The use of Electronic Warfare and Information Signaling in Network-based Warfare

Mohammad Reza Hassani Ahangar[1], Saeed Talati [2*], Ali Rahmati [3], Hamid Heidari [4]
1- Department of Electronic Engineering, Imam Hussein University, Tehran, Iran.
Email: MRHasani@ihu.ac.ir
2- Department of Electronic Engineering, Shahid Sattari University of aeronautical Science and Technology, Tehran, Iran.
Email: saeed.talati@yahoo.com (Corresponding author)
3- Department of Electronic Engineering, Shahid Sattari University of aeronautical Science and Technology, Tehran, Iran.
Email: Rahmati_Ali312 @yahoo.com
4- Department of Electronic Engineering, Shahid Sattari University of aeronautical Science and Technology, Tehran, Iran.
Email: Heidary.hamid88@gmail.com

Received: January 2020 Revised: March 2020 Accepted: May 2020

ABSTRACT:
Network- based warfare is known as the symbolic element of the Age Information War. The network-based approach has been built around information sharing, and this information sharing in the battle is possible through the networking of all elements on the battlefield. A coherent networking force improves the quality of information sharing and, as a result, survival and command speed, improves the efficiency of battlefield elements, saves time and resources, and adds value for combat capability. There are various levels, including the lowest level, that is, an infantry soldier, which ultimately results in an amazing increase in the effectiveness of combat operations. Recent developments in microelectronics, mechanics, and ergonomics, as well as the movement and return, the importance and emphasis from tanks and missiles to soldiers, have examined future soldier projects. Electronic science has led to the integration of small individuals with advanced technology equipment and infantry soldiers with advanced communication, command and control (C3) systems, or communications, command, control, computer and information (C4I). All this was to try to see the infantry soldier as a complete unit instead of a small part of the great force. Each country has its own special soldier project. Considering the importance of the subject, identifying the opportunities and threats facing the Iranian warrior is necessary. In this study, we will study the future soldier project in advanced and sensitive countries and focus on communication and Network- based systems.

KEYWORDS Network-based Warfare, Information Warfare, Electronic Warfare.

1. INTRODUCTION

Advances in information technology are not only changing the way we fight, they are also changing the nature and purpose of war. In fact, that's how the war begins. How it ends, how long it lasts, and who participates in it will all change with the pervasiveness of information and communication technology. The degree of complexity of systems does not increase just because several factors affect them simultaneously, but it is more important to understand how these factors interact with each other and interact with each other. Nowadays, due to the existence of sensitivities, networks, and communication systems, it is possible to obtain a lot of information about the battlefield and better coordinate the actions of independent military units and platforms. But all of this progress is causing the military organization and the war machine to move exactly on the brink of chaos. It is very difficult to understand what effect these parts of these networks will have on the overall performance of the military and the war machine if parts of these networks are disrupted or destroyed. In other words, due to the high dependence of modern life, especially economically, on the reliable flow of information, the meaninglessness of time and space constraints in cyberspace, and finally the availability of information and communication technology, the parties involved are very interested in opening Bob. The new war will have information. History teaches us that immediate and direct effects are usually different and generally less important than indirect effects. Every action has a reaction, and the production of each new weapon leads to the growth of new defense industries. In the field of military and combat operations, information technology transforms almost everything, from manpower training to readiness and support and even public relations. Advanced manufacturing and production of advanced intelligence and information systems not only enable the guidance and coordination of the units deployed on the battlefield, but also provide new capabilities such as

intelligence due to the inclusion of microprocessors in weapon systems. The greater intelligence of weapons, to some extent, leads to their autonomy in the act of quick decision-making. In future wars, rapid advancement in the field of information will be a key and vital factor in success. Information has been important in all past wars, but it will play a central role in future wars. In modern warfare, it is no longer possible to claim that victory depends on which side brings the most capital, personnel, and technology to the battlefield, but rather which side has the best information about the battlefield[1], Since the end of World War II there have been many advances in the areas of science, genetic algorithms[2], hardware[3], software[4], phase lock loops[5], distributed production resources[6], Neural networks [7], cryptography and watermarking[8].

