UDC 623.41:355.40:355.356
DOI: https://doi.org/1034169/2414-0651.2025.1(45).29-38

O. O. HOLOVIN, *Doctor of Technical Sciences*
Senior Research Fellow
https://orcid.org/0000-0003-4662-4559

V. L. PALIY
https://orcid.org/0009-0008-0458-3289
(Central Scientific Research Institute of Armament and Military Equipment of Armed Forces of Ukraine, Kyiv)

ORGANIZATIONAL ASPECTS OF THE SYSTEM OF TECHNICAL INTELLIGENCE OF WEAPONRY AND MILITARY TECHNOLOGIES IN NATO COUNTRIES

The study and scientific-technical analysis of samples (fragments) of the enemy's military equipment (ME) is an integral part of maintaining the defense capability of the state and is critically important for effective defense and deterrence in modern conditions.

The article discusses the organization of scientific-technical and technical intelligence systems, as well as the technical operation of NATO countries. It shows the purpose of each of these processes, their components and the results to be achieved.

A typical list and content of reports formed as a result of the relevant studies are provided.

It is determined that, in modern conditions, the effective implementation of NATO approaches to scientific-technical analysis of samples (fragments) of the enemy's ME in Ukraine requires the development of an appropriate scientific-methodological framework for conducting research.

Keywords: *scientific-technical intelligence (S&TI), technical intelligence (TECHINT), technical operation (TO), weaponry and military equipment.*

Modern armed conflicts are characterized by the rapid development of technologies that constantly alter the balance of power on the battlefield.

The military aggression of the russian federation against Ukraine further demonstrates the high relevance of conducting scientific research on captured enemy weaponry (fragments left after their use). The results of these studies not only allow for the assessment of the enemy's technical capabilities but also help to identify their vulnerabilities, develop effective countermeasures and improve domestic military technologies.

The purpose of this article is to analyze approaches to conducting such research in NATO countries, determine their impact on military science and practice and justify the necessity of developing an appropriate scientific-methodological framework for the technical analysis of enemy weaponry and military equipment (ME) samples.

Modern weapon systems, such as UAVs, ballistic and cruise missiles and electronic warfare tools, which are actively used by the russian federation against Ukraine, highlight the exceptionally high pace of military technology development and the creation of new threats to Ukraine's defense forces in repelling armed aggression.

Consequently, the study and scientific-technical analysis of enemy ME samples (fragments) create opportunities for:

– identifying new technologies before they become widespread, enabling quick adaptation to changes on the battlefield while maintaining a technological advantage and more effectively countering new challenges;
– the evaluation of the combat effectiveness of enemy weaponry samples involves determining their actual technical characteristics (ATH), which may differ from those officially published;
– the development of effective methods for neutralizing enemy weaponry and countermeasures based on data regarding identified weaknesses in applied designs or technologies, as well as data on suboptimal technical decisions made by developers during the design of weaponry samples, is also crucial;
– moreover, the development and improvement of domestic weaponry can be achieved by integrating elements of enemy technologies into domestic systems;
– this process facilitates the operational decision-making of command on force deployment, strategy development and operation planning based on more accurate assessments of the enemy's intentions and strategies;
– furthermore, the identification of sources and supply channels of weaponry and its components to the enemy and the implementation of corresponding sanctions policies are also key outcomes of such studies;
– the evaluation of the technological potential of an enemy state and forecasting its further development, as well as identifying technological capabilities, such as the level of weaponry development, applied materials and components, as well as innovative solutions, are integral parts of these analyses;
– new tactical approaches in response to the capabilities of the enemy can also be formulated and collective security can be strengthened by pooling resources for conducting expertise and exchanging information between NATO countries and partner states, which ensures collective readiness to respond to new threats;
– the fight against the proliferation of dangerous technologies is another outcome, based on information about discovered technologies and materials that may pose a threat (such as chemical, biological, or nuclear weapons).

Thus, the study of weaponry samples (fragments) of the enemy is an essential part of maintaining the defense capability of the state and their relevance lies in ensuring technological, informational and strategic advantages, which are critically important for effective defense and deterrence in modern conditions.

In NATO, scientific research on captured enemy weaponry samples (fragments left after their use) is conducted within the framework of the existing intelligence system.

This is due to the fact that intelligence operations provide a comprehensive assessment of current and future threats, a systematic approach to analyzing samples by integrating data from various sources and ensure a thorough analysis and maximum effectiveness of using the obtained data to achieve NATO's strategic and tactical objectives.

According to the provisions of the Joint Intelligence, Counterintelligence and Security Doctrine [1], the components of this system (Fig. 1), within which the study of enemy weaponry samples (fragments) is carried out, include Scientific and Technical Intelligence (S&TI) and Technical Intelligence (TECHINT).

One component of TECHINT is Technical Exploitation (TE).

