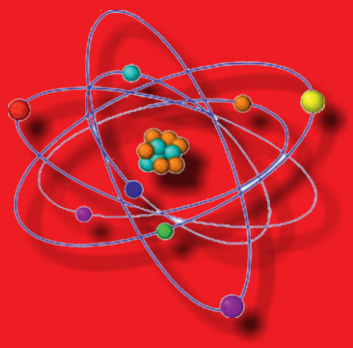
ISSN 2521-1331

Azərbaycan Respublikası Silahlı Qüvvələrinin Hərbi Akademiyası

MİLLİ TƏHLÜKƏSİZLİK VƏ HƏRBİ ELMLƏR

elmi-praktik jurnal



№ 4(5)

Bakı – 2019

ISSN 2521-1331

Azərbaycan Respublikası Müdafiə Nazirliyi
Silahlı Qüvvələrin Hərbi Akademiyası

MİLLİ TƏHLÜKƏSİZLİK VƏ HƏRBİ ELMLƏR

Elmi-praktik jurnal

Cild 5, №4, 2019-cu il

Azerbaijan Republic Ministry of Defense
War College of the Armed Forces

NATIONAL SECURITY AND MILITARY SCIENCES

Scientific-practical journal

Volume 5, №4, 2019

Bakı – 2019

“Milli təhlükəsizlik və hərbi elmlər” jurnalında verilmiş materiallardan istifadə zamanı mütləq jurnala istinad edilməlidir.

Jurnal 09.07.2015-ci il tarixində Azərbaycan Respublikası Ədliyyə Nazirliyində qeydə alınıb. Qeydiyyat nömrəsi: 3991.

“Milli təhlükəsizlik və hərbi elmlər” jurnalı elmi tədqiqatların əsas müddəalarının nəşr edilməsi üçün Azərbaycan Respublikası Prezidenti yanında Ali Attestasiya Komissiyası tərəfindən tövsiyə olunan nəşrlər siyahısına daxil edilmişdir.

Təsisçi: Silahlı Qüvvələrin Hərbi Akademiyası.

Ünvan: AZ1065, Azərbaycan Respublikası, Bakı şəhəri, Yasamal rayonu, akademik Şəfaət Mehdiyev küçəsi 136, “Qırmızı Şərq” hərbi şəhərciyi, Silahlı Qüvvələrin Hərbi Akademiyası, Adyunktura və elm şöbəsi.

The journal was registered on 09.07.2015 in the Ministry of Justice of the Republic of Azerbaijan. Registration Number: 3991.

“National security and military sciences” journal has been included in the list of recommended publications by Higher Attestation Commission under the President of the Republic of Azerbaijan for the publication of main theses of scientific researches.

CEO: War College of the Armed Forces.

Address: AZ1065, Republic of Azerbaijan, Baku, Yasamal district, str. Shafaet Mehdiev 136, “Red East” military settlement, War College of the Armed Forces, Adjuncture and science department.

CONTENTS

MÜNDƏRİCAT

UDC 621.391.827; 645.16

NEW APPROACH TO DEVELOPMENT OF FIELD SIGNAL CENTERS BY EMPLOYING MODERN TELECOMMUNICATION TECHNOLOGIES

colonel Ramiz Imanov, ScD, professor Azad Bayramov
War College of the Armed Forces, Azerbaijan Republic
E-mail: imanov-said@mail.ru

Abstract. In this article role of modern telecommunication technologies in development of field signal centers is shown, the set-up of a military field signal center in the form of modules has been proposed.

Keywords: signal center, network, management system, data transmission, modular.

Introduction

Improvement and development of the military management system is one of the most important challenges facing each state in ensuring the defense capacity. Nowadays, one of the main directions of the military management system development is the improvement and wide automation of field communication networks of the military authorities. Therefore, states continue to advance their tactical networks to counter these emerging threats, enable new forms of maneuver and maintain integration with military IT services available stateside while taking advantage of rapid innovation from the commercial IT industry. Specific to network modernization, communicating securely with command-and-control and other units within the increasingly communications-reliant battlefront landscape is critical to ensure the success of the mission and the safety of warfighters. However, as the battlefield evolves and missions require units to be mobile and support myriad tactical capabilities (Wi-Fi, LTE [Long Term Evolution, a standard for high-speed wireless communication for mobile devices and data terminals], etc.), critical communications infrastructures are becoming more difficult to establish and maintain [1].

Additionally, innovations in the cloud, "internet of things," sensors, robotic and autonomous systems, analytics, artificial intelligence and deep learning are driving tactical network developers to consider deploying war-fighting systems that are highly reliant on high-performance computing and storage. Yet, in the face of potentially degraded communications, those resources may only be available if deployed all the way out to the individual warfighter or small teams conducting operations in austere and hostile environments, such as forward operating bases or combat vehicles-locations known as the tactical network's edge [2].

Development of field signal centers based on modern telecommunication technologies

Taking into account the achievements of modern digital technologies, the implementation of the process of integration of communication and automated management systems into a single information and telecommunication system is one of the important issues. This single system contains information, telecommunications and organizational measures.

When we talk about military information and telecommunication systems, they should be understood as the organizational and technical integrity of communications, automation forces and tools that provide information exchange with the use of information and network technologies. In this case, the information section can include database, information itself, mathematical software, technical means and linguistic maintenance. The telecommunications part involves the communication system and network technologies that determine the architecture, type, and operating rules of communication networks. Organizational measures can include legal, regulatory mechanisms that provide effective functioning of information and telecommunication systems [3].

One of the main direction of development of perspective information and telecommunication systems is the improvement of the field communication and management system, which is an integral part of the overall management system. There are some shortcomings of the currently operating field communication system, that make difficulties to integrate them into the single system and it is necessary to revise these issues. These are – a number of old modification of communication facilities in communications divisions and sections, the fact that some of the communication equipments are analogue and others are digital modern technologies.

Additionally, it should be noted that, since the modern communications facilities used in the field communications networks, themselves have different indicators and different tactical requirements, issues of electromagnetic compatibility remain unresolved.

The abovementioned problems in many cases, creates difficulties in fulfillment of electromagnetic compatibility issues for all radioelectronic means, vitality of communication networks, intelligence protection, convenient use of communication and automated management system tools, broadband maneuvers with communication channels, as well as communication security, timely and precise data transmission.

The military communication system should ensure that the authorities have the opportunity to communicate by required channels and means at the scheduled time. Signal centers are the basis of the communications system, therefore it is required to undertake a number of measures to address the aforementioned issues [2].

It is also important to take into consideration the requirements of the modern forms and methods of predicting operations, the organization and implementation of combat operations, and the requirements of modern era in the management of troops and the weapons.

In addition, operational and technical requirements to the prospective field signal centers, the capabilities of modern communication facilities, the organizational and technical structure of the signal centers and the technical supply of its elements should be specified. Besides, this system should also provide the transmission of various data and the provision of integrated communication channels for the full satisfaction of the information needs of the troops [7].

It should be noted that it is advisable to set perspective field signal centers in the form of unified digital communication facilities, complexes and newest telecommunication technologies, as well as accessible automated systems for everyone.

The apparatus – software tools, which is being implemented on the basis of technologies of integration of channels, communication, encryption and management, will allow to create new structure-based signal centers. These tools, in turn, will create conditions for the groundbreaking review of the structure of the signal centers, the rejection of their centralized construction and the creation of modern structured field signal centers, taking into account the development tendencies of the control stations [4].

As the main option for their further development and improvement it is possible to set up a military field signal center in the form of modules, In this case, the field signal center can be presented as a set of coordinated components. This, in turn, can make it easier for customers to use the types of communications they provide, as well as improve intelligence protection, survival and flexibility of signal centers. It is also reasonable to implement the principle of hybrid switching (switching of channels and packages) in perspective digital signal centers [3].

These field communication nets can include radio relay, cable (fiber-optic) communications, transmitters, switch equipment and radio communication facilities that allow authorities to access the network when they are in motion. An important objective in the design of field signal center is often to reduce equipment cost, complexity and power consumption whilst also minimize the bandwidth occupied by the signal and/or transmission time (bandwidth is a measure of how rapidly the information bearing part of a signal can change and is therefore an important parameter for field signal centers design) [5].

It is important to pay special attention to the automated management systems during the construction of the proposed field signal centers. Automated control systems in this case are designed to provide the management of planning, organization and quality control of communications channels, ensuring security of communications and data protection, ensuring a unified automated management system interconnection with communication systems of troops, and collection of information about the situation [6].

During the creation of modern military-purpose field communication networks, the following must be implemented:

- increasing network capabilities and overall communication capabilities by applying integrated switch devices and broadband digital channels;
- wide automation of communications management and communication processes with the use of high-efficiency computing techniques;
- integration of encryption, switching, signal transformation functions into one device by switching to the modular design of communication means;
- provision the establishment of communication equipment on a new element base;
- the application of fiber optical means, which allows to increase the level of agility and the reliability of signal centers;
- increase the level of utilization of communication means, reduction of their service life;
- automation of repair and maintenance process to achieve more reliable communication;
- provision of direct access by separate means by the operator;
- application of communication means with higher interference and intelligence protection.

The installation of signal centers on a modular basis can provide not only communication interconnection, but also the integrity of the communication system's external interference, the higher level of vital in the conditions of the barriers, the agility, and the unification of their organizational-technical structure.

The development and improvement of the field signal centers implies the establishment of a single telecommunications network, which are based organization of digital networking technologies, modern digital channels, automation of switching process, distribution of channel resources and access to broadband access to the network, supporting and integrating all types of power supply with their own resources.

Modern information and telecommunication technologies, as well as hardware and software, which were developed on their basis, allow for all types of information processing and communication issues to be carried out directly at the workplaces. A new class of modular, tactical data centers is becoming available for tactical and expeditionary programs, capable of hosting cloud and storage, artificial intelligence and analytics applications. Using ultra-small form-factor modules for computer, storage and networking functions that reduce size, weight and power requirements, these systems can be deployed dismounted, at forward operating bases, in command posts, and on ground vehicles and aircraft-supporting a diverse array of use cases in disconnected, intermittent and limited environments. The widespread expansion of the nomenclature of telecommunication services to users requires from field signal centers multicast communication networks [1].

There is a difficult task for abovementioned multilevel communication networks to reconcile the transmission of different information across a single network infrastructure. At that time, its features are also subject to serious requirements.

First, the minimum network capability for each type of traffic should be ensured. Because, the multi-threaded networks need to be set up for each traffic type, the transmission speed agreed upon with each intermediate network device. Transmission of a traffic type should not negatively affect others. Each attachment (video, database, etc.) running on the network must be separately provided with a specific agreed network of that network.

Second, minimal possible downtime for multimedia traffic should be provided. The use of long information packets for data transmission is more efficient. Thus, the execution of these operations

may reduce the useless use of the network. However, transmission of voice or video traffic may become a problem.

Documents sharing networks can be created at the expense of the properties (topologies) of the respective local computing networks, which have access to the field communication networks for the exchange of information with the top headquarters, interacting and controlling entities of the subordinate units. This organization can provide an informational-computing system with distributed functions, which optimally assists in the solution of exchange tasks with all types of information. The application of multi-contour local computing networks in signal centers and in their elements can be used to reduce the number of communications devices, as well as to raise the operational-tactical and technical characteristics of the field communications networks.

Conclusion

Modern perspective telecommunication technologies and their integration capabilities create high-speed digital networks in a vast space. These networks can, in turn, provide transmission of all types of information and a range of additional communication services, which are specific to the military. The field signal centers always must be ready to launch at the right time and be ready to expand the communication system. Therefore, it is necessary to take into consideration the conditions provided for the solution of the issues of the application of new technologies and techniques in the development and improvement of the field signal centers.

References

1. Zlobin, V.I. Intellectual adaptive communication and management systems, Monograph. / V.I. Zlobin, M.V. Ivashenko, Q.V. Ivanova – M.: RF MOD, – 2005. – 276 p.
2. Samochin, V.F. Improvment and development mobile communication networks // Military idea, – 2008. №9, – p. 5-11.
3. Imanov, R., Bayramov, A. Analysis of the communication part of command centres // – Baku: National Security and Military Sciences, – 2019. (5) №1, – p. 14-21.
4. Vasilev, V.I. Communication system / – M.: High school, – 1987. – 280 p.
5. Qalkin, V.A. Digital mobile radio communication. Manual for university / – M.: Helpline-Telecom, – 2007. – 432 p.
6. Kimberly, A.H. Network Centric Operations Conceptual Framework: [Electronic resource] / IT Value in the Netcentric Organization: Integrating Commercial and Military Perspectives, December 9-10, 2003. URL: https://bit.ly/39IQeeO.
7. Williams, T. EMC for products developers / T. Williams, Eds. V.S. Karmashova, L.N. Kechieva. Moscow: “Technology”, – 2004. – 290 p.

Xülasə
Müasir telekommunikasiya texnologiyalarının tətbiqi ilə səhra rabitə qovşaqlarının inkişafına yeni yanaşma
Ramiz İmanov, Azad Bayramov

Məqalədə səhra rabitə qovşaqlarının inkişafında müasir telekommunikasiya texnologiyalarının rolu qeyd olunur, hərbi təyinatlı səhra rabitə qovşaqlarının modul şəklində qurulma metodu təklif edilir.

Açar sözlər: rabitə qovşağı, şəbəkə, idarəetmə sistemi, məlumat ötürülməsi, modul.

Аннотация

Новый подход к развитию полевых узлов связи с применением современных телекоммуникационных технологий

Рамиз Иманов, Азад Байрамов

В данной статье отмечена роль современных телекоммуникационных технологий в развитии полевых узлов связи, предложен метод модульного построения военных полевых узлов связи.

Ключевые слова: узел связи, сеть, система управление, передача данных, модуль.

Məqalə redaksiyaya daxil olmuşdur: 13.09.2019
Təkrar işlənməyə göndərilmişdir: 12.10.2019
Çapa qəbul edilmişdir: 08.11.2019

UDC 528; 623; 912

ESTABLISHMENT OF INTERACTIVE GEO-INFORMATION CENTER IN AZERBAIJAN

[1]Ilgar Musayev, [2]ScD, professor Elshan Hashimov
[1]Azercosmos Open Joint-Stock Company,
[2]Armed Forces War College of the Azerbaijan Republic
E-mail: ilqar-refiler@rambler.ru

Abstract. The creation and development of a single geo-information space in the Republic of Azerbaijan in the interests of defense and security in law enforcement agencies, as well as for civilian purposes, is one of the most topical and urgent issues of our time. This will allow to unite all specialists and institutions in the field of geo-information, avoid repeating the creation of GIS in the same field to different organizations and ensure a more efficient use of geo-data.

In the article, analyzing in detail the existing situation on the use of geo-information by state bodies of the republic and after studying world experience in the field of geo-information, it is proposed to create an Interactive Geo-information Center to form a single geo-information space in the country.

Keywords: Geographic Information System, single geo-information space, Interactive geo-information center, geo-portal.

Introduction

Institutional reforms aimed at centralizing e-services in our country in recent years have led to the optimization of governance, enhancing transparency and accessibility to general information on public administration sectors. Obtaining these achievements was possible by the joint activities of the "ASAN Service" and "ASAN Communal" centers.

Application of "ASAN service" experience in the field of geographical information (hereinafter – geo-information) service is today's requirement.

Scientific research shows that 80% of the world's information is geographically related. If information is not geo-dependent, it loses its value, it is difficult to use, and it is uncertain [4, p.124]. Keeping space information in different and separate centers creates problems in their efficient use. The only way to solve this problem is to concentrate, analyze, classify, and adopt this information in a single geo-informational center. After that, it will easily ensure the use and exchange of information on accepted standards.

In order to organize joint activities of the geo-information systems of the ministries and other state bodies of the Republic of Azerbaijan and to ensure that the services provided in this area will be coordinated in a unified geo-information space, there is a need to establish an Interactive Geo-information Center (IGC).

With the establishment of the IGC, there will be an organized management of geospatial information gathered at different institutions (ministries of power), and the center will serve to further development of defense and economic power of our country.

In order to form a single geo-information space, we need to analyze the current situation of geo-information services in the country.

Analysis of the current situation of geo-information services in Azerbaijan

Awareness of the use of geo-information services in state agencies is low. Lack of electronic bases of Geographic Information System (GIS) in some organizations, still using paper carriers, not

giving priority to the opportunities of modern technology, using non-updated data prevents the continual increase of productivity.

The level of modern logistic supplies is insufficient for the use of geo-information services in agencies. Insufficient of logistic supplies mean that there is a lack of expensive specialized equipment and specialized licensed software that is intended for the processing of cartographic materials and aerospace images, which are currently not produced in our country and are purchased from foreign countries.

There are few qualified specialists in geodesy, cartography, topography, photogrammetry and geometrics. The number of specialists with experience and skills in working with special software on modern computer and cartography is small.

In some state agencies, they keep the same geospatial information in separate distinct centers, which creates problems for the more efficient use of them. Absence of a single base for GIS data is result the implementation of similar projects repeatedly by the various agencies. Vector data on a map database (relief and relief elements, settlements, socio-cultural facilities, railways, motorways, highways and trails, vegetation, hydrography, hydro-technical installations, bridges, power transmission and communication lines, streets, addresses etc.) are not included in a centralized way. This often inaccurate or misleading data usage. It is too difficult to coordinate the same projects by the various agencies.

One of the main reasons for the low level of information exchange between state agencies is innovation conservatism, the solution of which is the adoption of the normative base and documentary.

At present, topographic maps of coordinate system “SK-42” are used as topographic data base in state bodies and other organizations of the republic. The SK-42 coordinate system (Pulkovo coordinate system) was calculated based on reference ellipsoid of Soviet geodesist Fyodor Krasovcky [2, p.39]. The “SK-42” coordinate system has geometrical deformations compared to modern international coordinate systems (International GRS-80 and WGS-84, Russian EP-90 and GSC-11) and is therefore not precise (Table 1). Today, coordinated systems WGS-84 (Word Geodetic System 1984), EP-90 (Earth Parameters) and GSC-2011 (Geodetic System Coordinate 2011), based on the ellipsoid of high precision, are used in many countries, especially in NATO countries and the Russian Federation [3, p.2]. WGS-84 is an Earth-centered, Earth-fixed terrestrial reference system and geodetic datum. It is based on a consistent set of constants and model parameters that describe the Earth's size, shape, and gravity and geomagnetic fields [4, p.1].

Considering that in our days geodetic, topographic and cartographic measurements, also navigation are often based on satellite technology, it is not advisable to produce new topographic maps in the “SK-42” coordinate system and use them as a geo-informational database. Because, all the modern geo-information technologies and equipment available in foreign countries are used in the above-mentioned modern coordinate systems [5, p.31].

The essence of the creation of an Interactive Geoinformation Center

The main purpose of the IGC is to create a single geo-information space in the country to ensure the joint use of GIS in the defense, security and other state institutions of the Republic of Azerbaijan, and to conduct mutual exchange of information. This center does not focus on physically maintaining and protecting data in a single database, but it will play the role of a central interface that provides accessibility to other geo-spatial information for every governmental organization.

The essence of the creation of the Center is also to study international experience, to prepare specific technical proposals and solutions, to obtain and install the necessary equipment and software.

Table 1

The Earth reference ellipsoids

Ellipsoid names	**Year of calculation**	**The semi-major axis of the ellipse, a, (metre)**	**The semi-minor axis of the ellipse, b, (metre)**	**Countries and international organizations**	**Type of ellipsoid**
Bessel	1841	6 377 397	6 356 082	Europe, Asia	referens–ellipsoid
Eyr	1849	6 377 563	6 356 255	United Kingdom, Northern Ireland	referens–ellipsoid
Delamber	1810	6 376 428	6 355 958	Belgium	referens–ellipsoid
Denmark		6 377 104	6 355 847	Denmark, Iceland	referens–ellipsoid
Plessisa		6 376 523	6 355 860	France	referens–ellipsoid
Struve		6 378 298	6 356 655	Spain	referens–ellipsoid
Heyford	1909	6 378 388	6 356 912	Europe, Asia, South America, Antarctica	referens–ellipsoid
Everest	1830	6 377 276	6 356 075	India, Pakistan, Nepal, Sri Lanka	referens–ellipsoid
Clark	1858	6 378 293	6 356 620	Australia, Ireland	referens–ellipsoid
Clark	1866	6 378 206	6 356 585	North and Central America	referens–ellipsoid
Clark	1880	6 378 249	6 356 517	Africa, Barbados, Jamaica, Israel, Jordan, Iran	referens–ellipsoid
Krasovski (СК-42)	**1940**	**6 378 245**	**6 356 863**	Former socialist countries	referens–ellipsoid
Australia	1984	6 378 160	6 356 771	Australia, Papua New Guinea	referens–ellipsoid
GRS 80	**1980**	**6 378 137**	**6 356 752,314**	The International Union of Geodesy and Geophysics (IUGG)	geocentric ellipsoid
WGS-72	1972	6 378 135	6 356 753	USA (up to the 80s)	geocentric ellipsoid
WGS-84	**1984**	**6 378 137**	**6 356 755**	US and NATO countries	geocentric ellipsoid
ПЗ-90	**1990**	**6 378 136**	**6 356 754**	Russian Federation	geocentric ellipsoid
ГСК-2011	**1990**	**6 378 136, 5**	**6 356 754**	Russian Federation	geocentric ellipsoid

Providers and Users

The IGC, which will be created to form a single geo-information space in the Republic of Azerbaijan, and will meet the broad demand of the defense, security and other state institutions of the republic and will meet ISO (International Organization for Standardization), OGC (Open Geospatial Consortium) and NATO Geospatial and Geographical Information standards.

Access to information will be based on security level rules. However, the center will also be open to the country's population and civil society organizations [5, p.37].

Geoportal

The IGC geoportal is an interface that provides protection, use and publication of geospatial data. It will be possible to access images, electronic maps, layers and metadata over the geoportal. Geoportal will perform the following tasks:

- sources, information, material and services will be provided after registering in an electronic catalog or registries;
- users could be looking for the generated information or services on the web-page or in registries;
- information that is not obtained as a result of searches may be requested to the information provider (supplier) or to the service provider.

Management and coordination

In the IGC it is required to establish a governing body for strategic decision-making, system management, coordination of inter-agency activities, and implementation of necessary verification and supervision procedures. It is proposed that the composition of the Management Board be organized by the representatives of ministries, state organizations and institutions. Management Board's missions are the next:

- managing the IGC issues;
- establishment of a coordination group;
- control over the activities of the IGC.

The IGC Coordination Group co-ordinates the Management Board's decisions with the bodies at the ministries, departments and agencies. The coordination group is composed of representatives of various ministries and state organizations and is divided into working groups by the necessary branches. Working group promotes the development of technical principles, exchange of knowledge, coordination of ideas and thoughts, as well as science and economic issues.

The activities of the IGC must meet the following requirements:

- operational compatibility – ability to exchange general information over standardization interfaces;
- possibility to expand – expand on newly created components;
- universality – can be applied at all levels of government, regardless of specialization in science and economics;
- availability – should provide affordable access to consumers based on legal conditions, norms and standards;
- efficiency – fast processing of requests based on users' legal conditions and capabilities;
- testing capabilities – checking the compatibility level with the help of special programs;
- capacity – the ability to share and expand the system's separate components in order to provide sufficient production capabilities;
- security – secure protection of space data and services and the ability to use them at all times.

Expected results

With the establishment and operation of the Interactive Geoinformation Center, the following results are expected in the country's defense, security and other state agencies, as well as civilian populations and organizations:

- this Center, based on the modern coordinate system that meets NATO, ISO and OGC standards, will increase the accuracy of calculations, measurements, designs, analyzes, scheduling and decision making;
- IGC will further boost combat readiness and operational capabilities of defense and security agencies;
- thanks to the technical support of the Center's geoportal from the "bottom to top", it will be possible more effectively solve the problems arising from the various situation [6, p.4];
- it will expand tactical, operational and strategic planning capabilities through analysis, optimization, simulation and planning capabilities;
- thanks to the joint use of the center, its resources and capabilities will be used more efficiently, inter-institutional co-ordination will be enhanced, complementary functions of agencies will be enhanced, and overall battle planning and management will be easier;
- thanks to the Center's activities, it will save financial resources by preventing duplication of single-purpose projects in separate entities;
- the Center's capabilities, which have higher definition content, more precise, new and detailed information and extensive analytical capabilities, are also will be widely used for civilian purposes (spin-off).

References

1. Musayev, I., Gojamanov, M. Special base of military geo-information system // Eurasian GIS conference, Collected papers, – 2018, – p. 123-126.
2. Musayev, İ.F. Müasir Peyk-naviqasiya cihazları ilə 1942-ci il koordinat sistemli topoqrafik xəritələr üzrə iş prosesində ortaya çıxan xətalar // – Bakı: Milli Təhlükəsizlik və Hərbi Elmlər, – 2015. №1, (1), – s. 34-41.
3. Постановление Правительство Российской Федерации Об установлении государственных систем координат, государственной системы высот и государственной гравиметрической системы. – Москва, – От 24 ноября 2016 года, №1240.
4. World Geodetic System 1984 (WGS84): [Electronic resource] / URL: https://bit.ly/2sRi87M.
5. Musayev, İ.F., Qocamanov, M.H., Həşimov, E.Q. Azərbaycanda İnteraktiv geoinformasiya mərkəzinin yaradılması // – Bakı: Hərbi İcmal, – 2019. №1, (4), – s. 29-39.
6. Hendricks, M. Army Geospatial Organizations & Systems: [Electronic resource] / – 2005, 19 p. URL: https://bit.ly/37Ihnwm.

Xülasə

Azərbaycanda vahid coğrafi informasiya məkanının yaradılması

İlqar Musayev, Elşən Həşimov

Hüquq-mühafizə orqanlarında müdafiə və təhlükəsizlik, habelə mülki məqsədlər üçün Azərbaycan Respublikasında vahid coğrafi informasiya məkanının yaradılması və inkişafı dövrümüzün aktual və zəruri məsələlərindən biridir. Bu, geoinformasiya sahəsindəki bütün mütəxəssisləri və qurumları birləşdirməyə, eyni sahədə CİS-in yaradılmasının müxtəlif təşkilatlarda təkrarlanmamasının qarşısının alınmasına və geodatanın daha səmərəli istifadəsinə imkan verəcəkdir.

Məqalədə respublikanın dövlət orqanları tərəfindən geoinformasiya məlumatlarının istifadəsi ilə bağlı mövcud vəziyyətin ətraflı təhlili ilə məşğul olan (geoinformasiya sahəsində dünya təcrübəsini öyrəndikdən sonra Azərbaycanda vahid geoinformasiya məkanının formalaşması üçün) İnteraktiv Geoinformasiya Mərkəzinin yaradılması təklif olunur.

Açar sözlər: coğrafi informasiya sistemi, ümumi coğrafi informasiya məkanı, interaktiv coğrafi informasiya mərkəzi, geoportal.

Аннотация

Создание единого геоинформационного пространства в Азербайджане

Ильгар Мусаев, Эльшан Гашимов

Создание и развитие единого геоинформационного пространства в Азербайджанской Республике в интересах обороны и безопасности в силовых структурах, а также в гражданских целях является одним из актуальных и необходимых вопросов современности. Это позволить объединить всех специалистов и учреждений в области геоинформации, избежать повторения создание ГИС в одной и той же сфере разными организациям и обеспечить более эффективное использования геоданных.

В статье подробно анализируя существующую ситуацию по использованию геоинформационных данных государственными органами республики и после изучения мирового опыта в области геоинформации предлагается создание Интерактивного геоинформационного центра для формирования единого геоинформационного пространства в Азербайджане.

Ключевые слова: географическая информационная система, единое геоинформационное пространство, интерактивный геоинформационный центр, геопортал.

Məqalə redaksiyaya daxil olmuşdur: 19.09.2019
Təkrar işlənməyə göndərilmişdir: 26.10.2019
Çapa qəbul edilmişdir: 15.11.2019

UDC 528; 623; 912

APPLICATION OF GEOGRAPHICAL ANALYSIS SYSTEM SOFTWARE PLATFORM FOR THE MILITARY PURPOSE IN THE REPUBLIC OF AZERBAIJAN

Yashar Nasibov
ANAS Institute of Geography, Azerbaijan
E-mail: yasharnasibli@yahoo.com

Abstract. The paper is devoted to the advantages of applying Geographic Analyzing System in the Armed Forces of the Republic of Azerbaijan. This system was made on the basis of Geographical Information System and is used successfully in Turkish Armed Forces.

Keywords: Geographical Information Sistems, Geographical Analyzing System, terrain study and assessment, battle organization.

Introduction

As it is known, the features of terrain influence much on combat operations. Therefore, at the stage of battle organization, the analysis of geography of the battle terrain for the purpose of optimal deployment of attack units, artillery and rocket troops, material support units is one of the most important tasks. The investigation of the geography factors affecting military operations is carried out by detailed analysis and evaluation. The detailed analysis and correct assessment of terrain gives a prognostication for commanders about an enemy's probable movement.

For the purpose of battle organization and optimal management of the forces, each commander must know an enemy location, information about enemy's activities, features of the terrain for the future military operation. The observation information must be obtained and brought to commander's notice in time. In the modern high mobile battle it is very important comply with these demands [1, p.3].

In advanced Armed Forces the stage of terrain study is one of the parts of operation planning, and it is carried out in whole frame. For this purpose Geographical Analyzing Systems (GAS) is used. In contrast to usual methods, if a terrain is studied by application of modern technologies, the commanders save time and obtain more correct results. By using developed technologies in the modern wars, the formed asymmetric structure with usual methods complicates a decision making. When planned military operations is carried out on the basis of GAS software platform, then the terrain and reconnaissance assessment remove considerably the possible hardships [2].

GAS gives a complete description of all features of the Earth and space, saves information about them, analyses and integrates various data, based on these results that prepare various prognosis and scenarios [3, p.17]. GAS has six main components: sets, software, information, personnel and methods. GAS computer is a main system. GAS helps to carry out investigations of nature and artificial events [4, p.5; 5, p.204]. By using artificial satellites and Unmanned Aerial Vehicles (UAV) the observation terrain in real time mode leads to solution of security problems. Made on the basis of GAS the special raster and vector maps are used by staffs, helicopters, tanks, self-propelled artillery and electro-optical observation sets [5].

The GAS modules

The developed industrial local and national platforms of defence form a basis of security of the country. When a quantity of technologies in military platforms increases then a reliability and importance of the used software platforms start to heighten. The application of foreign or open source software platforms can lead to weakness of security.

Recently, the local software platforms, military products and systems have been used broadly in Turkish Armed Forces (TAF). Applied in TAF GAS software platform meet the full requirement in Turkish capabilities in cartography and eliminates the foreign dependence. In the last 15 years the 50-th researcher's group has created a GAS code with thousand's lines. This software platform has been applied in all Turkish Armed Forces structures. Each day 5000 employees of these structures use actively this GAS software platform (Fig. 1) [6].

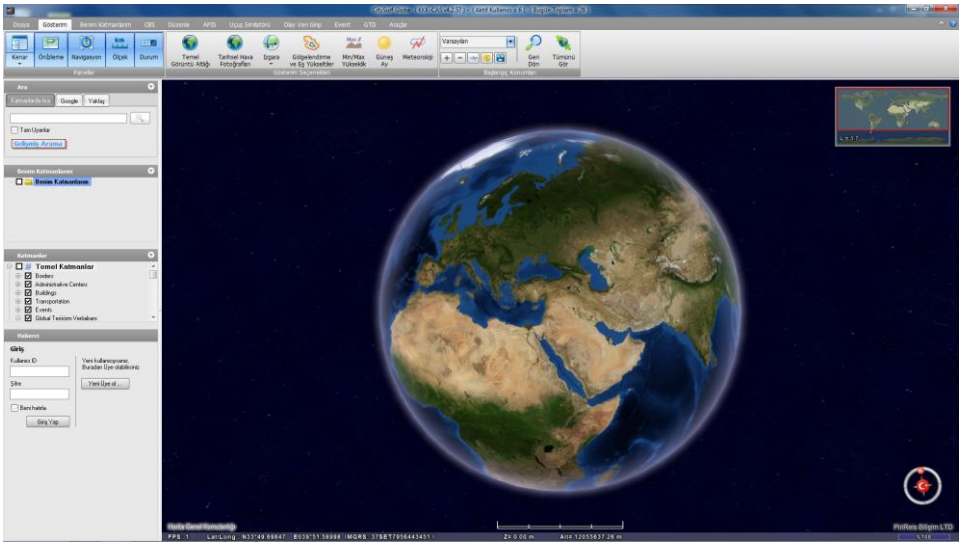


Fig. 1. GAS software platform window

GAS software platform is constructed on the basis of PC, Laptop, pad or tablet. The software platform can be applied in the mobile form. Used algorithms of the software platform demonstrate promptly space data with high resolution and precision, develop and, at the same time, distribute these data among all users. There are web and mobile program solutions used jointly with GAS platforms. GAS supports all geography data used in Turkish departments and institutions. The GAS software platform develops and analyses satellite's images, aero photographs, digital and raster maps, and sea maps. The GAS software platform codding is national, therefore it can be easily supplemented with various modules.

There are following modules in GAS software platform:

1. GAS – meteorological module

It demonstrates (daily and regular) weather forecast, sun and moon diurnal rotations in 2D or 3D formats. It is used actively in operation planning (Fig. 2).

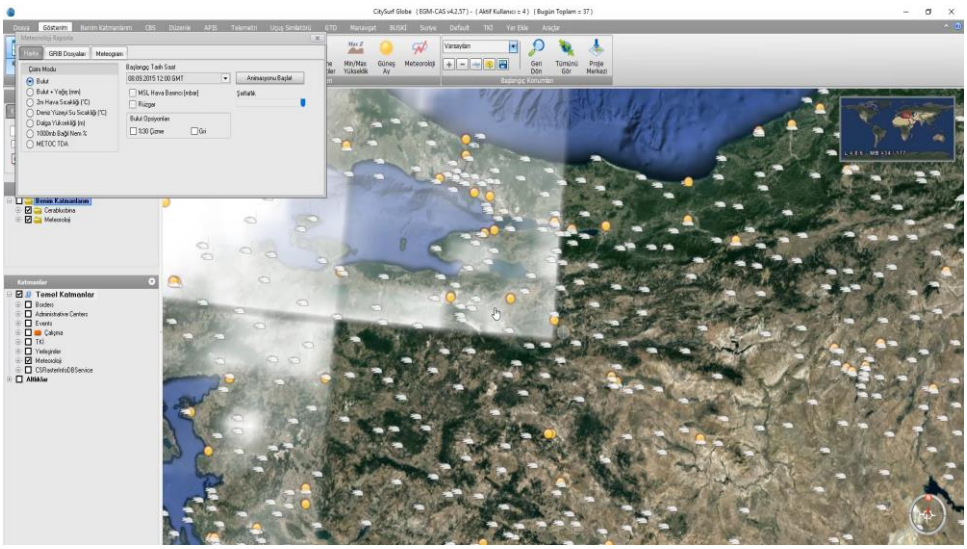


Fig. 2. GAS – meteorological module

2. GAS – Units tracking module

It provides a military units tracking in real-time mode in the planned operation area in rear or another place. This module has been used actively in Turkish Staff Command Center. In Staff Center or under field canvas in real-time mode the commandant can follow a track of unit under the command in 2D or 3D formats.

3. GAS – data transfer module

It has a goal providing safety and fast information exchange between HQs. Images and symbols are sent to opposite side, the data are not changed and only appointed personnel can see these data. If the sent data are corrected then in real-time mode the opposite side can see these changes (Fig. 3).

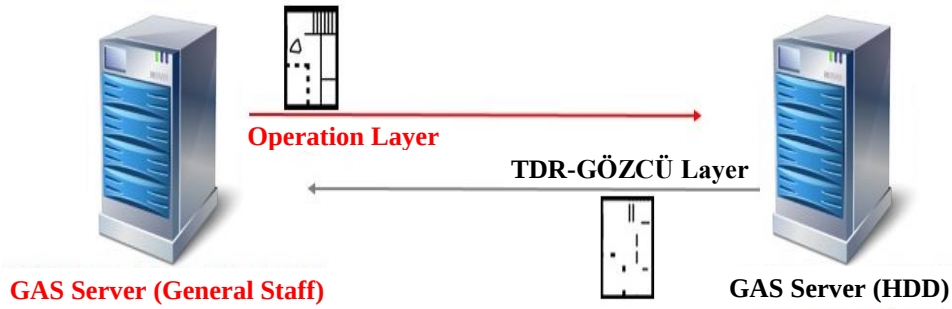


Fig 3. GAS – data transfer module

4. GAS – Operation Center Data System module

It ranks events occurred in units in accordance with time and spatial show in software platform. By using this platform all collected in Staff Center events are shown in software platform in 2D and 3D formats (Fig. 4).

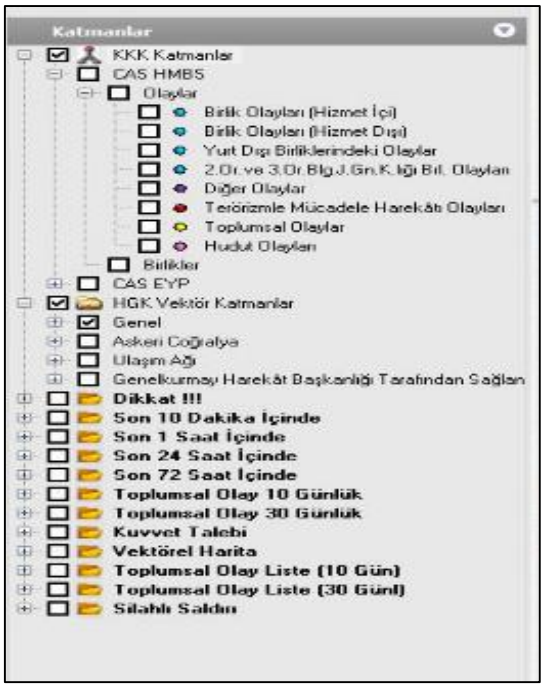


Fig. 4. GAS – Operation Center Data System module

5. GAS – Events Trucking System module

This module shows all collected information (operation conditions changes, violation of a border, terrorist act, mass riots, road traffic accident, etc.) in software platform to duty officer (about the events in his duty zone) in time-phased form (last 10 minutes, 1 hour, 1 day, 3 days, week, last month, last year). This module has been actively used in Turkish Armed Forces Staff Command Center.

6. GAS – Operation module

It is a support means for operation planning. Targets (projected or unexpected); fire support (artillery, aerial means); units (jointly with terrain positions); obstacles (point, linear, mined zone, etc.); lines (front lines, intermediate lines, belt or maneuver roads, support roads, etc.) and operation condition (friend and enemy forces) are shown in this software platform. This module has been actively used in Turkish Armed Forces Staff Command's Center (Fig. 5).

