PRINCIPLES OF OPERATIONAL COMMUNICATIONS SYSTEM

Colonel (ret.) Professor Gruia TIMOFTE, Ph.D*
(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania)

Abstract: *This article includes a brief analysis of the principles of tactical and operational communication systems used in modern combat space, highlighting their requirements and qualities in ensuring an optimal information flow for the development of complex military actions. They are the core around which they develop and satisfy the requirements for command and control, as well as for complex integrated systems (C3I, C4I, C4ISR, C4IRISTA. etc.) being substantiated and developed in the following period. The continuously growing information requirements and the explosive technological developments in the field require the highest priority approach to the study, design and realization in record time of the means for these integrated systems.*

Keywords: *command and control, integrated system, information requirements, connectivity, transfer.*

1. Introduction

The big operative and tactical units require a secure, robust, and reliable communications system to assimilate information, communicate and exercise authority, and direct forces in large geographic areas and a wide range of conditions. A communications system must provide connectivity from the strategic to tactical levels in order to plan, conduct, and sustain operations, and enable information superiority[1].

The communications system is main tool to collect, process, store, disseminate, and manage information; supports the development and dissemination of the commander's intent and planning guidance, fostering decentralized execution. The communications system enables the inter-connection (networking) of geographically separated forces, which permits network-enabled operations to exploit information and networking technology to integrate dispersed human decision makers, situational and targeting sensors, forces and weapons into a comprehensive system. Network connectivity is mission-critical and can determine mission viability during planning and execution[2].

2. Operational Communications System Principles

Big unit employment decisions are influenced by the communications system's ability to network the force, and this links

* Full-member of Academy of Romanian Scientists, email: timofte.gruia@gmail.com.

[1] JP6-0, *Joint Communications System,* Joint Staff, Washington, DC, 2015, pp. I-4 to I-8.

[2] FINCKE DALE, *Principles of Military Communications for C3I*, Army Command and General Staff, Fort Leavenworth, Kansas, 1986, pp. 5-9, 22-23, 31-32.

network control to C2 (Command and Control) prioritization and decisions. The communications system must be interoperable, agile, trusted, and shared to provide the flexibility to dynamically meet mission objectives[3].

2.1. Continuity

Definition: The unbroken and consistent existence or operation of something over time.

Synonyms: continuation, persistence, durability, endurance**.**

Continuity of communication has risen to contemporary prominence for several reasons: the increased maneuver tempo and depth of modern combat operations; development and fielding of more complex and lethal weapons and information systems; the inherent necessity for mobility and dispersion of command post functions as well as combat and sustain forces; the increased ability of the enemy to disrupt communications systems, etc. In short, continuity of communications--flawless transmissions of information critical to the commander-- is much more important than volume to the continuity of command and control. The means by which such continuity of communications is attained consist of the application of the qualitative subordinate elements of: *survivability, reliability, redundancy*, and *repair-ability*[4].

Survivability is the capability of the communications to sustain combat loss or degradation and continue to provide requisite information flow and direction among the commander, his staff and all other forces involved. Since there will always be combat losses and degradation, the key questions which must be answered are whether communications can be made survivable at an affordable cost and with what resultant (C3I, C4ISR, C4RISTA, ISCC - integrated systems for command and control, etc.). another important subordinate element of continuity of communications is *reliability* (dependability, responsibility, trustworthiness; the quality of being trustworthy or of performing consistently well).

The effectiveness and quality of the entire ISCC process depends on the reliability of the communications means and the consistent acquisition and exchange of information and direction. On the other hand, competence in decision making depends largely on the quality and completeness of critical information used. Decisions made with insufficient information can be dangerous because they can lead to arbitrariness. The contemporary combat environment is different from that of previous conflicts because of the significant increase in numbers and complexities of modern combat and support systems and the decrease in time available to acquire, decide, disseminate, coordinate, and synchronize. These must be accomplished

[3] ROBERT GALLAGER, *Principles of Digital Communications*, Cambridge, 2007, pp. 1-3, 11-14.
[4] *Ibidem*.

within the required time constraints and under the expected operating conditions. The communications means should ensure that the time necessary to transfer information and direction, without sacrificing security and exercise of initiative and surprise by striking before the enemy can react.