S&TI (strategic level of research) examines foreign developments in the field of fundamental and applied sciences, materials and technologies that may potentially be used for military purposes, specifically to improve weapon systems. S&TI is a critical component of national security, as the dynamic nature of modern warfare and the continuous evolution of threats require weapon systems to be adaptable to these threats and scalable [2, 3].

Within the S&TI process, based on the assessment, analysis and interpretation of foreign scientific-technical information, the characteristics of weapon systems, their capabilities, vulnerabilities, limitations, effectiveness and the industrial potential of countries are studied. R&D results, within which certain weapon systems and technologies for their production are developed, are also examined.

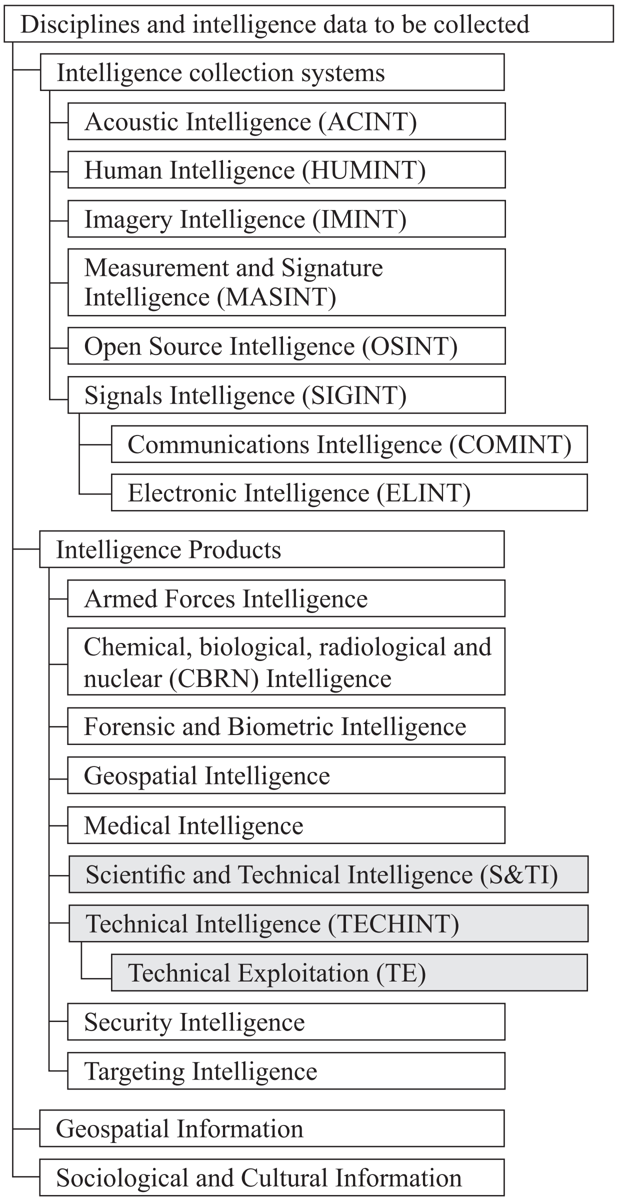
This area of intelligence also involves evaluating the scientific and technical achievements of the enemy and their potential for the development or improvement of domestic strategic technologies.

In addition, within the framework of S&TI, the creation of prototypes and their testing is carried out to accelerate the implementation of new technologies or capabilities into prospective weapon systems (WS). Examples of S&TI products include the characteristics of weapon systems, their capabilities, vulnerabilities, effectiveness and limitations regarding their use [4].

Thus, the results of S&TI are used to provide early warnings about foreign technological developments and capabilities, as well as to consider them when conducting domestic R&D for the development of weapon systems. TECHINT is a broad field of intelligence activity, encompassing the collection, analysis, forecasting, use and dissemination of information on technical devices, systems and equipment.

The Joint Publication 1-02 [5] defines TECHINT as intelligence data obtained through the collection, processing, analysis and use of information concerning foreign equipment and material means to prevent technological surprise, assess foreign scientific-technical capabilities and develop countermeasures to neutralize the enemy’s technological advantages.

Another definition of TECHINT is given in AAP-06 (NATO GLOSSARY OF TERMS AND DEFINITIONS (ENGLISH AND FRENCH)), which states: «Technical Intelligence – intelligence information regarding foreign technological developments, the effectiveness and operational capabilities of foreign material means, which have or may have practical military applications» [6].



F i g . 1. Main components of the intelligence system of NATO countries

The Joint Publication on Joint Intelligence JP 2-0 [7] defines TECHINT as intelligence data obtained through the use of foreign materials for strategic, operational and tactical level command. Accordingly, the aim of TECHINT is to assess the enemy's potential and vulnerabilities in their technology, as well as to provide baseline data for long-term planning and forecasting.

The mission of TECHINT involves [8]:

– preventing the unpredictable development of enemy technologies and maintaining a technological advantage over them;
– providing intelligence data to the command to improve awareness of the enemy and develop protective measures for own forces;
– developing and applying effective measures to target the enemy's weapon systems;
– ensuring individual, timely and precise TECHINT support for personnel throughout the entire spectrum of military operations;

– conducting technical intelligence and assessing the technical capabilities of the enemy.

