УДК 623.618

Y. Pashchuk, Y. Salnyk

Army Academy named after Hetman Petro Sahaydachnyi, Lviv

IMPLEMENTATION OF ISTAR IN UKRAINIAN ARMED FORCES

The article reveals appropriateness and means of ISTAR implementation in the Intelligence System of the Ukrainian Armed Forces. This study is urgent for developing of effective military intelligence of Ukraine.

Key words: *concept, intelligence system, ISTAR system, intelligence cycle, intelligence, surveillance, target acquisition, reconnaissance, interoperability, NATO.*

Problem statement

Analyzing advanced intelligence systems and their support to military forces across the operational continuum we should underline a key role of national and coalition integrated ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) systems in achieving of information superiority, namely, ability of armed forces to "see first, understand first, act first, and finish decisively" [22]. In its macroscopic sense, ISTAR is the process of integrating the intelligence process with surveillance, target acquisition and reconnaissance tasks in order to improve commander's situational awareness and consequently their decision making. Applying of ISTAR assets creates an intelligence synergy and provides a dynamic and continuing process of collection, processing and dissemination of timely, accurate, relevant and reliable information and intelligence on the composition, deployment activities and capabilities of an enemy force, together with terrain and meteorological data that is essential to the successful prosecution of combat operations.

The ISTAR operations are conducted by the world leading countries during peace, crisis, and war. Practically, the USA and other North Atlantic nations have been using the ISTAR systems within broad strategic, operational, and tactical operations since 1990-s. It should be considered that one of the first Alliance military operations with employment of coalition ISTAR assets was a sustained NATO air campaign in Bosnia and Herzegovina (code-named by NATO Operation Deliberate Force) in 1995 [17]. In fact, in April of the same year the US Army started equipping intelligence units with AN/TSQ-219 Tactical Exploitation Systems (TES) that receive, process, exploit and disseminate intelligence data from direct downlinks and other ground stations, as well as form a key part of the US RSTA (Reconnaissance, Surveillance, and Target Acquisition) system architecture [18]. Incidentally, relevant "Doctrine for Reconnaissance, Surveillance, and Target Acquisition Support for Joint Operations (RSTA)" (Joint Pub 3-55) was adopted by the US Armed Forces in 1993 [11].

The analysis and findings from studies of recent NATO operations [8-12, 17-20] affirms that the ISTAR systems employment enhances an allied nation's ability to conduct military operations on a global theater, or regional basis, as well as capability of the North Atlantic Alliance to dominate the battlespace that arose from the advantages of gained information superiority. Apropos of this, Richard Cheney, Vice President, said [16]: "With less than half of the ground forces and two-thirds of the military aircraft used 12 years ago in Desert Storm, we have achieved a far more difficult objective ... In Desert Storm, it usually took up to two days for target planners to get a photo of a target, confirm its coordinates, plan the mission, and deliver it to the bomber crew. Now we have near real-time imaging of targets with photos and coordinates transmitted by e-mail to aircraft already in flight. In Desert Storm, battalion, brigade, and division commanders had to rely on maps, grease pencils, and radio reports to track the movements of our forces. Today, our commanders have a real-time display of our armed forces on their computer screen…"

When the most of world leading countries are on the way "The issue then . . . is not whether ISTAR is useful but how it can be made more effective" [8, 9, 12, 17-20, 23] Ukraine is facing a dilemma: how to reform (improve) its Intelligence System against the backdrop of a chronic under-funding and technological lagging of the Ukrainian Armed Forces as well as "non-aligned" (neutral) status of the recently adapted National Military Doctrine. Furthermore, permanent transformation of the Ukrainian security system, in particular the Armed Forces, has been resulted to its reduction and degradation.

Despite Ukraine is not presently seeking NATO membership, our country still has a "Distinctive Partnership" with this organization and continues practical cooperation with the Alliance in a wide range of areas including current contribution to the NATO-led missions in Kosovo and Afghanistan. The close relationship with NATO demands from the Ukrainian Armed Forces to achieve the appointed goals especially regarding military units and formations interoperability, their readiness to participate in NATO led operations. In this connection Ukraine should enhance its intelligence capabilities as well as develop ISTAR capabilities which can support tactical units when deployed in multinational missions.