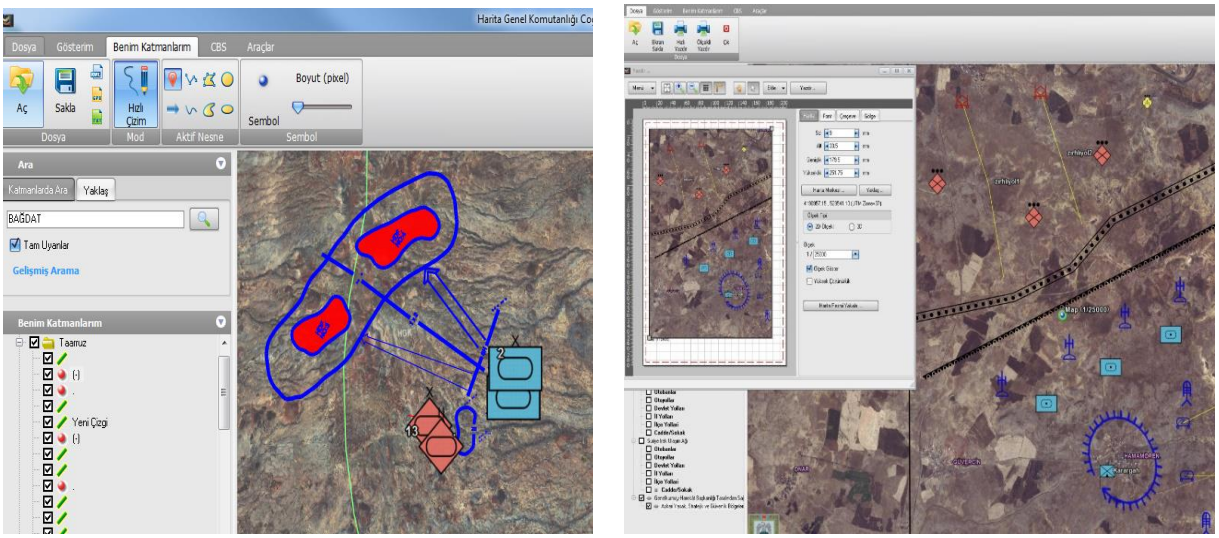


Fig. 5. GAS – Operation module.

7. GAS – Data Exchange module

This module provides data exchange between the personnel in real-time mode. Digital data about operation area, operation orders, documents and another various information in real-time mode are transferred fast and safely between the personnel. Duty officers in real-time mode study the same map and transfer the results each to other (Fig. 6).

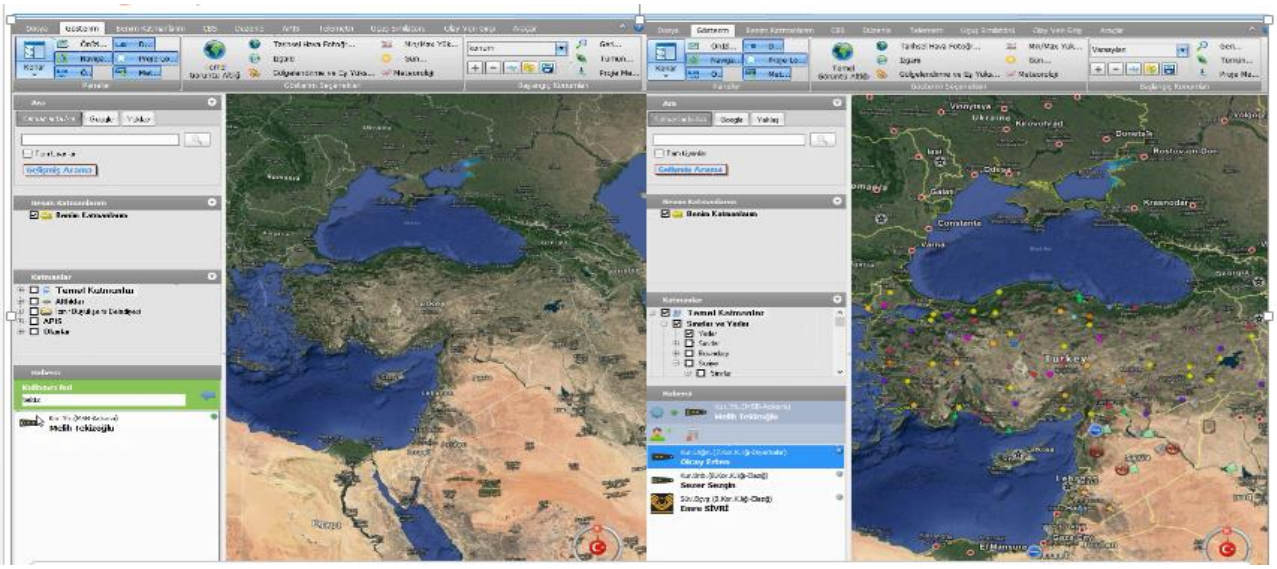


Fig. 6. GAS – Data Exchange module

8. GAS – Improving data module

This module shows events in spatial form and archives the documents about carried out operations or investigations jointly with side information (tables, named list, operation plan, image acquisition, figures, voicegram, etc.). It was prepared under the order of Turkish Ministry of Internal Affairs. By using the state query function the archive files can be used (Fig. 7).

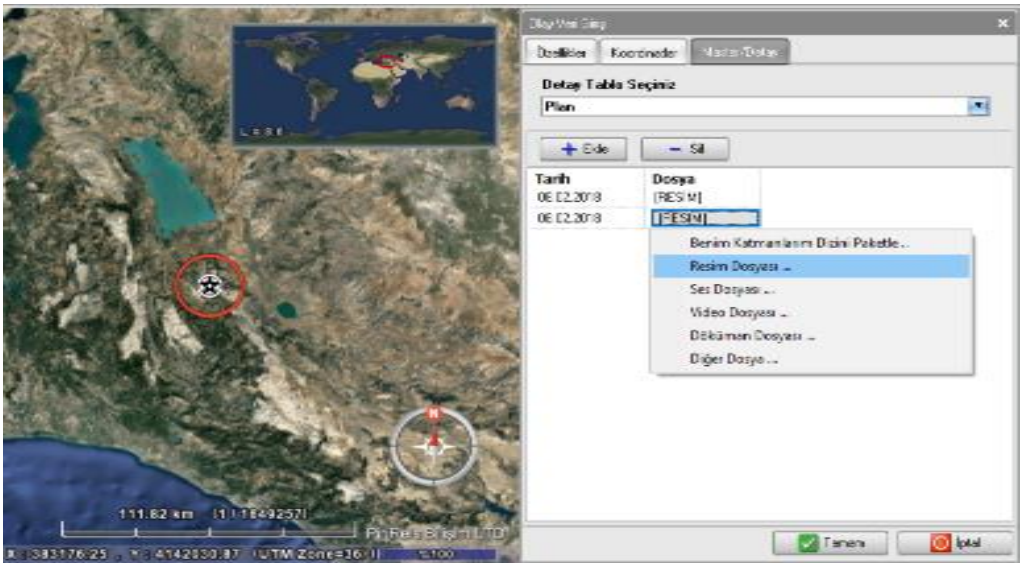


Fig. 7. GAS – Improving data module

9. GAS – Sea module

This module shows the information of beacons, navigation messages, training areas, bathymetry data, sea navigation maps, vector data, etc. in software platforms. It is possible to obtain current and archival information by using state query function. Now this module is used in Turkish Naval Forces and Navigation & Oceanography Department. "Management water surface" subsidiary module carries out applications of information about ships (rotation, entrance and leaving harbor, etc.), planning of operation area, preparation of training fields, etc.

10. GAS – Ship trucking module

In real-time mode this module shows ships' rotation in software platform. Concurrently 600 ships are shown in software platform. By using the symbols of Naval Tactical Data System these ships are shown in software platform.

11. GAS – Helicopter Obstacle Determination and Warning System (HODWS) module

The purpose of this module is to inform the helicopter pilot about natural and artificial obstacles in visually and sound modes, and prevent the collisions. This module is used by pilots in air navigation. The system includes a software platform, corresponding to military standards, a secret tablet, a GPS receiver and antenna. Besides natural and artificial obstacles on the terrain, when helicopter approaches to national boundary, forbidden zones, etc., then warning system is activated. There is sound communication between pilot and tablet. System obtain only energy supply from helicopter (Fig. 8).

Fig. 8. GAS – HODWS module

The Direction Vector algorithm calculates the natural and artificial obstacles on the line of helicopter movement. On the basis of this algorithm the demonstration on the screen is carried out in three states and at the same time for all stages of the flight (take off, landing, flight). Connected by algorithm with velocity of the helicopter the Direction Vector is calculated constantly. If the velocity of the helicopter equals zero, then the Direction Vector is not calculated. It prevents formation of false warning. Sometimes, before take-off the pilot observes new artificial vertical obstacles on the terrain (new constructed television tower, GSM antenna and other objects) not included in system. The system helps the pilot to temporarily include this kind of new obstacles in the system. Then, these data are checked and included into server. The system records all flights (black box) (Fig. 9).

Fig. 9. GAS – Direction Vector algorithm demonstration

Loaded in tablet system the digital maps can be manipulated by finger up-down, left-right. Pilot can see helicopter trucking in the screen of tablet in 2D and 3D formats in real-time mode. At the same time, he can obtain terrain height profile along with the truck for the selected distance (Fig. 10).

Fig. 10. GAS – sensor property

FPM (feet per minute) algorithm of the system calculates a speed of climb in feet per minute for a pilot for safety obstacle fly-around, and jointly with pilot reaction in real-time mode and demonstrates on the screen. In the surprise situations, this algorithm automatically determines a landing trajectory for the pilot to the nearest airport.

In UAVs support operations Helicopter Obstacle Determination and Warning System (HODWS) module creates a radio communication between UAV's operator and helicopter's pilot. Operator and pilot can send a massage to each other. By using GSM card in real-time mode sent from UAV target's coordinates and images data are re-sent to the GAS-HODWS module. It creates a possibility of observation of the same images at the same time for UAV's operator, helicopter's pilot

and Staff personnel. The demonstration of UAVs' telemetry data in the module creates a possibility for pilot to see in the tablet all UAVs in air (Fig. 11).

Fig. 11. CAS – HODWS tablet

12. GAS – Helicopter Trucking and Following System (HTFS) module

It provides demonstration of helicopters flight in software platform. The Staff commander or operation duty personnel can watch in software platform the helicopters in air in real-time mode in 2D and 3D formats. It is possible due to the position coordinates obtained from SIM card (Fig. 12).

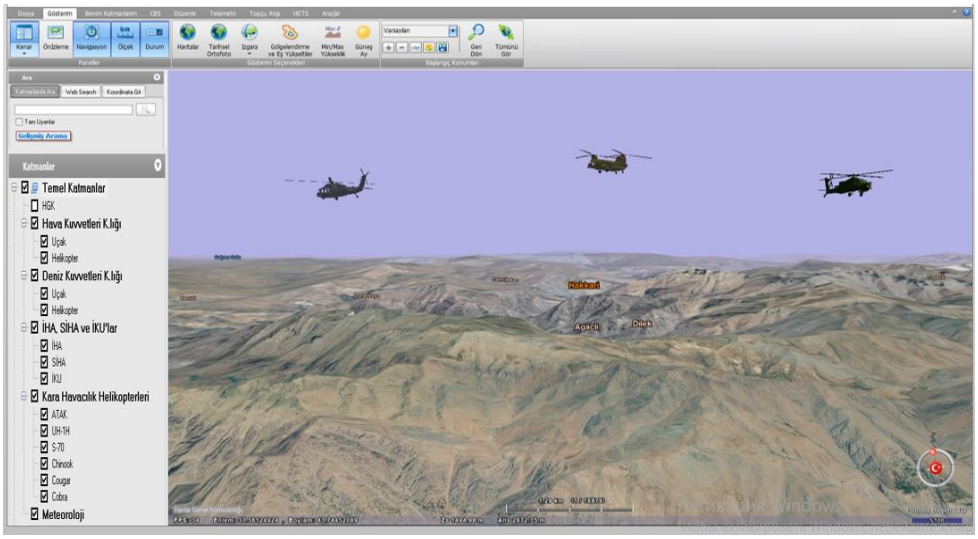


Fig. 12. GAS – Helicopter Trucking and Following System module

13. GAS – Telemetry module

This module provides observing in real-time mode in 3D format all aircrafts telemetry data in GAS Virtual Sphere software platform. This module is one of the most important software platforms for UAVs combat tasks planning and ground center controlling. There are all necessary functions for UAVs pursuing and controlling in GAS Virtual Sphere software platform. UAVs' coordinates, observation angle, camera observable area, trajectory and other data (models, name, flight height, etc.) are shown in GAS Virtual Sphere software platform in 3D format.

By applying this module UAVs can be used more effectively in operation area. The module supports processes of planning and decision making during the operation preparation and processing provides reinforcement of situation control and analysis of operation area in real time. Besides, in HQs and UAVs' control centers the UAVs polling can be carried out. The UAV's positions changes in air (left-right rotations, etc.) can be observed in program. It is possible to pursue UAVs from up, from cabin, from behind and under the various angles. Data about UAVs' flights can be archived and then analyzed (Fig. 13).

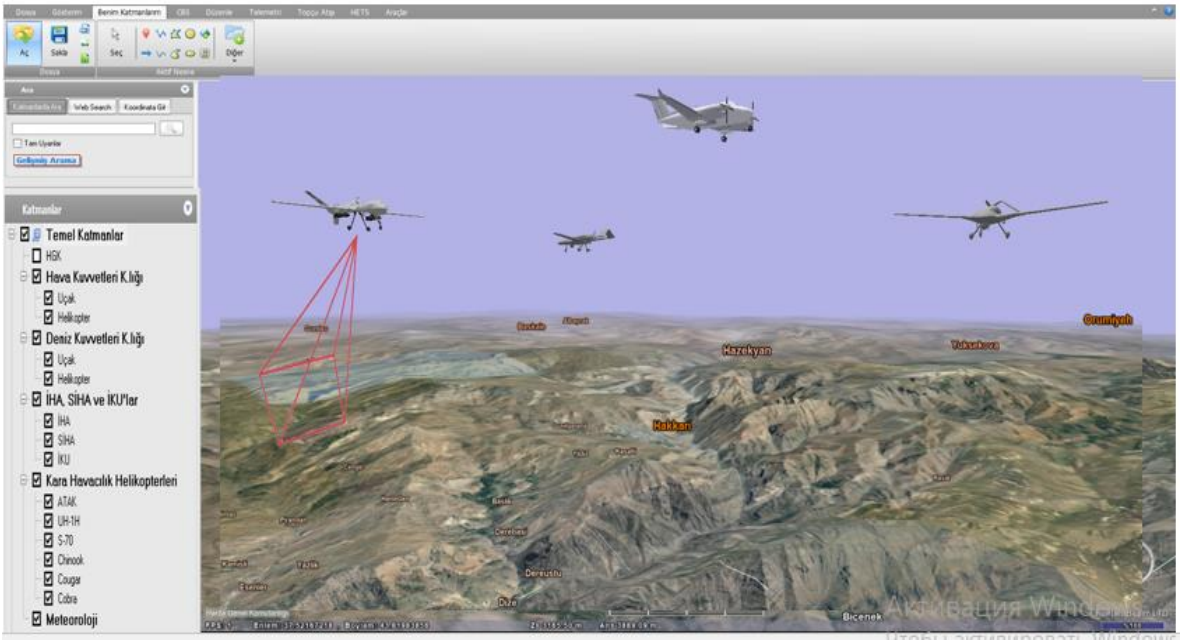


Fig. 13. GAS – Telemetry module

When UAVs approach dangerously to each other, if there are higher terrains than UAV flight height route and if the flight echelon cannot be changed then Control Operator forms sound and visible warning (Fig. 14).

Fig. 14. Danger warning

The image acquisition from UAV is shown in software on another screen. It is possible to take any terrain image from the image acquisition on the screen. The obtained images with real coordinates can be sent to another users. By using the functions of module it is possible to assess and comment upon obtained images (targets determination, reconnaissance data collection, images decoding, etc.). The module shows automatically the UAV's coordinates and the ground address.

The module shows automatically UAVs' coordinates and new address of the camera observed terrain. When UAV is followed at the same time the weather conditions can be observed. For the purpose of determination of UAVs' routes and tasks planning, the Route Planning function is included in module.

Telemetry data of all flights are kept in the server. By using of the server it is possible analysis and carry out a query of last flights' zones and time. For instance: in the result of *"In *** zone on 20 January – 20 May in 2019 all flights"* query all flights list is observed. Taken from the results and uploaded in the system some flight telemetry data shows the route of this flight and target's points in GAS.

14. GAS – Machinery and Personnel Following System (MPFS) module.

By using ASELSAN radiostations this module provides following in real-time mode of all personnel and military machineries in software platform. The commanders of the units can watch their locations in real-time mode. The new and old (for analysis) coordinates of radiostations location are saved in server.

In the operation area a radiostation group (transferring) can transfer information in real-time mode to radiostation and tablet (uploaded GAS-MPFS module) used by the commander of the group. The commander of the group can watch visually unobservable personnel and machineries on the tablet. Determined last movement data are saved in server. The commander of group send data by on-line to the Turkish Armed Forces (TAF) network. If in this moment there is not network connection, then when TAF network is opened, saved data are transferred to the GAS server of Land Forces Staff. The unit's (personnel's) position coordinates, and also target's coordinates can be sent to neighboring units, artillery division or helicopter's pilot.

Only authorized users can used this module. The user can follow only permitted units. The connection broken units are demonstrated in the module by various colours and operator is informed soundly about it. If the conditions (the velocity limit, broken route, unexecuted task in determined duration, etc.) are changed then the operator gets warning-message. It is possible to distribute the queried units' coordinates and targets' data in the module with comments and analysis. All data are recorded in the server. If some personnel's group presses the urgent call button then their position is watched on the tablet and the operator obtains warning-message.

The ASELSAN's product KESKİNGÖZ (GÖZCÜ-2) portable electron-optical sensor system is used for calculation of targets' coordinates in real-time mode. This module can be integrated in ASELSAN produced ŞAHİNGÖZÜ electron-optical observation devices [7; 8] (Fig. 15).

Fig. 15. CAS – KESKİNGÖZ (GÖZCÜ-2)

Conclusion

GAS software platform is an application of table 3D "Virtual Sphere" processed in server-user architecture. GAS can be used both as on-line and off-line modes and function in laptops, pads and tablets, mobile telephone and in PCs. GAS shows data very fast and provides just distribution of data among users. GAS software platform provides the users with an opportunity to carry out various queries and analysis, create new data and change current data. The buffer analysis, the profile determination, the visible and the "dead" zones determination, the dangerous zone analysis are the most simple examples of geographical analysis. Users can calculate 2D and 3D distance, area and perimeter of terrain.

GAS software platform has modular structure and due to the national code of source it can be upgraded for progress. By intensively using the software platform the safety of Defence and Security Forces can be provided.

The application of GAS software platform in the Armed Forces of the Republic of Azerbaijan is very important in order to form visual description of operation area for military units, investigate the depth of enemy defence, obtain information about the features of terrain, analyze step-by-step or on the whole operation area by using satellite images and aero photographs.

References

1. Hərbi kəşfiyyatçının hazırlığı. – Bakı: Hərbi Nəşriyyat, – 2000. – 180 s.
2. Coğrafi Analiz Sistemi (CAS) ile Askeri Karar Verme Süreci Etkinliğinin Artırılması // Harita Teknolojileri Elektronik Dergisi, – 2015. Cilt: 7, No: 2, s. (56-68).
3. Bayramov, A., Nəsibov, Y.A. Dağlıq ərazidə texniki müşahidə sisteminin imkanlarının reqressiya analizi // Milli Təhlükəsizlik və Hərbi Elmlər, – 2018. №4 (4), – s. 17-22
4. Principles of Geographic Information Systems, Second edition / A. Rolf [et al.] – The Netherlands, – 2001. – 490 p.
5. Nəsibov, Y.A, Həşimov, E.Q., Bayramov, A.A. Coğrafi İnformasiya Sistemlərinin Hərbi Məqsədlər Üçün İstifadəsi // Milli Təhlükəsizlik və Hərbi Elmlər, – 2017. №4 (3), – s.56-62.
6. CitySurf Kullanıcı Globe Kılavuzu Dokümanı / – Ankara: Pirireis Bilgi Teknolojileri şirketi yayınları, – Ocak 2008. – 28 p.
7. Bayramov, A.A., Hashimov, E.G., Nasibov, Y.A. The supervisory control systems deployment in mountainous terrain // VIII Intern. Confer. "Modern development trends of ICT and control methods", – Poltava, Ukraine, – 26-27 April, – 2018, – p. 3-4.
8. Nasibov, Y.A. Modelling of the rationally deployment of observing systems / Y.A.Nasibov, A.A.Bayramov, E.N.Sabziev [et. al.] // Advanced Information Systems, – 2019. v.3 (2), – p. 10-13.

Xülasə
Coğrafi Analiz Sistemi Proqram platformasının hərbi məqsədlərdə tətbiqi
Yaşar Nəsibov

Bu məqalədə, Coğrafi İnformasiya Sistemləri əsasında hazırlanmış və Türkiyə Silahlı Qüvvələrində uğurla istifadə olunan Coğrafi Analiz Sisteminin Azərbaycan Respublikası Silahlı Qüvvələrində tətbiqi və faydalarından bəhs edilir.

Açar sözlər: Coğrafi İnformasiya Sistemləri, Coğrafi Analiz Sistemi, ərazinin öyrənilməsi və qiymətləndirilməsi, döyüşü təşkil etmək.

Аннотация
Применение программной платформы Географической
Анализирующей Системы в военных целях
Яшар Насибов

Статья посвящена преимуществам применения в Вооруженных Силах Азербайджанской Республики Географической Анализирующей Системы, созданной на основе ГИС и успешно используемой в Вооруженных Силах Турции.

Ключевые слова: географические Информационный Системы, географическая Анализирующая Система, изучение и оценка местности, организация боя.

Məqalə redaksiyaya daxil olmuşdur: 27.09.2019
Təkrar işlənməyə göndərilmişdir: 25.10.2019
Çapa qəbul edilmişdir: 20.11.2019

UDC 623

EVALUATION OF COMPETENCE IN ACTIVE AND PASSIVE PROTECTION SYSTEMS AND EVALUATION OF THEIR EFFECTS ABOUT TECHNOLOGICAL DEVELOPMENTS IN THE FUTURE WAR AREA

Ayhan Aytaç[1], Büşra Aslan[2], Uğur Çakir[1]
[1]*National Defense University, Turkey,*
[2]*Ministry of Industry and Technology, Turkey*
E-mail: aytac@kho.edu.tr,
busra.aslan.esogu@gmail.com,
ucakir@kho.edu.tr

Abstract. The purpose of this study is to examine the technologies that affect active and passive protection systems and the development of antitank weapons by conducting a literature research. In addition, our purpose is to carry out an assessment of the effects of the current and possible combinations of technological developments in this area on the future war zone. Thus, it is aimed to describe the future war zone and increase the competence of the national industry in line with the needs and the ability of the Turkish Armed Forces to eliminate the threats that are directed at military platforms, as soon as possible, at the farthest point and with the least cost.

Keywords: Active Protection Systems, Passive Protection Systems, Future War Zone, Armor Systems.

Introduction

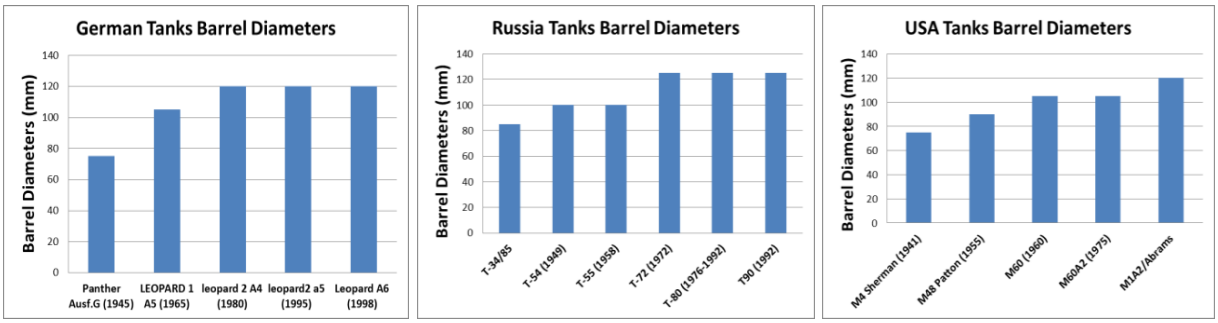
In this study, it is assumed that ideological and economic conflicts of interest will continue in the future. Therefore, the impact of technological developments and current status of Turkey and the world about active and passive protection systems had been evaluated to make a provision for Landwehr.

Use of Tanks in Battlefields

The first tanks were designed as infantry support and intended to be used for the destruction of enemy defensive lines, machine guns or artillery capable of firing high-impact explosive ammunition on armored bodies carried on pallets that could move on worn-out terrain.

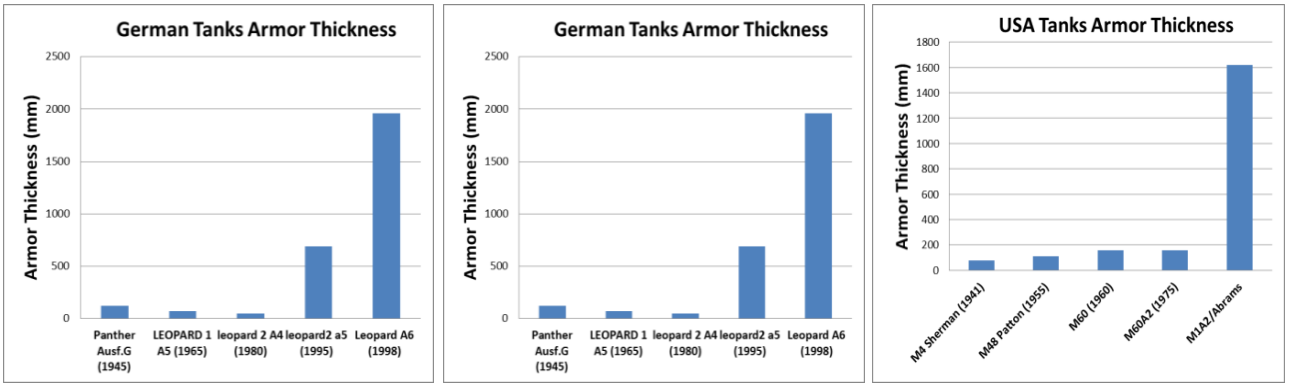
The first use of tanks in battlefields was observed in 1916 with the British Mark-1 tank [1].

By honoring the idea of using tanks directly as an offensive weapon in World War II, the biggest threat for tanks also became enemy tanks. Therefore, there was an increase in the thickness of armor protection as well as the need for armor protection against the ammunition used by enemy tanks. An increase in the initial velocity of the projectiles used to destroy enemy tanks was carried out in an environment with barrel diameters reaching 120 mm in NATO and 125 mm in Eastern Bloc countries (Graph. 1).



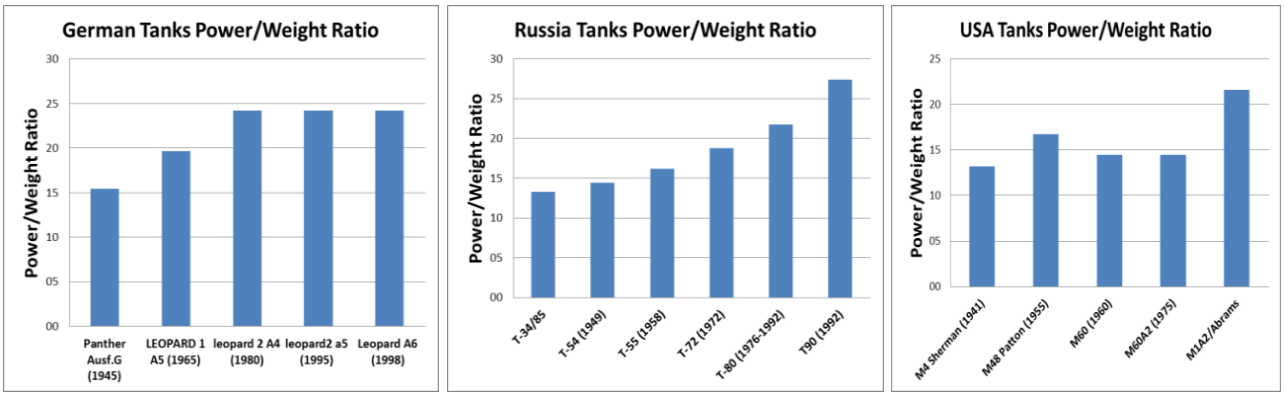
Graph. 1. Change in barrel diameters according to the origin and model of the tanks

As the technology of chemical and kinetic energized armor-piercing ammunition used in advanced tanks, there was also an increase in armor protection. Especially with the introduction of composite and reactive armor containing a certain amount of explosive, the concept of equivalent armor protection has emerged. Composite and reactive armors used on the latest technology tanks can provide protection equivalent to the protection provided by armor steel of 1600 mm. (Graph. 2).



Graph. 2. Change in armor thickness according to the origin and model of the tanks

The increase in armor thickness and the increase in weight resulting from the growth of the weapons used led to the need to increase the engine performances used in the tanks. Firstly, the use of gasoline engines in tanks left their places to diesel engines. In addition, the weight ratio per ton (Power/Weight) was an important criterion in the assessment of mobility of tanks. It is evident that the Power/Weight ratio is above 20 in many tanks produced today (Graph. 3).



Graph. 3. Weight/Power Ratio changes according to the origin and model of the tanks

As a result of the increasing technology about guided anti-tank missiles (ATGM) which can be used by one person against tanks, since the late 1950s, active protection systems have been developed to detect and neutralize such missiles directed towards them.

Development of Antitank Weapons

The first ATGMs, which were developed in the late 1950s, used manual guidance systems, requiring the operator to steer the missile to the target with a joystick or a similar controller. The disadvantage of these systems was that, it required extensive operator training and that after the firing the operator had to remain in the firing position where possibly in danger until the missile reached the target. Examples of these systems include the British Vigilant missile and the Soviet-made Sagger, one of the most widely produced ATGMs [2].

Semi-automatic guidance systems developed in the mid-1960s, requiring the operator to aim the gun at the target only when the missile was in flight, reduced the difficulty of using ATGM. In these systems, the missile is directed to the target by wire, radio frequency or laser. Many ATGMs

have been developed then, such as the US-made TOW, Chinese-made Hongjian-8, and Russian-made Cornet [2].

Advanced ATGMs such as the recently produced US-made Javelin and Israeli-made Spike allow the operator to select targets with an optical or infrared imager connected to the missile launch tube with "fire and forget" technology. After firing these systems, the missile flies towards the target without further action by the operator.

Air-to-land missiles designed to be used against tanks also include "fire and forget" guidance systems. Most new ATGMs fly in high orbit and hit their targets from their weakest points, the top, without being detected [2].

Passive Protection Systems

In order to provide protection against shoulder rockets and increase the survivability of armored vehicles, cage, particle or mesh type flexible layered armor systems or different combinations thereof are integrated into military vehicles.

The particle-type armor system has lower areal weight and higher yields than the lattice-type armor system, but the application problem for window regions requiring visibility and the disadvantages of the tension force needed to stand in the fixed position.

Mesh armor system is lightweight and provides ease of installation. It provides fast entry and exit convenience from vehicles in case of emergency and is foldable for the transportation of armored vehicles. On the other hand, one of the disadvantages is that metal mesh types need frames for assembly.

Mines and ballistic protection can only be achieved by increasing the thickness of the armor, paving the way for a new generation of technologies and increasing the weight of the same effect without increasing the search for design alternatives.

Conventional armor used in vehicles is effective in stopping kinetic energy ammunition, but also it is ineffective about stopping RPG-7, Tow, Cornet etc. pit-shaped missiles and rockets. Even if the armor is thicker than 25 cm, these threats still can penetrate them. Therefore, in addition to conventional armor, active protection systems are developed in armored vehicles too [3].

To summarize the objectives:

- catch the threat before it hits the vehicle;
- provide short-circuiting of the cables providing the ignition by disrupting the conical outer structure of the threat ammunition;
- neutralize threat ammunition by preventing detonation and jet flow.

Besides, a study conducted between the US Army Tank – Automotive R&D and Engineering Center (TARDEC) and Michigan State University (MSU) Center for Composite Materials and Structures explores lightweight composite materials to protect the tank against mines and impacts. Graphene material, which is found to increase the strength of lightweight composite materials, was in the center of the studies [4].

Active Protection Systems

Despite the advantages it provides, it has been determined by literature research, that passive protection systems (hollow armor, composite armor, etc.) cannot provide effective protection in armored vehicles which are indispensable elements of armies. Therefore, the importance of active protection systems that developed with the opportunities offered by intelligent (cybernetic) electronic technology is clearly seen.

Active Protection is a defense system that increases the survival of the platform against the threat directed to it (light, medium-weight or heavily armored land vehicle) by; eliminating, deflecting or confusing them [5].

It is important to create a joint tactical picture correctly in the battlefield and to share the information instantly and accurately with the party concerned to win the war [6]. Designed with this perspective, APS has three units; sensing unit, control unit and countermeasure unit.

The detection unit consists one of the missile warning, laser warning and radar warning systems, but it can also be composed of multiple combinations of these three systems.

The control unit is a subsystem that warns the countermeasure unit by evaluating the threat information sent by the sensor unit. For example; the threat detected by the missile warning system is monitored and the relevant data is sent to the control unit. The controller then classifies the threat and determines if it will hit the platform. It also identifies the type of threat if it has the ability to diagnose.

If the countermeasure unit receives the information from the control unit that the approaching threat will hit the platform, it performs the active application. In this direction; calculates the countermeasure ammunition at which point it will meet the threat and ensures that countermeasure ammunition is disposed towards this reception point. The countermeasure ammunition at the calculated welcoming point destroy the threat [3].

In APS applications, two different countermeasures methods are used as 'hard-kill (physical destruction) and soft-kill (functional destruction) against threats. The aim of the soft-kill countermeasure method is to prevent the threat from reaching the platform by preventing the use of fogging and mixing than the missile guidance signs without physically destroying the threat. Once the threat signal has been detected by the relevant sensor on the platform, the controller automatically selects the appropriate soft-kill method or allows vehicle personnel to select, depending on the system mode. Since it is not possible to protect from unguided munitions such as RPG by soft-kill method, hard-kill countermeasure method becomes an alternative. In this method, it is aimed to destroy or change the direction of the threat by physical intervention [7].

In principle, a guided ammunition is first attempted to eliminate by applying soft-kill against the guiding signal; in case of failure, hard-kill is applied to the ammunition (Fig. 4).

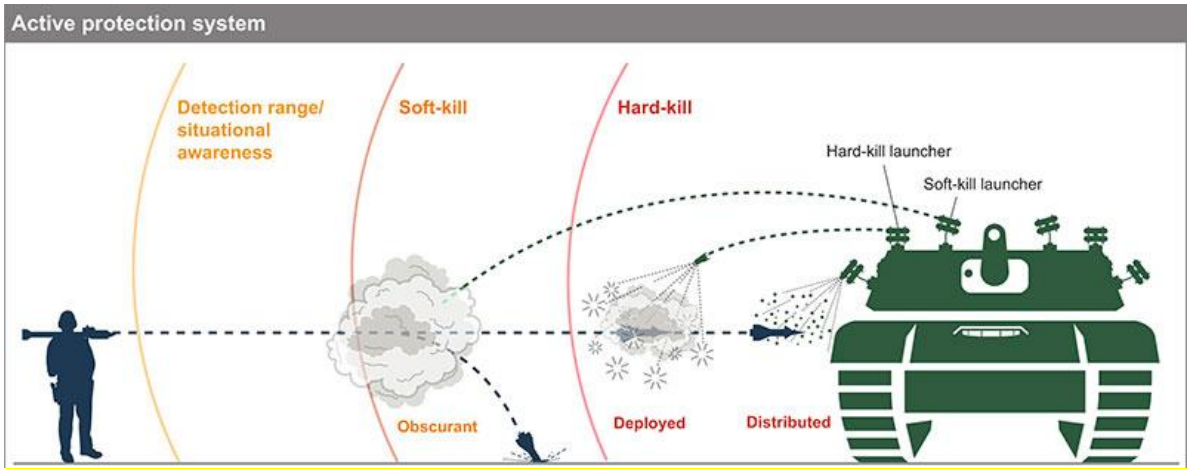


Fig. 4. Active Protection System Operation Principle [8]

Although the complexity of these systems brings important technical difficulties, it is considered that the R&D studies, especially the technological development of military vehicles, will be the focus of the coming years.

The development of APS belongs to the development of existing threats (eg. ATGM: Anti-Tank Guided-Missile). Therefore, technologies in threat types need to be examined at certain intervals. The first types of threats are the anti-tank weapons used in the Turkish Armed Forces inventory against tanks and helicopters.

In line with the developments in the threat area and the anticipated developments in the threat area, efforts are underway to increase the competence of APS. About this subject; Harrison stated that the studies on sensors and countermeasure technologies are priority research areas [9].

Current situation in Turkey

PULAT APS, that developed by ASELSAN, will provide a 360 degree full protection shield depending on the placement of modules against close-range anti-tank rockets and long-range launched anti-tank missiles, can provide simultaneous effectiveness against multiple threats with distributed protection modules installed to the platform (Fig. 5).

Although, it is accepted that a hard-kill process under 5–6 meters is not effective in APS, these operations are performed at 7 meters in the current situation. "AKKOR", can counteract the threat approaching the tank with countermeasure ammunition at a distance of 15-20 meters. It has coverage up to 70º on the ascent axis and can also be effective against Javelin-like anti-tank missiles with rockets thrown from the roofs (Fig. 6).

Fig. 5. PULAT APS [10, 11]

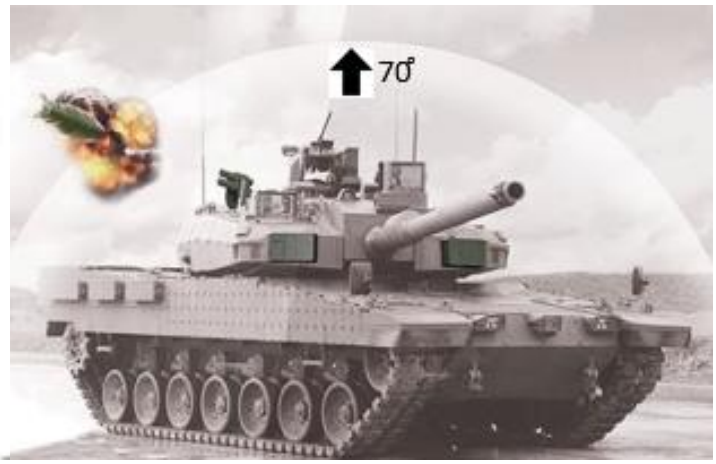


Fig. 6. Incandescent

In our country, flexible layered cage armor system studies are being carried out for armored vehicles. Assembly activities of the cage armor system which will protect the armored vehicle and personnel from the effects of RPG-7 pit spelling right ammunition are continuing. Vehicle modernization projects and development of armor systems for armored personnel carriers are continuing by ROKETSAN Ballistic Protection Center [12].

Current situation in the world

Other country studies, especially about Drozd, Trophy and Iron Fist, which are being developed from past to present, are examined under this title.

Drozd. The first APS was developed by the Soviet Union between 1977 and 1982 [13]. Drozd, which incorporates the hard-kill measure method, was installed in T-55A tanks in 1983 to fight guided tank missiles and rocket launchers during the Afghanistan War. The system was 80% successful, but it was found out that it was seriously damaging the soldiers fighting alongside the tank.

Trophy. Although Russia has Drozd and the updated version of this technology, such as the Arena, Ukraine and Zaslon, Israel is the pioneer in the field of active protection systems with the most casualties due to guided anti-tank missiles. There are two important hard-kill systems developed by armor engineers. These are: Trophy and Iron Fist APS [14]. The main purpose of Trophy is to protect ZPT vehicles with light armor, especially in powerful anti-tank weapon attacks.

Iron Fist. Iron Fist has a radar system developed by RADA Electronic Industries, founded by former CEO of Boeing Herzl Boedinger and supported by a passive infrared detector. It is distinguished from the Trophy by being extremely lightweight. One of the biggest advantages of this system is that it does not damage the soldiers outside the tank by destroying threatening rockets or other ammunition in the air by performing an undisturbed part.

