effective kinematic range of the missiles and can remove dependency on range limits of the organic/dedicated sensor.

IFC relies on the ability of participating sensors, weapons, and C2 nodes to share target information in real-time and eliminate correlation errors so the engaging weapon system can utilize the information as if it was produced by its organic sensor(s).

Collaboration among distributed warfare resources to perform integrated engagements takes many forms. Distributed collaboration can consist of simply receiving a threat cue from a remote source to the sophisticated integration required to pass engagement control to a remote unit.

This section summarizes the major types of IFC capabilities from an operational perspective.

- Transfer threat information received from remote platform sensor to local tracker.
- Launch missile on remote sensor data without holding the track locally.
- Launch missile on remote sensor data while engagement calculation are also conducted by remote platform.
- Handing off the control of the in-flight missile to another unit to complete the intercept.
- Launch decision made by a remote unit.
- Preferred Shooter Determination.

Preferred Shooter Determination is a capability in which the optimum weapon from a group of warfare units is selected to intercept a threat target.

As stated in the sensor management part, information data link is also enabler of fire control network.

3. Challenges for Achieving NCW/NEC

Information sharing is a more challenging problem for distributed Naval Platforms when compared with the governmental organizations and land based units of the Armed forces, where information exchange media is better established and comparably more stable. This section outlines the naval problems that inhibits the achievement of cooperative resource management and network centric warfare in general. Mostly encountered problems mentioned (Johnson and Green, 2002) are summarized below.

- The shift from platform-centric to network-centric has not completely taken place: network-centric concepts are not "designed-in" to systems.
- Current Naval systems are not designed from a network centric (multi-platform) point of view. Such network-centric design is necessarily a top down process starting with a design for Battle Force level and decomposing or allocating force-level requirements to the BF elements (or platforms/systems). The historical approach has focused on the design of each BF element individually and has attempted to achieve interoperability in an "after-the-fact" method by focusing on interfaces between the elements.
- The requirements for BF resource management are not specified from a BF-level perspective.
- The acquisition and program management practices prevent network-centric warfare. NAF, DODAF etc. type architecture framework and standards should be utilized.
- Legacy system constraints prevent an evolution to a network-centric systems.
- Existing sensor command and control mechanisms rely too heavily on manual participation. Involvement of automation and decision support systems should be considered.
- The legacy information architectures constrain cooperative BF resource management.

4. HAVELSAN Integrated C2 Solutions

Based on the NATO and National roadmap HAVELSAN has successfully developed various command and control based solutions for its national defense as well as friends and allies.

HAVELSAN positions itself as the Center of Excellence in command and control architectures and has proved its capability with its various field proven products.

Military Enterprise Information System has been the first and largest step of HAVELSAN's maturity and professionalism in the arena of Command & Control. This indigenous solution integrates many complex systems at strategic and operational level of military forces. This architecture is now in service with the Turkish and Pakistani Air Force.

As a tactical and joint command control solution, HAVELSAN has launched a new product called Defense out of Box (DOOB). This system solves from strategic to tactical C2 level problems and introduces an aspired solution for Joint Operational needs. It is a modular and scalable system that can be converted into any unit of the Armed Forces independent of its size.

HAVELSAN has developed several airborne command and control solutions in the past tailored for customer specific needs. Such an application was for the Turkish Maritime Patrol/Surveillance Aircraft program "MELTEM Project", where HAVELSAN has developed a unique airborne and ground mission system which can be adapted into any aircraft for patrol and surveillance purposes.

Turkish Airborne Early Warning Aircraft Program has further aggregated HAVELSAN's potency and capability to provide solutions to users of Early Warning capabilities throughout the world. Today HAVELSAN has the ability to transform different types of aircraft to special mission platforms.

Naval Command & Control Solutions

GENESIS is a world-wide acknowledged Combat Management System solution of HAVELSAN. It was first implemented on the Modernization of the Perry Class [ex-FFG] Frigates and has since been improved for the Turkish Corvette MILGEM, and the LST's.

HAVELSAN continues to invest in Network Centric Technologies. HAVELSAN will install its state-of-the-art solution Network Centric Combat Management system on the follow-up MILGEM and LPD platforms.

New features of the system include;

- Multi-Sensor Fusion,
- IP Based Network & Communication Infrastructure,
- Common Operation Control
- Display Technologies
- Multi-visual Data Processing Technologies, and Autonomous Systems.

HAVELSAN has been working on a solution for information exchange between different C2 systems and developed a Gateway called "Data Exchange Model", which facilitates the data exchange between different Command & Control Systems working with different software protocols. This introduces huge cost savings in systems modernization as it prevents expenditure on system upgrades for data transformation needs.

Finally as the enabler of seamless connection between geographically distributed naval units, HAVELSAN is developing prototype system called IP data link manager (DETTA).

5. Conclusion

Achieving net-enabled vision will require migration from the system-based implementation construct towards a shared services-based environment. Planning and executing the transition of C2 systems from the present-day client-server environment to a services-based, net-enabled enterprise is one of the major challenges we face today. Implementation planning involves identifying and prioritizing increments of C2 capabilities that are operationally meaningful, technically feasible, programmatically achievable, and fiscally affordable.

In the foreseeable future, these sources will be a mix of services and systems with the former gradually coming to predominate. C2 systems, platforms and facilities with reliable and robust access to a network will be the initial implementers of services, beginning the migration toward an SOE. However, some capabilities will remain to need traditional point-to-point information exchange solutions, particularly where required to support time critical sensor-to-shooter exchanges or disconnected, interrupted, and low bandwidth (DIL) operational environments.

References

Alberts, D. S., Garstka, J. J., & Stein, F. P. (2000). Network Centric Warfare: Developing and Leveraging Information Superiority. Assistant Secretary of Defense (C3i/Command Control Research Program) Washington Dc.

Declaration, P. S. NATO Press Release 127, 21 November 2002, Internet, accessed 12. 03. 2014.

Johnson, B.W., and Green J.M. (2002). Naval Network-Centric Sensor Resource Management. 7th International Command and Control Research and Technology Symposium.

Young, B.W. (2005). Future Integrated Fire Control. 10th International Command and Control Research and Technology Symposium.

ACT IS/NNEC Integrated Capability Team (October 2009), NATO Network-Centric Enabled Capability (NNEC) Introduction to the NNEC Roadmap Report

NC3A Program of Work (2005), Project Multinational NNEC Feasibility Study.

ACT IS/NNEC Integrated Capability Team (October 2009), NATO Network-Centric Enabled Capability (NNEC) Introduction to the NNEC Roadmap Report

www.act.nato.int/nnec, NATO Network Enabled Capability (NNEC), Internet, accessed 20. 01.

Command & Control Implementation Plan Version 1.0 (October 2009), U.S.A.Department of Defense.

Başaran, C.. (2014). A Review on Integrated C2 Systems, Journal of Military and Information Science, 2(3), 77-83.