The objectives of this article are to examine appropriateness and means of ISTAR implementation in the Intelligence System of the Ukrainian Armed Forces, and to analyze main tasks of the ISTAR units and their composition.

Main part

1. General analysis of ISTAR concepts

According to the military experts viewpoints [3-9, 17, 19-20] ISTAR is a 'rapidly evolving area' and a key military capability that generates and delivers specific information and intelligence to decision makers at all levels in support of planning and conducting of operations. ISTAR links intelligence, surveillance, target acquisition and reconnaissance systems and sensors to cue manoeuvre and offensive strike assets, with particular emphasis on the timely passage of critical and targeting information [5]. Moreover ISTAR is a complex management information system that includes standard protocols and procedures, appropriate architecture, key interfaces and formats needed to support military operations [12].

On the basis of the world leading countries experience of creation and combat use of ISTAR systems, the process of ISTAR implementation in the Intelligence System of the Ukrainian Armed Force can be considered as urgent necessity for further development of the Ukrainian Military Intelligence System. Inasmuch as there is no single stand alone ISTAR concept, we should examine different Alliance countries strategies pertaining to ISTAR including the common NATO concept. Their general provisions focus on the definition, elements, components, principles of, and considerations for, ISTAR as well as on fundamental approach of planning, prioritizing, tasking, and coordinating of ISTAR operations to support military forces across the operational continuum [3-12, 18-20, 23]. In short ISTAR represents the ability of intelligence system to obtain quickly information on the composition, deployment activities and capabilities of an enemy force, together with terrain and meteorological data that is essential to the successful prosecution of land combat operations. With appropriate processing this information will yield valuable intelligence and target information with which the commander can allocate force levels and resources, determine target priorities and establish the right conditions before commencing combat operations.

In view of the aforesaid Ukraine should develop its own ISTAR Concept taking into account our capabilities and relying on advanced ISTAR concepts without "reinventing the wheel". First of all regarding to definition of ISTAR, we can find out different approaches to a problem. For instance, according to the NATO Joint Publication AJP-2 (July 2003) ISTAR is defined as 'An operations-intelligence activity that integrates and synchronizes the planning and operation of sensors and assets, and the processing, exploitation, targeting and dissemination systems in direct support of current and future operations' [5].

Under the UK doctrine ISTAR provides fundamental support to Network-Centric Warfare and especially to targeting in order to achieve information superiority, improve situational awareness and force protection [8, 23]. ISTAR is 'The coordinated acquisition, processing and dissemination of timely, accurate, relevant and assured information and intelligence which supports the planning and conduct of operations, targeting and the integration of effects and enables commanders to achieve their goals throughout the spectrum of conflict' [8, 23]. As per the Netherlands Armed Forces policy 'ISTAR is a system of systems. It consists of separate systems, units, headquarters and formations that become more effective and efficient by means of interfaces and central coordination of their information and activities, without adversely affecting the responsibility of the various levels.' [19]. Above all the NATO ISTAR System is defined as not a physical system, because it consists of the protocols needed to integrate multiple national ISTAR systems, the operational concepts, architecture and interoperability framework, key interfaces and formats needed to support coalition operations [12].

Beyond that, NATO countries agreed to distinguish three principal elements of ISTAR [5]:

1. Information. It exists in the form of either raw data, or as collected, processed information.

2. Processes. ISTAR continually integrates the Intelligence Cycle with parts of the Operation Planning Process and the Targeting Cycle. ISTAR supplements, but does not replace, the Intelligence Cycle (fig. 1 below shows how they contribute to each other).