2. NETWORK-BASED WARFARE:

The term network-based warfare is a way of thinking about military operations in the information age and the relationship between intelligence superiority and competitive superiority. Network-based warfare is an instrumental concept. It is a tool for empowering strategies to achieve goals.It can be used at all levels of war and does not depend on the size and composition of the force, mission and geography. Advanced Network Warfare uses advanced information technology to connect the components of power through extensive, integrated local networks, and with the help of the basic concepts and principles of warfare, to dramatically increase military capabilities and, in fact, to collect, process, and manage information. It relies on the use of existing power in information networks.

3. NETWORK-BASED WARFARE STRUCTURE

Network Warfare consists of three basic elements: information tour, sensor tour, and tour, which we will explain below.

3.1. Information Tour

Physical infrastructure that allows communication, processing, storage, flow, and data protection.

3.2. Sensor Tour

A set of sensors, such as radars and ES receivers, that provide information or data needed to know the battlefield.

3.3. Firefighting Tour

The design and execution of combat operations is based on the information obtained from the information tour in this tour.

4. WARFARE ZONES

To understand how information affects our ability to conduct military operations, consider the following:

4.1. Physical field

The physical realm is where conflict, attack, defense, and maneuvering take place, and can be land, sky, or sea, where there are physical platforms and communication networks, and ideally in Network- based warfare, all the components of force are in it. The domains are networked to enable confidential and integrated communication and interaction.

4.2. Information Field

Where information is created, created, collected and distributed, and the exchange of information between the components of the force is possible, and the commands of the new military force control command are transmitted. Ideally, in this area, the force has the ability to share, access, and protect information by linking, combining, and analyzing to create and maintain an intelligence superiority over the enemy.

4.3. The Field of Perception.

It is a realm in the mind of the components of power, and it is a place where perceptions, consciousnesses, thoughts, and beliefs exist, and it is a place where decisions are made, and it is a place where many wars lead to victory or defeat.Ideally, in this field, the force has the ability to create high-quality awareness and share it, and the ability to create the same understanding, including the commander's intent

5. BASIC CONCEPTS OF NETWORK-BASED WARFARE

5.1. Information Superiority

The ability to create and use information by local forces and destroy this ability for the enemy, and the most important feature of network-based warfare is to turn this superiority into combat capability. To compare two forces in terms of information superiority, the ratio of the information needs of one force to another is considered. The most important determinants of information needs or the amount of needs for a force are defense or offensive orientation, operational concepts, type of weapons and platforms, risk level, ability to accept military and civilian casualties, and so on.

5.2. Information Superiority Methods and Tools

A. Classical military methods

Such as: destruction of facilities, deception and denial or denial of information

B- Computer methods such as using viruses

C- Jaming and listening methods

D- Using public telecommunication environments

E) Using enemy information systems or information received from him.

5.3. The Superiority of Decision Making.

Decision-making superiority means the ability of a

combat system to make better decisions faster than the enemy, and decision-making superiority is made possible by superior intelligence. Superior decisions are made when information is passed through the filter of experience, knowledge, training, judgment, and judgment of a commander and his forces, and the commander's ability to achieve decision-making excellence is not necessarily automatically derived from information superiority.

5.4. Cooperation

"Collaboration means the active sharing of data, information, knowledge, knowledge (awareness of situations) or concepts during teamwork to achieve an effective common goal." Cooperation has various dimensions, each of which can change and includes: environment, time required, continuity, scope, structure and role of members; Cooperation in many military situations is difficult and impossible unless advanced technologies are available, and further cooperation depends on the mutual understanding of members. In other words, members must be familiar with each other's national and organizational backgrounds, teachings, and cultures. Otherwise, it will take some time to introduce and discuss the various features within the group. In addition, the role of members must be recognized in order for effective cooperation to take place.

5.5. Synchronization

The output synchronization of command and control processes is considered to regulate the actions in order to achieve the goal and to continuously coordinate their communication in time and space.

The following are required to achieve synchronization:

A: The organizational concept of command and control

B: A level of centralization that provides appropriate guidance and flexibility for the environment, mission, troops, and intelligence support facilities.

6. EVALUATING AND IMPLEMENTING NETWORK-BASED WARFARE

Network-based warfare creates an all-encompassing network between local forces that increases their combat capability, and by providing intelligence superiority, accelerating and streamlining the flow of information between individual units, sharing intelligence, and accelerating the command and control process, seeks to excel in all military dimensions. Achieve victory in future battles.