Future warfare area. Technological globalization has led to the emergence of a new war theory based on information, communication, network, computer and sensor technologies, defined as

the adaptation of modern armies to the facts and conditions of the Information Age [15]. Although almost all developed defense platforms use the frequency band at a certain rate, according to Karaağaç [16]: The decisive factors in the success of military operations were "Land Superiority", "Sea Superiority", "Air Superiority" and "Knowledge Superiority". Now, in addition to "Air-Space Superiority" and "Cyber Space Superiority", the concept of "Electromagnetic Spectrum Superiority" has come to the fore. According to Stillion and Clark [17], modern combat networks, command-control systems, target detection sensors and other reconnaissance-surveillance-intelligence facilities, weapon systems and platforms, and all these elements that connect the electronic-based communications capabilities. In this direction:

- maintaining the frequency band required for our own systems;
- measures should be taken to prevent the use of frequency spectrum of enemy systems and to protect friendly forces from their air defense systems;
- electronic warfare tasks are to performed as close and remote mixing to prevent detection by the enemy.

Operative UAV systems with useful loads to enable electronic mixing, deception and attack can be used in place of manned systems for tasks performed in environments where enemy air defense threat is high. Table 1 gives inferences regarding the UAV system and capability requirement, which is predicted to play an important role in the future operational environment [18].

Table 1

UAV System and Capability Needs in the Future Operational Environment [18]

Today	**Concept**	**Tomorrow**
Homeland security Peace support operation	Scenario	Conventional warfare
Border security Counterterrorism Low level power usage	Main purpose	Early warning Full power usage Protection of country resources
Country lands International operations area	Operating environment	Enemy territory
Zero-Low	Air defense threat level	Medium-High
Zero-Low	Link mixing level	Medium-High
Mini Small Tactical	Priority platform requirement	Nano Operative Strategic
Flight time Precision engagement Shipping weight	Priority requirement	Speed Range Altitude Maneuver Invisibility Autonomy Flock Link Security Self-protection

The predictions regarding the capability and capability needs of armored vehicles today and in the future are interpreted in Table 2.

Table 2

Capability needs of armored vehicles

Today	Ability / Attribute	Tomorrow
✓ Residential area ✓ Counter Terrorism	Scenario	✓ Residential area ✓ Conventional Warfare
✓ Firepower ✓ Infantry Support ✓ Tank-Tank Battle	Main Purpose	✓ Protection of Strategic Resources ✓ Damage to the Enemy ✓ Firepower Superiority
Land Operations	Operation Environment	Land Operations
✓ Fire-and-forget (FaF) ✓ Aircraft	Threat	✓ An unmanned combat aerial vehicles (UCAV) ✓ Autonomous High-fire and Movement-Armed Vehicles ✓ Aircraft and Helicopters
✓ Medium ✓ Tactical	Platform requirement	Operative and Strategic
✓ Machine Gun ✓ Tank cannon ✓ Guided Missile ✓ Diesel Engine ✓ Active Protection Systems (APS) ✓ Composite and Reactive Armor	Capability / Protection Level	✓ Autonomous Vehicles Equipped with APS ✓ High Power / Weight Ratio (Hybrid Motors) ✓ Invisibility ✓ High Firepower (Laser, Guided Missiles) ✓ Composite Armor Against Light Weapons

As a result, according to Astan [19], soldiers, who are the cornerstones of each army, will maintain their existence and importance in the operational environment in the future no matter how advanced the technologies for the use of unmanned elements and remote-controlled systems and similar technologies are.

Conclusion

It is clear that studies for solutions that are lighter for the future do not restrict mobility and offer a higher level of protection, and therefore R & D (research and development) studies for nanomaterial's will be important.

The followings are inferences in order to guide future warfare activities, taking into account the technologies that affect active and passive protection systems and the current situation:

– the performance of APSs can be measured by the distance to address threats. A detailed examination of the parameters determining the performance will serve the development of the systems. These parameters are: radar threat detection time, lancet turn speed, countermeasure speed, radar range, threat firing distance, threat speed, number of ammunition found in the lancer. A negative value in the distance measurement indicates that the detection will hit the platform before the countermeasure ammunition is launched. Sub-details of this calculation are the subject of a separate study;

– the integration of graphene into active and passive armor systems is expected to contribute greatly to the R & D activities carried out in this field;

– the perception of the signals produced by the APS by the enemy and thus their function is open to improvement;

– R & D studies should be carried out for the threat of RPG-30, which consists of two parts: surprise and actual ammunition. This threat, unlike the others, fires the ammunition in advance and

enables the APS to take action for itself. Thus, the duration of the APS between the two reactions limitation of the original ammunition. Solution is the development of countermeasure ammunition to be divided into two parts in the air, just like the threat of RPG-30.

- the inclusion of APS in tank modernization projects is critical in order to achieve rapid gains.
- it should be kept in mind that the transition of investments from automation to cyber-physical systems, so that technologies such as the Internet, big data, cloud computing will change the concepts of armor protection and the battlefield of the future.
- it is important to update cyber capabilities by the law of armed conflict for the war environment of the future. It is also expected that a regulatory international mechanism for attack cyber capabilities will be established and a verification regime will be put on the agenda of the countries as soon as possible. Active and passive protection systems, vehicle / headquarters and so on. The ability to protect the platforms can be expressed in absolute terms that will shed light on the way to become a leading country in this field.

References

1. Ellis, C., Chamberlain, P. Tanks Marks I to V // AFV Profile, Profile Publishing, 1969. No.3, p. 9-10.
2. The Editors of Encyclopedia Britannica: [Electronic resource] / – 18.05.2018. URL: https://www.britannica.com/technology/antitank-guided-missile.
3. Vivek, R., Roopchand, J. Active Protection System for AFV application – Current trends and future requirement – A study report // Int. J. Computer Technology & Applications, – 2012. V.3 (4), – p. 1450-1454.
4. Enhanced blast protection with polymer composites containing xgnp® graphene nanoplatelets. Modeling & simulation, testing and validation (MSTV) technical session / R.Privette, H.Fukushima, L.Drzal [et al]. – Michigan, – 2017.
5. Döğüşken, C., Kılıçarslan, E., Ertekin, Ö. Kara platformları için aktif koruma sistemleri // Savunma Bilimleri Dergisi, – Mayıs 2011. 10(1), – s. 96-106.
6. Tuğcu, M., Gürel, O. Taktik Data Link Teknolojilerinde Birlikte Çalışabilirlik ve Kritik Simülasyon Bileşenleri // Savunma Bilimleri Dergisi, – Mayıs 2012. 11(1), – s. 239-250.
7. Evensen, P. Modelling and implementation of a generic active protection system for entities in Virtual Battlespace (VBS) / P.Evensen. – Norwegian Defence Research Establishment (FFI), – 2017. – 33 p.
8. Wey, P. Analysis of Active Protection Systems: When ATHENA Meets Arena / P. Wey, P. Chanteret, V.Fleck – France, Saint-Louis: French German Institute, – 2001. – 16 p.
9. Harrison, M. National Defense Industrial Association. Joint Armaments Conference & Exhibition Army Aviation and Missile Research, Development, and Engineering Center, ABD, – 2012.
10. ASELSAN, AKKOR, Broşür: Aktif Koruma Sistemi: [Electronic resource] / – 08.06.2018. URL: https://bit.ly/36uPZC6.
11. ASELSAN, PULAT, Broşür: Aktif Koruma Sistemi: [Electronic resource] / – 08.06.2018. URL: https://bit.ly/2tx9zio.
12. Uzunçakmak, Y. Ruzin, Kal Z. Türkiye'nin Zırh Mükemmeliyet Evi: Roketsan Balistik Koruma Merkezi // – Ankara: Roketsan Dergisi, – Temmuz 2011. Sayı 1.
13. Meyer, T. Active Protection Systems: Impregnable Armor or Simply Enhanced Survivability? // ARMOR – May-June 1998. – p. 7-11.
14. Feickert, A. Army and Marine Corps Active Protection System (APS) Efforts / A.Feickert. – Congressional Research Service, – 2016. – 31 p.
15. Isır, T., Polat, M., Demirel, A. Değişen Savaş Koşullarının Uluslar Arası Organizasyonlar İle Askeri Karargâhların Yapısına Yansımaları: Bilgi Karargâhları // Journal of Economy & Knowledge Management (1), – 2007.

16. Karaağaç, C. Uçan Robotlar: Geleceğin Askeri Harekât Ortamında İnsansız Hava Aracı Sistemleri / C.Karaağaç. – Ankara: STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş., – 2016. – 20 p.

17. Stillion, J., Clark, B. What it Takes to Win: Succeeding in 21st Century Battle Network Competitions / J.Stillion, B.Clark. – CSBA, – 2015. – 110 p.

18. Kasapoğlu, C. Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında: [Electronic resource] / – 06.05.2018. URL: https://bit.ly/2QOYRvH.

19. Astan, G. Gelişen teknolojiler ve değişen muharebe şartlarında geleceğin askerine yönelik teknoloji öngörü çalışması / Yüksek lisans tezi / Ankara, – 2015. – 221 p.

Xülasə

Aktiv və passiv qoruma sistemlərindəki imkanların incələnməsi və onların texnoloji inkişafının gələcəkdə hərb sahəsinə təsirinin qiymətləndirilməsi

Ayhan Aytaç, Büşra Aslan, Uğur Çakir

Bu işin məqsədi aktiv və passiv qoruma sistemlərinə təsir edən texnologiyaların və tank əleyhinə silahların inkişafının elmi mənbələr əsasında ortaya qoyulması və bu sahədəki texnoloji inkişafın mövcud və mümkün kombinasiyalarının gələcəkdə hərb sahəsinə təsirinin qiymətləndirilməsidir. İş nəticəsində milli sənayemizin, Türkiyə Silahlı Qüvvələrinin ehtiyacları istiqamətində istiqamətləndirilməsi və ölkəmizin, xüsusilə aktiv qoruma sistemləri mövzusunda hərbi platformalarımıza yönəldilən təhdidlərin ən qısa müddətdə, ən uzaq nöqtədə və ən az xərclə aradan qaldırılması məqsədilə gələcək hərb sahəsinin şərhinə cəhd edilmişdir.

Açar sözlər: aktiv qoruma sistemləri, passiv qoruma sistemləri, gələcək müharibə zonası, zireh sistemləri.

Аннотация

Исследование возможностей в системах активной и пассивной защиты и оценка влияния их технологического развития в будущем на военную область

Айхан Айтач, Бюшра Аслан, Угур Чакыр

Целью этого исследования является изучение технологий, которые воздействуют на системы активной и пассивной защиты, и разработку противотанкового оружия путем проведения научных исследований и оценка влияния существующих и возможных комбинаций технологического достижения в этой области в будущем на военную область. В конечном итоге сделана попытка изложения будущей военной области с целью направить национальную промышленность в направлении потребностей Вооруженных Сил Турции и особенно в тематике активной защиты в целях устранения угроз в самое короткое время, в самой далёкой точке и в минимальных затратах направленных на военную платформу нашей страны.

Ключевые слова: системы активной защиты, системы пассивной защиты, зона будущей войны, бронированные системы.

Məqalə redaksiyaya daxil olmuşdur: 27.09.2019
Təkrar işlənməyə göndərilmişdir: 30.10.2019
Çapa qəbul edilmişdir: 22.11.2019

UDC: 623.451

INVESTIGATION OF INELASTIC COLLISION OF BULLET WITH HOLLOW CYLINDERS OF MATERIAL

[1]Anatoly Kovtun, [2]Vladimir Tabunenko, [3]Oleg Bogatov, [4]Azad Bayramov
[1]National Academy of the National Guard of Ukraine
[2]Kharkiv National University of Air Force, Ukraine
[3]Kharkiv National Automobile and Highway University, Ukraine
[4]War College of the Armed Forces, Republic of Azerbaijan
E-mail: kav-60@ukr.net; tabunenko55@ukr.net;
bogatovoleg@mail.ru; azad.bayramov@yahoo.com

Abstract. In the paper, the armored protection improvement has been considered. The constructional material, which consists of nested elements interconnected with hollow cylinders, can be an alternative to armored materials. One of the materials of personal protective equipment is a fabric resistant to high-energy impact, made of synthetic fibers of special composition and structure, which is used in the form of a package of several layers that can hold up debris and low-velocity bullet. Rigid plates are used to hold high-speed striking elements, and a shock-absorbing layer is used to dampen the blows. A numerical model for determining the depth of penetration of a bullet into an obstacle in the form of a set of hollow cylinders is proposed. The results of the calculations and experimental investigations are presented.

Keywords: armored protection, high-velocity bullet, barrier, plastic deformation, hollow cylinder, dynamic penetration, experiment.

Introduction

The analysis of the work on the improvement of modern weapons and ammunition shows that their penetrating ability has greatly increased in recent years and this growth will continue in the near future. Therefore, the tasks of developing modern means of individual armor protection remain relevant. The existing experience in the field of creation of armor materials shows that the most promising ways to increase the effectiveness of armor protection of weapons, military equipment and personnel today are associated with the creation of:

- protective structures of a new generation by developing armor materials and heterogeneous armor from light alloys (including aluminum and titanium);
- aramid fabrics and fiber-composite materials based on high molecular weight polyethylene fibers;
- a new generation of high-strength materials based on nanotechnology;
- armor elements from shock-resistant ceramic materials [1].

An alternative to armor materials are constructive methods. One of them is the method, which consists of nested elements as a protective structure (a protective structure is a set of interconnected hollow elements, for example, hollow cylinders) [2].

Modern means of protection are diverse. The main material of individual protective equipment is a fabric resistant to high-energy impact, made of synthetic fibers of a special composition and structure. This fabric used as a multi-layer bag retains debris and low-speed bullets. Rigid plates are used to hold high-speed striking elements. In addition, a cushioning layer is used to soften the blows.

Rigid plates undergo the main impact of the high-speed striking elements. They can be made from high-strength metals or double-layer panels. When co-stressed with such a panel, the toe of the bullet is destroyed. As a result, the area of interaction between the bullet and the panel increases, the deflection and splitting of ceramics occur while the bullet is destroyed simultaneously.

In the scientific literature, the greatest attention is paid to determining the required thickness of the barrier depending on the impact velocity [3-14]. It is noted that, when the impactor interacts with the obstacle at low speeds, the inertial forces are negligible compared to the strength characteristics of the elements. The deformation covers the entire structure and is mostly elastic in nature. At medium impact speeds, inertia forces are comparable to static penetration resistance, the deformation is local and is characterized by high values of plastic deformation and its speed. At high impact speeds, inertial forces become prevailing, the flow of material of the interacting elements approaches the hydrodynamic one.

Different researchers have obtained various empirical formulas that take into account the main parameters of the strike [3, 4] (Petri, Nobile, Siacchi and Krupp, Le Havre, Thompson, Davis, Berezanskaya and others) based on experimental data garnered during shelling sheets of armor under various conditions, which limit their scope.

Formulation of the problem. However, most studies draw attention to the mechanical characteristics of materials, and the structural parameters of obstacles are estimated to a much lesser degree. It is common to the well-known studies that the protective barrier is represented in the form of a plate (set of plates), while one of the components of small arms is a mechanical system consisting of a drummer (bullet) and a barrel (pipe).

Thus, the presented data indicates that the theory of mechanical interaction of a bullet with various types of obstacles has not been fully completed. The processes occurring during the impact interaction of elements of mechanical systems have not been fully studied. The applied models and calculation methods depend on the required accuracy obtained results without evaluating the design parameters of the obstacles. Further improvement of individual armor protection can be achieved by applying the optimal combination of new materials and modern design and circuit solutions.

The processes occurring during the penetration of obstacles are very diverse and depend on many factors. The speed and direction of impact, the size and shape of the bullet, the design and manufacturing technology of protective equipment, the physical and mechanical properties of the materials of bullets and protective barriers are the main factors.

The reliability of the impact's results prediction of a bullet with an obstacle increases by comparing the results of analytical and numerical modeling, as well as data from field tests. A comprehensive experimental and computational study of the characteristics of the interaction of bullets with obstacles is the most important condition for a reliable prediction of the results of the interaction of elements and can significantly improve the efficiency of development of structural solutions.

Such a research scheme (the study of the behavior of structural elements under real-world dynamic penetration conditions, numerical and experimental study) allows creating the basis for developing and substantiating recommendations for rational design and selection of materials, their structural state, ensuring an increase in the efficiency of their use in structures.

Theories of elasticity, plasticity and strength of materials, the theory of reliability of protective barriers, mathematical modeling, and mathematical planning of experiments are the scientific basis for research of the process of passing through barriers by high-speed bullets.

The goal of the article is to investigate the process of interaction of a high-speed bullet with a protective barrier in the form of a set of hollow cylinders.

Penetration process

The process of penetration of bullets into traditional protective barriers unites several physical mechanisms. In this case, they are: the stage associated with the expansion of the barrier material and the stage of knocking out the plug.

When a bullet strikes an obstacle, several types of disturbance waves occur in it, spreading at different speeds. These disturbances in the design cause a complex stress state, the intensity of which quickly decreases with time.

Penetration can be defined as the entrance of the drummer into the barrier and its further movement. Under non-penetration, the drummer does not extend beyond the back surface of the barrier. If a drummer bounces off the obstacle surface, or penetrates into it along a curved path, and then comes out of it at a slower speed, then this phenomenon was called rebound. When punching, the drummer penetrates through the barrier, leaving from the back. In addition to the processes of direct penetration of the impactor into the obstacle, wave processes play an important role in collisions. With ballistic contact, a shock wave of compression arises in the material of the obstacle, which propagates to the back surface with the speed of sound vibrations (significantly exceeding the kinematic speed of the impactor).

Having reached the back surface of the obstacle, the shock wave is reflected, turning into a stretching wave propagating in the opposite direction. As a result, for brittle or anisotropic materials, fracture in the form of spalling may occur. When spalling happens, some materials come off under the action of tensile stresses of the reflected shock wave, from the back surface of the barrier and gain speed in the direction of the impactor. It facilitates the process of penetration, and can lead to a super gradual defeat through penetration of the drummer.

The initial stage of bullet penetration into an obstacle is determined by at time during which the bullet penetrates into the barrier to a depth of about two of its diameters. During this period, for a non-deformable bullet with a cone-shaped head, the nature of the movement and the stress-strain state of the material of the barrier change, and the penetration force reaches a steady-state value that differs from the force in the surface layers. (In the case of the interaction of a bullet with a relatively strong barrier at the initial stage, there is an intense deformation of the head part of the bullet and the formation of its new form).

After reaching, a certain critical depth of penetration there may start forming the crater size stops changing and the main channel of the cavity. The final stage of punching the barrier is considered a part of the punching process, which begins when the bullet approaches the back surface of the barrier at a certain critical distance and ends at the exit of the bullet from the barrier. The achievement of the specified distance, associated with the exit to the back surface of the plasticity zone, causes a change in the stress-strain state of the internally acting elements. When a bullet approaches the backside of the barrier, appears in the form of an expanding conical funnel. Because of these stresses in the material may be damaged or cracked. Further movement of the bullet leads to the breaking of part of the material of the barrier σ_r and σ_f, a zone of tensile radial and tangential stresses.

The nature of the penetration of a bullet into an obstacle may change if the obstacle is a structure consisting of a set of hollow cylinders (Fig. 1).

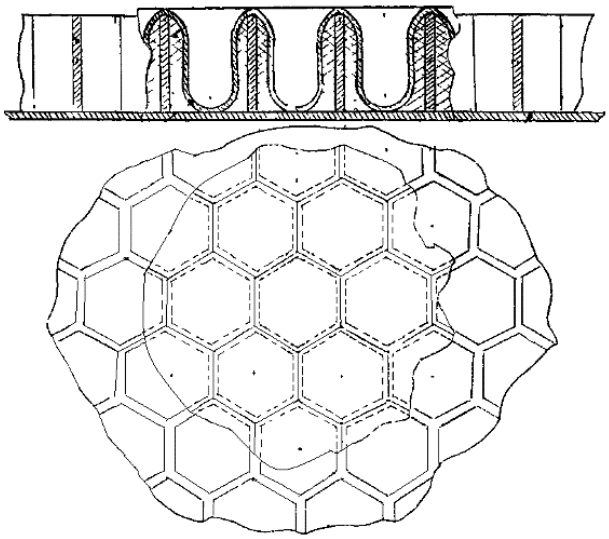


Fig. 1. Construction of the barrier in the form of a set of hollow cylinders

Structurally, a protective barrier of this type may contain outer, intermediate and inner layers [2]. In this case, the outer layer is made in a form of a set of interconnected hollow cylinders with a closed bottom and an expanding upper part made of materials with the property of plasticity. The inner layer is a power frame in the form of a spatial grid consisting of a plate connected to the stiffeners perpendicular to it, the distance between which is greater than the outer diameter of the cylinder of the outer layer.

The outer and inner layers are interconnected by means of an intermediate layer of visco-elastic material. The design of the outer layer of the protective barrier allows you to convert the kinetic energy of the impactor into the work on the plastic deformation of cylinders. The use of the inner layer, as a power frame, allows you to redistribute the energy of the striker over a larger area. The use of an intermediate layer of visco-elastic material allows reducing the energy transmitted by the impactor to the inner layer of the protective barrier.

Upon contact of the bullet with the outer layer of the barrier, due to the presence of an expanding upper part, the bullet enters the hollow cylinder that fits tightly to the side surface of the moving bullet, which creates resistance to its movement. When a bullet moves in a cylinder, the kinetic energy of the bullet is transformed into the energy of deformation of the cylinder and the work is done to overcome the friction force. At the same time, part of the energy of the bullet is extinguished by the intermediate layer and redistributed to the strength frame of the inner one.

The experiments' results and discussions

Consider the process of interaction of a bullet with a hollow cylinder (tube) (Fig. 2). An analytical solution of this problem is given in [2].

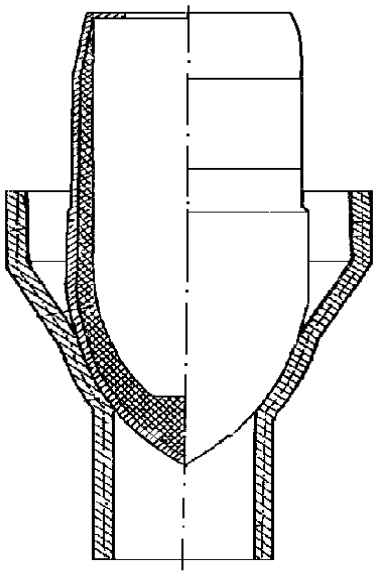


Fig. 2. The interaction between the bullet and a hollow cylinder

In the process of research there has been used the method of mathematical modeling based on the "Iskra" program which is based on the finite element calculations, which is an adaptation of the CASA / GIFTS software package developed at the University of Arizona.

The algorithm of estimating the value of absorbing, in the process of interaction between a bullet and energy barrier is based on the following assumptions:

1. At a sufficiently high impact velocity, elastic-plastic deformations appear in the colliding elements. If the contact time t_k that is small in comparison with the period of the highest-order pitch of the natural oscillations of an obstacle, when determining the magnitude of the contact force, it is necessary to take into account only local deformations of the obstacle. The magnitude of the contact force is determined by the formula [14]:

$$P_k = k[\frac{4n+1}{4n} \cdot \frac{mV_0}{k}]^{\frac{2n+1}{4n+1}}, \quad (1)$$

where $$k = \frac{2n}{2n+1} \cdot \frac{E_1 E_2}{E_1(1-\mu_2^2) + E_2(1-\mu_1^2)} \sqrt{\frac{1 \cdot 3 \cdot 5 \ldots (2n-1)}{2 \cdot 4 \cdot 6 \ldots 2n}}, \quad (2)$$

$$m = \frac{m_1 \cdot m_2}{m_1 + m_2}, \quad (3)$$

where E_1, E_2 are the elastic modules of materials of the colliding bodies;
μ_1, μ_2 are the Poisson's ratios of materials of the colliding elements;
n is the coefficient taking into account the density of contact between elements;
V_0 is a bullet speed;
m_1 is the mass of the bullet; m_2 – is the mass of the barrier;
m is the reduced mass.

2. Elastic characteristics of materials (E, μ) do not depend on the penetration rate. At the same time, the yield strength σ_2 significantly depends on the penetration rate.

3. The actual tension-compression diagram of the material of the barrier is replaced by the equivalent in energy of destruction. The equivalent diagram corresponds to the work of the sample before fracture in the zone of elastic deformations with some fictitious modulus of elasticity E_f and yield strength σ_s:

$$E_f = \frac{\sigma_s + 0,5(\sigma_f - \sigma_{s)}}{0,5\delta}, \qquad \sigma_f = E_f \cdot \delta, \quad (4)$$

in σ_f – the strength of the material; δ – elongation at failure.

4. When the barrier element is deformed, the stress cannot exceed the fictitious yield stress. The relative deformations at failure are equal to the residual deformation of the sample in the real tension-compression diagram.

5. The effect of the elastic base of the obstacle during the collision is neglected. In this case, the resultant displacement of the barrier can be determined by assuming that at the moment of collision, only the speed of the barrier changes.

The considered barrier has openings located along the cellular circuit (Fig. 3).

The total number of holes in the plate with a size of 0.25x0.33 m is 1927 pieces.

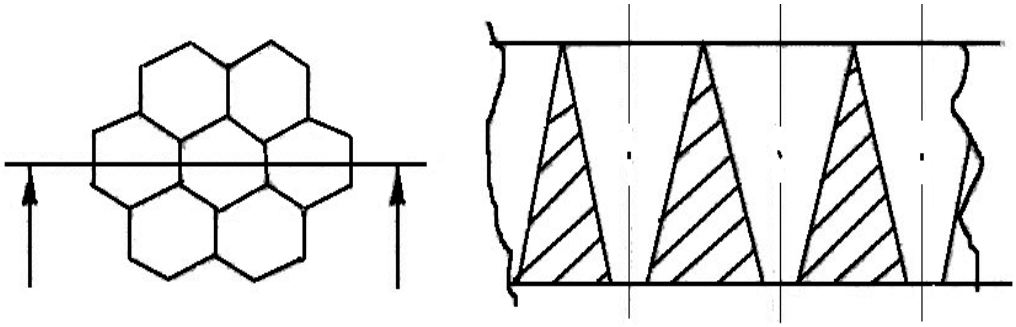


Fig. 3. The barrier scheme.

The material of the barrier is steel: $\sigma_s = 10^9$ Pa, δ = 18%, E = 2.1 • 10^{11} N/m^2

Characteristics of the material operating in the elastic region and equivalent in energy of destruction to the real material: E_f = 0,15 MPa, σ_f = 2750 MPa.

Since the evaluation of the protective properties of the barrier takes into account only local deformations, the design scheme contains one cell (7 cells). Each cell represents a cylinder with an outer diameter of 0.0076m with a tapered bore in the center. The rigidity of the six cells surrounding

the central one is modeled by elastic elements placed along a circle in eight points and in height on five tiers.

The assessment of the destruction energy of the obstacle's cell, in which the damaging element (pool) fell, was carried out according to the following algorithm.

1) Calculated the radial rigidity of the cell on an elastic base under the action of an annular mandrel load on the inner surface. The movement along the cone guide was set at a given level and the running effort needed for this was recorded. The nature of the cell deformation is shown in Fig. 4.

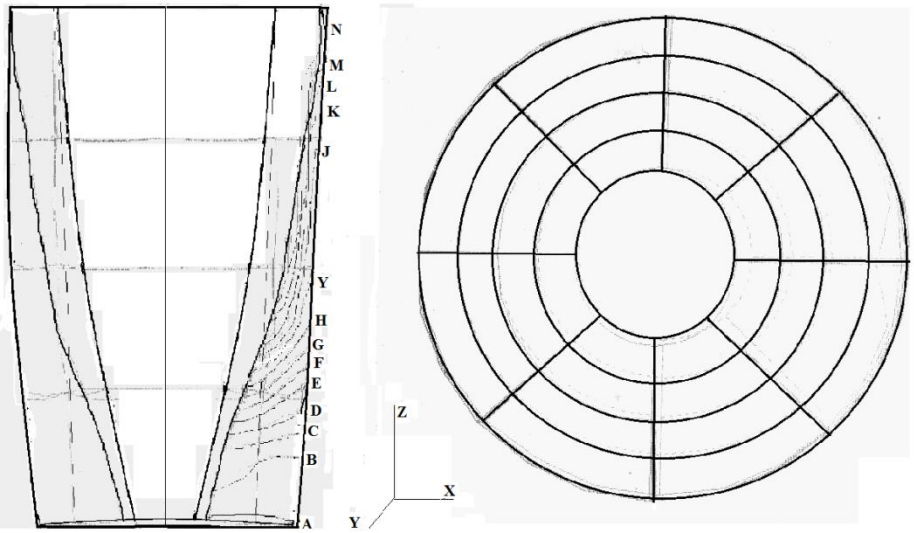


Fig. 4. The nature of cell deformation

2) Calculated work on the deformation of the cell to a relative elongation of the guide cone at each level of 18%.

3) The work on the deformation of the subsequent layers along the cell radius was calculated under the assumption of constancy of stresses equal to σ_f. The value of the force at each level with increasing radial deformation changes. To simplify the calculations for each level, the magnitude of this force is assumed to be constant and equal to the average value between the forces on the internal and external radii of the section. The magnitude of the final deformation of the cell is assumed under the assumption that all the impact energy goes only to the destruction of the cell, and the striking element does not change its geometry.

The kinetic energy of a 7.62 mm caliber bullet is:

$$A = \frac{m_1 \cdot V_0^2}{2} = \frac{0{,}01 \cdot 900^2}{2} = 4050\,J$$

where m_1 - is the mass of the bullet; V_0 - is the initial speed of the bullet.

The total work on the deformation in the radial direction of the cell when exposed to a damaging element of 7.62 mm caliber is A_1=3058 J.

The work on overcoming the friction forces A_2 = 992 J while the movement of the striking element in the cell channel is estimated approximately. The friction force is assumed to be constant and equal to the average value for the channel (node level 41, Fig. 5):

$$A_2 = f \cdot P_p \cdot h,$$

where f is the friction coefficient, f=0.3;

$P_p = 523 \cdot 10^3\,N$ is the magnitude of the force that deforms the cell in the radial direction;

h is the depth of bullet penetration into the cylinder.

Whence $h = \frac{A}{f \cdot P_p} = 0{,}026\,\text{m}.$

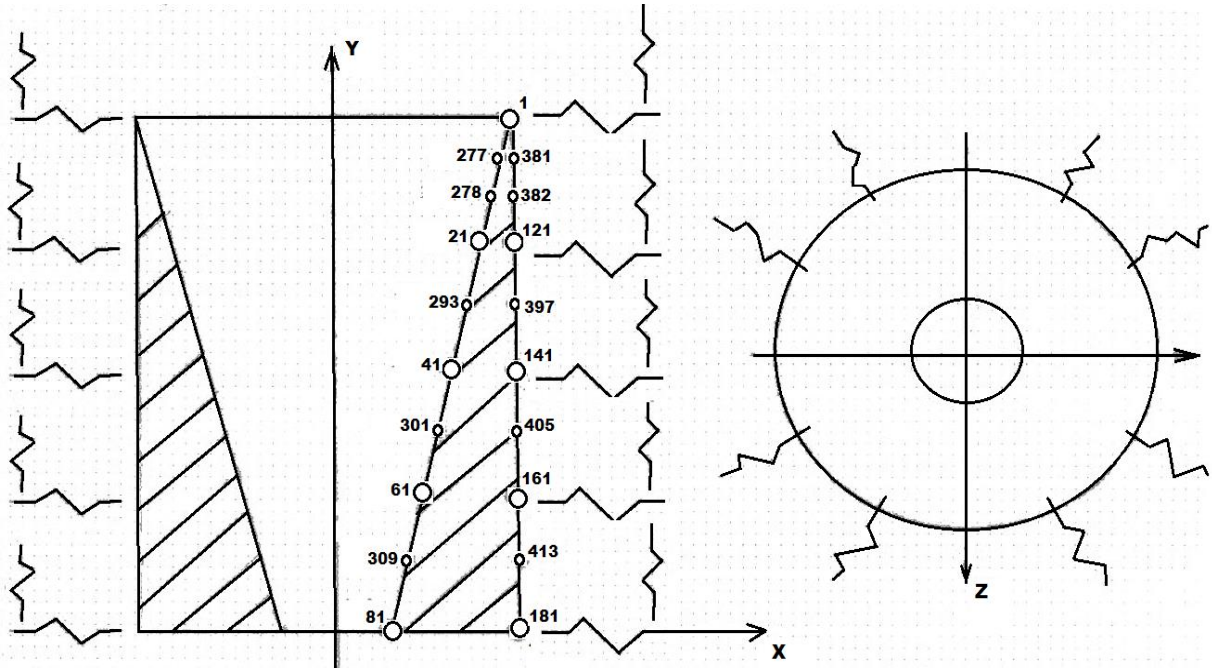


Fig. 5. The diagram of cell node

The kinetic energy of a 5.45 mm caliber bullet is:

$$A = \frac{m_1 \cdot V_0^2}{2} = \frac{0{,}006 \cdot 900^2}{2} = 2430\,\text{J}.$$

Work on the deformation in the radial direction of the cell when exposed to a striking element of the caliber of 5.45 mm is 1300 J.

The depth of penetration of the bullet into the cylinder:

$$h = \frac{A}{f \cdot P_p} = \frac{2430}{0{,}3 \cdot 523 \cdot 10^3} = 0{,}015\,\text{m}.$$

Based on the results of the calculation of the protective properties of the barrier from steel 3, we can assume:

1) when exposed to a striking element of 7.62 mm caliber, which has a kinetic energy of 4050 J, all the energy of the striker will be absorbed as a result of the deformation of the pre-gradient element (cell);

2) when exposed to a striking element of 5.45 mm caliber, which has a kinetic energy of about 2430 J, as a result of the deformation of the cell, all the energy of the striker will be absorbed.

To confirm the results of numerical simulation, experimental studies were conducted on the penetration of a protective barrier in the form of a set of hollow cylinders.

The purpose of the experimental studies is the experimental determination of the nature of the interaction of high-speed bullets with a protective barrier.

A structural element consisting of a base and associated cylindrical elements with a conical upper part was used as a protective barrier. The internal radius of the cylinders is 0.0025 m, the thickness is 0.001 m, and the length is 0.02 m. The material is steel 3. The elements were fired at by bullets with a steel core from an AK-74 (5.45 mm bullets) machine from a distance of 5 m.

The depth of penetration of the bullet into the cylinder was determined by direct measurement after each shot.

h is the depth of bullet penetration into the cylinder, N is the number of bullets showing the same depth of penetration. The results of the experiment are presented in Table 1 and Fig. 6.

Table 1

The results of the experiment

h, mm	8.3	8.1	7.6	7.4	6.8	6.5	5.4	4.8
N	2	3	3	4	5	5	3	3

Fig. 6. The results of experimental studies

The final measurement result of the depth of penetration of the bullet into the cylinder is: 6.8 ± 0.4 mm, P = 0,95.

Conclusion

In the paper, the process of interaction of a high-speed drummer (bullet) with a protective barrier in the form of a set of hollow cylinders has been investigated. The numeral model for determining the depth of penetration of a high-speed drummer into a hollow cylinder has been offered. The results of field experiments confirm the fundamental possibility to stop bullets with a barrier from a set of hollow cylinders.

Further investigations are related to the destruction of the structural integrity of a bullet with a steel core and a lead cover, the possibility of which must be taken into account while designing protective armored structures.

References

1. Korchak, V.Y. Reservation of military vehicles // – Moscow: Journal Military thought, – 2010. 10, p. 41-46 (in Russian).

2. Grekov, V.F., – Bulletproof protective clothing. Pat. 20386, Ukraine / A.V. Kovtun, S.I. Nesterenko, V.A. Nedelko. – 1998 (in Ukraine).

3. Popov, N.N. Calculation of structures for dynamic and special loads / N.N.Popov, B.S.Rastorguev, A.V. Zabegae; – Moscow: High School 320, – 1992 (in Russian).

4. Kalashnikov, V.V. Aleksentseva, S.E. Investigation of the influence of the construction of a bullet on the process of penetration of steel barriers Kalashnikov // Journal Mechanical Engineering Series Technical sciences, – 2009. 2 (24), – p. 60-68 Herald Samara State Technical University (in Russian).

5. Afanasyev, S.A. Study of shock-wave phenomena in composite materials / S.A.Afanaseva, N.N.Belov, Yu.A.Biryukov [et. al.] // IFJ. – 2011. T.84, №1, – p.47-56. (in Russian).

6. Kharchenko, V.V. Models of processes of high-speed deformation of materials taking into account viscoplastic effects / V.V.Kharchenko. – Kiev: Institute of Strength Problems named after G. Pisarenko, – 1999. (in Ukraine).

7. Beer, J. Vector mechanics for engineers. Statics & Dynamics. Seventh Edition / J. Beer. – 2004. – 1326 p.

8. Broos, H. Explicit FE modeling of ballistic impact on textile armour systems / H.Broos, K.Herlaar // Finite Element Modelling of Textiles and Textile Composites. St. Petersburg, – 2007 (CD edition). LS-DYNA Keyword user's manual. 970. LSTC, 2003.

9. Ivanov, D.S. Failure analysis of triaxial braided composite / D.S.Ivanov, F.Baudry, B. van den Broucke [et. al.] // Composites Science and Technology, – 2009. Vol.69, №9, – p. 1372-1380.

10. Roberts, J.C. Modeling nonpene-trating ballistic impact on a human torso / J.C.Roberts, P.J.Biermann, J.V.O'Connor [et. al.] // Johns Hopkins Applied Physics Laboratory Technical Digest, – 2005.

11. Rupert, H., Pengelley, J. Medium-caliber ammunition innovations for AFV applications // Armee Rundschau, – 2004. №1, – p. 52-56.

12. Segletis, S.B. A model for rod ricochet // Int. J. Impact Eng., – 2006. V.32, №9, – p. 1403-1439.

13. Velichko, L.D. Petruchenko, O.S., Kondrat, V.F. Dynamics of protective design when a bullet or shell fragment is struck // Military-technical collection / Academy of Land Forces, – Lviv: AIS, – 2015. No. 13, – p. 13-19 (in Ukraine).

14. Petruchenko, O.S., Flud, O.V., Velychko, L.D. Dynamic and kinematic characteristics of the ball penetration into the armor // Military Technical Collection / National Academy of Land Forces, – Lviv: NASV, – 2017. No.16, – p. 8-11 (in Ukraine).

Xülasə

Güllənin içiboş silindrlərdən ibarət materialla qeyri-elastik toqquşmasının tədqiqi

Anatoli Kovtun, Vladimir Tabunenko, Oleq Boqatov, Azad Bayramov

Məqalədə, zirehin təkmilləşdirilməsi sahəsində perspektiv istiqamətlər araşdırılır. Bir-birinə daxil olan və birləşən içiboş silindrlərdən ibarət konstruktiv materiallar zirehli materiallara alternativ ola bilər. Xüsusi strukturlu və sintetik liflərdən düzəldilmiş və yüksək enerjiyə malik gülləyə davamlı parça şəxsi mühafizə vasitəsi kimi hesab olunur. Bu parça bir neçə laydan ibarət paket şəklində qəlpələri və aşağı sürətli güllələrin qarşısını almağa qadirdir. Yüksək sürətli zərbə vuran elementləri tutmaq üçün sərt lövhələr, zərbələri yumşaltmaq üçün isə amortizasiya qatı istifadə olunur. Güllənin içiboş silindrlərlə doldurulmuş zirehə daxil olma dərinliyini müəyyən etmək üçün hesablayıcı model təklif edilir. Hesablamaların və eksperimentlərin nəticələri göstərilir.