A final caution on reliability of communications: reliability as defined by engineers for components of a system does not always translate directly into combat effectiveness for the commander. The total communications means must be evaluated against combat effectiveness and usefulness to the commander and his total ISCC requirement.

Communications systems reliability can be significantly improved through *redundancy*, the third subordinate element of the principle of **continuity**. In general, the properties and structure of the communications system must reflect the overall requirement for which it was intended. For a commander and his staff to entrust command and control responsibilities to a communications system, they must have confidence in the availability of critical information when and where they need it. A redundant communications system directly supports the principle of **continuity** by providing critical information availability continually throughout the battle area. This information must be processed by intelligent source terminals at points of use, whether grouped or geographically dispersed. The system should permit an interactive conversational exchange of ISCC information. It should permit all sources to be interconnected, however heterogenous and regardless of their internal designs, and to share and exchange information. It should also provide decentralized capability for real time information re-routing. Decentralization of capability and control ensures that the failure of any single communication means will disrupt only that single path. Related information elements, even though stored at multiple source terminals and transmitted by multiple means must able to be updated as changes occur and acted upon by one or more user terminals as required to accomplish the C3I mission. A redundant communications system also supports principle of **security** by promoting indeterminacy *(the state of not being measured, counted, or clearly known.)* of communications. Thus, the qualitative criteria for redundancy of communications are the abilities of source term: to exchange critical information, provide multiple source terminals or intelligent devices access to the same information transfer network, make the communications system transparent to the source (e.g., user), and to provide automatic, real-time re-routing and reorganization within the network. The entire system doesn't have to be redundant, only the number of

paths necessary to ensure the required degree of availability under identified conditions[5].

Continuity of communications can be significantly improved through *repair-ability* (the fault tolerance ability of the system to detect, diagnose, contain and repair its own failures). The qualitative criterion for *repair-ability* is how automatic it is. This requires that the communication means are partitioned in such a way that any component can diagnose itself and its subordinate parts. This suggests that critical control functions must be decentralized so they can vary as new users and requirement are added to the communication system--a complex requirement. Adding to this complexity is the need for a compilation of the options and available routes to be maintained in real time, so that the system can reconfigure continually as the situation dictates. Finally, complete and concise information related to the failure or damage and the maintenance procedures required must automatically be communicated to those responsible for operation and maintenance.

2.2. Homogeneity

Definition: Quality or state of being all the same or all of the same kind.

Synonyms: become homogeneous or similar, equalize, match, make equal, uniform, corresponding, or matching.

Homogeneity of communications is achieved by selecting uniform means and methods to achieve integrated information acquisition and transfer. Application of this principle assures the commander capability to synchronize direction of combined arms, all support units of the other services and allies at the tactical and operational levels. The preceding examples show how the concept of **homogeneity** of communications affects the ability of the commander and his forces to achieve unity of effort.

The subordinate elements which support this principle are *modular commonality, network synthesis and integration*.

Modular commonality is the physical and electronic standardization of component parts of joint service communications means, such that they can be temporarily or permanently combined with other such assemblies without loss of interoperability. Such commonality can be achieved only through common design. Every effort should be made to ensure minimum size and weight and simplicity of operations without loss of inter-operable performance, flexibility, or reliability[6].

---

[5] SIMON HAYKIN, MICHAEL MOHER, *Introduction to Analog&Digital Communications,* Ontario, Canada, 2017, pp. 11-16.

[6] M*ilitary Communications and Information Technology a Trusted Cooperation Enabler*, Vol. 1, Military University of Technology, Warsaw, Poland, 2012, pp. 417-419.