Because network warfare is young and growing, and especially for developing countries that lack information on modern technology, they need to address the shortcomings over time.

6.1. Restrictions on the Implementation of Network-based Warfare

* Lack of support for existing information infrastructure and human processes within it from network-based concepts and operations

* The incompatibility of the organizational structure of the forces with the required structure of the Network-based warfare and the high vulnerability of the existing structure, the lack of suitable conditions for emergence

* Experiment with innovation and turn these ideas into military capabilities

* Lack of sufficient experience and lack of necessary conditions to gain real experience and test the lack of full support for information technology from the implementation of network-based warfare

* Lack of sufficient resources and scientific foundations, tools of measurement criteria necessary to understand network-based warfare processes

* Restriction on the coordinated expansion of compatible units with network-based warfare.

6.2. The First Steps to Implement Network-Based Warfare, Taking into Account the Limitations

* Expanding rituals, measures, methods, trends and organizational behaviors for network-based operations

* Creating new rules of warfare in the information age and improving network-based warfare theory by modeling, simulating and testing,

* Accelerate the deployment and application of network-based warfare concepts and capabilities

* Beginning of the joint forces networking process at the strategic, tactical and operational levels

* Scientific experience of network-oriented concepts and capabilities to develop better methods of conducting network-based operations

* Consider the challenges of network-based operations between different forces

* Battle scene management, collecting information by secure links (links 16 and 22) and providing it to command control and analysis by experts and sending it to carry out the mission.

6.2.1. Strategic Area

Important orders are sent to the Commander-in-Chief under difficult conditions from the President, the Pentagon and the Secretary of Defense via long-range drones, satellites and B1 / U2 aircraft.

6.2.2. Tactical domain:

Signal information is received through E2C / D, C-130 and Shenuk aircraft and provided to the control of the command.

6.2.3. Operational domain

In addition to collecting information via regional AWACS and JSTAR and KC35 aircraft, the information

received from tactical and strategic, all information is analyzed by skilled experts and then to users through secure communication links and Resistant to enemy electromagnetic waves.

7. ESTABLISHING A SECURE COMMUNICATION NETWORK

Information technology is both an opportunity and a threat. If we do not pay as much attention to its "security" as we do to its development and learning, it could easily become a major threat. Given the growing need for new and innovative technologies in the field of information and communication, the need for an information security management system is becoming more apparent.

7.1. 3D Protection of Organization Information

* Maintain confidentiality of information by ensuring access to information only by authorized persons.
* Maintain the integrity of the information in terms of accuracy and completeness and processing methods
* Ability to access related information and assets by authorized persons when needed.

7.2. Causes of Security Problems

The causes of security problems are:
* Weak technology,
* Weak configuration
* Weak policies

7.3. Weakness of Technology

Weaknesses of technology include: weakness of TCP / IP protocol, weakness of operating system and weakness of network equipment.

7.4. Weakness of Configuration

* Unsafe use of user accounts
* Use a system account whose password is easily recognizable.
* Lack of proper configuration of Internet services
* Non-secure default settings in some products
* Lack of proper configuration of network equipment

7.5. Weak Policies

Perhaps the main weaknesses are the lack of a written security policy, the existence of organizational policies, the abandonment of network security management, installation and making changes contrary to defined policies, and the lack of codified plans to deal with unforeseen events.

7.6. Security process:

In general, the security process can be classified into computer security, network security, organization security, and user security. In order to achieve secure information systems, native standardization of all information networks is necessary according to the needs, so the purpose of preparing the standard is to provide a model based on which an information security management system can be created, implemented, exploited, monitored, reviewed, Maintain and improve and upgrade. According to this view, it is often not possible to secure the information exchange space of organizations, and this needs to be done continuously in a safety cycle, including design, implementation, evaluation and correction.

7.7. Tips for all Standards:

* Determining the steps of securing and how to form the information and communication security cycle of the organization
* Details of safety steps and technical techniques used in each step
* List and content of security plans and programs required by the organization
* Necessity and details of establishing policy-making, executive and technical organizations to provide information and communication security of the organization
* Security controls required for each of the organization's information and communication systems

7.8. Implementation and Operation of Information Security Management System

A) The organization is required to develop a risk management plan in which the management measures, resources, responsibilities and management priorities determine and identify information security risks.