Açar sözlər: zireh, yüksək sürətli güllə, maneə, plastik deformasiya, içiboş silindr, dinamik daxil olma, eksperiment.

Аннотация

Исследование процесса неупругого столкновения пули с материалом из пустотелых цилиндров

Анатоли Ковтун, Владимир Табуненко, Олег Богатов, Азад Байрамов

В статье рассматриваются перспективные направления улучшения бронезащиты. Альтернативой броневым материалам могут стать конструктивные материалы, которые состоят из вложенных элементов, связанных между собой пустотелыми цилиндрами. Одним из материалов индивидуальных средств защиты рассматривается устойчивая к высокоэнергетическому удару ткань, изготовленная из синтетических волокон специального состава и структуры, которая применяется в виде пакета из нескольких слоёв, способных задержать осколки и низкоскоростные пули. Для удержания высокоскоростных поражающих элементов используются жёсткие пластины, а для смягчения ударов, применяется амортизирующий слой. Предложена численная модель определения глубины проникания пули в преграду в виде набора пустотелых цилиндров. Приведены результаты расчетов и экспериментальных исследований.

Ключевые слова: броне защита, высокоскоростная пуля, преграда, пластическая деформация, пустотелый цилиндр, динамическое проникновения, эксперимент.

Məqalə redaksiyaya daxil olmuşdur: 12.09.2019
Təkrar işlənməyə göndərilmişdir: 16.10.2019
Çapa qəbul edilmişdir: 11.11.2019

UDC 93/94;623; 355/359

FORTIFICATIONS IN ALBANIA

ScD, professor Nurulla Aliev
Armed Forces War College of the Azerbaijan Republic
E-mail: nurullaliyev@mail.ru

Abstract. This article, based on a wide range of sources, shows the construction and evolution of castles and military fortifications during the Albanian period, including their geopolitical significance for the region. The article explores the development of artificial fortifications built on the territory of Albania during the war, the defense system developed by the military and local defense systems. It also analyzes the use of various tactical tricks during combat in the army.

This work was supported by the Science Development Foundation under the President of the Republic of Azerbaijan **– Grant № EİF/MQM/Elm-Tehsil-1-2016-1(26)-71/01/5.**

Keywords: military affair and military art, arms and protective equipment, war tactics, fortress and fortifications, combat arm and defense tools.

The constant threat from the north that existed for several centuries, forced a number of powerful fortifications – Beshbarmag, Gilgilchay and Darband – on the western coast of the Caspian Sea, in Caucasian Albania. These structures were erected before our era by the Caspian, and then by the Albanian state [1, p.181-191]. However, a powerful system of fortifications was erected in the 5th – 6th centuries by the efforts of the Sassanids' kings Ezdigerd II (438–457), Peroz (459–484), Kavad (488–531) and Khosrov I (531–579).

Fig. 1. Stone tombstones of Turkic warriors' graves of the 3rd – 6th centuries in Azerbaijan: on the left – from Agdam, on the right – from Khynysly (Shamakhy)

Beshbarmag fortifications, the southernmost ones in the defensive system, consisted of two parallel clay shafts stretching from the foot of Mount Beshbarmag to the sea (1.75 km long) at a distance of 220 m from each other. There was a strongly fortified stone fortress with towers located on the slope of the mountain [2, p.111].

The second line in the northern fortifications was located 23 km north of the Beshbarmag wall. It was the Gilgilchay (Shabran) defensive wall, with a total length of about 50 km. The wall was built on the southern bank of the Gilgilchay River, which served as an additional natural defensive obstacle. The wall began directly at the Caspian Sea and crossed the entire low-lying part of the Greater

Caucasus southeastern slope. Remains of the wall and about three hundred towers of this grandiose structure were preserved in the northwestern part of the site near the settlements of Alikhanly, Eynibulag, on the section from the sea to the Baku-Davachi main road [3, p.441-465].

The Gilgilchay wall was completed at the top of the mountain, in the Meshriiv area, by the fortress of Chirag-gala. Chirag-gala, located at an altitude of 1,600 m above sea level, was built on a cliff. Surrounded by steep and high cliffs almost on all sides, Chirag-gala was almost unassailable for the enemy. The north-eastern side of the fortress had no walls, because at this place it was protected by a cliff. The thickness of the walls of the citadel reached 5 m. There were 17 towers in the fortress, and the tower at the top of the cliff had a height of over 13 m. [4, p.8-10].

Fig. 2. Narrow passage between the mountain Beshbarmag and the sea.
Modern photo from the mountain Beshbarmag

The main purpose of the fortress was the reception and transmission of light signals from other fortresses, hence its name ("fortress – lamp"). Darband and Beshbarmag fortifications are clearly visible in clear weather from the top of the tower, too. Having received a light signal from the Darband fortress, the permanent 10–15 personnel guard garrison of Chirag-gala transmitted it by means of a signal fire on the upper platform of the tower to the Beshbarmag fortifications; from there, an alarm signal was transmitted to the fortress of Shamakhy, Baku, etc. up to the mountain fortresses of Nakhchivan and South Azerbaijan [5, p.108]. Such a warning system made it possible to gain time necessary for sudden attacks by numerous enemies, when troops were put on combat alert, concentrated in the designated area, and provided a timely response to the aggressor.

The Darband defensive line was the northernmost and strategically important military defense system on the western coast of the Caspian.

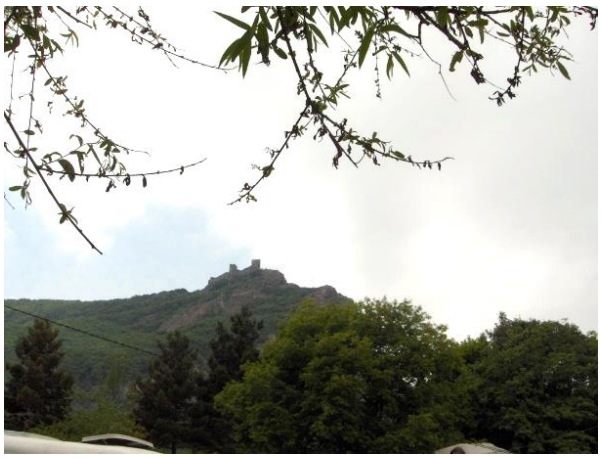


Fig. 3. Chirag-gala. View from the plain

Darband (Persian Darband – i.e., "knot, connection, lock of the gate"), due to its unique geographical position, played an exceptional role in the military-political events unfolding in Azerbaijan for many centuries.

Rome and Parthia, Sassanian Persia and Byzantium, the Arab Caliphate and the Khazar Khaganate, Seljug state and the Golden Horde, the Safavid state and the Ottoman Empire and, finally, the Russian Empire since Peter the Great claimed the Darband passage, where the first fortified settlements appeared in the 8th – 7th centuries BC.

Fig. 4. Chirag-gala. View from the nearest mountain

The emergence and the significant role that Darband played not only in the history of Azerbaijan but also in world history, is primarily due to the special position that it occupied on the western coast of the Caspian Sea, which was an excellent springboard for an offensive from the south to the North Caucasus, and North to South and further to the countries of the Near East [6, p.3-8].

Fig. 5. Darband. Engraving, the 16th century

Darband passage – a narrow coastal plain between the sea and the mountains, 3.5 km wide was the only convenient rad from Southeast Europe to the Near East. Ancient Greeks and Romans called this area the Caspian or Albanian gates; Albanian early medieval authors – Chor's Gate (Jora, by the name of the region), the gate of the Huns, sometimes the Sea Gate or Darubandi; Byzantine authors – fortifications of Tzor (Tzur); Persians from the 6th century – Darband; the Syrians – the gate of Thoraya; Arabs – Bab al-abwab (gate of the gate), Bab al-hadid (Iron gates); the Mongols – Kahulga (gate), the Turks – Demir-Gapy; Russian – Darband or the Iron Gate. In medieval eastern literature, there is widespread opinion about the founding of Darband and the erection of powerful fortifications by Alexander the Great (Zul'-Karnayr), although this is not supported by reliable sources [7, p.14, 18-22, 25].

Emergence at the end of the 4th century a new formidable force in the face of associations of nomadic tribes – the Huns, which pose a real threat to the countries of the South Caucasus and the Far East, significantly increased the military-strategic importance of the Darband Passage. Considering this factor, the Sassanids did their best to retain firm control over this area.

The Darband defensive complex consisted of three parts: the northern and southern walls of the city – each of them with more than 3.5 km; the fortified citadel of Naryn-gala, located on a high hill; the mountain wall, stretching to the inaccessible peaks of the Greater Caucasus more than 40 km. The distance between the walls that went far into the sea reached about 350 m near the citadel and 450 m at the sea. The thickness of the walls, reaching a height of 18 m, was up to 4 m. A number of powerful towers were built along the wall line, the total number of which in the northern and southern city walls reached 73, of which the majority – 46 were located on the north wall.

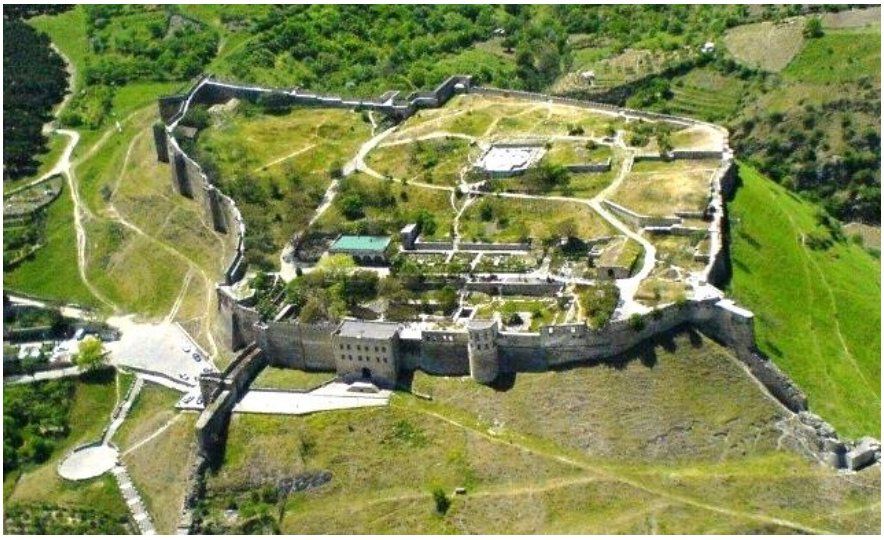


Fig. 6. Darband Citadel. Up-to-date photo

The walls of the Darband fortifications that went into the sea did not allow the enemy to go around them in shallow water. A port was built between the sea walls; the ships could not enter and leave the port without permission, since a chain was stretched at the entrance to the port [8, p.24-25].

The citadel, 25 m high, had the shape of an irregular polyhedron, reaching more than 700 m in the perimeter. The north and east walls of the citadel occupied the edge of the hill, the slopes of which were very steep; it made it almost impregnable from this direction. The south-east tower covered access to the citadel from the south.

From the south-west corner of the citadel, there was Dagbari (Mountain Wall), which stretched along the edge of the gorge, and extended to the mountains for tens of kilometers. The wall was fortified by a system of forts located strategically in the most important directions. Forts had a rectangular or square layout with round towers at the corners. In addition to the forts, there were halffort-ledges facing the east in the wall fortification system, i.e. toward the expected attack of the enemy [7, p.76, 100-102].

The mountain wall with a system of forts and semi-fortifications was, along with the fortifications of Darband, a single defensive system; this system not only reliably blocked the Caspian lane, but also closed the bypass roads, while controlling the internal communications of the region.

Darband, as the largest port and the only fortified city on the Caspian Sea at that time, was the main military-political stronghold of Albanian rulers and Sassanids in the Caucasus. A large Persian garrison (only cavalry to 10,000 horsemen) was always here, and none of the Persian rulers in the South Caucasus had such a significant garrison.

The mountain roads in the north-west of Albania were protected by the Zagatala stone wall, built by the Sassanids, and perhaps even earlier [9, p.90]. The thickness of the defensive walls in the Zagatala reached almost 1.5 m, the height – 5 m, the diameter of the towers – over 12 m. [5, p.109].

Fig. 7. View of the city from Darband Citadel

The geopolitical significance of the northern fortifications for the region was also realized by Arab authors of a later epoch. Thus, the Arab historian of the 10th century Masudi noted that their construction and placement of garrisons here, allowed the Sassanids' kings to resist the invasion of the North Caucasian nomadic tribes – Khazars, Alans, Savirs, Turks, etc. [10, p.212-213].

Thus, the Caspian fortifications were a whole system of deeply echeloned defense, clearly thought out from a military point of view and maximally adapted to the terrain. The system of northern defensive structures, also in the north-west of Albania, also included the fortresses Gabala, Gunduz, Gel-Dec, Baku, Khachmaz, Bum, and other [11, p.10-16]. Thus, for example, the fortress of Javansheer-gala was characterized by its reliability; it was built in a wooded area near the village of Talystan [5, p.111].

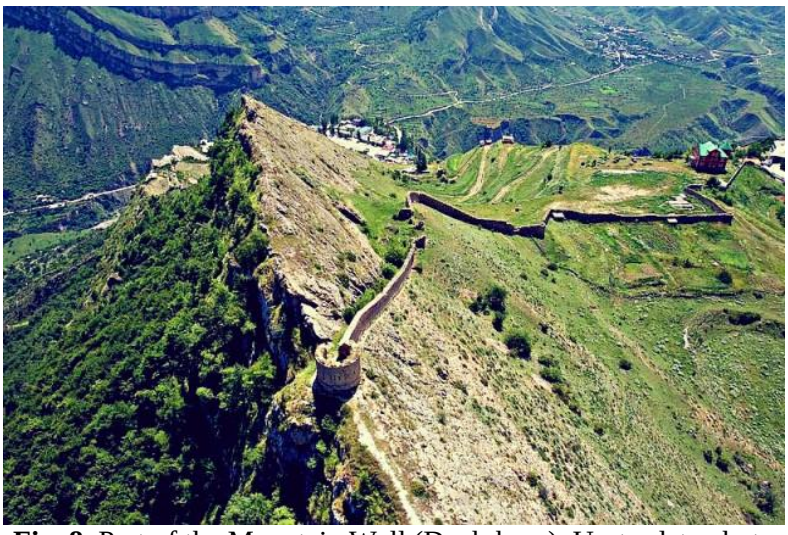


Fig. 8. Part of the Mountain Wall (Dagh-bary). Up-to-date photo

Another way from the North Caucasus to the South passed through the Darial Pass (Dar-Alan). This way served as means of the Sassanids' political pressure on Byzantium, which paid gold the Persian shahs to protect this passage from the invasion of the Huns in the Byzantine possessions in the South Caucasus and the Euphrates. During the reign of Bahram Gur (422–438), in 422, the Sassanids and Byzantium concluded an agreement according; whereby, the Byzantines undertook to pay Sassanids annually a certain amount to keep the guard in the Daryal Gorge. Although the northern people managed to establish their control over this passage for a while, however, as a result of a prolonged war with the Savirs, Shah Kavad about 508 succeeded in gaining a foothold in the Daryal Passage, where from that time a permanent garrison was stationed [12, p.58].

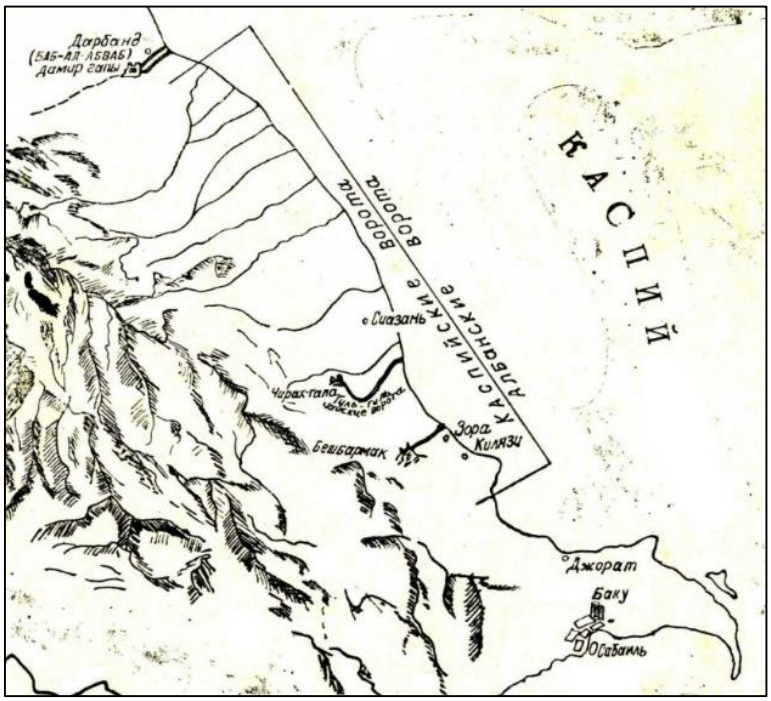


Fig. 9. The Northern fortifications (D. Akhundov)

The southern Azerbaijani fortress cities – Ardabil, Tabriz, Maragha, Janagar, Iskandarsar and others, where Persian garrisons were located, were also surrounded by sufficiently powerful walls [5, p.110].

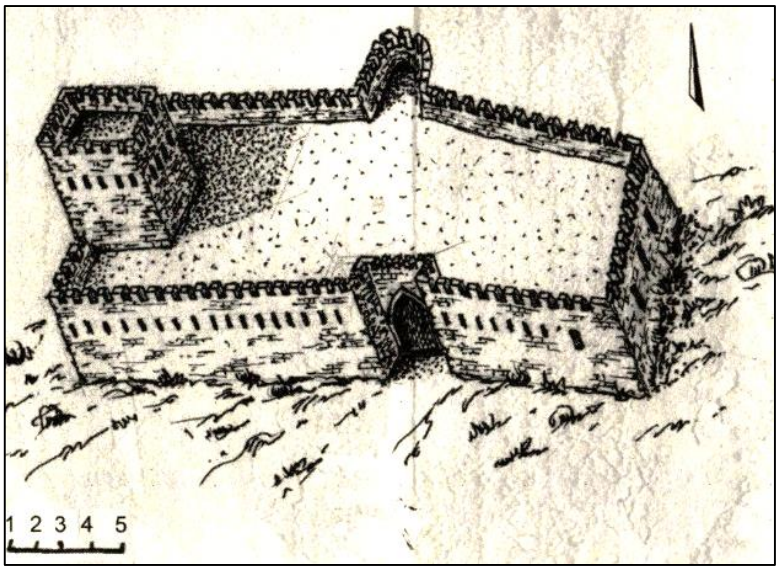


Fig. 10. The castle of Gyrlar-tepe.
One of the first feudal castles in Albania (according to Osmanov)

The constant threat from the north that existed for several centuries, forced a number of powerful fortifications. A powerful system of fortifications was erected in the 5th – 6th centuries by the efforts of the Sassanids' kings.

In the first centuries of our era, the leading type of fortifications in Albania is the square-shaped castle and the city fortification. Moreover, during this period the terrain relief no longer played a decisive role, i.e. the defense system itself is being improved, built on artificial supports, which were relatively small (Sarygala, Barda). At the same time, in the larger fortresses, the natural terrain continues to play an important role in the organization of defense (Beylagan, Shamkir, Shatal, and Ganja, in the 5th century) [2, p.109-110].

References

1. Ахундов, Д.А. Архитектура древнего и раннесредневекового Азербайджана / Д.А.Ахундов. – Баку, – 1986. – 311 с.
2. Мамедов, С.Г. История войн и военного искусства Азербайджана / С.Г.Мамедов. – Баку: Изд-во “Nafta-Press”, – 1997. – 271с.
3. Алиев, А. Новые исследования Гильгильчайской оборонительной стены / А.Алиев, И.Алиев, М.Гаджиев [и др.] // Магнитогорск: Проблемы истории, филологии, культуры, – 2004. – с. 441-465.
4. Алиев, А.А. Гильгильчайское оборонительное сооружение / А.А.Алиев. – Баку, – 1986. – 346 с.
5. Azərbaycanın hərb işi tarixi. 1-ci cild, – Bakı: Hərbi Nəşriyyat, – 2006. – 520 s.
6. Əliyev, N.A. Dərbəndin hərbi-strateji əhəmiyyəti və onun tanınmış hərbçiləri / N.A.Əliyev. – Bakı, – 2016. – 240 s.
7. Кудрявцев, А.А. Древний Дербент / А.А.Кудрявцев. – М., – 1982. – 176 с.
8. Алиев, Н.А. Военно-Морская история Азербайджана / Н.А.Алиев. – Баку, – 2002. – 343 с.
9. Пахомов, Е.А. Закатальская «длинная» стена // Труды АГУ им. С.М.Кирова. Серия историческая, – 1950. – Вып.1 – с. 90.
10. Минорский, В.Ф. История Ширвана и Дербента X–XI вв / В.Ф.Минорский. – М., – 1963. – 270 с.
11. Гадиров, Ф.В. Северные оборонительные сооружения Азербайджана: / Автореф. дисс. канд. ист. Наук / – Баку, 1969. – 24 с.
12. Джафаров, Ю.Р. Гунны и Азербайджан / Ю.Р.Джафаров. – Баку: Азернешр, – 1993. – 107 с.

Xülasə
Albaniyanın istehkamları
Nurulla Əliyev

Təqdim olunan məqalədə geniş mənbələr əsasında Albaniya dövləti dövründə qala və hərbi istehkamların tikintisi və onun təkamülü, o cümlədən onların bölgə üçün geosiyasi əhəmiyyəti göstərilir. Müharibə aparılan dövrdə Albaniyanın ərazisində tikilmiş süni istehkamların, hərbi nöqteyi nəzərdən düşünülmüş və yerli relyefə uyğun müdafiə sisteminin inkişafı məsələləri araşdırılır. Həmçinin, orduda döyüş aparılması zamanı müxtəlif növ taktiki fəndlərinin istifadəsi prosesi təhlil olunur.

Bu iş Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun maliyyə yardımı ilə yerinə yetirilmişdir – **Qrant № EİF/MQM/Elm-Təhsil-1-2016-1(26)-71/01/5.**

Açar sözlər: hərb işi və hərb sənəti, silah və mühafizə təchizat, döyüş taktikası, qalalar və istehkam tikintiləri, döyüş silahı və müdafiə vasitələri.

Аннотация
Фортификационные сооружения в Албании
Нурулла Алиев

В представленной статье на основе исследования широкого круга источников показано строительство и эволюция оборонительных сооружений и крепостей в период Албанского государства, их геополитическое значение для региона.

В статье анализируются вопросы совершенствования системы обороны, четко продуманной с военной точки зрения и максимально приспособленные к рельефу местности, построенная на искусственных укреплениях в период ведения войн на территории Албании.

Так же, проводится исследования процесса использования в армии при ведении боя различных тактических приемов.

Данная работа выполнена при финансовой поддержке Фонда Развития Науки при Президенте Азербайджанской Республики – **Грант № EİF/MQM/Elm-Tehsil-1-2016-1(26)-71/01/5.**

Ключевые слова: военное дело и военное искусство, боевая тактика, вооружение и защитные снаряжения, крепости и фортификационные сооружения, боевое оружие и средства защиты.

Məqalə redaksiyaya daxil olmuşdur: 20.09.2019
Təkrar işlənməyə göndərilmişdir: 23.10.2019
Çapa qəbul edilmişdir: 15.11.2019

UDC 351/354

THE ROLE OF DEFENCE EDUCATION ENHANCEMENT PROGRAMME IN ENHANCING MILITARY INTEROPERABILITY WITH NATO

major Khayal Iskandarov[1],
PhD, assoc. prof. Piotr Gawliczek[2]
[1]War College of the Armed Forces of the Azerbaijan Republic
2University of Warmia and Mazury, Poland
E-mail: xayal1333@gmail.com,
pgawliczek@gmail.com

Abstract. The aim of this article is to review NATO's Defence Education Enhancement Programme and to highlight the challenges and implications of its implementation and to examine the extent to which this initiative contribute to the cooperation in the field of education. The importance of Defence Education Enhancement Programme has been underscored in increasing interoperability between the allies and partners. Taking the broad meaning of interoperability into account the authors attempted to bring to the fore the desperate need for increasing only intellectual interoperability with outside expertise.

Keywords: NATO, DEEP, education, cooperation, interoperability.

Having adopted a New Strategic Concept in 1991 NATO began to focus on the development of multinational force projection in order to adapt to the post-Cold War era and expand its capabilities for crisis management operations. In pursuit of future strategic goals, NATO had to broaden and deepen cooperation with the countries beyond its traditional borders. Thus, the Alliance was in urgent need of partners those would be able to keep abreast of NATO standards. This approach in turn required member, as well as partner forces to work together for out-of-area operations.

The first initiative to invite those nations to cooperation was PfP programme, which was launched in 1994. The ultimate goal of this programme was and still is to support partners in their efforts to reform their national defense structures and to assist them in developing their national capabilities. If partner nations who signed the framework of this programme wanted their militaries to operate together, they would follow procedures mainly determined in Brussels by the Allies. This initiative proved to be really successful tool.

Shortly afterwards the Alliance embarked upon Partnership Planning and Review Process with the aim of promoting the development of forces and capabilities by partners that are best able to cooperate alongside NATO Allies in crisis response operations and other activities to maintain security and stability. It provides a structured approach for enhancing interoperability and capabilities of partner forces that could be made available to the Alliance for multinational training, exercises and operations. This strategy continued over the ensuing years and the Alliance initiated new programmes and mechanisms (Operation Capabilities Concept, Membership Action Plan, Individual Partnership Action Plan, etc.) for closer and deeper cooperation with its partners. The objective of NATO's partnerships is to safeguard security together, as stated in all three post-Cold War Strategic Concepts [1].

Comparative analysis, synthesis, inductive and, deductive methods have been used in the paper to come up with conclusive outcomes and recommendations for the countries in the region.

Since 1994, NATO has created partnerships as an institutional framework for its relations with countries that cannot or do not want to become Alliance members. In the past 25 years, the circle of countries involved has become ever larger, the associated agenda ever more heterogeneous, and the goals pursued by NATO ever more diverse [2]. The cooperation among the allied and partner states and their military educational facilities is an important factor in attaining interoperability, necessary

for dealing with current security challenges. NATO gives the best direction on professional development and education. The Alliance has published a professional military education curriculum for both officers and non-commissioned officers, which are designed as a start point for NATO member nations to develop their own national curriculums, and purport to foster intellectual interoperability and greater professionalism in allied armed forces [3]. Remarkably, the education has been accelerated to levels no one would have ever predicted, as evidenced by the institutional changes that have occurred in Central and Eastern Europe over the last twenty-five years [4]. Thus, NATO's partnership tools provide golden opportunity for the enhancement of the cooperation between NATO and partner countries.

The military forces of partner states regularly take part in NATO exercises and peacekeeping operations. Their contributions to NATO missions have shown that they have the will and capability to provide the security along with member states. Thus, it is important to elaborate on the programmes and mechanisms, which provide a blueprint for interoperability with NATO and structural reorganization according to NATO standards. Interoperability does not mean that allied or partner states should have or purchase common military equipment. It is as much or more about human teamwork. We will focus on DEEP, which is the main tool to upgrade the military education systems with the purpose of enabling the partner nations to be intellectually interoperable with the Alliance.

Intellectual interoperability first and foremost establishes a baseline of trust and security at the individual, institutional and at the national level [5]. According to Maj. Gen. Robert H. Scales, an Ex Commandant of the U.S. Army War College: "This would be a fine system if tactical genius and strategic genius were related. But experience has shown that great tactical skill does not equal great strategic skill. In fact, tactical and strategic genius are unrelated. Officers with potential for strategic leadership are morally as well as physically brave. They may not be able to make the convoys run on time, but they have a special talent for seeing the future and conjuring a battlefield that has yet to appear. These are young men and women who are intellectually gifted. They can think critically. They are more interested in studying warfare than practicing it" [6].

As Maj Gen PK Mallick, the former Chief Signal Officers of a Command and a Senior Directing Staff at the National Defense College of India stated: "Tactically talented officers can move hundreds. Strategically talented officers can maneuver hundreds of thousands, if not millions. Tactically talented officers know how to fight enemies they know. Strategically talented officers are prepared to fight enemies yet unforeseen. The tactically talented read the manuals and put existing doctrine into practice. Strategically talented officers continually question doctrine and eventually seek to change it. Tacticians see what is; strategists conjure what might be. Not every officer promoted to flag rank needs to be a professional strategist" [6]. However, intellectual and institutional changes require time and patience to implement. There is a perfect precedent in the history that justifies this point. In October 1806, Prussian Army marched against the invading forces of Napoleon Bonaparte. At the Battle of Jena-Auerstedt, Napoleon's army devastated the highly regimented and drilled Prussians. This defeat shattered the illusions that Prussians held of their military excellence. The humiliated officers who survived the battle realized that warfare had changed and their system was no longer relevant. This battle displayed the inability of the Prussian Army. This defeat provided the catalyst for change that would lead to their predominance seventy years later. Major General Gerhard von Scharnhorst is touted as the father of Prussian Army reforms. Scharnhorst did not believe an army could simply wait for a genius general like Napoleon to manifest at times of need; rather that successful military competency could be cultivated through education. His reforms aimed at creating a system that identified and cultivated talent through education [7].

Battle of Jena-Auerstedt demonstrated that executing orders was not enough; officers had to use sound judgment and critical thinking in the preparation, planning, and execution of military operations. Scharnhorst firmly believed in the benefits of higher level education and experimented with specialized learning venues when he established the Military Society in Berlin in 1801. This society fostered a free-thinking exchange of ideas and sought to develop judgment and reasoning.

General Scharnhorst incorporated the concept of advanced education into his reforms by creating a tiered army education system to meet the developmental needs of officers as they progressed from the tactical applications of war to the strategic. The Kriegsakademie War College at that time was focused on developing strategic and critical thinking [7].

Until the mid-2000s, NATO support to partner states had primarily focused on the guidelines of the 1999 Training and Education Enhancement Program (TEEP), which was intended to promote interoperability "in the field". NATO defense reform efforts gained additional momentum with the creation of the Partnership Action Plan on Defense Institution Building (PAP-DIB) at the 2004 Istanbul Summit. The PAP-DIB Action Plan outlines the specific goals that NATO and partner states want to achieve in the area of defense institution building [8].

Dr. David Emelifeonwu of the CDA led a multinational team of educators from allied and partner states to draft a Reference Curriculum for Defense Institution Building, the first multinational collaborative effort of its kind on behalf of partner defense education. The term "Reference Curriculum" carries special meaning in this context. It is offered to partners not as an exact prescription to be adopted wholesale but rather as a set of generic suggestions to consider in drafting their own course content, drawing on the methods in curriculum development they see in the document. Another Reference Curriculum followed two years later, an ambitious effort centered on generic Officer Professional Military Education. A third effort is on Non-Commissioned Officer Professional Military Education [9].

In 2006, the Education and Training for Defense Reform Initiative was introduced, paving the way for the creation of a new area of cooperation with partners. Finally, in 2007 Defense Education Enhancement Programme (DEEP) was launched [10]. Kazakhstan was selected as the place to test all these ideas. With strong support from both the United States Central Command and the Office of the Secretary of Defense, the Consortium launched its first pilot DEEP with Kazakhstan's NDU in late 2007. Most of the "rules of the road" for future DEEPs were developed in this pilot project. The first step was the selection of the program leader, Dr. Al Stolberg of the U.S. Army War College. Familiar with planning and implementing security cooperation programs in many nations in Europe and Eurasia as part of his assignments to the Joint Staff and United States European Command, Dr. Stolberg's position on the teaching faculty of the War College made him a natural choice to lead the DEEP [9]. This initial success in Kazakhstan provided the essential confidence for the Consortium to launch other DEEPs in 2008. NATO played a key role at this point. Working informally with the NATO Missions of Georgia, Azerbaijan, and Armenia, and using the mechanism of the Individual Partnership Action Plan (IPAP), NATO's International Staff urged these countries to add defense education to their IPAP goals. In quick succession, a senior MOD official from these countries asked a senior NATO official, usually at the Assistant Secretary-General level, to open a dialogue on potential education reforms. The Kazakh DEEP opened the door to launch these additional programs [9].

In the current strategic concept (2010), the three core tasks of NATO are collective defense, crisis management and cooperative security. Out of these, cooperative security is very much about partnerships. Thus, cooperative security is a broad task consisting of numerous elements. Generally speaking it consists of three components: strengthening partnerships, contributing to arms control, non-proliferation and disarmament and assisting potential new countries to prepare for NATO membership. An important sub element of both strengthening partnerships and preparing new countries for potential membership is interoperability. In short with the new NATO missions and engagement in operational theatres there has been a dramatic shift from a single nation fighting on its own to coalitions where multinational units, down to the level of platoons, are working together [1].

On the other hand, the mechanisms that support achieving interoperability are: effective implementation of allied agreed standards (STANAGs), doctrine and tactics, joint training, participation in NATO/multinational exercises, application of NATO policy related to lessons learned, conduct of demonstrations and tests. According to the NATO Strategic Concept 2010,

partnerships with third countries "can make a concrete contribution to enhancing international security, to defending the values on which the Alliance is based, to NATO's operations and to preparing interested nations for membership of NATO".

The implementation of the Alliance grand strategy requires the continuous improvement of military effectiveness. In this regard, interoperability is a sine qua non for the success of any operation/mission in coalition warfare [1].

According to an action plan approved by NATO Defense ministers interoperability has three dimensions:

– technical (hardware and systems);
– procedural (doctrine and procedures);
– human (language, terminology and training).

The human dimension is inextricably linked with intellectual interoperability. As NATO allies and PfP partners work together to build defense institutions and develop human capital programs need to be put in place to educate national security professionals in new ways and produce graduates with different skill sets [12].

One of the functional subject areas in which NATO provided support since the mid-2000s, via the International Staff, was that of defense education. Defense education support was designed to address interoperability "of minds" – a set of common references, doctrines and approaches to problem solving that would allow officers from different backgrounds to understand each other [8]. DEEP is an invaluable tool to develop educational institutions in the defense sector and contribute to all dimensions of interoperability. The main goal of the Program is to enhance the international security throughout professionalization of the officers and civilian employees' education system in the partner states according to the NATO standards [13].

Through faculty development, curriculum development and peer-to-peer consultations, the DEEP Programme fosters defense capacity building, cooperative capability development and standardization, and promotes interoperability of processes and methodologies to enhance democratic institutions [10]. According to Dr. Raphael Perl, PfP Consortium executive director, "what makes DEEPs attractive is implementing a non-cookie-cutter approach to defense education and defense institution building in post-Communist societies and beyond" [14].

The key aspect of DEEP is the connections it facilitates between senior educators from defense education institutions in NATO countries and affiliated institutions. Another key function of DEEP is in helping sustain regional stability through multinational education and research [4].

A successful and effective DEEP requires stakeholders, participating nations and volunteers to balance the short view with the long view. Rapid change is not always sustainable change. A possible indicator of success is to have host nation defense institutions meet their IPAP goals, incorporate reference curriculum methods and sources into their own programs of instructions and adopt learner-centric knowledge delivery methods. The aim is the attainment of the "operational" objectives of the program; intellectual interoperability, like-mindedness, in short, integration [5].

DEEP endeavors through dialogue and encouragement to influence partner educators in the direction of the following objectives [15]:

– guide and mentor reforms in professional and military education, both in individual defense education institutions and in a defense-wide holistic approach to professional military education;
– promote learner-centered education and innovative use of instructional technologies;
– encourage and enable the use of learning objectives which facilitate a depth of learning that can be readily applied through practice and partner experience;
– assist in the development of faculty assessments and action plans to employ these methods in support of partner goals contained in their IPAPs with NATO or bilateral arrangements with the U.S.

In coordination with the PfP Consortium of Defense Academies and Security Studies Institutes, the Partnership Training and Education Centers, the George C. Marshall Center and the Bureau for International Language Coordination as well as with specific allied and partner defense education institutions, NATO is leading or supporting eight tailored DEEPs [8].

Since 2007, NATO has conducted DEEPs with Armenia, Azerbaijan, and Georgia. The PfP Consortium of Defense Academies and Security Institutes (PfPC) has played a leading role in bringing together allies and partners to develop and execute DEEPs. These programs, which are tailored to meet individual partner requirements, provide opportunities for the PfP partners to develop both their defense education curricula and faculty. Good curricula would also contribute to understanding the holistic nature of professional military education, the hierarchy of schools that lead from Cadet to Colonel [9]. Not only do these programs provide an effective way to transform national security establishments and enhance the security capabilities of partners, they also do so in a way that does not provoke neighboring nations. In the case of the countries fraught with frozen conflict, it may be the best means to avoid the region becoming a "shatter zone" along the rim land, and "marginal areas" to Mackinder's pivot and heartland thesis – a prominent line of thought in NATO as it wrestles with security challenges and opportunities in the region [12].

The United States, working in close cooperation with North Atlantic Treaty Organization (NATO) headquarters, has signaled the importance of defense education in its engagement with a number of former Soviet Union states and NATO partner nations of interest through the creation of the Defense Education Enhancement Program (DEEP) [16].

DEEP facilitates (or provides the opportunity to incorporate) the incorporation of Western or modern norms and methods in the field of PME for officers and NCOs while preserving host nation prerogatives as independent States, as well as ensuring ownership of the outcome [5].

Conclusion

Different countries have a variety of reasons for cooperating with NATO, even though they do not implement NATO-initiated programs with the same intensity. Their integration into NATO is a political issue, which in its turn creates obstacles for particular nations. However, utilizing DEEP in pursuit of peace and prosperity in those countries is professional and non-political. Potential areas of cooperation, like preparation of junior and senior officers, improvement of professional NCO system, distance learning, curriculum development at master and PhD levels, exchange of academic experience based on this program contribute to peace and security all the nations are concerned with. The active implementation of NATO's DEEP program significantly affects the integration process of these countries regardless of different obstacles. It would be an auspicious start for them to revamp their PME, especially in terms of academic rigor and critical thinking.

References

1. Nasirov E., Iskandarov, Kh. The prospects of Azerbaijan to enhance military interoperability with NATO // Connections QJ 16, – 2017. No. 4, – p. 91-101.

2. Kaim, M. Reforming NATO's Partnerships // SWP Research Paper, Stiftung Wissenschaft und Politik German Institute for International and Security Affairs: [Electronic resource] / – Berlin, – January 2017. URL: https://bit.ly/2komnUa.

3. National styles of professional military education, PME Investigation Paper: [Electronic resource] / – June 2017. No 2. URL: https://bit.ly/2ml30vR.

4. Willschick, A. In too "DEEP". NATO as an institutional educator: [Electronic resource] / – February 22, 2013. URL: https://bit.ly/2m9fGG9.

5. Labarre, F., Jolicoeur, P. Shaping and measuring military culture development: a case study of the Defense Education Enhancement Program // Canadian Foreign Policy Journal, – 2016. Volume 22, Issue 2, – p. 135-146. URL: https://bit.ly/2kddfSg.

6. Mallick, PK. Professional Military Education-An Indian Experience: [Electronic resource] / New Delhi: Krish Printers. – September 8, 2017. URL: https://bit.ly/2mbQn64.

7. Ruiz, L. The Roots of Modern Military Education: [Electronic resource] / – July 17, 2018, https://bit.ly/2lVbTMc.

8. D'Andurain J. and Stolberg A.G. Defense Education Enhancement Program: The NATO Functional Clearing-House on Defense Education // Connections, – Fall 2012. Vol. 11, No. 4, – p. 53-58. URL: https://bit.ly/2k7vkRt.