Components should be easily changed, faults capable of being diagnosed down to the sub-unit level, and minimum amounts of spares carried. The communications means should be capable of efficient operations after only a brief period of instruction, so that it can be used by relatively unskilled personnel. It should be capable of efficient operation in the expected battlefield environments, in high ambient noise levels and while stationary or on the move.

In sum, the qualitative criteria for modular commonality are: the extent of inter- and intra-service communications interoperability, the degree of standardization of the component parts among the services, the flexibility provided the commander to tailor his communication requirements to fit the situation, and the ease with which non-technical personnel can reconfigure or repair the communication means.

So characterized, this subordinate element of **homogeneity** of communications promotes inter- and intra-service cooperation, reduces and simplifies logistics, is adaptable to NATO standardization agreements for coalition interoperability, and provides the commander with a significant reorganization capability. It is also the means by which to develop a universal compatibility among source ISCC terminals and communication networks[7].

Perfect *commonality* may be difficult to achieve, but the degree to which modular commonality is achieved will have a direct effect on the introduction of improved equipment into the force. The lack of upward and downward compatibility requires force package fielding of improved capabilities in unit sets for all units required to communicate with each other.

Network synthesis is the ability of communications to provide automatic passive and active connectivity to all terrestrial and non-terrestrial means for all required users, regardless of whether they are mobile or stationary. This enables any user, regardless of how or by what mode he is connected into the communications system to achieve immediate and automatic connectivity with any other user. This is accomplished without the caller needing to be aware of the other party's physical location and without any constraint resulting from distance or mode of communication, provided that at least one available route exists between both. This ensures two-way, multi-mode, multi-means ISCC information transfer among higher, lower, and lateral headquarters, and among supporting air, land, sea, space and allied elements.

[7] ANGELA YARNEL, CINDY DULLEA, Principles of Effective Communications, Walter Reed Army Institute of Research, Maryland, 2018, pp. 170-173.

The use of satellite communications must be an integral component of *network synthesis*. The contribution of satellite communications to achieving depth, agility and synchronization deserves special consideration.

Integration is the automatic interconnection of user source terminals with the communications system.

In the design and development of integrated ISCC ingenuity and automation offer large rewards in assisting field commanders to employ and control their resources effectively and responsively.

Information acquisition, processing, and transfer is a continual process not inhibited by maneuver or location on the battlefield because access to the communication system is automatic. The command post contains its own internal power source, is environmentally self-contained, configured for both wheeled and tracked vehicles and, through homogeneity of equipment, can be readily re-configured and repaired. Staff operations can be dispersed for survivability without penalty to the exchange of required information.

2.3. Versatility

Definition: Ability to adapt or be adapted to many different functions or activities.

Synonyms: creativity, inventiveness, originality, resourcefulness, imaginativeness.

Versatility is the ability of communications to adapt readily to unforeseen ISCC requirements. This must be achieved without restricting the agility of the commander's forces or his exercise of initiative and synchronization. To accomplish this, commanders and their staffs require versatile communications which can adjust to their changing needs. The subordinate elements which support this principle of communications are agility, flexibility, decentralization and autonomy.

Agility of communications is ability to support the maneuver of supported forces. Such agility is achieved through a combination of the mobility of components of the system and their electronic elasticity. Maneuver is the centerpiece by which to gain positional advantage, achieve surprise, and concentrate decisively to sustain the initiative to command immobility or the inability of the forces to execute the will of the commander[8].

Electronic ISCC elasticity describes the ability of the system to expand, contract, or change electronically as the situation evolves. At the tactical level it permits moving force elements to communicate with

[8] *Manual for Employing Joint Tactical Communications,* Joint Staff, Washington, DC, 1998, pp. II B1-B6.

adjacent, higher, lower and support elements without the constant movement of the supporting network.

The qualitative criteria for agility of communications are:

- whether it possesses the physical mobility characteristics to accompany forces and headquarters, and whether it is sufficiently elastic to sustain ISCC with the required elements without continual physical movement of the entire network.