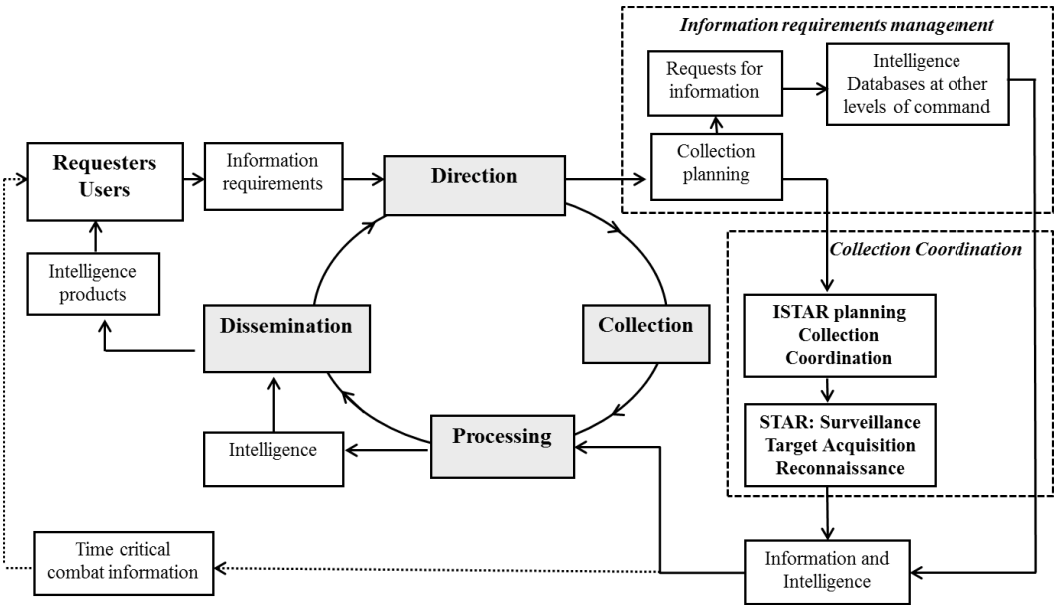

Fig. 1. **ISTAR and the Intelligence Cycle**

3. The ISTAR Architecture. This encompasses the collection assets and their controlling organisations, analysis elements, the users (requesters) of the product and the Communications and Information System (CIS) infrastructure that links them all together at all levels of command.

Furthermore, elements of the network enabled ISTAR system include the sensor platforms (i.e. satellites, fixed and rotary wing, manned and unmanned aircraft, ground and sea based sensors), their associated ground and exploitation workstations as well as network enabled remote workstations and C2IS that are not directly associated with an ISTAR system or sensors.

According to AJP-2 [5] ISTAR, as its name implies, has four primary components activities: Intelligence, Surveillance, Target Acquisition, and Reconnaissance. Intelligence is a key component of ISTAR that drives the STAR (Surveillance, Target Acquisition, and Reconnaissance) collection effort and that this in turn – feeds the intelligence analysis process (fig. 2). As any management information system ISTAR includes three domains:

– physical domain (where events take place and data are received by people and sensors),

– information domain (transmits data),

– cognitive domain (where data is subsequently received and processed).

The component parts of ISTAR are closely linked and often overlap. Together they involve four intelligence areas [7].

1. Area Surveillance. Continual area surveillance provides for the collection of general information on an enemy or potential enemy.

2. Reconnaissance in Depth. Reconnaissance in depth aims to provide detailed information in areas beyond the range of direct fire weapons. It can be initiated as the result of area surveillance or by intelligence deductions.

3. Combat Reconnaissance. Combat reconnaissance satisfies the requirements for both combat information and target acquisition essential for troops in or near contact with the enemy.

4. Target Acquisition. Target acquisition is the process of providing detailed information and locating enemy forces with sufficient accuracy to enable weapon systems to engage, suppress, or destroy those elements selected as targets. NATO allies consider that "conceptually, ISTAR is delivered through two distinct but inter-related capability areas".

1. The collection side. It aims to provide capabilities that can gather accurate and timely information across the environments and can detect, track and identify enemy, neutral and friendly entities within a defined area, day and night, and in all weathers.

2. The direction, processing and dissemination side. It aims to provide capabilities that can direct collection effort and then process and disseminate derived information and intelligence to all levels in national and coalition operations [11, 23].