9. Berry, J. Defense Education Enhancement Program: The Consortium Perspective // Connections: The Quarterly Journal 11, 2012. No. 4, – p. 27-33.

10. Defense Education Enhancement Programme (DEEP): [Electronic resource] / Last updated: – March 05, 2019. URL: https://bit.ly/2wBdQSU.

11. Iskandarov, Kh. The South Caucasus – NATO cooperation / Kh. Iskandarov. – Riga: Lambert Academic Publishing, – 2019. – 152 p.

12. Keagle, J., Petros, T. Building partner capacity through education: NATO engagement with the Partnership for Peace // Connections: The Quarterly Journal 10, – 2010. No. 1, – p. 46-63.

13. Annual summary of the NATO DEEP programme: [Electronic resource] / Tuesday, July 02, 2019. URL: https://bit.ly/2lL2iaG.

14. NATO Allies underscore Defense Education Enhancement Program: [Electronic resource] / – September 18, 2014. URL: https://bit.ly/2kBVg8a.

15. Annual Report 2012, PfP Consortium of Defense Academies and Security Studies Institutes: [Electronic resource] / – Vienna and Garmisch-Partenkirchen, – March 11, 2013. URL:https://bit.ly/2lMOOLU.

16. Stolberg, A.G., Johnson, S., Kupe, L. Building Partner-Nation Capacity through the Defense Education Enhancement Program: [Electronic resource] / – Jan 31, 2018. URL:https://bit.ly/2rn7Fg3.

Xülasə
NATO ilə hərbi uyarlılığın artırılmasında
Müdafiə Təhsilinin Genişləndirilməsi Proqramının rolu
Xəyal İskəndərov, Pyotr Qavliçek

Bu məqalənin məqsədi NATO-nun Müdafiə Təhsilinin Genişləndirilməsi Proqramını təhlil etmək, onun həyata keçirilməsinin müxtəlif məsələlərini və təsir imkanlarını vurğulamaq və bu təşəbbüsün təhsil sahəsində əməkdaşlığa verdiyi töhfəni əsaslandırmaqdır. Məqalədə müttəfiq və tərəfdaşlar ölkələr arasında uyarlılıq səviyyəsinin artırılmasında Müdafiə Təhsilinin Genişləndirilməsi Proqramının əhəmiyyəti vurğulanır. Uyarlılığın mahiyyətinin geniş olduğunu nəzərə alaraq, müəlliflər xarici təcrübə əsasında yalnız intellektual uyarlılıq səviyyəsinin artırılması üçün zəruri ehtiyacı diqqət mərkəzinə gətirməyə çalışmışlar.

Açar sözlər: NATO, DEEP, təhsil, əməkdaşlıq, uyarlılıq.

Аннотация
Роль Программы Расширения Оборонного Образования
в усилении военного взаимодействия с НАТО
Хаял Искандаров, Пётр Гавличек

Целью данной статьи является обзор Программы Расширения Оборонного Образования НАТО, также освещение проблем и последствий ее реализации, и изучение того, в какой степени эта инициатива способствует сотрудничеству в области образования. Важность Программы Повышения Оборонного Образования была подчеркнута в повышении взаимодействия между союзниками и партнерами. Принимая во внимание широкое значение

интероперабельности, авторы попытались выдвинуть на первый план острую потребность в повышении только интеллектуальной интероперабельности с привлечением внешнего опыта.

Ключевые слова: НАТО, DEEP, образование, сотрудничество, интероперабельность.

Məqalə redaksiyaya daxil olmuşdur: 27.09.2019
Təkrar işlənməyə göndərilmişdir: 10.10.2019
Çapa qəbul edilmişdir: 02.11.2019

UDC 351/354

US ENERGY POLICY IN THE CAUCASUS REGION AND TURKEY

Asgar Zeynalabdinov
Baku State University
E-mail: zeynalabdinov86@mail.ru

Abstract. In order to strengthen its position in the Caucasus since the 1990s, USA has pursued a more active foreign policy course in this direction. After the signing of the "Contract of the Century" in the Caucasus policy of the USA the energy factor became a priority. Turkey, as the closest U.S. ally in the Near and Middle East, played an important role in the energy policy of official Washington.
Keywords: energy, Azerbaijan, USA, Caucasus, Turkey.

US, pursuing an active foreign policy has achieved great opportunities for strengthening its political, economical and military interests in the Caucasus region at the beginning of the nineties of the XX century. Looking to the Caucasia as the Russia's sphere of influence between 1991 and 1994, after signing "Contract of the Century" US began to change its policy towards the region.

"Contract of the Century" was signed in Gulistan Palace of Baku on September 20, 1994, which was later named as the "Contract of the Century" due to its tremendous importance. Production Sharing Agreement related to the development of "Azeri – Chirag–Guneshli" deep-water oil fields has been reflected on 400 pages and 4 languages.

11 companies (Amoco, BP, McDermott, Unocal, SOCAR, LukOil, Statoil, TPAO, Pennzoil, Ramco, Delta) from 7 countries (Azerbaijan, USA, UK, Russia, Turkey, Norway, Saudi Arabia) participated in signing of the Contract of the Century. This Contract has paved the way towards the signature of other 26 contracts with 41 oil companies from 19 countries [1].

From this time official Washington began to pay special attention to energy policy in the Caucasus region. Energy policy in the United States has focused on three major goals:

1. Assuring a secure supply of energy;
2. Keeping energy costs low;
3. Protecting the environment.

In pursuit of those goals, government programs have been developed to improve the efficiency with which energy is utilized, to promote the domestic production of conventional energy sources, and to develop new energy sources, particularly renewable sources [2, p.1]. The relations with Azerbaijan was at the forefront of this policy.

But it should be noted that during 1991-1993 USA did not pay much attention to the relations with Azerbaijan. What reasons disturbed development of the relations of USA and Azerbaijan during the specified period? It can be explained with the following factors [3, p.204]:

1. Incompetence in the sphere of foreign policy of the government formed after gaining independence in Azerbaijan;
2. "907th amendment" of Freedom Support Act approved by US Congress in 1992.

After coming to power Haydar Aliyev established a balanced foreign policy and attached special importance to the relations with US and bilateral negotiations were held during his visits to US. Of course Azerbaijan's growing importance for Washington due to its rich economic resources played a crucial role in strengthening US-Azerbaijan cooperation.

The most important step for development of bilateral relations was taken in 1994 during visit of the president Haydar Aliyev to USA for participation at the 49th session of the United Nations General Assembly. During his visit the president of Azerbaijan held a number of meetings with the US President and other representative of the American government.

That's why starting from the mid-90s of the XX century US began to give special attention to the Caspian oil in order to exert its influence on Caspian basin and Caucasian region for ensuring control over the oil resources. In 1994 the Clinton Administration established a special inter-agency working group to focus on Caspian policy.

From this time being interested in joint exploitation and safe transportation to the world markets of the existing oil and gas reserves in the Caspian Sea, US expanded cooperation with Azerbaijan and Turkey in this sphere.

Bilateral agreements signed with major oil companies in the world formed a suitable environment for Azerbaijan for production and export of energy resources. After that, the main issue on the agenda was to provide safe transportation of Azerbaijan oil to the world markets. Naturally, the US, the biggest shareholder in the oil sector was quite interested in this process. But US involvement in the region irritated Iran and Russia.

Iran decided to participate at least in the export of Azerbaijan energy reserves though it was not included in "Contract of the Century". Therefore, official Tehran proposed the transportation oil through the realization of Baku-Basra pipeline. But Russia proposed Baku-Novorossiysk pipeline for this. The proposal propounded by Iran was not accepted by US and Azerbaijan governments. But what were the factors that prompted them to act like this? Why did Azerbaijan give priority to cooperation with the United States of America and Turkey in transportation of energy resources to world markets? This can be explained by the following factors:

1. Efficient use of rich energy resources;
2. To increase the economic and military power of Azerbaijan by ensuring the development of country's economy;
3. To spread the truth about Nagorno-Karabakh conflict in the international arena;
4. Ensure Azerbaijan's security.

It should be noted that after signing "Contract of the century" on the 9th of October 1995 the initial export routes of Azerbaijan oil were announced by Azerbaijan Republic and consortium countries. First, Russia (Novorossiysk) and secondly, Georgia (Supsa). At first, US came up with the idea of transportation of Azerbaijani oil through the territory of Armenia, thinking this pipeline as a peacemaking factor between Azerbaijan and Armenia. However, unsuccessful policy of Armenia did not allow them to take advantage of this suitable opportunity.

Playing a crucial role in these projects for ensuring energy security resulted in the economic growth of Azerbaijan Republic. Because of its aggressive policy and hostile attitude towards Azerbaijan and Turkey, Armenia remained on the sidelines of these projects.

Because official Yerevan after gaining independence did not take steps towards the formation of mutual beneficial relations with neighboring (Azerbaijan and Turkey) countries. As a result, Armenia missed out on big projects which would have great importance for the weak economy of Armenia. This in turn had a negative impact to the US-Armenia economical collaboration. Because USA is the participant of important projects in Caucasia [3, p.207].

To construct a new oil pipeline and its passage through Georgia was not in the interests of Russia. Therefore a spokesman for the Ministry of Foreign Affairs of Russia Grigori Karasin said that Georgian version was not real and the route through Russia could be cheaper and more promising. But Prime Minister of Turkey Tansu Chiller said that the new oil pipeline would give an opportunity to Turkey to play a crucial role in export of Caspian oil and bridge this important region with West.

In this regard in January 1995 official Washington expressed its support to BTC (Fig. 1) and opposition to the main oil pipeline through the territory f Iran and advised Georgia or Armenia's territory for it in a letter sent to Turkish government [4, p.170].

Fig. 1. Baku-Tbilisi-Ceyhan pipeline

In this process the importance of Georgia as the transit country came to the fore. That's why the revival of the US-Georgia relationship began in the second half of the 90s.

One of the main reasons of this revival was not to remain on the sidelines, when one of the most important projects which will emerge after signing the "Contract of Century" in 1994 [3, p.205].

In January 1997, Bill Clinton's administration declared three South Caucasus and five Central Asia's Republics politically and economically important for USA [5, p.169]. The same year in one of his interviews US Secretary of Energy Federico Pena said that one of their biggest concerns was to decrease dependence on the Gulf, and they believed that the development of the Caspian region would result in diversification of oil sources and promote global security.

It is to be specially emphasized that for US the main means of secure existence in the global system is to control the energy routes and it carries out its policy in this frame [6, p.26-27].

In May 1998, the US Trade and Development Agency, the US Export-Import Bank and the Overseas Private Investment Corp. announced the formation of the Caspian Finance Center in Ankara to facilitate the development of energy and other infrastructure projects in the Caspian region. Then in July 1998, President Clinton appointed Ambassador Richard Morningstar to the new position of Special Advisor to the President and Secretary of State for Caspian Basin Energy Diplomacy [7].

In order to achieve the development of South Caucasus region squeezed between Russia and Iran, as well as strengthen its political, military and economical position official Washington showed its support for the construction of Baku-Tbilisi-Ceyhan oil and Baku-Tbilisi-Erzurum gas pipelines.

It should be noted that Turkey (Fig. 2) has a significant importance in the US Caucasus energy policy.

Fig. 2. Turkey and the South Caucasus

Turkey is geographically located in close proximity to 71.8% of the world's proven gas and 72.7% of oil reserves in particular those in Middle East and the Caspian basin. Turkey as an energy transit corridor implies a variety of oil and gas pipelines and other sorts of transportation, originating from Russia, Caspian and the Middle East not only for Turkish market, but also for Europe and other markets via Mediterranean [8, p.163].

In this regard, Azerbaijan's rich energy resources, Azerbaijan and Turkey's participation as main initiators in the world's realized important projects in the region and others to be realized, Georgia's importance as a transit country, Turkey's importance in transporting energy resources to the European market, its significance as US supporter and shareholder of the major projects in the region play an important role in the development of South Caucasus region.

It should be noted that Russia's policy towards Georgia (the war of 2008) and Ukraine (Crimean issue), its stance on frozen conflicts in the Caucasus (Nagorno-Karabakh, Abkhazia and South Ossetia) and its control over Armenia spell trouble for US. Another important reason is the intensification of Russian influence in the region. Azerbaijan and Turkey's close relationship and their mutual support in economic, military and political issues, as well as Azerbaijan's rapprochement with the United States and Georgia's West orientation policy are the most important factors that irritate Russia.

From these realities, USA increases the volume of gas supply in the global arena in order to play an important role for ensuring energy security and is interested in realization of energy projects such as TANAP (Trans-Anatolian Natural Gas Pipeline), TAP (Trans Adriatic Pipeline) (Fig. 3).

Fig. 3. TANAP and TAP

Trans-Anatolian Natural Gas Pipeline – TANAP Project is one of the prime examples of the successful collaborative projects undertaken by Turkey and Azerbaijan in the field of energy. Augmenting and sustaining their historical bonds of brotherhood with the modern ideal of "Two States One Nation", both Turkey and Azerbaijan place a great deal of importance in the TANAP Project, which will have repercussions throughout the global energy market [9, p.1].

In March 2015, the three presidents from Azerbaijan, Turkey and Georgia launched the Trans Anatolian Natural Gas Pipeline project, as a gas pipeline to the EU that by passed Russia.

According to the agreement Turkey's state owned pipeline operator BOTAS will take a 30% stake in TANAP, while SOCAR holds 58% and BP 12% [10]. It should be noted that 10 billion cubic meters gas will go to Europe, 6 billion cubic will go to Turkey, overall 16 billion cubic meters Azerbaijani gas is expected to be transported through TANAP. According to official information, the initial capacity of 16 billion cubic meters is to be increased to 23 billion within a few years of completion and up to 31 billion by 2026.

After signing agreement on march 17, 2015, Amos Hochstein, Special Envoy & Coordinator for International Energy Affairs at U.S. Department stressed that the United States see Southern Gas Corridor as a culmination of the Baku-Tbilisi-Ceyhan process pipeline, which started 20 years ago. Stating that the TANAP project is very important for US Government.

President Ilham Aliyev said that Azerbaijan has established an active cooperation between the project members, which will enable to gain success in other branches of economy as well. He also noted the importance of the energy cooperation in relations with the European Union [11].

Berat Albayrak, Turkish Minister of Energy and Natural resources, stressing that Turkey will continue its political, economic and technical support in TANAP realization, a significant part of the Southern Gas Corridor [12].

Prime Minister of Georgia Giorgio Kvirikashvili said that Georgia's role as a reliable transit country will further increase, together with strengthened energy security and economic development. In addition, this major project will increase economic development in Georgia [13].

It is very important project and will open new opportunities for the region. Income from the project will be beneficial for the countries' economic growth. In addition, it will expand economical relations among participant countries, also will reduce dependence of Europe on Russian gas. It should be noted that the inauguration ceremony of the TANAP project was held in the city of Eskisehir, Turkey on 12 June 2018. President of the Republic of Azerbaijan Ilham Aliyev attended the event.

Conclusion

In order to stymie the development of Russia and Iran in the region, as well as play an important role in the energy projects which will be implemented soon, US must take some serious steps:

1. First and the most important of these steps is cooperation with Turkey. Because Turkey is an important factor in the US Caucasus policy. Turkey as a NATO member and close ally of USA in the Middle East, also Azerbaijan's close, brotherly relations with Turkey and each country's interests in the region should be taken into account in the foreign policy. Besides as President of the Azerbaijan Republic Ilham Aliyev said that TANAP was the joint work of Azerbaijan and Turkey in offering great opportunities for the future of Europe. From this point of view, we consider that US appreciates mutual cooperation with Turkey and Azerbaijan in all spheres and takes this into account in its foreign policy. Because it is impossible to realize any project in the South Caucasus region without participation of Turkey and Azerbaijan.
2. US, in the framework of its economic interests, must play an important role in ensuring security of major projects, which are supported by official Washington. For this US must pursue active policy in order to solve the conflicts in Caucasus.

References

1. Oil sector: [Electronic resource] / – Baku, – March 31, 2016. URL: en.president.az/ azerbaijan/contract.
2. Yacobucci, B.D. Energy policy 114th Congress Issues // Congressional Research Service, – New York, – 30 September, 2006. – s.1-8.
3. Zeynalabdinov, A.A. US Caucasus policy (1992-2000) // Proceedings of INTCESS15- 2 nd International Conference on Education and Social Sciences, Istanbul, – 26-27 april 2015. – p. 203-210.
4. Kasım, K. Soğuk savaş sonrası Kafkasya / K.Kasım. – Ankara: USAK yayınları, – 2011. – 290 s.
5. Гаджиев К.С. Большая игра на Кавказе вчера, сегодня, завтра / К.С.Гаджиев. – Москва: Международные отношения, – 2010. – 462 s.
6. Özkan, A. XXI yüzyılda ABD-nin küresel stratejileri / A.Özkan. – Istanbul: Tasam yayınları, – 2006. – 128 s.
7. Jaffe, A. US policy towards the Caspian region: can the wish-list be realized?: [Electronic resource] / – New York, – 2001. URL: http://amymyersjaffe.com/content/pdf/wish-list.pdf
8. Ersin, O. Creative energy alternatives: cheap and clean future energy for Turkey / Handbook of research on developing sustainable value in economics, finance, and marketing. New York: Hershey, – 2015. – 549 p.
9. Seyma, E. Trans-Anatolian Natural Gas Pipeline aims to deliver peace// Daily Sabah. – March 17, 2015. – p.1
10. Tinas, M. TANAP Secures first step with groundbreaking ceremony?: [Electronic resource] / – Istanbul, – 18 March 2015. URL:http://www.naturalgaseurope.com.
11. Opening speech by Ilham Aliyev at the second meeting of the Southern Gas Corridor Advisory Council-[Electronic resource] / – Baku, – 26 February 2016. URL: https://en.president.az/ articles/18119.
12. US, UK and Turkey support Southern Gas Corridor: [Electronic resource] / – Baku, – 29.02.2016. URL:http://m.apa.az/en/news/240019/.
13. Genewieve, H. TANAP will increase economic development of Georgia: [Electronic resource] / – Tbilisi, – 31 March 2016. URL: https://agenda.ge/en/article/2016/29.

Xülasə
ABŞ-ın Qafqazda enerji siyasəti və Türkiyə
Əsgər Zeynalabdinov

XX əsrin 90-cı illərindən başlayaraq ABŞ Qafqaz regionunda öz siyasi, iqtisadi və hərbi maraqlarını gücləndirmək məqsədilə fəal xarici siyasət kursu həyata keçirməyə başladı. 1994-cü ildə "Əsrin müqaviləsi"nin imzalanmasından sonra ABŞ-ın Qafqaz siyasətində enerji faktoru önə çıxdı. Yaxın və Orta Şərqdə ABŞ-ın ən yaxın müttəfiqi olan Türkiyə rəsmi Vaşinqtonun regionda enerji siyasətində mühüm rol oynadı.

Açar sözlər: Azərbaycan, ABŞ, Qafqaz, Tükiyə, enerji.

Аннотация
Энергетическая политика США на Кавказе и Турция
Аскер Зейналабдинов

С целью укрепить свои политические, экономические и военные интересы в Кавказском регионе, начиная с 90-х годов XX века США стали проводить более активный внешнеполитический курс. После подписания "Контракта века" в Кавказской политике США приоритетным стал энергетический фактор. Турция, будучи самым близким союзником США на Ближнем и Среднем Востоке, в энергетической политике официального Вашингтона сыграла важную роль.

Ключевые слова: Азербайджан, США, Кавказ, Турция, энергетика.

Məqalə redaksiyaya daxil olmuşdur: 20.09.2019
Təkrar işlənməyə göndərilmişdir: 21.10.2019
Çapa qəbul edilmişdir: 13.11.2019

UDC 004

FIGHTING MEANS OF NATO STATES AGAINST CYBER THREATS

Nuran Mahmudov
War College of the Armed Forces of the Azerbaijan Republic
E-mail: mahmudovnuran@outlook.com

Abstract. NATO's cyber security policy and its activities on this field are enlightened in this article. NATO's struggle and its activities against non-traditional threats particularly cyber threats emerged after Cold War are enlightened in this article.

Keywords: NATO, cyber, cyber security, cyber defence**,** cyber-attacks**,** threat.

Introduction

Peace and security is an essential fact in the life of societies since the existence of humankind. However, the parameters associated with the end of the Cold War, international relations and the foreign policy of states, the concepts of "risk, threat, security, and protection" have been changed. Today, "Strategic security" instead of "strategic defence" have come to the force and security of communities and the conditions that threaten peace differ from the direct military threats of the Cold War era. For example, many of the tensions that were suppressed and frozen in Central and Eastern Europe throughout the Cold War have now become a confrontation as ethnic, religious and nationalistic conflicts and threaten the security of the whole of Europe. Thus, after the Cold War new kinds of threats emerged called non-traditional treats. According to Mely Caballero-Anthony Non-traditional security threats may be defined as "challenges to the survival and well-being of peoples and states that arise primarily out of non-military sources, such as climate change, cross-border environmental degradation and resource depletion, infectious diseases, natural disasters, irregular migration, food shortages, people smuggling, drug trafficking, and other forms of transnational crime" [1].

NATO has also struggled to adapt to the new conditions, while still ensuring the security of its member states from new developments. According to the NATO perspective, "NATO's purpose is to guarantee the freedom and security of its members through political and military means" [2]. From this point of view NATO is fighting against non-traditional threats. After the September 9/11 attack, NATO began to carry out "out of range", that is, extraterrestrial missions, especially against Afghanistan, Libya, Mediterranean and sea pirates in the Gulf of Aden and Somalia. At the same time, NATO has undertaken new tasks, such as energy security, fighting terrorism, fighting cyber defence and combating banditry. Finally, NATO is currently engaged in missions for education and support without fighting in Afghanistan, peacekeeping operations in Kosovo, monitoring operations in the Mediterranean, peacekeeping missions supporting the African Union in Africa, air traffic protection in Ukraine and fighting banditry in the Horn of Africa. Thus, it was established that NATO had evolved from a collective defence organization during the Cold War into a global security organization in the post-Cold War era. Although, NATO is trying to protect member states from non-traditional threats it is very difficult to protect them.

The primary purpose of this work is to determine how NATO took on new roles and transformed the process of disintegration into a process of transformation. In this context, it will consider how NATO, which was created as a single defence organization in the era of the Cold War, was transformed, assuming new roles in the post-Cold War era. This paper will focus on how cyber will be a threat to the Alliance and NATO's strategy to combat cyber threats.

NATO and defence against cyber threats

After the end of the Cold War, new asymmetric risks and threats arose along with technological developments. One of the most important of these cross-border threats, which are more complicated than traditional risks and threats, are cyber-attacks against information systems that are widely used in critical infrastructures [3]. These attacks directed at such systems can lead to severe damage, impeding the fulfillment of social, economic and political functions of states. For this reason, governments and other international organizations should develop appropriate policies in the modern world, exposing the dangers and threats of cyber-attacks as seriously as traditional risks and threats.

In NATO documents, a cyber-attack is defined as the use of electronic systems to stop, delay, modify and influence the expected function of information and communication systems. The attack on the computer network is expressed in the glossary of terms and definitions of NATO as actions performed on a computer and/or computer network with the purpose of interrupting, destroying the computer and/or the computer network itself [4]. Today, NATO members and partner countries face the risk of cyber-attacks aimed at destroying their knowledge-based assets. Such attacks can lead to the nation losing its global competitive ability, which will lead to such consequences as the spread of false information and the seizure of confidential information in the military arena. This can also lead to damage to energy, water, communications and commercial assets, which we call the critical infrastructure necessary to support the economy and society [4, p.161]. These attacks can be carried out for political purposes, as well as ordinary criminal acts that constitute criminal offenses. An individual, states or persons supported by states, can handle it [5]. Such cyber-attacks can be called cybercrime, and cyber-terrorism, depending on the factors and the point of action [6].

Estonia, a member of NATO, was subjected to a major attack in April and May 2007, destroying its critical Internet infrastructure. The duration and destruction of the period of the attacks brought NATO into action. The Alliance quickly responded to the crisis and developed tools and capabilities to protect against attacks on its members [4, p.157]. After that attack, NATO managed to create a document on civil defence policy, and two essential milestones were allegedly recorded:

1. The Cyber Defence Management Authority (CDMA).
2. The Cooperative Cyber Defence Center of Excellence (CCD COE) [7].

Cyber threat and development of Cyber Defence Policy

When NATO launched military operations against Serbia in the Balkans in the late 1990s, many Serbian and Chinese hackers attacked NATO's Internet infrastructure to damage the combat capabilities of NATO. The public relations website, which transmitted the situation with relevant news, could not function for several days due to the "Distributed Denial-of-Service (DDoS)" attacks. When preparing for DDoS attacks, an attacker poisoned many unsafe computers in the world for future use with a malicious program. During the attack, the attacker sends commands to visit the victim's computer by sending small data packets to the unsecured computers it sees. The victim computer that faces millions of desires reaches such an extent that it cannot meet these requirements, and its systems are ineffective. Due to these attacks, NATO e-mail servers have been subjected to millions of e-mail streams [5, p.298-305]. As a result of this experience at the 2002 Prague Summit, NATO leaders decided to launch the NATO Computer Incident Response Capability (NCIRC) and establish the ability to respond to computer incidents in NATO [4, p.157]. With the establishment of the NCIRC Coordination Center in Brussels, NATO was in many ways equipped to deploy critical missions within the organization, computer viruses, unauthorized penetration of NATO networks, and the management of cryptographic devices on the Internet [8]. In addition, NATO experts have contributed to political and legal issues, as well as technical support in the field of computer security [9]. The importance of efforts to prevent cyber threats came to the fore with the help of DDoS-attacks, which Estonia faced in April-May 2007. All the communication systems of the country, the two big banks, were unable to work for several days [6, p.136]. Estonia is particularly vulnerable to such an

attack because of its highly developed electronic infrastructure. Such applications as national parliamentary elections in the electronic environment in the world, national identification data for identification, using electronic signatures, electronic banking and information technology services for the health sector are still intensively implemented in Estonia [10]. Estonia also focused on providing information at a high quality and affordable level for training public and private sectors and noted the importance of providing high-level information to security professionals. All of these studies have led to the establishment of a Cooperative Cyber Defence Center of Excellence (CCD COE). This center was a research body that improved the capabilities of cyber defence of NATO and its allies in 2008 [7, p.54].

NATO viewed cyber-attacks against Estonia as a serious problem of "operational security" and instructed its experts to support the Estonians in this unique attack. Before the attack, NATO focused on protecting its own internal system, and not on helping its allies in matters of cyber defence [10, p.58]. After these attacks, experts indicated that the attacks are a "wake-up call" for developed countries.

In 2008, when Russia entered Georgia, Russian websites distributed software targeting the websites of the Georgian government, which anyone with the internet could use [11]. The government of Georgia and several independent sources, they noted that this was done by the organization "Russian Business Network," originating from St. Petersburg. Although there is no evidence to confirm that the attacks were conducted by the Russian government [12]. While Estonian and Georgian authorities focused mainly on Russia with the cause of such attacks, American sources have brought to mind that organizations such as Hamas and Hezbollah have plans for Israel and USA. The same sources claim that Russia and China also placed severe sources of cyber-attacks against the United States [13].

The result of all these developments, at the NATO Summit in Bucharest in 2008, the Allies first dealt with the concept of cyber defence in the framework of an official summit. In the conclusion, report of the NATO and Cyber Defence Summit held concurrently with the Bucharest Summit, it was emphasized: "In the global information economy, keeping the internet clear and bigger for the business world is equivalent to keeping the sea and the air corridor open" [14]. Throughout the summit, experts and NATO officials took note of lessons learned from the experience of Estonia. The 47th article of the Bucharest Summit Declaration concluded that the importance of the Cyber Defence was emphasized; "NATO depends on its commitment to strengthening the Alliance's core information systems against cyber attacks. We have adopted the Cyber Defence Policy and are developing the structures and bodies that will implement the policy. Our policy on Civil Defence emphasizes NATO and member states' own responsibilities to protect basic information systems, share exemplary practices, and provide assistance in the direction of the Allies to prevent cyber-attacks. We hope that the development of the capabilities of NATO's cyberwar and the strengthening of ties between NATO and the national authorities will continue" [15]. The two most important consequences of the NATO Cyber Defence Policy approved at the summit are the establishment of the "Cyber Defence Management Authority" at the operational level and the opening of the Cooperative Cyber Defence Center of Excellence at the strategic level [7, p.55].

Cyber Defence Management Authority (CDMA)

As its name suggests, CDMA is the administrative body of NATO, in which cyber defence activities are coordinated. CDMA is ready to help and cooperate with the allies in case of cyber-attack [14, p.85]. The creation of a new administrative body in Brussels is a serious attempt to centralize operational opportunities in the field of cyber defence. According to NATO reports, the CDMA goal in Brussels is to create a central body for coordinating the allies' reaction to cyber attacks. With limited knowledge sharing on its capabilities, it is known that CDMA is engaged in research that includes real-time advanced electronic monitoring capabilities to identify cyber threats and intelligence sharing. It is expected that over the next few years CDMA will turn into a "war room

operation center," where tactical responses are prepared for the cyber defence of NATO [16]. At least, contrary to the attacks in Estonia, at present, there are a number of countries in which member states can cause a real cybernetic catastrophe. CDMA, which has been active since April 2008, has made significant progress in its field. So far, the executive committee met five times and developed operational policy. The second cyber defence exercise was conducted twice. After the first exercise in November 2008, 21 members of NATO participated in the second event in November 2009. CDMA has developed a policy on some issues, ranging from the legal aspects of cyber defence and ending with partner relations with partners [14, p.85]. Thus, it was one of the NATO's respond against cyber-attacks.

Cooperative Cyber Defence Center of Excellence (CCD COE)

The second outcome of the Bucharest Summit is the "Cooperative Cyber Defence Center of Excellence", based in Tallin [17]. The NATO Center of Excellence (CoE) is tasked with facilitating NATO's transformation process. The CoE, NATO and the Partnership for Peace are open to governments and provide opportunities for enhancing interoperability and skills, developing doctrines and validating operational concepts through experiments [18]. Currently, there are 24 centers of excellence in cooperation with the Center of Excellence, which opened in Romania in March 2010 [19]. Estonia, which uses information and communication technologies most intensively to reverse the cyber victim status, has also taken the lead in hosting NATO's first Cyber Defence Center of Excellence. CDMA will ensure the long-term development of NATO's doctrine and strategies in the field of cyber defence, and NATO's mission is to coordinate the protection of cyberspace at the operational level [14, p.84]. Founded officially in May 2008 and based on NATO's full accreditation in October 2008, the center began work on how Allies can improve their long-term cyber defence capabilities [20]. As indicated on the website, the Center organizes seminars, events, and seminars for the public from the private sector, Alliance members, and partner countries. The main responsibilities of the center:

1. Education and training (including exercise support).
2. Analysis and lessons learned.
3. Concept development and evaluation/standardization.
4. Doctrine development and standards to ensure effective Interoperability [21].

CCD CoE, funded by fully sponsored countries, can be considered as a research and learning center where best practices are developed and shared.

NATO's Cyber Defence Policy

Seven weeks after Estonia's first cyber-attack, in June 2007, at a meeting of NATO defence ministers, NATO experts prepared a report that used lessons learned from recent events and presented further work on the field of cyber defence [14, p.84]. At the next meeting of the NATO defence ministers in October 2007, the ministers presented a more detailed report describing the Alliance's approach to cyber defence [22]. In the report the implementation of new measures against the cyber-attacks was recommended to the Allies. The report, called the "Policy on Cyber Defence" document, was adopted in January 2008 and ratified by the heads of state and government at the Bucharest summit in April 2008. A rapid agreement on the Policy on Cyber Defence has been reached among NATO allies, as long as the seriousness of cyber threats and the NATO's consensus on this potential issue are present. The relevant military and technical bodies of the North Atlantic Alliance continue to work on the implementation of the policy [23]. The exact details of NATO's Policy on Cyber Defence are kept secret.

Cyber-attacks are one of the most severe asymmetric dangers faced by the Alliance. The open nature of the Internet makes it difficult to protect against cyber-attacks [6, p.138]. Effective international cooperation is critical to fighting cyber-attacks. NATO, the world's largest defence

organization, has such responsibilities as the promotion of cyber defence, the coordination of defence measures and the containment of such actions. It is expected that in the new strategic concept of NATO, the fight against cyber-attacks will be reflected, which is one of the most critical security threats to security in the 21st century. The North Atlantic Council plays an important role in taking measures on cyber security, their implementation at the national level and accelerating the implementation of NATO's Cyber Defence Policy [24].

Conclusion

The changing perception of the security of the 21st century is based on the presence of new threats, which are more complex and dangerous than in the past. The spread of asymmetric threats, which can be called "unknown unknowns" and their impact on the global level, causes an increase in the sense of insecurity of states and societies. It is also has effected NATO's member states.

Cyber-attacks are one of the most severe asymmetric hazards the Alliance has faced, with nuclear proliferation, climate change, and terrorism. The open nature of the Internet makes it difficult to protect against cyber-attacks. Effective international cooperation is critical in combating cyber-attacks. The world's most significant defence organization, NATO has such responsibilities as the promotion of cyber defence, the coordination of defence measures and the containment of such actions. In the new strategic concept of NATO, it is expected that the fight against cyber-attacks, which are among the essential security threats of the 21st century. National parliaments play a crucial role in putting cyber defence measures into force, implementing them at the national level, and accelerating the implementation process of NATO's cyber defence policies.

References

1. Emmers, R. ASEAN and the Institutionalization of East Asia / R.Emmers, – The USA and Canada: Routledge, – 2012. – p.27.

2. "What is NATO?": [Electronic resource] / February 12, 2018. URL: https://www.nato.int/nato-welcome/index.html.

3. Srikanth, D. Non-Traditional Security Threats in the 21st Century: A Review // International Journal of Development and Conflict, – 2014. V.4, №7, – p. 940.

4. Graeme, H. Understanding NATO in 21st Century / H.Graeme, J.Kriendler – The UK: Routledge, – 2013. –155 p.

5. Burton, J. NATO's cyber defence: strategic challenges and institutional adaptation. // Defence Studies, – 2017. V.15, №4, – p. 300.

6. Mehdiyeva, V. NATO-nun kibermüdafiə siyasəti // Strateji Təhlil, – 2016. 3-4 (17-18), – p. 133-138.

7. Saltzman, I. Cyber Posturing and the Offense-Defence Balance // Contemporary Security Policy, – 2013. v. 34, №1, – p. 40-63.

8. NCI Agency: [Electronic resource] / – February 22, 2018. URL: https://bit.ly/2tBd47m.

9. Myriam, C.D. Cyber Security and Threat Politics: US efforts to secure the information age / C.D.Myriam. – The UK: Routledge, – 2008. – 79 p.

10. Laasme, H. Estonia: Cyber Window into the Future of NATO // Joint Force Quarterly, – 2011. V.63, №4, – p. 58-63.

11. Bebber, A., Robert, J. Cyber power and cyber effectiveness: An analytic framework // Comparative Strategy, – 2017. V.36, №5, – p. 426-436.

12. Jon, S. Georgia: Russia 'conducting cyber war': [Electronic resource] / The Telegraph. – February 22, 2018. URL: https://bit.ly/39G6xc9.

13. Trey, H., Laura, B. The Iranian Cyber threat is real: [Electronic resource] / The Telegraph. – February 22, 2018. URL: https://bit.ly/35olb4w.

14. Gergely, S. The NATO Policy on Cyber Defence: The Road so Far // Academic and Applied Research in Military Science, – 2013. V.12, №1, – p. 83-91.
15. NATO, "Bucharest Summit Declaration": [Electronic resource] / February 24, 2018. URL: https://bit.ly/2uqS581.
16. Yağlı S., Dal S. Active Cyber Defence within the Concept of NATO's Protection of Critical Infrastructures // International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering, – 2014. V.8, №1, – p. 909-913.
17. Hughes, R.B. "NATO and Cyber Defence": [Electronic resource] / February 24, 2018. URL: https://bit.ly/2SXe7cx.
18. NATO, "Operational Capabilities Concept for NATO-led PfP Operations": [Electronic resource] / February 24, 2018. URL: https://bit.ly/2MYSlS3.
19. NATO, Centres of Excellence: [Electronic resource] / February 24, 2018. URL: https://bit.ly/2R3H6sP.
20. History of CCD CoE: [Electronic resource] / February 24, 2018. URL: https://bit.ly/2QsKLRB.
21. Guy, B. R. NATO'S Centers of Excellence: A Key Enabler in Transforming NATO to Address 21st Century Security Challenges: [Electronic resource] / February 24, 2018. URL: https://bit.ly/2s4tdSE.
22. Jens, R. Taking Stock of NATO's response Force: [Electronic resource] / February 26, 2018. URL: https://bit.ly/2rYe5Gb.
23. NATO, Cyber defence: [Electronic resource] / February 26, 2018. URL: https://bit.ly/39CGLWe.
24. Marios, P. NATO Smart Defence and Cyber Resilience: [Electronic resource] / February 26, 2018. URL: https://bit.ly/2R3GK5t.

Xülasə
NATO-ya üzv dövlətlərin kiber təhdidlərə qarşı mübarizə üsulları
Nuran Mahmudov

Məqalə NATO-nun kiber təhlükəsizlik siyasəti və onun bu istiqamətdəki fəaliyyətindən bəhs edir. Soyuq Müharibə dövründən sonra meydana çıxan qeyri-ənənəvi təhdidlərə, xüsusilə də, kiber təhdidlərə qarşı NATO-nun apardığı mübarizə və üsulları məqalədə geniş işıqlandırılmışdır.
Açar sözlər: NATO, kiber, kiber təhlükəsizlik, kiber müdafiə, kiber hücum, təhdid.

Аннотация
Методы борьбы стран участников НАТО против кибер-угроз
Нуран Махмудов

В статье говорится о политике кибер-безопасности НАТО и его деятельности в данном направлении. Широко освещены мероприятия НАТО по борьбе против нетрадиционной угрозы, особенно против кибер-угроз появившейся со времен Холодной Войны.
Ключевые слова: НАТО, кибер-безопасность, кибер-защита, кибер-атака, кибер-угроза.

Məqalə redaksiyaya daxil olmuşdur: 06.09.2019
Təkrar işlənməyə göndərilmişdir: 10.10.2019
Çapa qəbul edilmişdir: 07.11.2019

UDC 004

CYBER THREAT INTELLIGENCE. UNDERSTANDING FUNDAMENTALS

Ensar Seker
NATO CCD COE Tallinn, Estonia
E-mail: ensar.seker@ccdcoe.org

Abstract. Threat intelligence is proved based on information, including setting, instruments, pointers, suggestions and noteworthy guidance, around a current or developing threat or risk to assets (such as unauthorized access, unauthorized use of assets, discloses sensitive information, unauthorized changes to an asset, deny access). Studying advanced adversary tactics, techniques and procedures are also part of cyber threat intelligence (CTI) and it can help find breaches or a typical movement, as well as help to get adversaries and prevent threats even before they take place. Minimizing false positives (and false negatives) with cyber threat intelligence increase the effectiveness of the cyber defense. Before using CTI, it is important to define and understand it. This article aims to describe and explain all the basics about CTI.

Keywords: cyber threat, intelligence, intrusion, tools and standards.

Introduction

ISO 27005 defines threat as [1]; “A potential cause of an incident, that may result in harm of systems and organization”. According to ENISA, a threat is [2]; “Any circumstance or event with the potential to adversely impact an asset [Anything that has value to the organization, its business operations and their continuity, including Information resources that support the organization's mission (ISO/IEC PDTR 13335-1)] through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. More detailed description of a threat can be found in “Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems” by NIST. Based on this document, a threat is [3] “Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.”