Flexibility is also an integral subordinate element of the principle of *versatility* of communications. While agility expresses the ability of communication system to move and project command and control as fast as the force it supports, flexibility of communications enables prearranged concepts, plans and operations to be altered to meet changing situations and unexpected developments. The communications system must be capable of adapting to these new circumstances regardless of the original configuration, so that it is possible rapidly to plan, coordinate, and shift operations to gain or prevent surprise.

Implicit in flexibility of communications is the ability to accommodate component change whether through force expansion or change in the character of supported forces.

The complexity of modern weaponry, associated control systems and the sophistication of information acquisition means have resulted in unpredictable uses and increases in the volume of information flow.

Decentralization of communications demands network synthesis. In return, it greatly increases the autonomy of individual commanders in their engagement or battle and reduces the need for centralized staffs.

Survivability requires staff functions be dispersed, the loss of efficiency of the staff in support of the command should be minimized.

Decentralization of command and control requires uniform access to critical information throughout the battlefield. That access requires reliable and unrestricted exchange of information among local, higher, lower and lateral commanders, forces and staffs. In turn such a reliable and unrestricted exchange requires a dynamic, multiply connected, integrated but decentralized system of communications means.

Autonomy, another important subordinate element of **versatility**, is also essential to decentralized command and control.

The qualitative criteria for autonomy are the ability of local ISCC capabilities to maintain current information until interrupted, and to function effectively in a stand-alone mode given an interruption of communications with higher headquarters. Autonomy can be enhanced by automation through the concept of local area network capability that can interconnect with the larger systems.

2.4. Security

Definition: Security is the state of being or feeling secure; freedom from fear, anxiety, danger, doubt, etc.

Synonyms: certainty, safety, reliability, dependability, etc.

After the principle of **Continuity**, the principle of **Security** of communications becomes the next most important element of command and control. A communications system which lacks adequate security for is not only a disadvantage, but worse, can threaten the very integrity of the force.

Security of communications for ISCC is significantly enhanced when the opposing force is presented with a picture of battlefield electronic indeterminacy. This requires the creation of random and redundant nodality throughout the battle area, completely unassociated with any single or multiple sources, or echelons.

This concept also provides multiple routes for information acquisition and transfer. The system should be self-organizing with the sources (e.g., users) free to relocate without regard for the location of communications nodes, but able to find multiple access. Transmission characteristics are adjusted automatically for optimum continuity and security. The nodes themselves could be both attended and unattended. The proliferation of attended and unattended communication nodes facilitates network synthesis.

Digital transmission conveys information in the form of bits (binary digits). A bit is always one of two things (pulse or no pulse, mark or space, 1 or 0, yes or no). By way of contrast, analog transmission conveys information by sinusoidal waves of continuously varying amplitude, frequency or phase, and every minute perturbation of the wave implies a corresponding degradation of the information content. *In analog transmission* the disturbance, once introduced, cannot be eliminated; the information content is degraded and ultimately the accumulated degradation limits total systems performance. *In digital transmission* however, minor perturbations of the signal do not change the information content[9].

The point therefore is simply this: in digital transmissions the degradation of the received signal by the transmission system does not alter the information content until the degradation is so severe that the receiving equipment reads a pulse as no pulse or vice versa.

Because of this fact, digital transmission is not limited by accumulated degradation, and, with digital error detection and correction techniques, the degradation threshold can be significantly raised.

[9] CRISTOPHER CARDINE, *Digitization of the Battlefield*, US Army War College, Carlisle, Pensylvania, 1994, pp. 18-21.

These characteristics also affect the reliability with which information can be re-transmitted over long distances by repeaters. A digital repeater reads its input signal, extracts the information and uses it to generate a new output signal for the next transmission section. Thus, with digital repeaters, there is no limit to the transmission distance which facilitates electronic elasticity. By contrast, analog repeaters are not regenerative and the output signal contains all of the accumulated degradation of the input signal.