Because ISTAR is an intelligence application it shares the principles of intelligence. However, there are further considerations for ISTAR [5]:

a. Command Driven. Direction of the ISTAR effort and determination of priorities must be driven by the Commander at each level of command.

b. Centralised Co-ordination. ISTAR must be coordinated centrally. This ensures the most effective and efficient use of limited resources in accordance with the commander's priorities.

c. Responsiveness and Timeliness. ISTAR must be responsive to the needs of commanders and other users,

ensuring that information and intelligence are provided to the commander in a timely fashion.

d. Accuracy. Information must be filtered and analysed to produce accurate intelligence. Intelligence must reflect the degree of confidence in intelligence assessments and judgements.

e. Robust and Tailorable Sensor Mix. The provision of a robust mix of sensor capabilities provides flexibility to the commander in acquiring the information he requires.

f. Source Protection. Collection assets must be adequately protected while gathering information.

g. Interconnectivity. A flexible, integrated, accessible network of collection assets, intelligence processes, weapon systems and situational databases is necessary to provide commanders and staffs at different levels of command with the best possible situational awareness. This network should provide the means to access information and intelligence from other formations, strategic collection systems, national and multi-national sources and agencies in order to meet the commander's information and intelligence requirements.

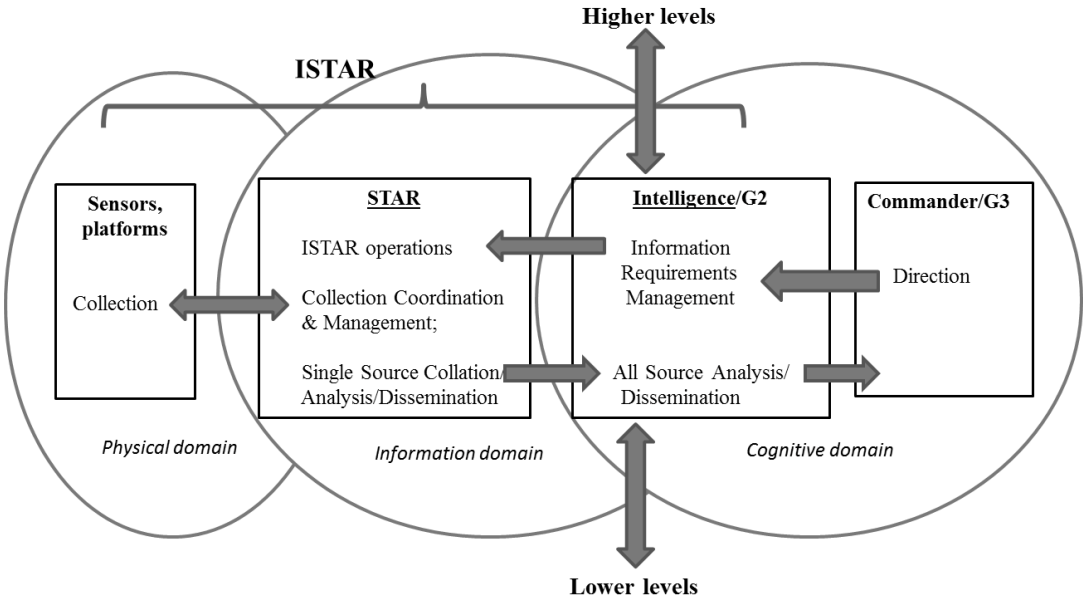

Fig. 2. **Standard ISTAR C2 Model**

The primary objective of ISTAR operations is to support military operations across the operational continuum. ISTAR operations are performed by forces with a primary ISTAR mission and other forces with either a collateral mission or the capability to perform such a mission. Modern intelligence collection systems can accumulate vast amounts of information. To be useful, the information must be relevant, accurate, analyzed, properly formatted, and disseminated in a timely manner to the appropriate user. Also, the information must be appropriately classified to protect the ISTAR system and its technology but sanitized to the degree necessary to allow dissemination to the appropriate user level. ISTAR mission areas include: indications and warning (I&W), planning and employment, and assessment [11].

Accordingly the ISTAR doctrines of NATO nations focus on how the results of ISTAR operations can be used within strategic, operational, and tactical areas. Reference mission areas and the manner in which the products are used are not meant to categorize types of systems as strategic, operational, or tactical. They illustrate ISTAR support at the various levels of war and establish the scope of application for the products of those operations. In this respect ISTAR capability can be broken down into three broad categories—Strategic, Operational and Tactical.