B) In order to achieve the set control objectives, the organization must implement a risk management program and take into account the necessary financial resources and maps and responsibilities.

(C) In order to achieve the control objectives, the organization must implement the selected control measures.

D) The organization must determine how to measure the effectiveness of control measures or a set of control measures.

E) The organization should implement training and awareness programs.

C) The organization should manage the operation of the information security management system.

G) The organization should be able to immediately identify security incidents and respond to security incidents.

7.9. Maintaining and Upgrading the Information Security Management System

A) The organization will be required to implement the reforms specified in the Check phase.

B) The organization must take appropriate corrective and preventive measures and apply what it has learned from the experiences of other organizations.

C) The organization should provide all the stakeholders with measures and reforms by mentioning the details.

(D) The organization shall ensure that the amendments meet its objectives.

E) Vulnerable points or threats that have not been properly considered in the previous risk assessment;

C) Results from effective measurements;

H) Follow-up measures from previous management reviews;

(H) Any changes that may affect the information security management system;

G) Recommendations and suggestions for improvement.

To make the operation a success on the battlefield, you need to create strong and impenetrable communication links to communicate command control with other users, otherwise the operation will fail.

7.10. Communication Platforms Links 11, 16 and 22

Today, the link16 communication network plays an important role in the battlefield. So that all air, sea and ground forces benefit from the above communication layer simultaneously and network. Due to the use of anti-disturbance methods such as frequency jumping (FHSS) with a jump rate of more than 70,000 jumps per second and direct tracking (DSSS), these communications are very secure and stable on the battlefield.

8. CONCLUSION

The results of the analysis of this article on network-based wars are as follows:

* Access to accurate information and threat (data collection) for scene management battle

Upgrading and updating electronic collection systems, electronic warfare and:

* Training in all dimensions:

* Threatology (analysis and extraction of signal parameters)

* Doing the right disruption (technique and tactics)

* Commitment and work conscience (template)

* Secure communication links

* Unified management

REFERENCES

[1] G. Liu, H. Gu, W. Su, H. Sun, **"The Analysis and Design of Modern Low Probability of Intercept Radar",** *2001 CIE International Conference, Page(s)*, pp. 120-124, 2001.

[2] Talati and Heshmat Noori. **"A Generic Algoritm Approach to Optimal Placment of Switching and Protective Equipment on a Distribution Network."** Vol. 11, No. 3, FEBRUARY 2016.

[3] O. Sharifi-Tehrani and S. Talati, **"PPU Adaptive LMS Algorithm, a Hardware-Efficient Approach; a Review on"**, *Majlesi Journal of Mechatronic Systems*, Vol. 6, No. 1, Jun. 2017.

[4] Hashemi. S. M., Abyari. M, Barati. Sh., Tahmasebi S., Talati, S. **"A Proposed Method to Controller Parameter Soft Tuning as Accommodation FTC after Unknown INPUT Observer."** *ARPN Journal of Engineering and Applied Sciences*, Vol. 11, No. 5, MARCH 2016.

[5] S. Talati, A. Rahmati, and H. Heidari, **"Investigating the Effect of Voltage Controlled Oscillator Delay on the Stability of Phase Lock Loops"**, *MJTD*, Vol. 8, No. 2, pp. 57-61, May 2019.

[6] S. Talati, B. Ebadi, H. Akbarzade **"Determining pf the fault location in distribution systems in presence of distributed generation resources using the original post phasors",** *QUID 2017, pp. 1806-1812, Special Issue No.1- ISSN: 1692-343X, Medellín-Colombia*. April 2017.

[7] S. Talati, M. HasaniAhangar, **"Analysis, Simulation and Optimization of LVQ Neural Network Algorithm and Comparison with SOM"**, *MJTD*, Vol. 10, No. 1, Jan. 2020.

[8] S. Talati, P. Etezadifar, **"Providing an Optimal Way to Increase the Security of Data Transfer Using Watermarking in Digital Audio Signals"**, *MJTD*, Vol. 10, No. 1, Feb. 2020.