Threats could be extremely harmful or even chaotic if they are not prevented. For this purpose, it is important to have some sort of information about them. Threat intelligence plays a very critical role to detect cyber-attacks before they happen and stop them in time. This kind of intelligence can provide information about behavior and intentions of adversaries as well as their past attacks and possible future attacks.

According to Gartner [4], “threat intelligence is evidence based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard”. One other description states that [5]; “cyber threat intelligence is knowledge about adversaries and their motivations, intentions, and methods that is collected, analyzed, and disseminated in ways that help security and business staff at all levels protect the critical assets of the enterprise.

As it is understandable from the descriptions as well cyber threat intelligence provides information on malicious actors, their tools, their infrastructure, and their methods for;

- Identifying types of attacks,
- Defining, guiding, and prioritizing operational requirements,

- Understanding threat actor capability, tactics, techniques and procedures, Deploying detection systems,
- Developing defense strategies.

Knowing the types of cyber threats, it can also help to understand cyber threats. Even though there are many types of cyber threats, in their 2016 Threat Landscape Report, ENISA classifies top cyber threats as follow [6];

- Malware,
- Web-based attacks,
- Web application attacks,
- Denial of Service,
- Botnets,
- Phishing,
- Spam,
- Ransomware,
- Insider threat,
- Physical manipulation/damage/theft/loss,
- Exploit kits,
- Data breaches,
- Identity theft,
- Information leakage.

More cyber threats such as Advanced Persistent Threats (APTs), unpatched software can be added to this list.

To be able to prevent or minimize the risks against such threats, it is important to understand, analyze and being advanced in five methods of threat detection and response [7];

1) Network and endpoint monitoring that is constant and comprehensive, including capabilities such as full packet capture and behavior-based threat detection on hosts.

2) Advanced analytics techniques that can sift through massive amounts of information, such as network traffic, in near-real time to spot suspicious behaviors and accelerate investigations.

3) Malware analysis using methods that don't rely on file signatures and go straight to the actual behavior of executables, whether collected on the network or endpoints, to detect hostile activity.

4) Incident detection and response practices that align security personnel, processes, and technologies to streamline and accelerate workflows so security operations teams can spend less time on routine tasks and more time defending high-priority assets and address the riskiest threats.

5) Open-source intelligence (OSINT) is collecting information from the public, open tools or resources to be used in an intelligence context. Data flow for OSINT can be categorized into 6 classifications. Media (newspapers, magazines, radio, television etc.), Internet (such as blogs, dark-web, websites, YouTube, Twitter, Facebook etc.), Public Government Data (public government reports, speeches, conferences etc.), Professional and Academic Publications (journal, academic papers, dissertation, theses etc.), Commercial Data (commercial imagery, financial and industrial assessments etc.), Grey Literature (technical reports, preprints, patents, business documents etc.) [8].

Related work

Even though cyber threat intelligence is crucial for effective defense, there haven't been so much academic work done so far.

MWR, CERT-UK, and the Center for the Protection of National Infrastructure published a whitepaper [9] about cyber threat intelligence with a purpose of explaining the terminology, upsides and drawbacks. Eclectic IQ's white paper [10] also gives an idea about cyber threat intelligence and they explained how to their threat intelligence maturity model works for organizations. Kim-Kwang Raymond Choo [11] studied the Routine Activity Theory and explained in his article how this theory can be applied. Increased variety and volume of attacks in the cyber threat landscape were

highlighted. Daan Planqué [12], analyzed cyber intelligence from the perspective of an enterprise and tried to answer the questions, such as 'how could the term cyber threat intelligence be defined?' and 'how could the cyber threat intelligence process be modelled?' from this perspective in his research. Alper Caglayan and et. al conducted a research for threat intelligence on the behavioral patterns of fast-flux botnets. For their work, they developed a specific threat intelligence infrastructure for fast-flux botnet to be able to do detection and monitoring [13]. In their "Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies" paper [14], Eric W. Burger and et. al. proposed taxonomy for classifying threat-sharing technologies. With this article, they aimed to classify existing technologies using an agnostic framework, identify gaps in existing technologies, and explain their differences from a scientific perspective.

Fundamentals of cyber threat

A. The Methodology of Cyber Attacks

Fig. 1 depicts 7 phases of a cyber-attack aka Lockheed Martin's "Cyber Kill Chain [15]". These attack steps were also presented in NIST SP 800-115 [16].

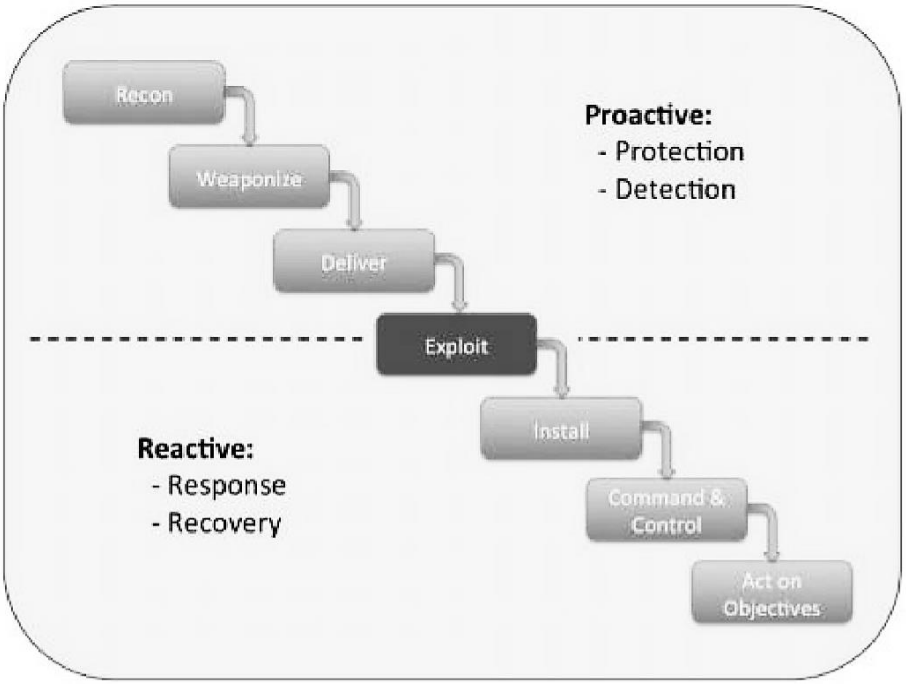


Fig. 1. Cyber Kill Chain

By following cyber kill chain steps, adversary can [17]:

1) identify and select a target(s) (Phase 1 – Reconnaissance);

2) packages an exploit into a payload designed to execute on the targeted computer/network (Phase 2 – Weaponize);

3) delivers the payload to the target system(s) (Phase 3 – Deliver);

4) executes the code on the target system(s) (Phase 4 – Exploit);

5) installs remote access software that provides a persistent presence within the targeted environment or system (Phase 5 – Install);

6) employs remote access mechanisms to establish a command and control channel with the compromised device (Phase 6 – Command and Control);

7) pursues intended objectives (e.g., data exfiltration, lateral movement to other targets) (Phase 7 – Act on Objectives).

Perceiving that a progression of preliminary steps and activities will go before a malicious attack, intelligence efforts can be sent to recognize [18]:

- who may be targeting a network?
- what are the intentions and capabilities of the malicious actors?
- when they will conduct their activity?
- where the activity will originate?
- how they plan to penetrate or affect the network?

B. Characteristics of Cyber Threat Intelligence

By perceiving and drawing in the enemy amid the reconnaissance, weaponization, and conveyance periods of the cyber-attack lifecycle, can give a chance to take necessary course of actions to protect the network and prevent the attacks. This also allows to create effective response and recovery strategies. To be more effective in threat intelligence, following characteristic should be adapted [15];

- *Timely:* For effective threat intelligence time plays a critical role. Intelligence ought to be quickly conveyed with insignificant idleness.
- *Relevant:* Threat intelligence needs to be applicable to related environment.
- *Accurate:* To be able take more reasonable and effective measurements against to attacks more accurate intelligence is necessary. Therefore, the information which is provided by threat intelligence should be correct, complete and explicit.
- *Specific:* More detailed and more specific threat intelligence can allow to defenders to choose suitable countermeasure.
- *Actionable:* Actions are needed to be identified by threat intelligence to ensure necessary data for the response against to threats.

One other recommended intelligence model is named as the Diamond Model of Intrusion Analysis. The model verbalizes and investigates the four key purposes of any occasion: adversary, infrastructure, capability, and victim. Understanding these four purposes of the model, finding the data identified with each, and understanding where in the attacker's kill chain the occasion happened fundamentally adds to understanding an attacker and in like manner delivering threat intelligence [19].

The Cyber Kill Chain and the Diamond Model help to distinguish intrusions and look past the possibility of a solitary intrusion and toward an identification and understanding of attacker techniques. Both of these nourish into the Active Cyber Defense Cycle as shown in Fig. 2 [20].

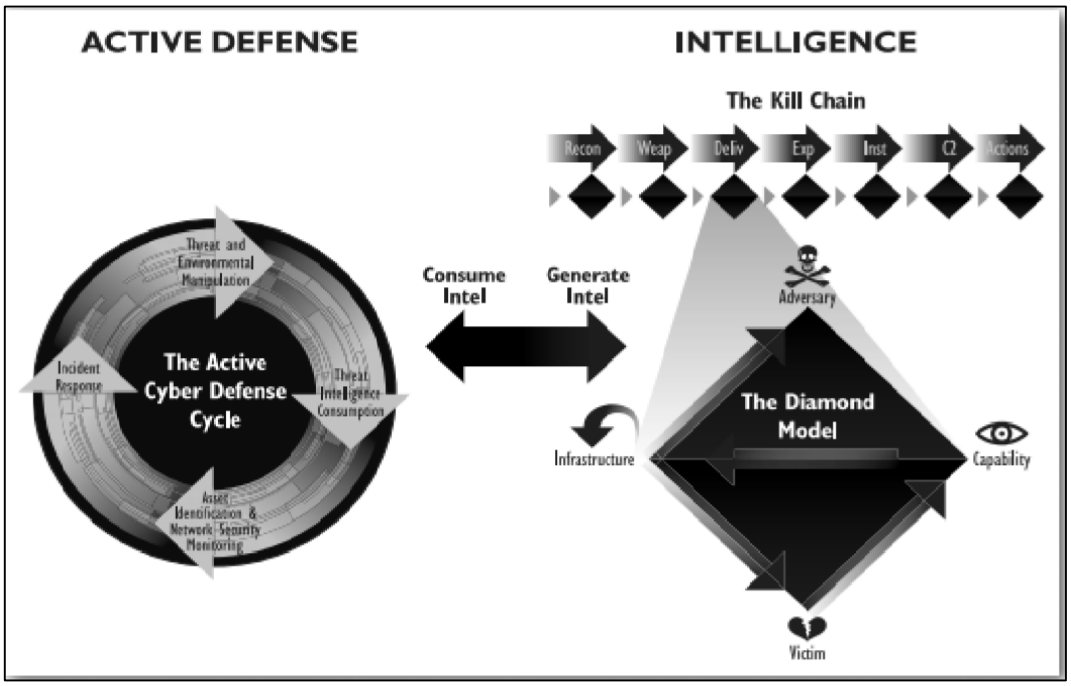


Fig. 2.The Continual Process of Generating and Consuming Intelligence for Hunting Threats

C. Cyber Threat Hunting

Cyber threat hunting is the procedure of proactively and iteratively seeking through networks to detect and isolate propelled threats that avoid existing security arrangements [21]. Hunting is an iterative procedure, that means it must be consistently done in a loop, starting with a hypothesis. There are three types of hypotheses [22];

- Analytics-Driven: "Machine-learning and UEBA (Unlike rule-based systems), used to develop aggregated risk scores that can also serve as hunting hypotheses".
- Situational-Awareness Driven: "Crown Jewel analysis, enterprise risk assessments, company – or employee level trends".
- Intelligence-Driven: "Threat intelligence reports, threat intelligence feeds, malware analysis, vulnerability scans".

D. Cyber Threat Levels

Cyber threat and preparedness levels were introduced by the MITRE Corp. Five cyber threat levels were proposed and each of which corresponds to a general strategy of cyber defense as it is shown in Table 1 [23].

Table 1

Cyber Threat and Preparedness Levels

Level	Cyber Threat Level	Cyber preparedness Level
1	Cyber Vandalism	Perimeter Defence
2	Cyber Threat/Crime	Critical İnformation Protection
3	Cyber İncursion/Surveillance	Responsive Awareness
4	Cyber Sabotage/Espionage	Architectural Resilience
5	Cyber Conflict/Warfare	Pervasive Agility

Threat Level 1: Cyber Vandalism, which corresponds to Perimeter Defense;

Threat Level 2: Cyber Theft/Crime, which corresponds to a defense approach of Critical Information Protection;

Threat Level 3: Cyber Incursion/Surveillance, which corresponds to a defense approach of Responsive Awareness;

Threat Level 4: Cyber Sabotage/Espionage, which corresponds to a defense approach of Architectural Resilience;

Threat Level 5: Cyber Conflict/Warfare, which corresponds to a defense approach of Pervasive Agility [18].

E. Cyber Threat Management

Cyber Threat Management (CTM) is much more than just risk assessment. It emerges best practice for managing cyber threats. CTM includes [24]:

- Manual and automated intelligence gathering and threat analytics.
- Comprehensive methodology for real-time monitoring including advanced techniques such as behavioral modeling.
- Use of advanced analytics to optimize intelligence, generate security intelligence, and provide Situational Awareness.
- Technology and skilled people leveraging situational awareness to enable rapid decisions and automated or manual actions.

Cyber threat management framework (Fig. 3) has different stages such as Observation, Orientation, Decision, Action which can help early detection of threats and limit damage actions [24].

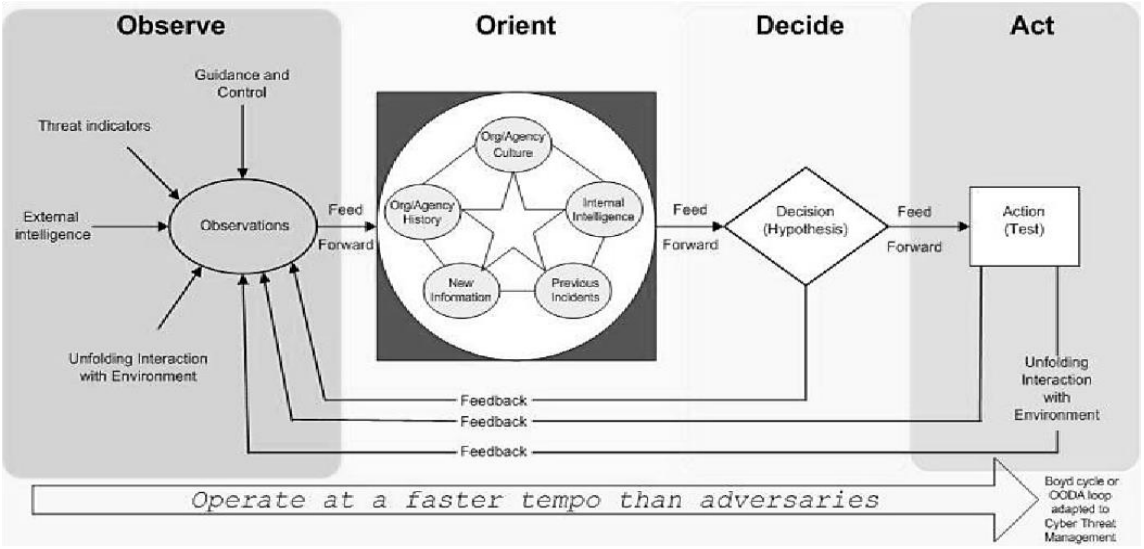


Fig. 3. Cyber Threat Management Framework

Understanding threats and intrusions

A. Threat Modelling

Threat modeling is a procedure by which potential threats, for example, basic vulnerabilities can be distinguished, specified, and organized – all from a hypothetical attacker's perspective. The motivation behind threat modeling is to give safeguards a precise examination of the plausible attacker's profile, the in all likelihood attack vectors, and the assets.

Threat modelling is an iterative procedure that begins amid the early periods of the plan and proceeds all through the application lifecycle. There two reasons. Applications are usually dynamic and they need to be enhanced and adapted. So while the application is getting evolving, the threat modeling process should be repeated. The other reason is, it almost impossible to describe all cyber threats with one-time process. Fig. 4 shows the threat modeling process using a six-stage process [25].

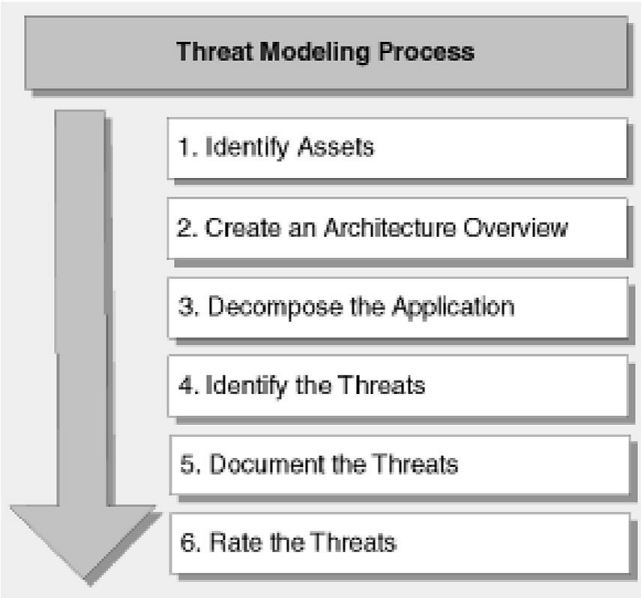


Fig. 4. An Overview of the Threat Modeling Process

Even though there are many threat modeling methodologies which are available for implementation, only the most well-known ones are mentioned in this article.

STRIDE: The STRIDE approach to threat modeling was introduced in 1999 at Microsoft [26]. The STRIDE acronym is framed from the principal letter of the following six categories [27];

- spoofing identity
- tampering with data
- repudiation
- information disclosure
- denial of service
- elevation of privilege

PASTA: The Process for Attack Simulation and Threat Analysis (PASTA) is threat modeling methodology with 7 stages building up to impact of threat [28].

TRIKE: Trike is an open source threat modeling methodology which was developed for enhancing the efficiency and effectiveness of existing threat modeling methodologies [29].

VAST: VAST is stand for Visual, Agile, and Simple Threat modeling. VAST is a threat modeling methodology which defeats a large number of the deficiencies – especially adaptability – intrinsic in past methodologies [30].

AS/NZS 4360:2004, CVSS, and OCTAVE are some other alternative threat models.

B. Intrusion Analysis

When intrusions happen, it's basic that an intensive and efficient analysis and examination of the assault is directed to decide the nature of the threat and the extent of data lost, stolen, or harmed amid the attack. The first step of performing analysis is taking an event record as generated by the sources. Network packet traces, OS audit trails and event logs could be the sources.

Intrusion analysis can be performed with different techniques. These approaches could be either anomaly based or signature based.

Misuse detection effectively conflicts with potential insider threats to vulnerable data. In this method. In misuse detection, all behaviors are described as normal other than the one which are described as abnormal [31]. This approach uses a pattern-matcher which can compare attack signatures with attack data and produce a warning if there is a match [32].

Anomaly detection is the identification of items, events or perceptions which do not comply with normal patterns or other items in a dataset. Anomaly detection techniques can divided into 3 categories; unsupervised anomaly detection, supervised anomaly detection semi-supervised anomaly detection [343].

Cyber threat intelligence tools and standards

A. Traffic Light Protocol (TLP)

TLP is an information sharing model which was created by the UK Government's National Infrastructure Security Coordination Centre (NISCC, now Centre for Protection of National Infrastructure - CPNI) in early 2000s for labelling and handling shared sensitive information [34, 35]. TLP has 4 different categories named by traffic lights which are red, amber, green and white and all colors have different meanings [34, 36];

RED/(TLP:RED): Non-disclosable information and restricted to representatives present at the meeting only. Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.

AMBER/TLP:AMBER: Limited disclosure and restricted to the members of the community who have a need to know in order to take action. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

GREEN/TLP:GREEN: Community wide. Information in this category can be circulated widely within a particular community and the organizations which take part in that community. However, the information may not be published or posted publicly on the Internet, nor released outside of the community of participating organizations. Sources may use TLP:GREEN when information is useful

for the awareness of all participating organizations as well as with peers within the broader community or sector.

WHITE/TLP:WHITE: Unlimited; public information. Subject to standard copyright rules, WHITE information may be distributed freely, without restriction. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

B. Managed Incident Lightweight Exchange (MILE)

The Managed Incident Lightweight Exchange (MILE) Working Group develops standards for exchanging incident data. The group described a package of standards such as Incident Object Description and Exchange Format (IODEF), IODEF for Structured Cyber Security Information (IODEFSCI) and Real-time Inter-network Defense (RID) [37, 38].

1) Incident Object Description and Exchange Format (IODEF): IODEF describes an information framework to represent computer and network security incidents. To do this IODEF has over 30 classes and subclasses including Contact, Monetary Impact, Time, Operating System and Application;

2) IODEF for Structured Cyber security Information" (IODEF-SCI): IODEF-SCI is an extended version of IODEF. The accompanying standards are proposed to be incorporated into IODEF-SCI, Common Attack Pattern Enumeration and Classification (CAPEC), Common Event Expression (CEE), Common Platform Enumeration (CPE), Common Vulnerability and Exposures (CVE), Common Vulnerability Reporting Format (CVRF), Common Vulnerability Scoring System (CVSS), Common Weakness Enumeration (CWE), Common Weakness Scoring System (CWSS), Open Checklist Interactive Language (OCIL), Open Vulnerability and Assessment. Language (OVAL), Extensible Configuration Checklist Description Format (XCCDF), Distributed Audit Service (XDAS) and ISO/IEC 19770;

3) Real time Inter-network Defense (RID): RID defines a protocol to facilitate sharing computer and network security incidents which is a standard for communicating for cyber threat intelligence. Five messages types are used by RID which are Request, Acknowledgement, Result, Report and Query.

Policy Class in RID allows different policies.

C. Open Indicators of Compromise (OpenIOC) Framework

OpenIOC gives a standard arrangement and terms for portraying the artifacts encountered during the course of an investigation. It was presented by Mandiant in 2011. OpenIOC contains definitions for specific technical details including over 500 indicator terms. It is easy to add new items. A specific malware sample or family can be described using Boolean logic [37, 39].

D. Vocabulary for Event Recording and Incident Sharing (VERIS)

VERIS is a framework to define and share incident which was proposed by Verizon in 2010. Its purpose is to provide a common language for describing security incidents in a structured and repeatable manner. VERIS is to collect, classify, analyze, compare and share information security incident data. There are five sections in VERIS schema [37, 40]; Incident tracking, Victim demographics, Incident description, Discovery & response and Impact assessment. There are multiple elements (with specific data types and variables names) in each section.

E. Open Threat Exchange (OTX)

OTX was created Alien Vault for sharing threat data in 2012. OTX is open to global community. It delivers communitygenerated threat data, enables collaborative research, and automates the process of updating your security infrastructure with threat data. To collect cyber threat intelligence OTX uses centralized system. OTX Threat [37, 41].

F. Collective Intelligence Framework (CIF)

CIF was introduced by the Research and Education Network Information Sharing and Analysis Center (REN-ISAC) in 2009 which is a client/server system for sharing threat intelligence data. It uses information for identification (incident response), detection (IDS) and mitigation (null route).

CIF data contains information on the type of threat, severity of an attack and the confidence of the data. It also has labeling data and access control features [37, 42].

G. MITRE Standards

MITRE has developed some standards for different needs of cyber threat intelligence management systems.

1) Cyber Observable eXpression (CybOX): CybOX is an institutionalized diagram for the determination, capture, characterization, and correspondence of occasions or stateful properties that are noticeable in all framework and network operations [37, 43]. It provides over 70 defined objects that can be used to define measurable events or stateful properties. CybOX supports a wide range of relevant cyber security domains including [44]: Threat assessment and characterization (detailed attack patterns), Malware characterization, Operational event management, Logging, Cyber situational awareness, Incident response, Indicator sharing, Digital forensics.

2) Structured Threat Information Expression (STIX): STIX is an another standard for defining threat information including threat details with the context of the threat which was first presented in 2012. It uses cases such as Analyzing Cyber Threats, Specifying Indicator Patterns for Cyber Threats, Managing Cyber Threat Prevention and Response Activities, Sharing Cyber Threat Information. STIX provides a unifying architecture (Fig. 5) tying together a diverse set of cyber threat information along with [45]:

- Cyber Observables (e.g., a registry key is created, network traffic occurs to specific IP addresses, email from a specific address is observed, etc.).
- Indicators (potential observables with attached meaning and context).
- Incidents (instances of specific adversary actions).
- Adversary Tactics, Techniques, and Procedures (including attack patterns, malware, exploits, kill chains, tools, infrastructure, victim targeting, etc.).
- Exploit Targets (e.g., vulnerabilities, weaknesses or configurations).
- Courses of Action (e.g., incident response or vulnerability / weakness remedies).
- Cyber Attack Campaigns (sets of Incidents and/or TTP with a shared intent).
- Cyber Threat Actors (identification and/or characterization of the adversary.

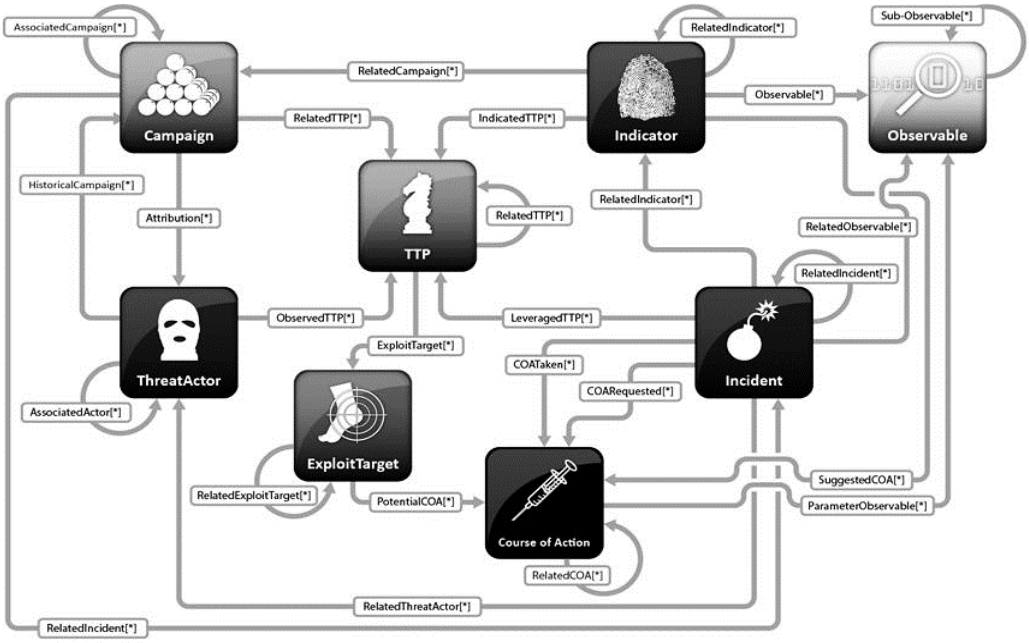


Fig. 5. STIX Architecture

3) Trusted Automated eXchange of Indicator Information (TAXII): TAXII is a set of services and message exchanges for exchanging cyber threat information. It utilizes a standardized cyber

threat information representation and defines a supporting exchange framework. Multiple sharing models are supported by TAXII such as hub and spoke, peer to peer, source/subscriber. Four core services supports the model like discovery, feed management, inbox and poll. XML and HTTP are used by TAXII for transporting messages and their context. TAXII also has been adopted as part of 'Microsoft Active Protections Program (MAPP) [37, 46].

Even though CybOX, STIX, TAXII are the most known standards by The MITRE Corporation, there are some others such as Common Attack Pattern Enumeration and Classification (CAPEC), and MAEC (Malware Attribute Enumeration and Classification) [47].

Conclusion

Utilizing national security as a relationship, pretty much everything without exception is a potential assault vector. There basically isn't sufficient time, cash, or labor to guard against each scenario. Rather the administration accumulates risk insight so it can comprehend which threats are most important or unavoidable and distribute assets in like manner to make preparations for those assaults.

It's essential for organizations to know about every potential threats, yet threats insight goes above and beyond and enables those organizations to devote security assets to reinforce resistances where important to fortify the security act against the assaults that are well on the way to really happen.

References

1. Information Technology – Security Techniques-Information Security Risk Management: [Electronic resource] / ISO/IEC FIDIS 27005, – 2008. URL: https://bit.ly/35FxMQR.

2. "Glossary", ENISA: [Electronic resource] / 14.11.2017. URL: https://bit.ly/38MAZ3Z.

3. Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems: [Electronic resource] / NIST, – 2006. URL: https://bit.ly/2FHVdyA.

4. McMillan, R. Definition: Threat Intelligence: [Electronic resource] / – Gartner, – 2013, URL: https://gtnr.it/2R6G92S.

5. Definitive Guide to Cyber Threat Intelligence: [Electronic resource] / iSight Partners, – 2015. URL: https://bit.ly/39ZQXZ9.

6. Threat Landscape Report, ENISA: [Electronic resource] / – 2016. URL: https://bit.ly/36KoXXB.

7. Intelligence Driven Threat Detection & Response: [Electronic resource] / RSA, – 2014. URL: https://bit.ly/36Muo86.

8. Richelson, J.T. The US Intelligence Community: [Electronic resource] / – 2011. – 624 p. URL: https://amzn.to/30aPE54.

9. Threat Intelligence: Collecting, Analysing, Evaluating: [Electronic resource] / – Jan 24 20185. URL: https://bit.ly/3a1zgsc.

10. Applying the Threat Intelligence Maturity Model to Your Organization: [Electronic resource] / Eclectic IQ, – 2015. URL: https://bit.ly/2sk2DFc.

11. Choo, K.R. The Cyber Threat Landscape: Challenges and Future Research Directions // Computers and Security, 2011. 30(8), p.719-731.

12. Planqué, D. Cyber Threat Intelligence - From Confusion to Clarity; An Investigation into Cyber Threat Intelligence: [Electronic resource] / – 2017. URL: https://bit.ly/2FINfVX.

13. Caglayan, A. et. al., Behavioral Analysis of Botnets for Threat Intelligence // Information Systems and e-Business Management, December 2012, Volume 10, Issue 4, p. 491-519.

14. Burger, E.W. et. al. Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies: [Electronic resource] / – November 2014. URL: https://bit.ly/35GvhOh.

15. Hutchins, E.M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains / E.M.Hutchins, M.J.Cloppert, R.M. Amin / Lockheed Martin Corporation, – 2009. – 14 p.

16. Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A. Technical Guide to Information Security Testing and Assessment / K.Scarfone, M.Souppaya, A.Cody, A.Orebaugh / SP 800115, NIST, – 2008. – 80 p.

17. Guide to Cyber Threat Information Sharing, SP 800-150, NIST, – 2016, – 43 p.

18. Mattern, T., Felker, J.R., Bamford, G. Operational Levels of Cyber Intelligence // International Journal of Intelligence and Counterintelligence, – 2014. 27, p. 702-719.

19. Caltagirone, S., Pendergast, A., Betz, C. The Diamond Model of Intrusion Analysis: [Electronic resource] – 2014. URL: https://bit.ly/2Thf2EO.

20. The Who, What, Where, When, Why and How of Effective Threat Hunting, SANS Institute, – 2016.

21. Gasper, P.D. Cyber Threat to Critical Infrastructure, Idaho National Laboratory, – 2008.

22. Cyber Threat Hunting: [Electronic resource]. – 19.11. 2017. URL: https://bit.ly/35xDvJg,

23. Bodeau, D., Graubart, R., Greene, J.F. Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels: [Electronic resource] / The MITRE Corporation, – 2009. URL: https://bit.ly/2FE1NGg.

24. What is Cyber Threat Management? Institute of Cyber Threat Management: [Electronic resource] / 20.11.2017. URL: https://bit.ly/38O2nyA.

25. J.D. Meier et. al., Improving Web Application Security: Threats and Countermeasures: [Electronic resource] / Microsoft Corporation, 2003. – 15.11.2017. URL: https://bit.ly/2Z3iq79.

26. Kohnfelder, L., Garg, P. Threats to Our Products, Microsoft, – 2016.

27. Shostack, A. STRIDE Chart, Microsoft, – 2007.

28. UcedaVelez, T. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis / T.UcedaVelez, M.Morana. – Wiley, – 2015. – 696 p.

29. Eddington, M. Trike v1 Methodology Document / M.Eddington, B.Larcom, E.Saitta. – 2005.

30. Agarwal A. VAST Methodology: Visual, Agile, and Simple Threat Modeling / A.Agarwal [et al.]. – Prescott Valley, – 2016.

31. Diaz-Gomez, P.A. Hougen, D.F. Misuse Detection: An Iterative Process vs. A Genetic Algorithm Approach: [Electronic resource] / –January 2007. URL: https://bit.ly/3a5Ttxd.

32. Fichera, J. Network Intrusion Analysis / J.Fichera. – Elsevier, – 2006.

33. Chandola, V., Banerjee, A., Kumar, V. Anomaly detection: A survey, ACM Computing Surveys: [Electronic resource] / – 2009. URL: https://bit.ly/2FD4lEJ.

34. Luiijf, E. Sharing Cyber Security Information / E.Luiijf, A.Kernkamp, GCCS, – 2015. – 66 p.

35. Stikvoort, D. ISTLP - Information Sharing Traffic Light Protocol: [Electronic resource] / NISCC (UK), – 2009. URL: https://bit.ly/30aUlMe.

36. Traffic Light Protocol (TLP) Definitions and Usage: [Electronic resource] / USCERT. – 20.11.2017. URL: https://www.us-cert.gov/tlp.

37. Tools and Standards for Cyber Threat Intelligence Projects, SANS Institute, – 2013. – 27 p.

38. Managed Incident Lightweight Exchange (mile): [Electronic resource] / 20.11.2017. URL: https://datatracker.ietf.org/wg/mile/about.

39. Gibb, W., Kerr, D. OpenIOC: Back to the Basics: [Electronic resource] / 20.11.2017. URL: https://bit.ly/36GRvkf.

40. The Vocabulary for Event Recording and Incident Sharing: [Electronic resource] / 20.11.2017. URL: http://veriscommunity.net.

41. Alien, V. Open Threat Exchange: [Electronic resource] / 20.11.2017. URL: https://bit.ly/2tlgcEi.
42. Collective Intelligence Framework: [Electronic resource] / 20.11.2017. URL:http://csirtgadgets.org/.
43. Information Sharing Specifications for Cybersecurity: [Electronic resource] / USCERT – 20.11.2017. URL: https://www.us-cert.gov/InformationSharing-Specifications-Cybersecurity.
44. Cyber Observable eXpression – CybOX: A Structured Language for Cyber Observables: [Electronic resource] / The MITRE Corporation. – 2014. URL: https://bit.ly/2TemYql.
45. Structured Threat Information eXpression – STIX: A Structured Language for Cyber Threat Intelligence Information: [Electronic resource] / The MITRE Corporation. URL: https://bit.ly/37Rs28a.
46. The Trusted Automated eXchange of Indicator Information (TAXII™) / J.Connolly, M.Davidson, M.Richard [et al.]: [Electronic resource] / The MITRE Corporation, – 2012. URL: https://bit.ly/2QHMS46
47. About STIX: [Electronic resource] / 20.11.2017. URL: http://stixproject.github.io/about/.

Xülasə
Kiber təhdid kəşfiyyatı. Əsas anlayışlar
Ensar Seker

Təhdid kəşfiyyatı real və potensial risklər haqqında məlumatlara, o cümlədən vasitə, göstərici, təklif və təqdirəlayiq bələdçiliyə (məsələn, icazəsiz giriş, aktivlərdən icazəsiz istifadə, məxfi məlumatların açıqlanması, icazəsiz dəyişikliklər, girişin inkar edilməsi) əsaslanır. Düşmənin qabaqcıl taktikalarını, metod və prosedurlarını öyrənmək də kibermüdafiə kəşfiyyatının tərkib hissəsidir və onlar qanun pozuntuları yaxud tipik manevrləri, eləcə də bədniyyətliləri aşkarlamağa və təhdidlərin qarşısını əvvəlcədən almağa kömək edir. Kiberhücumlardan istifadə edərək saxta pozitivlərin (və saxta neqativlərin) minimuma endirilməsi kibermüdafiənin effektivliyini artırır. Kiber təhdid kəşfiyyatından əvvəl onun mahiyyətini anlamaq vacibdir. Məqalə kiber təhdid kəşfiyyatı barədə fundamental məlumatları izah etmək məqsədi daşıyır.

Açar sözlər: kiber təhlükə, kəşfiyyat, müdaxilə, alətlər və standartlar.

Аннотация
Разведка киберугрозы. Основные понятия
Энсар Секер

Разведка угрозы основана на информации о реальных и потенциальных рисках, в том числе на средство, показатель, предложение и заслуживающего доверия проводника (например, несанкционированный доступ, несанкционированное использование активами, раскрытие конфиденциальной информации, несанкционированные изменения, запрет доступа). Изучение передовых тактик, методов и процедур противника также является составной частью разведки киберугрозы и они помогают выявить нарушения правил, или же типичные маневры, а также злоумышленников и преждевременно предотвратить угрозы. При использовании кибератак снижение до минимума фальшивых позитивов (и фальшивых негативов) увеличивает эффективность киберзащиты. До разведки киберугрозы важно понять его сущность. Целью статьи является разъяснение фундаментальных информаций о разведке киберугрозы.

Ключевые слова: киберугроза, разведка, вторжение, инструменты и стандарты.

Məqalə redaksiyaya daxil olmuşdur: 01.05.2019
Təkrar işlənməyə göndərilmişdir: 07.06.2019
Çapa qəbul edilmişdir: 12.07.2019

UDC 004

CYBER DEFENSE EXERCISES (CDXS) AS A TESTBED FOR CYBER SECURITY ASSESSMENTS

Ensar Seker[1], Kamile Nur Seker[2]
[1]NATO CCD COE, Estonia, [2]Istanbul Sehir University, Turkey
E-mail: ensar.seker@ccdcoe.org

Abstract. Cyber defense exercises (CDXs) are excellent testbed platforms to test and assess IT (İnformation Technology) and OT (Operational Technology) systems. They (CDXs) are also very important tools when it comes to enhancing the safety awareness of cyberspace, testing an organization's ability to put up resistance and respond to different cyber events to establish the secure environment, gathering empirical data related to security, and looking at the practical training of experts on this subject. The exercises can give ideas to the decision makers about the precautions in the cybersecurity area and to the officials, institutions, organizations, and staff who are responsible on the cyber tools, techniques, and procedures that can be developed for this field. The objective of this paper is to address the issue from a scientific point of view by taking CDXs as a testbed and lesson learned platforms to be able to create better and safer cyber environment.

Keyword: Cyber defense, security exercises, cyber resilience, cyber threat, cyber security, cyber-attack mitigation, cyber crisis management.

Introduction

In the cyber defense exercises, the scenarios that are simulated closest to reality which provides very important contributions by bringing together the necessity of making the best decisions and management capabilities under the cyber crisis by handling stress and coordinated movement as a team.