At the lowest tactical level it consists of individuals using their eyes and reporting what they can see, so equipping them with binoculars and a radio can significantly improve capability. At the strategic level it involves the collection and analysis of a complex range of information from maritime, land, air and space-based platforms. Low level tactical ISTAR assets (for example, thermal imagers) are organic to maritime, land and air formations where ISTAR is secondary to other functions such as targeting [8, 11, 12, 23]. Examples of the main equipment systems for the UK Armed Forces under each of the categories are set out below [8, 23]:

1. Strategic. The Fylingdales radar site provides early warning of ballistic missile threats to the UK. It is an integrated part of the US global early warning

network. And the Nimrod R1 system provided manned airborne electronic surveillance (28.06.2011 aircraft Nimrod R1 were phased out).

2. Operational. The Sea King Mk 7 Airborne Surveillance and Control (SKASaC) helicopter system operates off naval platforms or land and provides air and surface surveillance using a mix of electronic, radar and electro-optic sensors. And the Raptor reconnaissance pod system for Tornado GR4 aircraft provides long range ground surveillance.

3. Tactical. The Scarus man-portable system and the vehicle mounted INCE and Odette systems provide electronic surveillance for land forces

So ISTAR systems are key components of the intelligence systems of NATO nations that provide information and intelligence to support the commander and his decision making process and achieve information superiority 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.

2. ISTAR implementation in the Ukrainian Intelligence System

According to the military experts the continuing global expansion of information and space technologies, communications, along with proliferation of commercial and military technologies, allows even poor states, including Ukraine, to improve considerably their combat command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) capabilities, particularly create appropriate ISTAR systems. In this connection Ukraine also should exploit the real possibilities following from the Partnership with NATO nations as well as from participation of our military units in multinational operations.

Considering the actual state of the Ukrainian Armed Forces, especially, critical level of its technological development, it should be noted that implementation of ISTAR in the Military Intelligence System is possible only with stage-by-stage approach.

At the first stage Ukraine should develop its national ISTAR concept and then adopt a State (National) ISTAR Programme taking into consideration the further cooperation with the Alliance and paying special attention to intelligence interoperability on the tactical level. Beyond that, increased demands for timely and accurate surveillance and target acquisition data in NATO-led operations require from Ukraine to establish adequately manned and equipped ISTAR capabilities as soon as possible.

The previous Ukrainian military involvement in multinational missions and current political and other relevant circumstances indicate that in the near future Ukraine will continue to delegate units (most likely company or battalion sized units) for NATO-led operations. In view of the aforesaid, it is important to realize that appropriate intelligence support should be provided by a generated Ukrainian ISTAR unit (units) when contributing troops to multinational missions and this can be a starting point for launching the Ukrainian ISTAR Programme implementation.

On the basis of the NATO nations experience the ISTAR battalion is considered to be as an optimal size reconnaissance unit, tactical and modular ISTAR tool subordinated to corps (division) or brigade level. It must be a flexible force of ISTAR personnel, organizations, and equipment that provide appropriate commanders and staff with the capability to:

– direct and plan ISTAR operations;

– collect and process information;

– produce relevant intelligence;

– disseminate time critical combat information and intelligence to those who need it, when they need it.

Analyzing ISTAR systems of NATO nations and taking into account our capabilities and facility, resources we can posit that the Netherland's ISTAR concept and organization are the most appropriate for Ukraine. According to the Dutch approach ISTAR includes collecting assets, intelligence (analysis) elements and systems, military units, headquarters and formations that are all linked by the CIS infrastructure with central coordination of their information and activities. From the manoeuvre battalion upwards, each level has its own basic ISTAR capabilities (unit/assets) that complement each other and partially overlaps in the area of responsibility [19].

ISTAR provides surveillance, target acquisition and reconnaissance in the area of (intelligence) responsibility as well as converts data, information and/or intelligence from many different sources and collecting agencies into intelligence. The above mentioned system integrates activities between intelligence staffs and collection agencies at the same level and co-ordinates between the various levels. It achieves central monitoring and constant systematic implementation of collecting activities, target acquisition, information processing and intelligence reports with all available assets within the entire operational framework. Furthermore it ensures robust and uninterrupted coverage of the area of (intelligence) responsibility and is able to respond quickly to the needs of the commander and his units. It provides timely, relevant, objective information and intelligence for the command and control and/or target combating [11, 19, 20, 23].