Digital systems also have the advantage of greater information transfer capacity at quicker rates, greater security and clarity, high speed efficient and reliable switching and routing. And because it is independent of the transmission media (e.g., radio frequency, cable, optical, etc.) digital transmission readily accommodates improvements in these media[10].

To exploit the advantages of digital transmission it is necessary to convert primary source information into digital form for transmission and reconvert the digital information to an appropriate useable form at the receiver. Hence, the qualitative criteria for digital transmission are: that all future source (e.g., users) systems have the capability to convert information to a digital form, with integral error detection correction techniques, for information transfer, and that communication systems transfer information throughout the tactical and operational levels of battle by digital transmission. Communications should also have the integral capability, at all locations, to interface with available host nation and allied communication means, which, in all probability, may not be digital nor secure. Communications Security (COMSEC) must be integrated into the system which it supports rather than being one of a series of black boxes. COMSEC should be invisible to the user and not introduce technical complexity which limits the flexibility and usefulness of the communication means. To do otherwise will not only inhibit the ability of commanders to exploit the opportunities that their initiative has presented them, but may provide the originating or terminating source terminals, also subject the ISCC system to be quickly attacked by conventional enemy weapons systems. The qualitative criterion for COMSEC means is that information be transmitted in such a manner than it is useless to the enemy in real time and is as difficult as possible for him to understand at some later date. COMSEC equipment and techniques should be consistent with the principles of **Homogeneity, Versatility**, and **Simplicity**; provide traffic flow security, node-to-source and trunk security, and special compartmental security as needed, for voice, data, record, graphic and video information

[10] NICK REYNOLDS, *Getting Tactical Communications for Land Forces,* Rusi Journal, Vol. 166, London, 2021, pp. 64-67.

transfer; and should also accommodate, automatically, interconnection of the secure and non-secure communications for coalition information exchange.

A final subordinate element of the principle of SECURITY of communications for ISCC is the requirement automatically to employ *stealth* "type" techniques to eliminate or deceive the enemy as to the visual, aural, photographic, thermal and electronic signatures of the communication means. Items to be concealed include, but are not limited to, vehicles, power generation equipment, antenna systems, personnel, unattended nodes, cables, etc. Such concealment preserves the commander's communications combat effectiveness. The qualitative criteria for *stealth* in **Security** of communications for ISCC are: the degree to which the physical properties of communication nodes and source emitters are concealed from hostile detection, and the provision for protection against unacceptable damage or restrictive interruption of the communications mission. Included in this is the requirement for adequate self-defense from air and ground attack environment without degradation of communications performance effectiveness[11].

2.5. Simplicity

Definition: The quality of being easy to understand or use.

Synonyms: clearness, innocence, naturalness, uniformity.

Simplicity of communications is the ease with which the commander, his staff and soldiers use it, operators operate it and maintainers maintain it. The principle of simplicity of communications facilitates the application of the other operational principles of military communications. Simplicity in the form of increasingly sophisticated systems has had and will continue to have, a profound effect on the shaping of the conduct and efficiency of military operations at all levels of warfighting. Nowhere is this more apparent than in ISCC where the soldier, the commander and his staff have become more and more cybernetically connected with sophisticated equipment. The elaborate and sophisticated electronic, automated, command and control systems must be intelligible to those who use, operate, and maintain them and provide the commander and his staff the ability to anticipate and make changes in the probable course of forthcoming combat operations.

The two subordinate elements of the principle of **Simplicity** of communications for ISCC which must be considered are *technological sophistication* and application of *human factors*. When reviewing the two subordinate elements of the principle of **Simplicity**, consider the following: performance requirements to lead the increased technical sophistication,

[11] Joint Concept: *Multi-Domain Integration, Annex A*, MoD, London, 2020, pp. 72-73.

while consideration of human factors should lead to increased operational simplicity.

Technological sophistication is the totality of technological means and methods applied to implement the principles of military communications for ISCC while ensuring communications are more reliable, more maintainable and easier to operate in combat.