One of the most important outputs of the CDXs is the After Action Report (ARR). At this report, it is mentioned that the detailed performance of each blue teams (defense team) after the exercise, main scenario and sub-scenarios, injections, exercise purposes, participants, scoring, technical infrastructure, red team attacks (client-side, web, network), defenses techniques and methods by the blue team, defects in these defenses, observations notes from all teams and sub-teams, recommendations and evaluations are also covered. CDXs as a testbed give an opportunity to cyber experts to:

- performance testing without consequences,
- prevent downtime and provide complete business continuity,
- save time and money using virtualization,
- produce maximum benefit from IT and OT systems testing,
- create readiness, response and recovery plans for cyber-attacks in real life.

Related Work

CDXs have been identified as an efficient mechanism to practice IT security awareness training but are also an ultimate tool to reveal and define the different security needs of every organization. It provides an excellent opportunity and ultimate learning experience for the students to improve their skills in protecting and defending information systems are assessed in the context of realistic, true-to-life scenario. On the other side, as discussed by Vigna and Mink, the offensive security training is also an effective way to learn information security. The previous works in this area examined the structure and how to use of cyber defense competitions, overall effectiveness of live-attack exercises in teaching information security, curriculum and course format at CDXs in which teams design, implement, manage and defend a network of computers. Other literature has examined the benefit of

conducting cyber defense competitions at the K-12 level. The architecture of a cyber-defense competition and different tools and techniques used and how they fit into an active learning approach and how it focuses on the operational aspect of managing and protecting an existing network infrastructure were described by Green et.al. Patriciu and Furtuna presented a number of steps and guidelines that should be followed when designing a cybersecurity exercise. One another approach of such live attack exercises presented by White, lessons learned from illustrative examples of such exercises, as well as suggestions to help organizations conduct their own exercise. Other literature examined how to offer cyber defense competitions in the private sector, using a service provider model. Existing literature has examined the potential benefits of cyber defense exercises. One another benefit of cyber defense exercise that can be instrumented to generate scientifically valuable modern labeled datasets for future security research and help uncover gaps in IT Security policies, plans and procedures. It was claimed that cyber exercises can be developed with a focus on measuring performance against specific standards. In cyber defense exercises, to measure team effectiveness and gain knowledge how to do that, the role of behavioral assessment techniques was investigated as a complement to task-based performance measurement. In the literature, The RINSE simulator that is the real-time immersive network simulation environment for network security exercises was presented as a realistic rendering of network behavior. In addition to that to execute real-time security exercises on a realistic inter-domain routing experiment platform was presented in the past. A developed method for Job Performance Modeling (JPM) which uses vignettes for improving cybersecurity talent management through cyber defense competition design was described by Tobey.

Cyber Defense Exercises (CDXs)

In terms of cyber defense, cyber exercises have been playing a very important role in testing the technical cyber capacity of nations or organizations, cyber training, and cyber awareness raising that's why they have started to become widespread all over the world. Among the main objectives of the cyber defense exercises, they can increase:

- the ability to test and develop common and coordinated technical and strategic mobility against the cyberattacks that may occur on a national basis;
- the ability to test and develop common and coordinated technical and strategic mobility against cyber-attacks, which may occur on an international basis;
- ability to test and develop continuity and improving continuity processes with cybersecurity capabilities;
- strengthening cooperation and coordination between public and private sectors in the cyberspace;
- gathering empirical data related to cybersecurity research;
- the maturity level of legal and regulatory compliance.

From the planning stage through to the implementation, execution and finally to the evaluation stage, CDXs can provide important contributions to both the exercise planners and their participants. These processes of exercises also can give an idea to a developer who develops mechanisms for the cyber defense.

Life Cycle. In general, cyber defense exercises life-cycle has four major parts as following:

Identifying: Includes topics such as recognizing and creating participants profile, determining the type and size of the exercise, evaluating current scenario options.

Planning: Includes topics such as informing and training the people and teams involved in the exercise, setting up the media policy, inviting observers and media members, providing financial resources, setting the schedule and location of the exercise, distributing roles and creating a realistic scenario, preparing the exercise materials.

Conducting: Includes topics such as implementation of the exercise in the most appropriate frame and rules, implementation of the scenarios and injections according to the determined sequence, resolution of the problems and faults that can occur during the exercise in the shortest and quickest

manner, observation of participants and taking notes of decisions and activities of participants, and the management of the questionnaire and surveys for participants in order to support them.

Evaluating: Includes the creation of a group evaluating the exercises' results, the collection and evaluation of questionnaires and surveys answered by the participants, the collection of necessary information from the participants in the exercise, the preparation of documents to be submitted to the media, and the preparation of reports to be shared with the evaluators. Fig. 1 shows CDXs life cycle.

Fig. 1. CDX Life Cycle [43]

Teams. The teams are the followings:

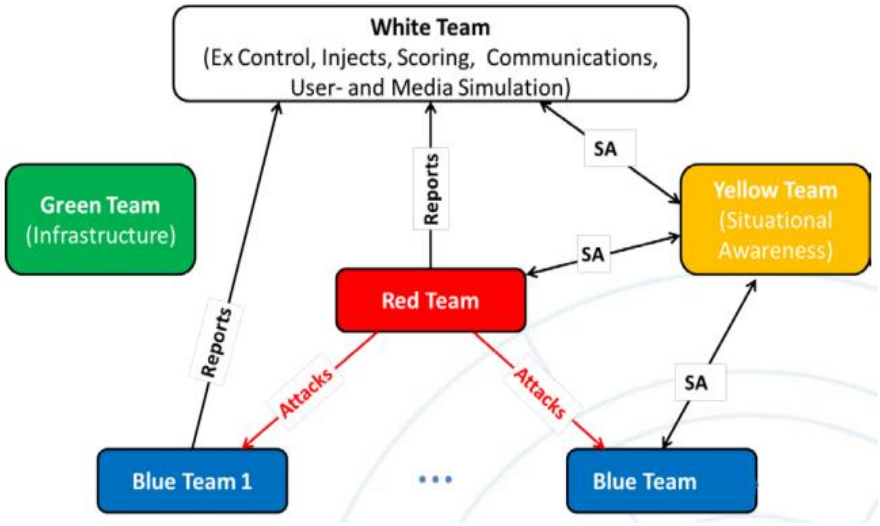


Fig. 2. CDX Teams

I) Blue Team (Defense);

Blue team is responsible for ensuring and defending the security of a company's or organization's information systems against virtual attackers (red team) in a virtual environment created within the scope of practice. In international cyber defense exercises, blue teams represent the national teams of each participating country. Against the simulated attacks, blue team should defend its network:

- over a given period of time;
- a defense based and operational context;
- following the exercise's rules.

Blue team also should identify and prevent any data leakage on their system. The team also responsible for the protection of privacy, integrity, and usability of their network. Since the cyber defense has been a part of national and international law and politics, media and national security strategies in recent times, the cyber defense exercises have also begun to be designed in this context. Only the technical defense by the blue team has begun to be seen as insufficient within the scope of cyber defenses. For this reason, legal, policy, strategy, and media scenarios have begun to be included in addition to technical scenarios, especially for international cyber defense exercises, so the responsibilities of the blue team have been increased. The responsibilities of the Blue Team must always be observed within the framework of the rules of engagement, the applicable laws and regulations, and any illegal action was taken by the team members is deemed unacceptable. Therefore, it is very important that all the actions and decisions taken by the blue team, even in the simulation environment, be performed without ignoring the existing laws and regulations. Another clear rule in the rules of engagement is that the blue team cannot attack the exercise infrastructure, other blue

teams, the red team and the virtual systems. Blue team members must provide the right information, which will not harm their operational safety when requested. Blue teams are able to communicate the green team that is responsible for exercises infrastructure, through the web page designed for them by submitting notifications and requests related to the technical problems about the exercise environment. The green team is responsible for resolving these technical problems within reasonable time. It is important that all reports created by the team are made through the command chain within the team. Blue teams are allowed to use their own tools and software products, but all responsibility for the licensed copy of these products belongs to this team. Within the white team, there is a group of people called 'blonde user' who are a response to occupy blue teams' users' services and systems. These users represent unconscious users and they may open harmful emails and files by clicking malicious links unconsciously. It is against the rules for the blue teams to deny these users' services and systems used by these users. It is also expected that the blue teams will be able to resolve the requests submitted by these users regarding technical problems related to the systems they are using, within a limited time. In order to transfer preliminary information about the systems to be used with the exercise environment, blue teams are informed through webinars before the exercises.

II) Red Team (Offense);

The aim of the red team is to achieve cyber-attacks equally to all the blue teams participating in the exercise. For this purpose, the red team follows a predefined scenario and has the permission to use security vulnerabilities that are already created in the blue team's systems. Successful attacks by the red team lead to a negative score for the blue teams. The red team and the white team must work closely together. The red team must always follow the instructions given by the white team. It is strictly forbidden for the red team to attack the services and infrastructure used by the green team. It is imperative that all attacks carried out by the Red Team remain within the exercise environment. This includes social engineering.

III) Green Team;

Green team is responsible for preparing and maintaining exercise systems and infrastructure. These infrastructures include systems that design, set up, and manage administrative computer nodes, virtualization platforms, storage, and core networking, as well as systems that blue teams must defend during the exercise. In order to ensure that these systems are functioning properly during the exercise, it is expected from the green team that they will be able to solve the technical problems submitted by the blue teams within a reasonable period of time.

IV) Yellow Team;

The role of the yellow team is to provide situational awareness during the exercise first for the white team and then for all participants in the exercise. The main sources of information for the yellow team are the interim reports provided by the blue teams, the reports of the attack campaigns from the red team members, and the reports provided by the system. The yellow team provides regular updates to white team leaders and blue teams.

V) White Team;

The white team is responsible for organizing the exercise and checking it during the execution. The white team determines the exercise objectives, the scenario, the high-level objectives for the red team, legal injections, rules, media preparations and communication plans. During the execution, the white team provides control of the exercise by determining when to start different stages, controlling the execution of the red team's campaign, and scoring issues. Management, blonde users, injections, scoring and media simulation are among the responsibilities of the white team.

Scenario. The desired outcomes of the exercise vary from one exercise to another, but these outputs always revolve around presenting realistic scenarios to demonstrate the cyber threatening methods of participation and to evaluate the success of the exercise programs. Exercise outcomes should aim to raise awareness of various cyber threats and to give an idea to make a plan to prevent them. An example scenario of an international cyber defense exercise in the past years as follows; Country X is an island republic located in the western part of Africa and is a member of an

international organization. There is a coalition force of this organization in the country. While the size of the island is comparable to that of Ireland, the climate and landscape are closer to Morocco. The Republic of X is a poor country, and especially sanitation, communication, medical services and education are quite inadequate. For example, the country has an insecure internet connection with the rest of the world, and the bandwidth of the connection is low. There are no law enforcement agencies or CERT to protect the country's information systems. This forces most international actors in the county to install and use expensive satellite communications or locally operated systems. The Republic of X is in diplomatic conflicts with the Country of Y (a neighbor), which has been criticized by the international community for having a vigilant anti-democratic government. For a long time, the Republic of X is exposed to the cyber-attack, which is predicted to originate from the Country of Y. Immediately following the last diplomatic crisis between the Republic of X and the Country of Y, cyber-attacks started to take place at the Air Force base of the Republic of X and a number of confidential information and documents were stolen. As part of the international coalition, the mission of the blue team is to take necessary precautions at the Air Force base, analyzing IT devices, preventing ongoing and possible future attacks, and reporting to the HQ. The Blue Team should try to fulfill the duties assigned to it in an unfamiliar system. They need to take in consideration the rules, media and strategy-based sub-scenarios and injections that will be included later throughout the exercise.

Scoring. Scoring is one of the most troubling issues for CDXs. Even if the scoring systems that are made are tried to be standardized, it is highly probable that objections always arise from the blue teams because scoring is usually made based on the initiative of the white team. For this reason, many CDXs, especially the ones that are organized at the international level, opposed the scoring system by arguing that scoring isn't the main purpose of the CDXs. Creating competition environment to build a better cyber defense is the main reason for score supporters. One of the examples of exercises that do not use the scoring system is Cyber Europe organized by ENISA. However, the use of the scoring system in such exercises was seen as a motivation tool for participants, and the positive competition between participants was a greater impetus for achieving more successful outcomes. Locked Shields, which was organized by NATO CCD COE, has been using scoring systems at the exercise.

Monitoring. Monitoring and logging is the basis for the scoring system and it helps identifying and responding to incidents during the exercise at an early stage. CDXs are performed in a limited time and too many attacks and network activity occurs via exercise team members in this period that makes difficult for organizers to monitor corporate data being created across multiple networks and nodes. Therefore, monitoring provides a good understanding and in-depth analysis of fields in event logs and alerts created via Syslog, Nagios, DPI, NetFlow, etc. It is believed that controlling and scoring is one of the primary and critical asset in CDX that helps understanding real-time situation and performance of teams throughout the exercise and provides fine-grained control over network links and hosts.

Media Activity Simulator. The media simulator allows the actors to view and interact with the media and social media as if they were in real life. All players have their own passwords for social media use. Live to broadcast on all media and social platforms such as Twitter, Facebook, TV, radio, online news and newspapers are available through the simulator. With this simulation, web pages for the institutions and organizations of the host country are also available based on the scenario. While blue teams are busy taking the necessary precautions against attacks from red teams, they have to take the necessary steps in the media dimension as well like in real life.

Injections. Injections can be divided into 4 categories as; scenario injections, media games, legal games, and forensics.

1. Scenario Injections; scenario injections prepared by the white team that includes taking necessary precautions against cyber threat and vulnerabilities, following the news, evaluating intelligence, gathering information about cyberattacks and preparing reports.

2. Media Scenario; As mentioned before, the purpose of the media simulation is to bring the media environment to exercise environment so to challenge the blue teams even further. The stories in the news include information about events that occurred on ongoing cyber events, negative comments for the current cyber-attacks as well as fabricated news about them.

3. Legal Games; The ability of the blue team to answer questions from the chain of command depends on having deep legal knowledge. To deal with complicated legal issues, to refute false statements and interpretations, and to communicate with the media in order to make the legal explanations related to the cyber-attacks intriguing to the general public understandable to those who are not experts and to respond in legal context to the news and analyzes that the media has published, are among the requirements of the game.

4. Forensic; Forensic aims to answer the questions related to current cyber-attacks such as who did it? What happened, when happened, how happened and why happened?

CDXs as Testbeds

CDXs are suitable platforms to test the IT and OT systems to be able to create better cyber security and cyber defense solutions. In this chapter, we will take a closer look to Locked Shields CDX to analyze how cyber exercises can be used as testbed environments. Lesson-learned sections and evaluation of the exercise by all participants, can give ideas to cyber experts to improve and strengthen their security. So, it's fair to say that CDXs can serve as excellent testbeds. Cyber experts from different fields who participate CDX can share their knowledge and experience each other via this exercises. Fig. 3 shows a model for exercise data information sharing.

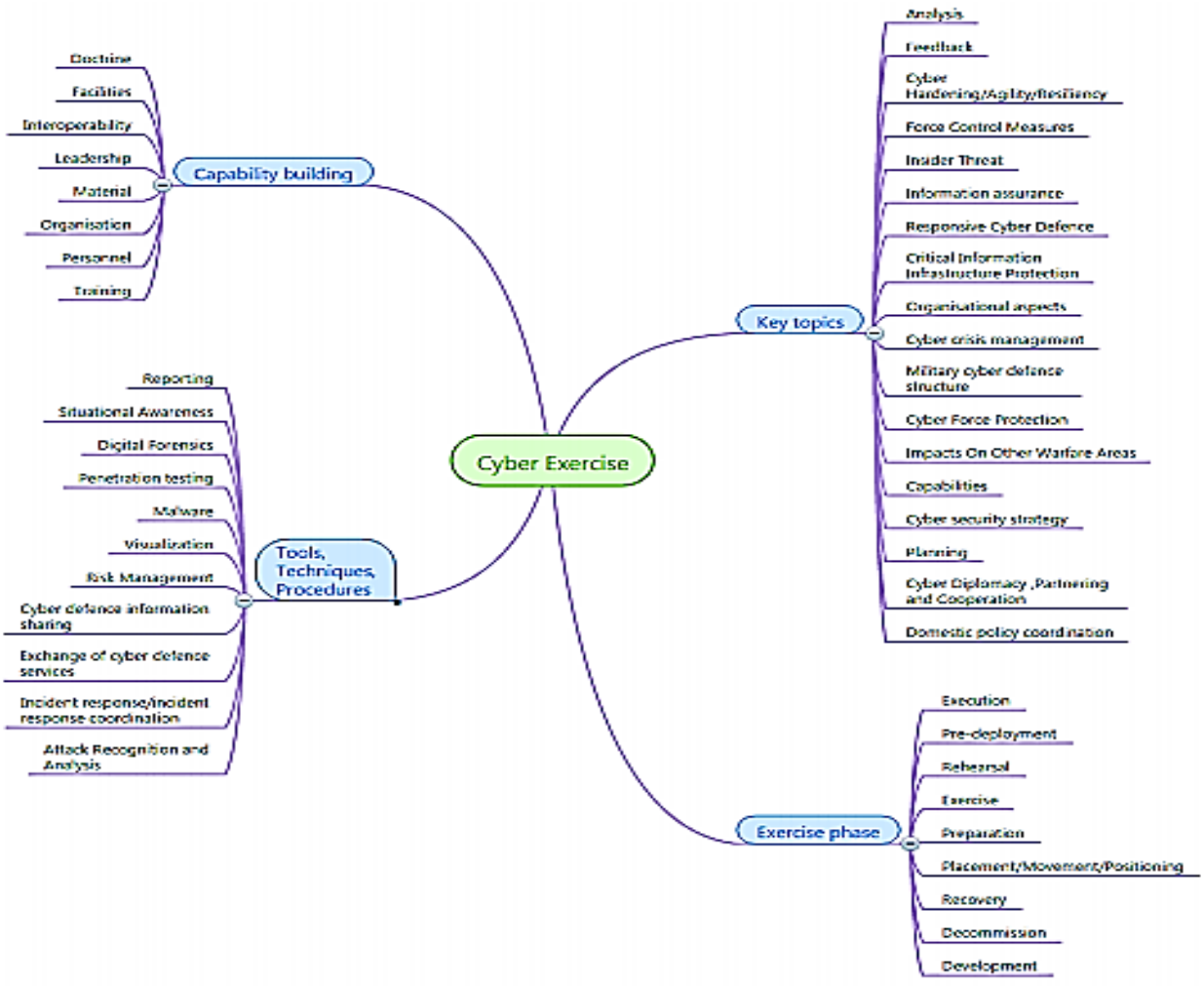


Fig. 3. Model for Exercise Data Information Sharing

Locked Shields (LS) cyber defense exercise is organized annually by the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE). It's accepted by the authorities that Locked Shields is the world's largest, most complex and technologically advanced cyber defense exercise. In Locked Shields, blue teams are created by the NATO member nations or NATO allied nations. So, it is an international cyber exercise in state level. Locked Shields could be a good example to show how CDX can be used as testbed. Fig. 4, 5, 6 shows some statistics about LS CDX. Based on Fig. 4, while there were 9 blue teams in 2012 LS CDX, the number was increased to 22 in 2018. In Fig. 6, the number of participants to LS CDX also growth (250, 250, 300, 400, 550, 800, 1000 respectively) in same period. This means LS CDX was able to attract more nations and more cyber experts every year. According to Fig. 5, number of virtual machines were increased dramatically from 25 to 4000 in 6 years. It means LS CDX is getting more advance and complicated each year. More than 1000 cybersecurity experts from around the world have been involved in the 2018 Locked Shields exercise and the national teams of 21 countries have participated as blue teams. The exercise involved around 4000 virtualized systems and more than 2500 attacks by the red team.

LS CDX follows a successful route to adopting information technology (IT) and operational technology (OT) systems. The organizers of LS CDX succeeded in providing an interesting and complex environment for the blue teams to defend these against an intensive attack campaign. While blue teams can put their skills to test, they can also analyze and test new technologies in a safe and secure environment.

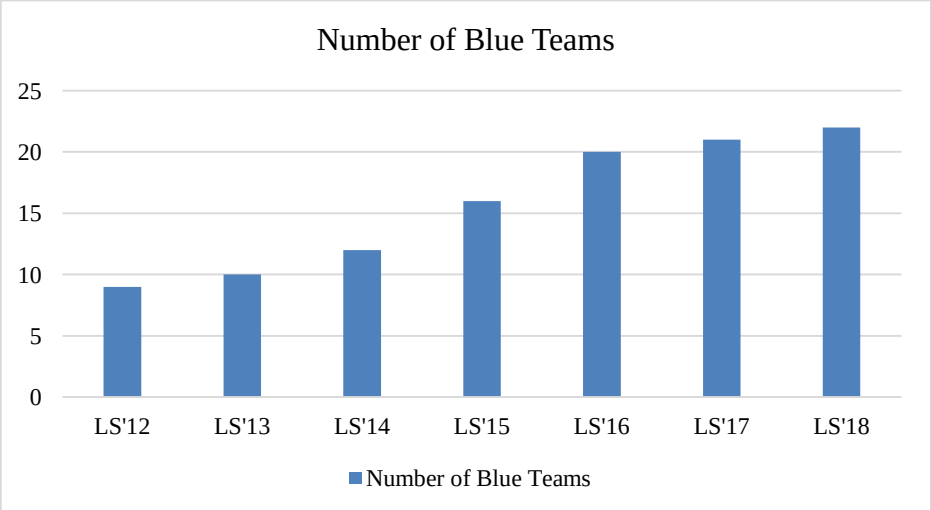


Fig. 4. Locked Shields CDX – Number of Blue Teams by Year (2012 – 2018)

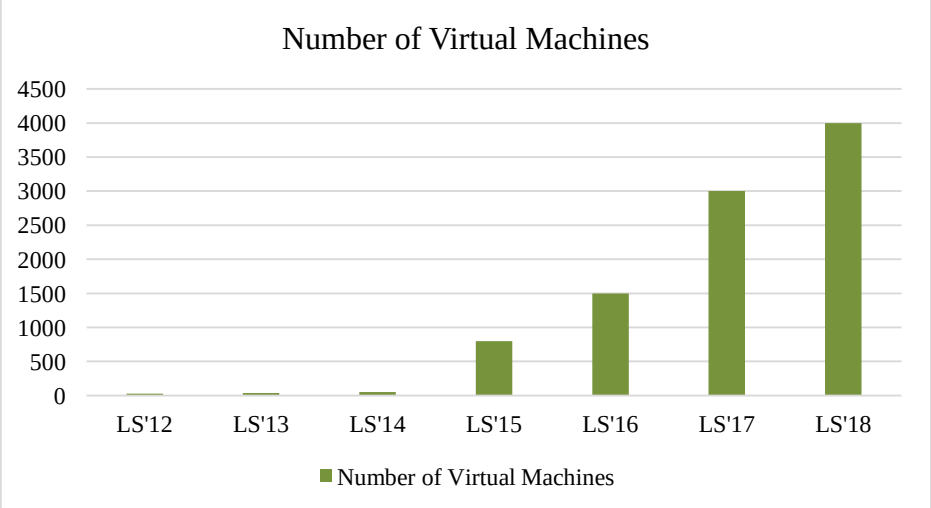


Fig. 5. Locked Shields CDX – Number of Virtual Machines by Year (2012 – 2018)

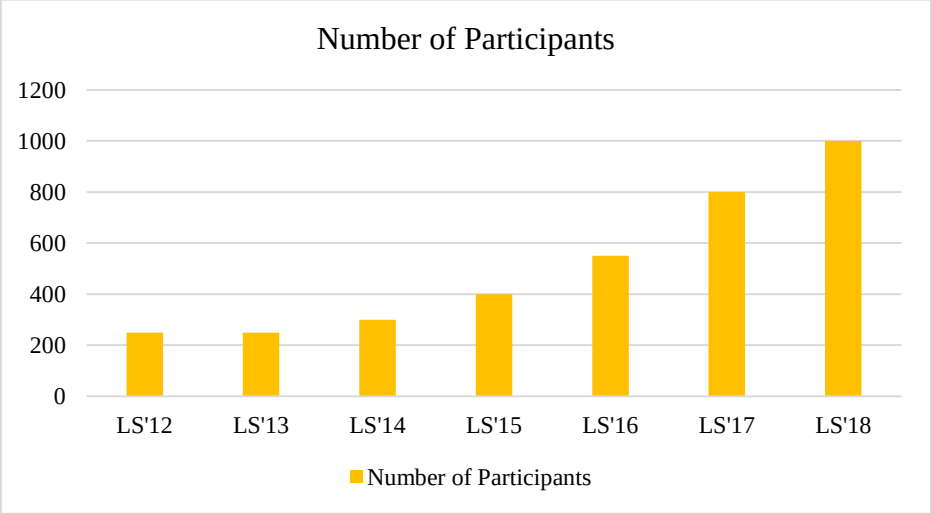


Fig. 6. Locked Shields CDX – Number of Participants by Year (2012 – 2018)

In the context of LS13, the following areas were most challenging for the blue teams:

- Defending web applications.
- Detecting custom malicious code.
- Mitigating BGP hijacking attacks.
- Initiating efficient information sharing.

In LS14, the most challenging areas are for blue teams:

- Filtering and detecting malicious traffic over IPv6.
- Monitoring for malicious WAN route changes and preventing BGP hijacking/man-in-the-middle.
- Protecting custom web applications.
- Finding pre-planted malicious programs and coping with RT's Anti-Virus evasion techniques (publicly available free tools were in most cases enough to evade AV solutions).
- Sharing actionable information with other blue teams.

In 2015, new attack vectors included ICS/SCADA systems and Windows 8 and 10 operating systems, as well as an element of active defense.

In 2017, the blue teams were tasked to maintain the services and networks of a military air base of a fictional country, which, according to the exercise scenario, experienced severe attacks on its electric power grid system, unmanned aerial vehicles, military command and control systems, critical information infrastructure components and other operational infrastructure. The size and scope of technologies, networks and devices used in Locked Shields 2017 has increased considerably – leading to more attacks and specialized systems involved. Specialized systems enable teams to practice the defense of systems that they are not working with on a regular basis. However, in the modern threat landscape incidents with specialized systems may potentially have a profound effect on a military mission or the entire society.

In 2018, the attacks cause severe disruptions in the operation of the electric power grid, 4G public safety networks, drone operation and other critical infrastructure components. While the aim of the tech game is to maintain the operation of various systems under intense pressure, the strategic part should serve as a forum to understand the impact of decisions made at the strategic and policy level.

When we analyze LS CDX, based on the statistics and After Action Reports (ARR), it can be said that, the exercise improved itself during the years and created a suitable testbed platform for cyber experts. Via this platform, professionals and decision makers in cyber security were able to share their knowledge and experience with each other and test their defense skills and strategies against new technologies and new attacks.

Future research directions

For future studies, a technical tool will be developed on the scoring system, which is a problematic issue for CDXs, and on the standardization of this system and the development of a fairer system. The integration of new technologies such as power grid systems and drone control systems into CDXs is a critical issue. With the integration of these special systems into the exercises, the existing problems and the methods to be followed are another work to be done in the future.

Conclusion

The importance of defense exercises is increasing day by day. It would be possible for countries to be involved in the global cyber defense exercises in the international arena, spreading the development and implementation of their own CDX platforms on a national basis, and allocating higher budget figures to the planning and development of these exercises could contribute to achieving beneficial outcomes in the future to create stronger cyber defense systems. The emphasis on these exercises on the national and international scene will provide benefits in terms of uncovering the vulnerabilities in the area of the cyberspace, as well as the revitalization of the cyber defense awareness, and also the integrated technologies that can be followed in exercises related to the cyber defense.

References

1. Locked Shields 2012: [Electronic resource] / URL: https://ccdcoe.org/locked-shields-2012.html.
2. Locked Shields 2013: [Electronic resource] / URL: https://ccdcoe.org/locked-shields-2013.html.
3. Locked Shields 2014: [Electronic resource] / URL: https://ccdcoe.org/locked-shields-2014.html.
4. Locked Shields 2015: [Electronic resource] / URL: https://ccdcoe.org/locked-shields-2015.html.
5. Locked Shields 2016: [Electronic resource] / URL: https://ccdcoe.org/locked-shields-2016.html.
6. NATO CCD COE. Locked Shields 2012 – After Action Report. Tallinn: NATO CCD COE.
7. NATO CCD COE. Locked Shields 2013 – After Action Report. Tallinn: NATO CCD COE.
8. NATO CCD COE. Locked Shields 2014 – After Action Report. Tallinn: NATO CCD COE.
9. NATO CCD COE. Locked Shields 2015 – After Action Report. Tallinn: NATO CCD COE.
10. NATO CCD COE. Locked Shields 2016 – After Action Report. Tallinn: NATO CCD COE.

Xülasə
Kibermüdafiə təlimləri (CDXS) kiber təhlükəsizliyin qiymətləndirilməsi mexanizmi kimi
Ensar Seker, Kamile Nur Seker

Kiber müdafiə təlimləri (CDX) İT və OT sistemlərini test etmək və qiymətləndirmək üçün əla sınaq platformalarıdır. Onlar (CDX) kiberməkanda təhlükəsizlik səviyyəsini artırmaq məqsədilə təşkilatın müqavimətgöstərmə və müxtəlif kibertəhdidlərə reaksiyavermə qabiliyyətini yoxlamaq, təhlükəsizliklə əlaqəli empirik məlumatları toplamaq üçün vacib bir vasitədir. Təlimlər, kibermüdafiə sahəsində təhlükəsizlik qaydaları ilə bağlı yeni ideyaların yaranmasında, kiber vasitə, texnika və prosedurlara cavabdeh olan vəzifəli şəxslərə, eləcə də qurum və təşkilatlara qərar verməkdə kömək edə bilər. Məqalənin məqsədi daha təhlükəsiz kibermühit yaratmaq üçün sınaqdan keçirilmiş və təcrübələrə söykənən kibermüdafiə təlimləri əsasında məsələyə elmi nöqteyi-nəzərdən yanaşmaqdır.

Açar sözlər: kibermüdafiə, təhlükəsizlik təlimləri, kiber dayanıqlıq, kiber təhdid, kibertəhlükəsizlik, kiberhücumun azaldılması, kiberböhranın idarə edilməsi.

Аннотация

Учения по киберзащите (CDXS) как механизм оценки кибер-безопасности

Энсар Секер, Камиле Нур Секер

Учения по киберзащите (CDX) являются отличными платформами для тестирования и оценки ИТ и ОТ систем. Они (CDX) также являются очень важным средством для повышения уровня безопасности в киберпространстве для проверки способности организации оказывать сопротивление и реагировать на различные кибер угрозы; сбора эмпирических данных, связанных с безопасностью. Учения могут помочь при создании новых идей для мер предосторожности в области кибербезопасности, должностным лицам, которые несут ответственность за кибер-средства, технику и процедуры, а также учреждениям и организациям для вынесения решения. Целью данной работы является подход к вопросу с научной точки зрения, для создания более безопасной кибер-среды на основе прошедших испытание и опирающееся на опыты учения по киберзащите.

Ключевое слово: киберзащита, учения по обеспечению безопасности, кибер-устойчивость, киберугроза, кибербезопасность, снижение кибератаки, управление кибер-кризисом.

Məqalə redaksiyaya daxil olmuşdur: 01.05.2019
Təkrar işlənməyə göndərilmişdir: 03.06.2019
Çapa qəbul edilmişdir: 06.07.2019

UDC 61; 613.6

THE ROLE AND SIGNIFICANCE OF MEDICAL INTELLIGENCE IN MILITARY OPERATIONS

Ali Abdulazimov
The Operational Capabilities Concept battalion of Azerbaijan Armed Forces
E-mail: dr.ali.abdulazimov@gmail.com

Abstract. This study examines the importance of medical intelligence in modern military operations. The article provides information on how to organize medical intelligence and shows its invaluable role in all types of military activities. Forms of medical intelligence, as well as the character and methods of collecting medical intelligence information, were explained in detail. The article explains the characteristics of the area where the troops are located and where the combat operations will take place, which is necessary to be considered in advance by the medical service.

Keywords: medical intelligence, intelligence report, intelligence requirements, health care system, characteristics of the area of operations

Introduction

Medical intelligence, which is also called MEDINT, is that category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information [1; 2]. MEDINT is used to get information about the socio-economic factors of the area that is important for medical maintenance, medical maintenance of enemy troops, and other issues. It is usually carried out by persons who have been selected from the medical personnel for this purpose or intelligence groups.

Although some of this information is on topographic maps, it is not sufficient for the practical work of medical services. Furthermore, military operations are characterized by the destruction of settlements, and the worsening of the sanitary and epidemiological situation. When the enemy retreats, it deliberately destroys the water facilities and in some cases, creates an outbreak of infectious disease among the local population.

Aspects of medical intelligence

One of the actions taken by the medical service to get this necessary information is medical intelligence. It includes intelligence on

- endemic or epidemic diseases, public health standards and capabilities, and the quality and availability of health services;
- medical supplies, medical services, health service facilities, and number of trained HSS (Health Service Support) personnel;
- location-specific diseases, strains of bacteria, insects, harmful vegetation, snakes, fungi, spores, and other harmful organisms;
- foreign animal and plant diseases especially those diseases transmissible to humans;
- health problems relating to the use of local food supplies;
- medical effects of and prophylaxis against chemical and biological agents and radiation;
- the impact of newly developed foreign weapons systems as they relate to casualty production;
- an enemy force as it relates to his state of health and fitness or his use of special antidotes;
- an area of operations such as altitude, heat, cold, and swamps that in some way may affect the health of the command or HSS operations [1].

The following information is important for the preparation of a comprehensive medical intelligence report:

To know the sanitary-epidemiological situation of the region where troops are located and where the upcoming fighting will take place. For this purpose, in this area the presence of infectious diseases among the population and epizootics in wild and domestic animals are revealed. Factors that can influence the course of the epidemic (living conditions of the local population and sanitation of apartments, condition of water sources, water quality, transmitters of transmitted diseases and etc.) are identified [3].

The characteristics of the area that can affect the health of the personnel and the presence of infectious diseases in enemy troops are clarified. In addition to estimating the medical and tactical aspects of climate, relief, and also the presence of poisonous plants and toxic representatives of wildlife should be known.

The condition of the medical care system of the enemy forces is being clarified [3]. For this purpose, information about infectious diseases among the personnel of enemy forces, as well as sanitary and epidemiological measures undertaken by the medical service, methods of treatment of wounded and sick, preventive methods, the location of stationary medical facilities and medical warehouses is obtained. Moreover, local medical supplies are being investigated.

Characteristics of the area of operatıons

The area of operations may have some significant effects on the number of casualties as well as their collection and evacuation. Some of the characteristics of the area of operations which must be considered by the HSS planner are the followings:

Terrain. Topography has a direct effect on the incidence of combat casualties. Natural conditions may favor large populations of insects which commonly are vectors of many diseases and therefore could directly increase the incidence of disease. Mountains, forests, and swamps can be expected to constrain evacuation resources. The duration of hazards from chemical and biological warfare agents may increase in the forest where the air is still and the foliage is thick.

Weather and climate. Weather influences the incidence of frostbite, hypothermia, snowblindness, trench foot, dehydration, sunburn, heat exhaustion, heat stroke, battle fatigue, and other medical manifestations that detract from combat effectiveness. Tropical, desert, and tundra conditions favor the growth of insect populations that can greatly increase the incidence of disease casualties. Humidity may affect storage life of medical supplies and equipment. Precipitation affects available water supply, may impact on hospital site selection, and may damage unprotected supplies. Temperature variations may require special protection of medical supplies and may increase patient load because of heat and cold injuries. Severe weather also produces an increase in disease cases [1]. Climate change effects impact military operations, whether they be war-fighting operations or humanitarian missions. For example, climate change can place significant burdens on the supply chains and logistical capacity of armed forces engaged in theater. Other extreme weather events, such as droughts and flooding, can also put stresses on critical military infrastructure.

Civilian population and enemy prisoners of war. Wartime stress and physical damage can lead to rapid deterioration of urban and rural utilities such as electricity, water, and sewage services. Consequent increases in civilian communicable disease could present a threat to which friendly forces are vulnerable. Enemy prisoners of war and refugee populations also tend to be sources of communicable disease.

Flora and fauna. Certain animal diseases or toxic plants may affect movement or the condition of troops, equipment, and/or animals. Some countries have very strict regulations and quarantine procedures concerning importation of animals and plants into their country. The effects of major diseases are delayed because of incubation periods. Knowledge of potential losses to malaria, typhus, and other endemic disease is invaluable in determining appropriate preventive and control measures. These measures include requirements for immunization, chemoprophylaxis, immunoprophylaxis,

vector control, or other appropriate measures. Should time not allow for immunizations, this information will be essential in estimating disease rates and, thereby, projecting strength changes in maneuver units.

Local resources. Information on the availability or location of such items as food, water, pharmaceuticals, and medicinal gases (oxygen) and their quality control procedures will affect requirements for supply stock levels and transportation.

NBC threat. The effects of NBC warfare could be severe on medical operations. Commanders must ensure that units and personnel are prepared to survive, defend, and continue operations in or near a contaminated area. Presence of critical facilities such as nuclear power plants or chemical plants could impact on medical operations. The Bhopal and Chernobyl incidents are excellent examples of how these facilities could impact on medical operations [1].

When an exposure hazard or health threat to deployed personnel is identified, it must be added to the physiological and psychological stress factors that normally affect a person before, during, and after deployment. All information related to such complex hazards will be of interest for medical intelligence purposes [4].

Table 1

Spectrum of potential environmental health hazards for deployed personnel as human involvement increases (4)

Type	Natural hazards (naturally occurring)	Human-made hazards (incidental)	Attacks with weapons (deliberate)
Chemical	– Fumes from a volcanic eruption – Smoke from forest fires	– Incidental chemical release or pollution due to failure of chemical storage or production facilities – Military or terrorist action that causes incidental release due to collateral damage to chemical storage or production facilities – Improper waste and hazmat management	Chemical weapons attack
Biological	– Endemic disease – Exposure to pathogenic microorganisms	– Antibiotic-resistant disease – Incidental release or pollution due to failure of biotech storage or production facilities – Military or terrorist action that causes incidental release due to collateral damage to biotech storage or production facilities – Improper waste and hazmat management	Biological weapons attack
Radiological	– Background radiation – Low-level radiation from naturally occurring materials	– Incidental release or pollution due to failure of radiological or nuclear storage or production facilities – Military or terrorist action that causes incidental release due to collateral damage to radiological or nuclear storage or production facilities – Improper waste and hazmat management	Radiological or nuclear weapons attack

The size of is likely to have both direct and indirect impacts on the local community. One challenge is to minimize the unintended environmental consequences of the operation, such as depletion of scarce natural resources, soil erosion, pollution, and chemical spills [4].

The significance of medical intelligence

Medical intelligence is critical to strategic and tactical planning and operations to conserve the fighting strength. It is a highly technical area which must be complete (collected, evaluated, analyzed, and interpreted) so that the end product is technically accurate and contains all required information [3].

– *at the strategic level*, the objective of medical intelligence is to contribute to the formulation of national and international policy predicated in part on foreign military and civilian capabilities of the medical or biological scientific community.

– *at the tactical level*, the objective of medical intelligence is to provide intelligence evaluation and analyses of the following factors in the theater:

- conditions concerning people or animals;
- epidemiological information (incidence, distribution, and control of infectious diseases);
- plants;
- enemy's field health service support;
- new weapons systems or employment methods that could alter health service support planning factors;
- medical implications of contamination from NBC weapons based on employment tactics and chemical or biological agents used;
- antidotes to protect against the nuclear, biological, or chemical threat;
- weather and/or terrain implications.