By analogy with 103 (NL) ISTAR battalion (main Dutch ISTAR unit) we can propose the following the Generic Ukrainian ISTAR battalion organization (fig. 3).

From an intelligence point of view, the 103 (NL) ISTAR battalion consists of human intelligence (HUMINT) assets, signal intelligence and electronic warfare assets (SIGINT/EW), unmanned aerial vehicles (UAV), weapons location radar and long-range reconnaissance sensors [19]. The composition of the Ukrainian ISTAR unit (units) will depend on the mission and can include some or all the following capabilities:

– reconnaissance subunits;
– military intelligence subunits;
– signal intelligence company (platoons);
– electronic warfare company (platoons);
– UAV company (platoons);
– battlefield surveillance radars;
– reconnaissance aircraft or helicopters;
– weapon locating platforms;
– force protection equipment;
– remote viewing terminals;
– unattended (unmanned) ground sensors etc.

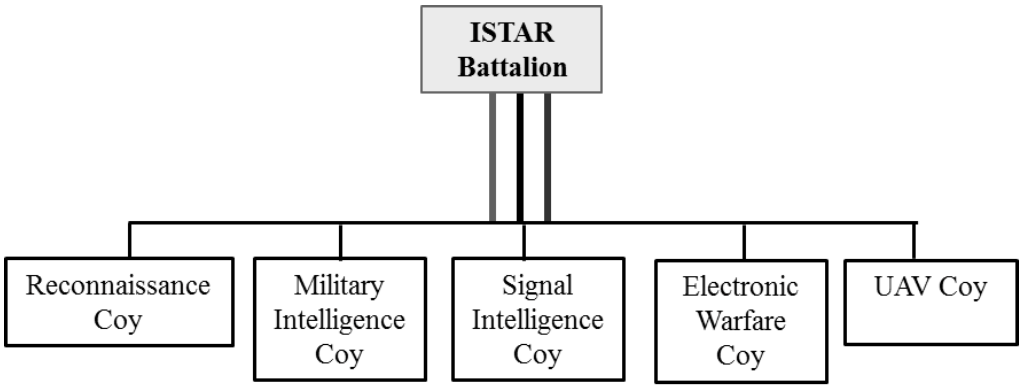

Fig. 3. **Generic Ukrainian ISTAR battalion organization**

The main 103 battalion tasks (functions) can be projected for the Ukrainian Battalion and they are [19]:

– information requirements management and collection coordination;
– collecting and processing data and information;
– data exploitation and all source analysis;
– producing intelligence for the appropriate users;
– dissemination of the combat information and intelligence;
– support to targeting;
– intelligence support to headquarters and units before and during their deployment.

The Ukrainian ISTAR Battalion should be ready to operate within the different strategic/operational environment like the 103 (NL) battalion as a battalion-sized ISTAR unit for multinational HQs, or by parts of the ISTAR battalion detached to multinational HQs or brigade-sized units, or independently operating battalions [19].

In consideration of current structure of the Ukrainian Armed Forces Command and Control (C2) Elements [2] there are two main alternatives for creation of the aforementioned ISTAR unit: 'temporary' and 'permanent' variants. Each of those approaches has own advantages and disadvantages. For instance, 'temporary' variant means a foundation of ISTAR unit (with periodic rotation of the personnel) for definitive mission by combining proper separate subunits (e.g. reconnaissance, military intelligence, signal intelligence, electronic warfare and UAV companies) under direction of generated ISTAR C2 module, which develops information requirements and translate them into tasks for the ISTAR units (subunits) based on the brigade commander's operational objectives. In this case there are no any substantial modifications of current Intelligence System and C2 System, except creation of the ISTAR C2 module and separate UAV company in the Ukrainian Army (it is also possible to involve UAV from the Air Force). Despite relatively less financial expenditure this approach has some disadvantages that are inherent to temporary military units (according to the own Ukrainian peacekeeping experience). These limitations are:

– required long-term activity (up to 6 months) to achieve a needed level of cohesiveness and close cooperation of ISTAR subunits;
– essential retrogression of professional training and military discipline, especially during the mission;
– inadequate level of ISTAR infrastructure which cannot provide minimum scale of CIS connectivity with national forces and other governmental entities, or with NATO forces in NATO-led operations.