For communications, the criteria for technological sophistication are: does it improve the quality, continuity, and performance of the commander' s aggregate ISCC capability in combat; does it improve the speed of information acquisition, transfer and distribution; does it improve the versatility of the communications equipment; does it improve the homogeneity of communication; and, does it improve and simplify the operation and maintenance of communications[12].

Human Factors. Further, communications which drive rigid patterns of operations or centralization may be counter-productive and extremely vulnerable in a mobile combat environment. Very often if sophistication in ISCC equipment, techniques and procedures leads to complexity (the opposite of **Simplicity**), it is because of the failure adequately to consider people requirements. The latest technical equipment will only provide assistance to the commander and his staff and, therefore, must be simple to use and maintain under extremely difficult combat conditions. Users and maintainers must, without becoming technologists, be more intelligent, responsible, and more adequately trained than ever before to cope with the unprecedented capabilities communications available on the battlefield of the future.

3. Conclusions

In the complex landscape of modern warfare, battlefield communications play a pivotal role in enabling efficient coordination, decision-making, and response mechanisms. These systems integrate various technologies, such as radios, encryption protocols, data links, and satellite networks, to establish secure and reliable channels for transmitting sensitive information. Essentially, battlefield communications serve as the backbone that connects different elements of the military forces, facilitating maneuvers and real-time exchanges of critical data. Operating under the principles of speed, accuracy, and security, effective communications ensure that command structures remain resilient and responsive amidst the chaos of combat. With the evolution of warfare tactics and technologies, maintaining robust and adaptable communication networks is essential for mission success.

[12] Jack Watling, *Supporting C2 for Land Forces on a Data-Rich Battlefield*, London, 2023, pp. 20-23.

International Panel on the Information Environment[13] concludes: 65% of experts agree that the most important feature on a healthy information environment is the availability of accurate information; owners of social media platforms are the greatest threat, followed by governments, politicians and political parties and 63% of experts expressed concerns about the potential of generative Artificial Intelligence to perpetuate biases, amplify harassment and spread misinformation.

BIBLIOGRAPHY

JP6-0, *Joint Communications System,* Joint Staff, Washington, DC, 2015, pp. I-4 to I-8.

FINCKE DALE, *Principles of Military Communications for C3I*, Army Command and General Staff, Fort Leavenworth, Kansas, 1986, pp. 5-9, 22-23, 31-32.

ROBERT GALLAGER, *Principles of Digital Communications*, Cambridge, 2007, pp. 1-3, 11-14.

SIMON HAYKIN, MICHAEL MOHER, *Introduction to Analog&Digital Communications,* Ontario, Canada, 2017, pp. 11-16.

M*ilitary Communications and Information Technology a Trusted Cooperation Enabler*, Vol. 1, Military University of Technology, Warsaw, Poland, 2012, pp. 417-419.

ANGELA YARNEL, CINDY DULLEA, Principles of Effective Communications, Walter Reed Army Institute of Research, Maryland, 2018, pp. 170-173.

Manual for Employing Joint Tactical Communications, Joint Staff, Washington, DC, 1998, pp. II B1-B6.

CRISTOPHER CARDINE, *Digitization of the Battlefield*, US Army War College, Carlisle, Pensylvania, 1994, pp. 18-21.

NICK REYNOLDS, *Getting Tactical Communications for Land Forces,* Rusi Journal, Vol. 166, London, 2021, pp. 64-67.

Joint Concept: *Multi-Domain Integration, Annex A*, MoD, London, 2020, pp. 72-73.

Jack Watling, *Supporting C2 for Land Forces on a Data-Rich Battlefield*, London, 2023, pp. 20-23.

Expert Survey on the Global Information Environment, Summary, IPIE, Zurich, Switzerland, 2024.

[13] *Expert Survey on the Global Information Environment, Summary,* IPIE, Zurich, Switzerland, 2024.