Medical intelligence also assists in identifying captured enemy materiel and equipment and how it can be used in treating enemy prisoners of war [3].

Accurate and timely intelligence is a critical combat support tool for planning, executing, and sustaining military operations. It is equally important in achieving optimum planning, execution, and sustainment of HSS operations, the medical readiness of the command, and the overall combat readiness of the unit. At the operational level, intelligence focuses on the joint campaign and operations. At the strategic level, the objective is to contribute to the formulation of national and senior military policy. At the tactical level, intelligence is oriented toward the specific area of operations and a given operation in greater detail. Intelligence, properly used and applied, can become a powerful force multiplier by providing the critical essential elements of information required to assist HSS staffs [5].

Intelligence requirements and requests for information

Intelligence required for medical planning and operations must be comprehensive, rapidly available, accurate and up to date. It can include information on:

- geographic factors such as effects of climate, topography, flora and fauna on health;
- epidemic and endemic diseases, their types and prevalence, local prophylactic measures, resistant strains, treatment;
- special environmental and occupational hazards such as radiation hazards, road movement hazards, pollution, toxic industrial hazards;
- CBRN capabilities of protagonists;
- military and civilian medical capabilities and resources available in the JOA (Joint Operations Area) [2].

Medical staffs are responsible for developing intelligence requirements in order to enable the intelligence staff to efficiently request, acquire, and disseminate the finished intelligence products

needed. Intelligence requirements are often categorized as either routine standing requirements or priority intelligence requirements (PIRs). Standing medical intelligence requirements are the recurring routine requirements for intelligence to be fulfilled in normal day-to-day strategic and operations planning. PIRs tend to be orientated to operational planning either for contingency or for crisis action planning. In the latter case, staffs develop and submit the most critical PIRs, usually just a few which are essential to plan development, and the formation of estimates. In either case, both standing requirements and PIRs are usually written in the form of questions about a specific topical area and can be used interchangeably. There will be times, especially during evolving crises, where intelligence is either insufficient or absent. In these situations, the medical planning staff will need to forward requests for information (RFIs) to the supporting intelligence staff. RFIs will usually be submitted in a format similar to a PIR, but should be very well defined, narrow in scope, and specific to a command mission or objective. Additionally the RFI must state the highest classification required and a workable time limit [2].

Types of medical intelligence

There are two types of medical intelligence:

- medical-tactical intelligence;
- sanitary-epidemiological intelligence [3].

Medical-tactical intelligence includes searching, collecting, evacuating injured, and deploying forces and means of medical service (the condition of the roads that are supposed to evacuate the injured, local vehicles that can be used by medical services).

Sanitary-epidemiological intelligence includes:

- detection of the presence and distribution of infectious diseases among the local population and personnel of enemy forces;
- collecting information on episodes of wildlife and pets;
- to clarify the capacity of local health authorities to carry out anti-epidemic measures;
- study of the sanitary and hygienic situation of the area where troops are deployed and where they will conduct combat operations.

It is impossible to exclude the possibility that the enemy could use a bacteriological weapon in modern war conditions. Such a situation also creates a need for bacteriological intelligence. Bacteriological intelligence is carried out in order to identify the enemy to be ready for the use of bacteriological weapons and to identify possible methods of its application, as well as timely detection of air, water, soil, food contamination by these means and determination of the type of bacterial weapon used.

Conclusion

Medical intelligence continues to preserve its role in the Armed Forces. It is carried out by all phases of medical care, starting from sanitary instructors in company to the Central Sanitary-Epidemiological Enterprise of the Armed Forces of the Republic of Azerbaijan. Medical intelligence is aimed at obtaining the necessary information to make a well-grounded decision that will ensure the successful conduct of the war. Climate, terrain, and local conditions have major impacts on the conduct and outcome of a war. That is why the medical intelligence report should include detailed information on climate, terrain, condition of water sources, water quality, flora and fauna, infectious diseases that are characteristic of the area, as well as medical system of enemy troops. Finally, all studies show that a well-prepared medical intelligence report will have a decisive impact on the outcome of a military operation.

References

1. Medical intelligence in a theater of operations / Headquarters Department of the Army. – Washington, DC: U.S. Government printing office, – 1989. – 47 p.
2. Allied Joint Doctrine for Medical Support. – Published by the NATO Standardization Office (NSO), – 2015. – 280 p.
3. Hərbi hissələrin döyüş fəaliyyətlərinin tibbi təminatının təşkili. – Bakı: Hərbi nəşriyyat, – 2009. – 312 s.
4. Birgitta, L. Medical and environmental intelligence in peace and crisis-management operations / L.Birgitta, W.Annica, S.Björn [et al.]. – London: Earthscan, – 2012. – 15 p.
5. Doctrine for Health Services Support in Joint Operations. – Joint Publication 4-02, – 1995. – 71 p.

Xülasə
Hərbi əməliyyatlarda tibbi kəşfiyyatın rolu və əhəmiyyəti
Əli Abduləzimov

Bu araşdırma müasir hərbi əməliyyatlarda tibbi kəşfiyyatın əhəmiyyətini təhlil edir. Məqalədə tibbi kəşfiyyatın təşkili qaydaları haqqında məlumat verilmiş və onun bütün növ hərbi fəaliyyətlərdəki əvəzolunmaz rolu göstərilmişdir. Tibbi kəşfiyyatın formaları, eləcə də tibbi kəşfiyyat məlumatlarının xarakteri və toplanma üsulları ətraflı açıqlanmışdır. Bundan əlavə, məqalədə qoşunların yerləşdiyi və döyüş əməliyyatları aparılacaq rayonun tibb xidməti tərəfindən öncədən nəzərə alınması zəruri olan xarakterik xüsusiyyətləri şərh edilir.

Açar sözlər: tibbi kəşfiyyat, kəşfiyyat hesabatı, kəşfiyyat tələbləri, səhiyyə sistemi, əməliyyatlar sahəsinin xüsusiyyətləri

Аннотация
Роль и значение медицинской разведки в военных действиях
Али Абдулазимов

Это исследование рассматривает важность медицинской разведки в современных военных операциях. В статье приводятся сведения о том, как организовать медицинскую разведку и показана ее неоценимая роль во всех видах военной деятельности. Были подробно раскрыты формы медицинской разведки, а также характер и методы сбора медицинской разведывательной информации. В статье изложены характерные особенности необходимости заблаговременного предусматривания медицинской службой особенности района расположения войск и прохождения боевых действий.

Ключевые слова: медицинская разведка, отчет разведки, требования разведки, система здравоохранения, характеристика района операций.

Məqalə redaksiyaya daxil olmuşdur: 02.10.2019
Təkrar işlənməyə göndərilmişdir: 06.11.2019
Çapa qəbul edilmişdir: 02.12.2019

UDC: 616.1

RISK OF THE CARDIOVASCULAR SYSTEM DISEASE IN ARMY PESONNEL

ScD, prof. Vasadat Azizov, Nigar Bayramova
Azerbaijan Medical University
Email: tomris007@yahoo.com

Abstract. In the paper, the comparison of cardiovascular health level between US Army personnel and civilians shows that a smaller portion of US Army personnel are in ideal cardiovascular health compared to civilians. Less than one-third of soldiers studied had ideal blood pressure compared to the civilian population, which account for 50%. Also, there have been presented the statistical results of investigations of a cardiovascular morbidity of the military personnel, observed by the medical services of EU countries and Serpukhov Institute for Russia Rocket Forces.

Keywords: cardiovascular, disease, Army serviceman, civilian populations.

Introduction

Cardiovascular disease (CVD) is the leading cause of death in the United States among both men and women, accounting for 1 in every 4 deaths annually. The active duty component of the US Army (hereafter, "Army") is afflicted more by CVD than by any other chronic disease. Moreover, CVD prevalence rates among active duty Army personnel have increased over the past decade (6.8% in 2007 versus 9.4% in 2014). Prevalence of risk factors associated with CVD, cancer, chronic respiratory disease, and other conditions has also increased in US military personnel in recent years. In 2011, active duty Army respondents reported the following: overweight or obesity 68%; cigarette use 27%; diagnosed high blood pressure (BP) 18%; and diagnosed high cholesterol 15%. Given the likely impact of these factors not only on potential military recruits but on medical readiness to deploy, CVD is a present threat to national security and poses significant financial costs to the military health system.

In this paper, there has been compared prevalence of 4 ideal cardiovascular health (CVH) metrics (current smoking, body mass index, blood pressure, and diabetic status) between a large sample of active duty US Army personnel and a corresponding subset of the civilian US population, from the National Health and Nutrition Examination Survey [1].

Statistic data results

Even at early adult ages, prevalence of ideal body mass index and blood pressure was strikingly low in both populations, suggesting the age-related decline in CVH shown in other studies has already adversely affected both Army and civilian populations of the ages of 17 to 29. Ideal CVH was even less prevalent in the Army, despite health-related exclusion criteria in Army recruitment.

The concept of CVH offers a promising new approach to this problem. The American Heart Association (AHA), in 2010, defined ideal, intermediate, and poor CVH in terms of 7 metrics and a 7- item composite score, comprising 4 modifiable health behaviors (current smoking, physical activity, diet score, and body mass index – BMI) and 3 health factors (systolic BP-SBP and diastolic BP-DBP), total blood cholesterol concentration, and fasting plasma glucose concentration). This reframing of the approach to reducing the population burden of CVD replaces the terms "risk behaviors" and "risk factors" with "health behaviors" and "health factors," respectively, shifting the focus to positive attributes and their promotion and preservation through primordial prevention strategies [2-5].

The choice of these metrics to define CVH was based, in part, on the supporting evidence: both long-term prospective population data showing better health, longevity, and quality of life with ideal CVH and intervention trials demonstrating modifiability of these 7 metrics. In addition,

corresponding data for each one would be available continuously for successive representative samples of the US population, through the National Health and Nutrition Examination Surveys (NHANES), permitting their ongoing surveillance for the civilian, non-institutionalized US population. On the basis of this definition, AHA adopted as its 2020 Strategic Impact Goal "to improve the cardiovascular health of all Americans by 20% while reducing deaths from cardiovascular diseases and stroke by 20%." Strategies to improve population CVH are potentially applicable to any population, including the US military.

The Army monitors service members' health to sustain a physically fit, combat-ready military force. This periodic assessment includes 4 of the 7 metrics now identified with CVH: smoking, BMI, BP, and diabetic status. Although some studies have compared CVD risk factors in the military, the status of military personnel in terms of this new concept, and how it compares to the CVH of civilians, is unknown. Therefore, there are determined the weighted age-standardized prevalence of each of these 4 CVH metrics in active duty Army personnel, in comparison with the US civilian population, represented by NHANES. Also, there are examined these data by sex, race/ethnicity, and age. Because of Army fitness standards, both at recruitment and after enlistment, it is hypothesized that ideal CVH would be more prevalent at every age in the Army than among civilians of comparable age [6-9].

There have been examined data for Army personnel, aged 17 to 64 years, who completed the Periodic Health Assessment in 2012. The Periodic Health Assessment monitors service members' medical readiness to deploy. Exclusions (aged ≥65 years or pregnant) yielded an analytic cohort of 263 430 active duty (full-time) service members. Army data were weighted to the estimated 2012 Army population of 497 490 active duty service members using age, sex, race/ethnicity, education, rank, service component, and deployment estimates and adjusting for nonresponse on the 2012 Periodic Health Assessment.

The data from US civilians, aged 17 to 64 years, from the 2011 to 2012 cycle of NHANES, a cross-sectional survey by the National Center for Health Statistics, Centers for Disease Control and Prevention, to monitor the health and nutritional status of the non-institutionalized US population have been examined. In NHANES, participants were interviewed at home and completed anthropometric and physiological examinations at a mobile examination center.

NHANES uses a complex, multistage probability design with oversampling of older people, Hispanics, blacks, Asian Americans, and low-income non-Hispanic whites. NHANES data are weighted using US population estimates (based on age, sex, race/ethnicity, and income) and adjusted for multistage sampling and response rates. There have been applied exclusions (aged ≥65 years or pregnant) to match those of the Army cohort. This yielded an analytic sample of 4797 civilians, which was weighted to an estimated US population of 198 146 000 civilians in the same age range [10, 11].

Measures

Demographic Characteristics. There have been obtained service members' demographic information (sex, age, race/ethnicity, educational attainment, and marital status) from the Defense Manpower Data Center (Seaside, CA). Civilian demographic information was assessed during the NHANES household interview.

Cardiovascular Health. 2 CVH behaviors (current smoking status and BMI) and 2 CVH factors (SBP and DBP and diabetes mellitus, presence or absence) have been examined. Each CVH metric was classified as ideal, intermediate, or poor using the closest possible consistency with AHA criteria when possible, modified when necessary. Army data as of 2012 were insufficient to assess the remaining 3 metrics: diet score, physical activity, and total blood cholesterol.

Smoking. Service members were asked "do you smoke any kind of tobacco products?" and categorized as ideal (if no) or poor (if yes). NHANES youth (aged <20 years) were asked "on how many of the past 30 days did you smoke a cigarette?" and categorized as ideal (if 0) or poor (if ≥1).

NHANES adults were asked “do you smoke cigarettes now?” and categorized as ideal (if not at all) or poor (if every day or some days).

Body Mass Index. BMI (weight/height, kg/m^2), calculated from clinical examination data for both Army personnel and civilians, was classified as either ideal (<25 kg/m^2), intermediate (25–29.9 kg/m^2), or poor (≥30 kg/m^2). Service member BMI was pulled from the Military Health System Data Repository or the Digital Training Management System when necessary to reconcile missing or out of range values.

Blood Pressure. SBP and DBP were recorded during clinical examinations in both populations. On the basis of a combination of SBP and DBP, there are categorized respondents' BP as ideal (<120/<80 mm Hg), intermediate (SBP, 120–139 mm Hg; or DBP, 80–89 mm Hg), or poor (≥140 or ≥90 mm Hg).

Diabetes Mellitus Status. Service members were asked “do you or have you ever had diabetes (mellitus)?” and categorized as either ideal (if no) or poor (if yes). NHANES participants were asked, “Other than during pregnancy, have you ever been told by a physician or other health professional that you have diabetes (mellitus) or sugar diabetes (mellitus)?” and categorized as ideal (if no, borderline, or prediabetes) or poor (if yes). Although this definition departs importantly from the AHA measure of fasting plasma glucose, it does permit comparison between Army and civilian populations with a relevant indicator of this factor.

The table presents demographic characteristics of the active duty Army group and NHANES group. There have been made statistical comparisons across the 2 study groups (active duty and civilian) and found statistically significant differences for each characteristic. The key weight-adjusted differences are described below (Table 1).

Table 1

Demographic Characteristics of US Army and NHANES Groups, 2011 to 2012

Characteristic	Active Duty Army personal (n = 263 430)	Active Duty Population (n = 497 490)
Age group, years		
17–29	149 166 (56.6%)	315 669 (63.5%)
30–39	77 612 (29.5%)	122 860 (24.7%)
40-49	33 269 (12.6%)	52 812 (10.6%)
50-64	3366 (1.3%)	6148 (1.2%)
Sex		
Men	224 761 (85.32)	442 358 (88.9%)
Women	38 669 (14.68)	55 132 (11.1%)
Length of service, years		
0-3	89 444 (33.95)	203 286 (40.9%)
4-8	64 203 (24.37)	116 241 (23.4%)
9-15	57 089 (21.67)	92 908 (18.7%)
> 15	52 694 (20.00)	85 055 (17.1%)

Among active duty service members, the youngest age category (17–29 years) heavily predominated in frequency (63%), whereas the population had only 27% in this category. The active duty Army group had few members in the 50 to 64 years category, whereas nearly one third of population participants were in this age range (1% versus 32%). The active duty Army group, but not the population group, was predominantly men.

Fewer Army personnel than NHANES participants (17% versus 63%) had more than a high school diploma or equivalent. Army personnel were more likely to have never married than NHANES participants (37% versus 23%) and less likely to be separated, widowed, or divorced (6% versus 16%). Among active duty Army personnel, 36% reported >8 years of service and 17% reported >15 years of service.

Active duty service members had slightly more frequent ideal status for smoking and diabetes mellitus and substantially greater frequencies of intermediate levels of BMI and BP than the NHANES group. In addition, although ideal BMI was fairly comparable across active duty service members and the NHANES group, ideal BP was substantially less prevalent among active duty Army personnel than among NHANES participants. In addition, although the age- adjusted prevalence of smoking was fairly comparable in both populations (≈20%), it was observed an unadjusted smoking prevalence among active duty personnel 17 to 29 years old of ≈30%, relative to just 23% among those 30 to 39 years old.

Discussion

Active duty Army personnel exhibited fewer favorable CVH metrics (classified as ideal versus intermediate or poor) than did NHANES participants, overall and within most sex, race/ethnicity, and age subgroups. This is the first study of CVH, as defined by the AHA, in Army personnel and compared with a US civilian population. Considering the Army's selective screening and policy of maintaining good physical and psychological health of Army personnel, it would be more favorable in the Army than the civilian population, at all ages. Contrary to our hypothesis, however, it is observed less ideal CVH in the Army relative to the NHANES group.

Demographics and Overall CVH. The estimated Army population of nearly 500 000 active duty individuals differed from the estimated NHANES population demographically in several key respects: younger; predominantly men; fewer Hispanics and more non-Hispanic blacks; and less post-high school education. There are compared the populations in terms of other measures of social disadvantage, which may be presumed to be more prevalent among Army recruits, a potential topic for further investigation. More than 55 000 women, 44 000 Hispanics, and 125 000 non-Hispanic blacks are included in the estimated Army active duty population, and it was estimated >85 000 individuals with >15 years of service longevity. Active duty Army personnel exhibited fewer favorable CVH metrics versus intermediate or poor than did the NHANES participants, overall and within most sex, race/ethnicity, and age subgroups.

In separate analyses comparing Reserve and National Guard personnel with NHANES civilians, it was found that aside from having less ideal BMI than NHANES civilians, the differences in CVH observed between active duty personnel and NHANES civilians in this study appear to extend to Reserve and National Guard personnel (data not shown). Future research should further examine differences between Army components and US civilians and examine whether factors, such as deployment history, are associated with differences in CVH between Army components.

Cigarette Use. Both active duty personnel and NHANES civilians exhibited current smoking rates of nearly 20%, with the exception of female and Hispanic service members (<15%). Studies of smoking behaviors among military personnel typically find either an elevated smoking prevalence or no difference when compared with civilian populations. In addition, the greater unadjusted smoking prevalence found among younger active duty personnel in this and other studies is particularly problematic given 17 to 29 year old service members (the age group with the greatest smoking prevalence) represent nearly two thirds of the active duty population. Many young service members report initiating smoking after joining the Army, and this could, in part, be because of substantially lower cigarette prices in military compared with civilian stores. Targeted Army interventions and population-based prevention strategies are needed to reduce the healthcare burden and economic impact of smoking behaviors, particularly among young service members.

Overweight and Obesity. This major public health problem afflicts the Army as well as civilians. Overall, only one third of active duty service members and civilians, but nearly half of female active duty personnel, demonstrated ideal BMI. This finding represents an opportunity to preserve ideal BMI for one segment of the active duty population, particularly given the increases in prevalence (unadjusted) of the poor category through the age of 49 years. Poor BMI was nearly twice as prevalent in civilians as in active duty personnel, suggesting selection against obesity in Army recruitment may account for an early relative advantage, but the effect is not sustained at older ages. Army training standards and demanding physical requirements may, in part, limit BMI increases in Army personnel, but not sufficiently to offset counterinfluences. In addition, as service members age and attain higher ranks, they typically move into staff positions, which tend to be more sedentary than in "line" positions within units (e.g., infantry). Study of measurement, determinants, and preventive strategies for excessive BMI in the Army is warranted.

Blood Pressure. Ideal BP was strikingly less prevalent among active duty Army personnel than among the NHANES group (30% versus 55%). This was unexpected considering military screening excludes recruits with elevated BP. Nevertheless, this pattern was consistent across race/ethnicity subgroups, although more pronounced among male rather than female active duty service members. Although this contradicts our hypothesis, other studies have also observed a high prevalence of prehypertension and hypertension in military personnel. Elevated BP readings may, in part, result from stressful military experiences, such as combat deployments, tobacco and alcohol use, or inconsistent dietary habits resulting from long work hours. Indeed, soldiers reporting multiple combat exposures are 1.33 times more likely to report hypertension compared with others. In addition, although NHANES civilians demonstrated a greater prevalence of ideal BP (55%), ample room for improvement remains in both active duty Army and civilians. These findings highlight the need to preserve ideal BP and reverse intermediate and poor BP through targeted intervention programs in both Army and civilian populations.

Diabetes Mellitus. Diabetes mellitus, although slightly less prevalent in active duty Army compared with NHANES, was rare in both populations. This disparity may be caused, in part, by selection against diabetes mellitus at entry to the Army; however, further investigation is needed. Consistent with previous research, ideal diabetes mellitus status was less prevalent among non-Hispanic black and Hispanic individuals and more prevalent among non-Hispanic white individuals. Given diabetes mellitus is associated with a wide range of serious medical conditions (e.g., heart disease, stroke, blindness, kidney failure, and coronary microvascular disease), prevention and management programs are needed to maintain ideal glucose levels in service members and civilians.

Statistical data in Russia

There are presented statistical results of investigations a cardiovascular morbidity, temporary disability, medical care organization in the military personnel, observed by the medical service of Serpukhov Institute for Russia Rocket Forces [12, 13]. A complex of social and hygienic methods was used: registry data selection, expert assessment of medical documentation, sociological survey (medical staff interview), and statistical analysis.

Cardiovascular disease are leading reason of death in the most of EU countries. But, in death structure, in accordance with World Health Organization (WHO) report [12] "Health level in Europe, 2003", if the level of death in developed West EU countries decreases and is 35–45%, that in Eastern Europe and Commonwealth of Independent States the part of death in result of circulatory system disease is 50–60%, and Cardiovascular disease is 20–21%.

Recently, there was observed some tendency to decreasing death in result of Cardiovascular disease, but Cardiovascular pathology is remain leading reason of death. Only in Russia, annually 1 million people die as a result of Cardiovascular disease, 429000 of them (30% of population: 80%-men) death in age able to work [14]. In Russia, in accordance with statistical reports of Defence

Ministry of Russian Federation, the cardiovascular disease and atherosclerosis are leading reasons of discharges and deaths of Army personals.

The level of health of soldiers is less than cadets and servicemen in duty one (age <30). This is due to various selection criterions of military service. Among of military servicemen <25 the vegetative vascular dystonia and inflammatory affection are reasons medical aid appealability. Among of military servicemen >25 high blood pressure and ischemic heart disease are dominated. The chronic form of high blood pressure and ischemic heart disease is 3,2%, for military servicemen of 25–55 ages is 16%. 4,4% of military servicemen have diastolic pressure ≥110 mm Hg.

Conclusion

In result of investigation of statistical data in US Army and Russia Armed Forces it can be concluded below.

Overall, ideal CVH in the Army is less prevalent than in the civilian population. This finding is surprising given the Army's selective health screening at entry, as well as the Army's policy commitment to physical and psychological fitness. More important, the low prevalence of ideal BMI and BP in both populations highlights a critical need for impactful efforts to promote, preserve, and improve CVH through both Army-based and nationwide behavioral and policy changes. Sex-specific analyses revealed differences in CVH were primarily between active duty Army men and civilian men.

Given men represent >80% of the Army, this difference in CVH could have important readiness and cost concerns for the Army. Preventive health interventions aimed at improving the BMI and BP of service members (particularly men) through physical activity and nutrition, for example, may yield substantial gains in CVH for the active duty force. Such efforts have the potential to improve military preparedness, CVH, and quality of life, while at the same time reducing healthcare costs.

In various age and professional profile groups of the military personnel, prevalence and structure of morbidity and temporary disability were not homogenous. Medical service organization features influenced temporary disability and morbidity levels. To optimize diagnostics and treatment process, it is necessary to develop Russian guidelines on diagnostics and management of patients with atypical or mildly manifested cardiovascular disease, whose working specialty requires initial and continuous professional selection.

References

1. Shrestha, A. Comparison of cardiovascular health between US Army and civilians / A.Shrestha, E.Tiffany, L.Loryana [et al.] // Journal of the American Heart Association, – 2019. 8, – p. 1-24.

2. Daviglus, M.L. Favorable cardiovascular risk profile in young women and long- term risk of cardiovascular and all- cause mortality / M.L.Daviglus, J.Stamler, A.Pirzada [et al.] // JAMA, – 2004. 292, p.1588-1592.

3. Calle, E.E. Overweight, obesity, and mortality from cancer in a prospectively studied cohort of U.S. adults / E.E.Calle, C.Rodriguez, K.Walker-Thurmond [et al.] // N Engl J Med, – 2003. 348, p.1625-1638.

4. Armed Forces Health Surveillance Center (AFHSC). Incidence and prevalence of select cardiovascular risk factors and conditions, active component, U.S. Armed Forces in 2003-2012. MSM R, – 2013. 20, p.16-19.

5. McGraw, L.K. A review of cardiovascular risk factors in U.S. military personnel / L.K.McGraw, B.S.Turner, N.A.Stotts [et al.] // J Cardiovasc Nurs, – 2008. 23, p.338–344.

6. Ommerborn, M.J. Ideal cardiovascular health and incident cardiovascular events: the Jackson Heart Study / M.J.Ommerborn, C.T.Blackshear, D.A.Hickson [et al.] // Am J Prev Med, – 2016, 51, p.502–506.

7. Dong, C. Ideal cardiovascular health predicts lower risks of myocardial infarction, stroke, and vascular death across whites, blacks and Hispanics: the Northern Manhattan Study/ C.Dong, T.Rundek, C.Wright [et al.] // Circulation, – 2012. 125, p.2975-2984.

8. Ford, S.E., Greenlund, K.J., Hong, Y. Ideal cardiovascular health and mortality from all causes and diseases of the circulatory system among adults in the United States // Circulation, – 2012. 125, p.987-995.

9. Fryar, C.D. Cardiovascular disease risk factors among male veterans, U.S., 2009-2012 / C.D.Fryar, K.Herrick, J.Afful [et al.] // Am J Prev Med, – 2016. 50, p.101-105.

10. Mirel, L.B. National Health and Nutrition Examination Survey: estimation procedures, 2007–2010 / L.B.Mirel, L.K.Mohadjer, S.M.Dohrmann [et al.] // Vital Health Stat 2, – 2013. 159, p.1-17.

11. Vie, L.L. The U.S. Army Person Event Data Environment: a military–civilian big data enterprise / L.L.Vie, L.M.Scheier, P.B.Lester [et al.] // Big Data, – 2015. 3, p.67-79.

12. Stupakov, I.N., Gerber, V.I. Cardiovascular morbidity in the military personnel // Cardiovascular therapy and prophylaxis, – 2005. 4 (2), – p. 12-17.

13. Rudchenko I.V. Noninvasive diagnostic of Russia NAVY personal pre-clinical atherosclerosis: / PhD dissertation, "Army-medical Academy" Defence Ministry of Russia / – Saint-Petersburg, – 2018. – 102 p.

14. Демографический ежегодник России. – стат. сб. Росстат. М., – 2015. – 263 с.

Xülasə
Hərbiçilərdə ürək-damar xəstələnmənin riski
Vəsadət Əzizov, Nigar Bayramova

Məqalədə ABŞ-nın hərbiçilərin və mülki əhalinin ürək-damar xəstəliklərin araşdırılması nəticəsində göstərilir ki, ürək-damar sisteminin vəziyyəti mülki əhalidə hərbiçilərə nisbətən yaxşıdır. Əsgərlərin cəmi üçdə birinin qan təzyiqi normaldır, halbuki mülki əhalidə bu göstərici 50%-a çatır. Bundan başqa, Avropa birliyi ölkələrində və Rusiyanın Raket Qüvvələrin Serpuhov İnstitutunda tədqiqata cəlb olunan hərbiçilərin ürək-damar xəstəliyinin statistik məlumatları təqdim edilmişdir.

Açar sözlər: ürək-damar, xəstəlik, hərbçi, mülki əhali.

Аннотация
Риск сердечно-сосудистых заболеваний у военнослужащих
Васадат Азизов, Нигяр Байрамова

В статье указывается, что в результате исследования сердечно-сосудистых болезней у военнослужащих и гражданских лиц США, состояние сердечно-сосудистой системы у гражданских лиц лучше, чем у военнослужащих. Меньше одной трети солдат имеют нормальное кровяное давление, в то время как у гражданских лиц этот показатель достигает 50%. Кроме этого, представлены статистические данные сердечно-сосудистых болезней у привлечённых к исследованию военнослужащих в странах Европейского союза и Серпуховском Институте Ракетных войск России.

Ключевые слова: сердечно-сосудистый, болезнь, военнослужащий, гражданское население.

Məqalə redaksiyaya daxil olmuşdur: 01.10.2019
Təkrar işlənməyə göndərilmişdir: 05.11.2019
Çapa qəbul edilmişdir: 10.12.2019

ELMİ MƏQALƏLƏRİN TƏRTİB EDİLMƏSİNƏ DAİR TƏLƏBLƏR

Təqdim edilən məqalələr jurnalın elmi istiqamətinə (hərbi-nəzəri elmlər, hərbi xüsusi elmlər, hərbi təbabət, milli təhlükəsizlik) uyğun, aktual elmi problemlərə aid tədqiqatların ilk dəfə dərc olunması üçün nəzərdə tutulmuş materiallara malik olmalıdır. Məqalələr üç dildə (Azərbaycan, rus və ya ingilis) təqdim edilə bilər.

Məqalə MS WORD mətn redaktorunda 12-lik Times New Roman şrifti ilə yığılmalı, sətirlər arası məsafə 1 olmalıdır. Məqalənin birinci səhifəsinin yuxarı sol tərəfində UOT (UDK) indekslər göstərilməlidir. Mətnin əvvəlində məqalənin adı, müəllif(lər) haqqında məlumat (onların adı tam şəkildə, elmi dərəcəsi, elmi adı və hərbi xidmətdə olanlar üçün hərbi rütbəsi), müəllif(lər)in işlədiyi müəssisə(lər) və həmin müəssisə(lər)in ünvan(lar)ı, müəllif(lər)in elektron poçt ünvan(lar)ı və telefon nömrələri qara rəngli qalın şriftlə verilməlidir. Bu məlumatlardan sonra üç dildə (Azərbaycan, rus, ingilis) 5–6 sözdən ibarət açar sözlər, daha sonra isə məqalənin yazıldığı dildə qısa xülasə (100 sözdən çox olmamaqla) göstərilməlidir. Xülasədə tədqiqat işinin mahiyyəti, müəllif(lər)in aldıqları elmi nəticələr, işin elmi cəhətdən yeniliyi, tətbiqi əhəmiyyəti və s. yığcam şəkildə öz əksini tapmalıdır.

Məqalənin mətni 6–10 səhifə (A4 formatında) həcmində olmalı, səhifələrdə isə bütün tərəflərdən 20 mm boş məsafə saxlanmalıdır. Səhifələrin nömrəsi səhifənin aşağı hissəsinin sağ tərəfində qoyulmalıdır. Cədvəllər, qrafiklər, diaqramlar, şəkillər və fotolar mətnin daxilində yerləşdirilməklə məqaləyə daxil edilə bilər.

Elmi məqalədə mövzu üzrə qısa təhlil verilməli, onun aktuallığı əsaslandırılmalı, həll olunmalı məsələlər açıqlanmalı və onların həlli yolları göstərilməli, əldə edilən nəticələr, işin elmi cəhətdən yeniliyi, tətbiqi əhəmiyyəti, iqtisadi səmərəsi və s. aydın şəkildə verilməlidir.

Elmi mənbələrə edilən istinadlar mətndə kvadrat mötərizədə verilməlidir (məsələn, [1] və ya [1, s.119]). Məqalənin sonunda verilən ədəbiyyat siyahısı istinad olunan ədəbiyyatların mətndəki ardıcıllığı ilə nömrələnməlidir. Ədəbiyyat siyahısında son 10 ildə nəşr edilmiş elmi məqalələrə, monoqrafiyalara və digər etibarlı mənbələrə üstünlük verilməlidir. İstinad olunan mənbənin biblioqrafik təsviri verilərkən Azərbaycan Respublikasının Prezidenti yanında Ali Attestasiya Komissiyasının "Dissertasiyaların tətbiqi qaydaları" barədə qüvvədə olan Təlimatının "İstifadə edilmiş ədəbiyyat" bölməsinin 10.2–10.4.6 bəndlərinin tələbləri əsas götürülməlidir.

"İstifadə edilmiş ədəbiyyat"dan sonra məqalənin adı, müəlliflər haqqında məlumat və xülasə (məqalənin yazıldığı dildən əlavə, yuxarıda qeyd edilmiş daha iki dildə) verilməlidir.

Müəllif(lər) məqaləni çapa tövsiyə edən kafedra və ya təşkilatın iclas protokolundan çıxarışı, məqalənin A4 formatında çap olunmuş nüsxəsini, məqalənin elektron variantı yazılmış CD və ya DVD diski, eləcə də məqalə müəllif(lər)i ilə əlaqə saxlamaq üçün telefon nömrələrini təqdim etməlidir.

Redaksiyaya daxil olmuş məqalələr anonim rəyçilərin rəyindən (2 müsbət rəydən) sonra sahə redaktoru və ya redaksiya heyətinin mütəxəssis üzvlərindən biri tərəfindən çapa tövsiyə olunacaq. Təqdim olunan məqalənin dərc olunmasından imtina edildiyi halda jurnalın redaksiyası yazılı şəkildə müəllifə imtina cavabı göndərəcəkdir.

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ НАУЧНЫХ СТАТЕЙ

Представленные для публикации в журнале статьи должны соответствовать научным направлениям (военно-теоретические науки, военно-специальные науки, военная медицина, национальная безопасность) журнала и содержать материалы отражающие результаты исследований научно-актуальных проблем, предназначенные для первичной публикации. Статьи могут быть представлены на одном из следующих языков – азербайджанском, русском или английском.

Статья должна быть подготовлена в редакторе MS WORD, шрифт Times New Roman – 12. Междустрочный интервал – одинарный. На левой верхней части первой страницы должны быть указаны индексы УДК (UOT). В начале статьи должны быть указаны в полужирным

черным шрифтом название статьи, сведения об авторе(ах) (полное имя, учёная степень, учёное звание) и воинское звание для военнослужащих, место работы с указанием адреса(ов), адрес электронный почты и номер телефона. Далее должны быть приведены ключевые слова на азербайджанском, русском и английском языках (состоящих из 5–6 слов), а затем краткая аннотация (не более 100 слов) на языке набранной статьи. В аннотации должны кратко отражаться сущность исследования, полученные научные результаты автора(ов), научная новизна работы, ее прикладное значение, и т.д.

Статья должна быть в объеме 6–10 страниц (в формате A4 машинописного текста). Поля страницы со всех сторон 20 мм. В статье могут быть размещены таблицы, графики, диаграммы, рисунки и фотографии.

В статье приводиться краткий анализ по содержанию работы, а также обосновывается актуальность темы, раскрывается решаемые задачи и указываются способы ее решения. Кроме этого, должны быть изложены полученные результаты, новизна работы, ее прикладное значение и т.д.

Ссылки на научные источники должны указываться в квадратных скобках (например, [1] или [1, с.119]). Указанный список литературы в конце статьи должен нумероваться в порядке последовательности цитируемой литературы в тексте. В списке литературы предпочтение должно отдаваться научным статьям, монографиям и другим надёжным источникам последних 10 лет.

Библиографическое описание цитируемого источника должно соответствовать требованиям раздела 10.2–10.4.6 “Использованная литература” положения “О правиле оформления диссертаций” Высшей Аттестационной Комиссии при Президенте Азербайджанской Республики.

После раздела “Использованная литература”, кроме языка, на котором написана статья, пишется название статьи, сведения об авторе(ах) и аннотация еще на двух других языках, указанных выше.

Автор(ы) вместе со статьей должен(ы) предоставить выписку из протокола заседания кафедры или учреждения рекомендовавшего ее для публикации, один экземпляр напечатанной статьи, его электронный вариант, написанный на диске CD или же DVD, а также контактные телефонные номера.

Поступившие в редакцию статьи после рецензирования (2 положительных заключения) по представлению редактора по специальности или одного из членов редакции будут рекомендованы в печать. При отказе печатать статью редакция журнала в письменной форме уведомит об этом автора(ов).

RULES TO COMPILE SCIENTIFIC ARTICLES

Artıcles, submitted to be published in this magazine must be appropriate to the norms and standards of researches being covered by this magazine (military theoretical sciences, military special sciences, military medicine, national security) The articles can be submitted in three (Azerbaijan, Russian and English) languages.

An article should be typed in MS WORD text edited in Times New Roman – with 12 shrift, 1 inter-line space. UDC (UOT) kind of indexes are to be put on the left of the top of the first page. The topic of the article, information about the author, (full name, scientific degree, scientific duty, military rank for servicemen), the names of the ventures where the authors work for, the address of the very ventures, authors’ e-mail account and phone numbers must be given in bald black colour. After this information, key words in three languages (Azerbaijan, Russian, English) consisting of 5–6 words, then abstract (no more than 100 words) in the language in which the article is produced are to be written. The essence of the study, scientific results got by author(s), scientific significance, practicality are to be briefly written in the abstract.

The text of the article is to be 6–10 pages (A4 format) and the dimension of the pages must be from all sides 20 mm. Numbering of the pages would be on the right side of the bottom of either page. Schemes, graphics, diagrams, pictures and photos may be included by inserting them in articles.

Brief analysis is to be given, the topicality of the subject is to be proved, the issues which are going to be solved must be clarified and the ways of the solution, the results, economic efficiency and etc. are to be clearly shown in a scientific article.

The references linked to the scientific sources, must be noted in bracket at the end of the sentence which is extracted from a source. (for example, [1] or [1, p.119]). The list of the reference at the end of an article is to be in sequence of the references within the article. The sources of latest 10 years should better be preferred in the reference list.

While giving the bibliographic description of the references, the requirements 10.2–10.4.6 "References" which is in force of "Rules for application of Dissertations" instruction of Supreme Attestation Commission of the Azerbaijan Republic attached to the President must be referred.

The abstract of the article is to be designed in two more languages besides the language, the article is written. The abstracts in various languages must appropriate to the content of the article. Scientific results, topicality for the subject, essence for applicability are to be reflected in the abstract. The abstracts must be seriously scientifically and grammatically edited. In either abstract, the full name of the article and the author must be put on.

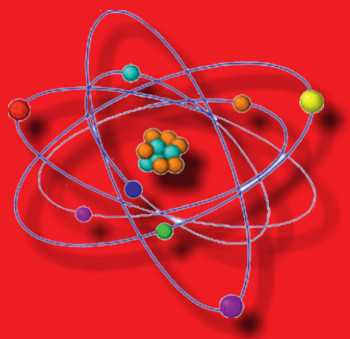
Contact number is to be noted at the end of the article to keep in touch with the author. While the author submits the article, an excerpt from a protocol of the organization or department where he or she works, a printed copy of the article, herewith a burnt digital copy on CD or DVD are to be handed over as well.

Only twice reviewed papers will be published in the journal after being considered by the editor. When paper is rejected then author will be informed about it.

Çapa imzalanıb 30.12.2019. Formatı 60x84 1/8. Fiziki ç.v. 12.

Silahlı Qüvvələrin Hərbi Akademiyasında çap olunmuş,
Hərbi Nəşriyyatın mətbəəsində cildlənmişdir.

Azərbaycan Respublikası Silahlı Qüvvələrinin Hərbi Akademiyası



№ 4(5)