From this point of view the second ('permanent') variant is more preferable. In that case the ISTAR battalion will comprise of current reconnaissance battalion composition (including intelligence assets) and some additional adequately manned and equipped detachments

or subunits (e.g. military intelligence, SIGINT, EW and UAV companies or platoons), will be integrated in generated information environment of Ukraine and will get an ability to receive large amounts of data (including near real time information), process it, and disseminate it to the appropriate levels of command. Also a created permanent ISTAR C2 module should have the necessary communication systems and interfaces to establish links with national and higher echelons to exchange C2 information and coordinating instructions on the ISTAR activities.

The national ISTAR Architecture should be developed within the framework of the State Task Programme for developing Common Automated Command and Control System (CACCS), as well as creation of common information environment of the Ukrainian Armed Forces. It should be noted that despite all current difficulties Ukraine has been taking some technical steps towards supporting network-centric warfare. For instance the Ukrainian MOD has mandated that the CACCS [1] will be a primary technical framework to support network-centric operations and all advanced weapons platforms, sensor systems, and command and control centers are eventually to be linked via this system of systems to result massive integration efforts.

Creation of the ISTAR battalion, establishment of adequately manned and equipped ISTAR capabilities should be considered as discharge of the Ukrainian commitments and meeting NATO requirements for timely and accurate surveillance and target acquisition data. Interoperability of the Ukrainian ISTAR units is an essential requirement in order to be able to operate in a multinational environment, and in the first place it is achieved by the implementation of a common data format that enables the transmission of ISTAR data throughout the network. Interoperability, in this case the ability to exchange information and intelligence, is the key to successful multinational operations.

Conclusions

In summary situational awareness for commanders and staff is vital. Any situation or contingency can be managed in optimal way if current information and intelligence is available. This is why the National Intelligence Structures need a great deal of effort in the management of intelligence, surveillance, target acquisition and reconnaissance information.

Owing that intelligence is a battle-winning factor, ISTAR implementation can be considered as way of enhancement (modernization) of the Ukrainian intelligence System on basis of improvement of organizational structures, intelligence procedures and protocols, using advances of technologies, first of all information technology. This process aims to increase effectiveness and efficiency of intelligence activities and as result to obtain the timely, accurate, relevant and reliable intelligence information necessary to accomplish all missions across the operational continuum. To put it briefly, the future Ukrainian ISTAR System can be characterized as the coordinated direction, collection, processing and dissemination of time critical combat information and intelligence, as a key military capability that generates and delivers specific information and intelligence to decision makers at all levels to support the planning and conduct of operations at all levels as well as in multinational environment.

The research of the Alliance countries experience of creation and use of ISTAR systems is very urgent for further improvement of the Military Intelligence System of Ukraine, its capabilities and military units' interoperability in NATO-led operations.

Literature

1. Біла книга – 2011. Збройні Сили України. – Київ, 2012 р. [electronic resource] – Access mode: http://www.mil.gov.ua/-files/white_ book/WB_2011.pdf.

2. AAP-31: NATO Glossary of Communication and Information Systems Terms and Definitions (November 2001). – 119 p.

3. AEDP-2 (Edition 1): NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA). [electronic resource] – Access mode: http://www.nato.int/-structur/AC/224/standard/ AEDP2/AEDP2_Documents/AEDP-02v1.pdf.

4. AJP-01(C): Allied Joint Doctrine (Dec 2010). – 268 p.

5. AJP-2 (Dec 2003): The ISTAR Concept (Chapter 1-4-1). – 64 p.

6. AJP-3.2: Allied Joint Doctrine For Land Operations. – 136 p.

7. ATP-3.2: LAND OPERATIONS. – 320 p.

8. Field Army ISTAR Handbook. [electronic resource] – Access mode: http://www.scribd.com/doc/36219969/Uk-Istar-Handbook-2007.

9. Interoperability: Connecting NATO Forces. [electronic resource] – Access mode: http://www.nato.int/cps/en/natolive/-topics_84112.htm.

10. JP 2-0: Joint Intelligence. [electronic resource] – Access mode: http://www.fas.org/irp/doddir/dod/jp2_0.pdf.

11. JP 3-55: Doctrine for Reconnaissance, Surveillance, and Target Acquisition Support for Joint Operations (RSTA). – [electronic resource] – Access mode: http://www.bits.de/NRANEU/-others/jp-doctrine/jp3_55(93).pdf.

12. NATO Interoperable ISTAR System Concept of Employment, MAJIIC Operations Working Group (OWG). – 14 March, 2010. [electronic resource] – Access mode: http://publicintelligence.net/-nato-interoperable-istar-system-concept-of-employment.

13. NATO STANAG 5048 (Edition 5): The Minimum Scale of Connectivity for Communications and Information Systems for NATO Land Forces (Feb 2000). – 38 p.

14. NATO STANAG 6001 NTG (Edition 3): Language Proficiency Levels // Brussels, 2009. – 21 p.

15. Net-Centric Environment, Joint Functional Concept. [electronic resource] – Access mode: http://www.dtic.mil/-futurejointwarfare/concepts/ netcentric_jfc.pdf.

16. Remarks by Richard Cheney, Vice President. – The White House. – 1 May, 2003. [electronic resource] – Access mode: http://www.iraqwatch.org/government/US/-WH/wh-cheney-050103.html.

17. R.S.T.A. Cycle Lessons Learned, Brig. Gen. Giuseppe Marani. [electronic resource] – Access mode: http://ftp.rta.nato.int/public//PubFullText/ RTO/MP/RTO-MP-001///$MP-001-01.pdf.

18. System Training Plan (STRAP) for the Tactical Exploitation System (TES). [electronic resource] – Access mode: http://www.google.com.ua.

19. The Dutch Approach of ISTAR Concept during NRF-4. [electronic resource] – Access mode: http://www.cdef.-terre.defense.gouv.fr/publications/doctrine/doctrine09/-version_us/foreign_studies/art04.pdf.

20. The ISTAR Capability of the Canadian Forces. [electronic resource] – Access mode: http://www.cdef.terre.-defense.gouv.fr/publications/doctrine/doctrine09/version_us/foreign_studies/art03.pdf.

21. Understanding Information Age Warfare, by Alberts, Garstka, Hayes, and Signori. – CCRP Press, 2001. [electronic resource] – Access mode: http://www.dodccrp.org/files/Alberts_-UIAW.pdf.

22. U.S. Army Field Manual (FM) 6-0: Command and Control of Army Forces. – Department of the Army. – Washington, DC, 11 August 2003. [electronic resource] – Access mode: http://www.bits.de/NRANEU/others/amd-us-archive/fm6(03).pdf.

23. House of Commons. Session 2007-08. Publications on the internet. Defence Committee Publications. Defence – Thirteenth Report. – [electronic resource] – Access mode: http://www.publications.parliament.uk/pa/cm200708/cmselect/cmdfence/535/53502.htm.

ВПРОВАДЖЕННЯ СИСТЕМИ ISTAR У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Ю.М. Пащук, Ю.П. Сальник

У статті розкриваються доцільність та шляхи впровадження системи ISTAR у систему розвідки Збройних Сил України. Це дослідження є актуальним у контексті подальшого розвитку військової розвідки України та підвищення її ефективності.

Ключові слова: *концепція, система розвідки, система ISTAR, розвідувальний цикл, розвідка, спостереження, визначення цілей, сумісність, НАТО.*

ВНЕДРЕНИЕ СИСТЕМЫ ISTAR В ВООРУЖЕННЫХ СИЛАХ УКРАИНЫ

Ю.М. Пащук, Ю.П. Сальник

В статье раскрываются целесообразность и пути внедрения системы ISTAR в систему разведки Вооруженных Сил Украины. Это исследование является актуальным в контексте дальнейшего развития военной разведки Украины и повышения ее эффективности.

Ключевые слова: *концепция, система разведки, система ISTAR, разведывательный цикл, разведка, наблюдение, определение целей, совместимость, НАТО.*