During combat operations, the TECHINT mission also involves the exploitation of captured or transferred enemy weaponry and accompanying documentation. TECHINT is a valuable tool for supporting the actions of unit commanders, as it enables early identification of the enemy's technical capabilities, vulnerabilities and intentions and facilitates the rapid development of countermeasures.

Since the enemy may temporarily achieve technological parity or superiority by acquiring modern weapon systems or acquiring certain capabilities, a coordinated TECHINT program is crucial to ensure the rapid and effective neutralization of this parity or advantage within the scientific-research process.

TECHINT includes the evacuation, identification, collection, evaluation and use of captured enemy equipment in accordance with technical intelligence requirements.

The process of executing TECHINT operations in a multidomain environment begins at the service level. Ground forces and the Air Force have specialized TECHINT units to support weapon system capture operations and analysis. Additionally, each service has TECHINT personnel who provide support and expertise on matters related to activities in this field.

Unified teams play an important role in implementing TECHINT tasks. Each joint command must have an officer within the intelligence staff (J-2) responsible for planning TECHINT and coordinating activities with national intelligence analysis centers and the joint staff.

NATO has a clearly structured approach to studying captured enemy weaponry samples. This process encompasses several key stages that help gather valuable information on enemy military technologies. Fig. 2 presents the TECHINT process algorithm.

Sample collection and transportation

– *sample capture (removal of munitions samples from the battlefield by specialized units);*
– *initial on-site inspection (expert assessment of the condition and potential value of the samples for further research);*
– *cataloguing (registration and description of each sample in order to avoid loss of information);*
– *packaging and transportation to specialized laboratories or NATO intelligence centers for further analysis, observing strict security measures*

→

Initial Assessment

– *preliminary examination of samples to determine their condition, functionality and potential value for research;*
– *determination of the basic characteristics, type and possible origin of the sample*

↓

Detailed physical and technical analysis

– *materials* studies including chemical studies of the materials from which the sample is made to determine its strength, impact resistance and potential weaknesses;
– *mechanical* analysis (study of the structure, moving parts and working mechanisms of the sample);
reverse *engineering:*
– *disassembly of the sample to create detailed drawings, technical diagrams and models; analysis of innovations that can be used to create or modernize your own samples of EW;*
physical analysis:
– *a thorough examination of the physical aspects of the sample (materials, mechanisms, size, weight, etc.);*
– *spectral analysis, radiography, electron microscopy to identify the materials used and production processes;*
functional analysis:
– *(testing samples for operability, which may include testing individual components (e.g., engines, electronics) in conditions that simulate real-world conditions;*
– *studying the tactical capabilities and effectiveness of samples;*
electronic analysis:
– *studying the software and electronic systems that can be integrated into the sample (radar systems, sensors, communications and other electronic components);*
– *analysis of codes, network protocols and possible vulnerabilities for their further use or suppression;*
– *cybersecurity assessment* (possible vulnerabilities that can be used to neutralize enemy systems)

↓

Data analysis and interpretation

– *comparative analysis of the studied sample with those available in NATO databases;*
– *analysis of the obtained data regarding the impact on NATO military strategies*

→

Generation of reports and recommendations

– *compiling a report with conclusions on the technical and tactical characteristics of the sample, its strengths and weaknesses;*
– *developing recommendations for improving its own technologies or creating new weapons systems;*
– *substantiating measures to counter specific types of weapons*

↓

Information exchange

– *the transfer of information to strategic and operational units, which use it to plan operations and improve military technology;*
– *the transfer of research results to NATO and allied command through centralized data exchange systems*

F i g . 2. TECHINT algorithm

A variety of approaches are used in the TECHINT process, each of which is aimed at the most effective collection, analysis and use of technical information. The main ones are shown in Fig. 3.

The movement of captured weapons samples between institutions and military command bodies in NATO countries is carried out according to a strictly regulated procedure. This process includes several stages and ensures the most effective use of the obtained data for operational, technical and strategic purposes.

Thus, at the first stage, after the capture of a weapon sample by military units or specialized teams, its identification (determination of the type and condition of the sample, assessment of its value), documentation (photography, description of technical characteristics and registration) and marking for transportation are carried out.

Next, the samples are transported to operational analysis centers (national intelligence centers) for initial technical analysis (checking for hidden explosive devices and means of self-destruction, obtaining initial data on the functioning of the system, analysis of software and data that may be stored in the system).

At the next stage, the samples are transferred to specialized laboratories or research institutions for detailed scientific and technical analysis. The direct process of moving TECHINT data from the teams that captured EW samples to national intelligence centers is shown in Fig. 4.

The result of TECHINT can be strategic reports, analytical assessments, forecasts or recommendations.

Reports on the results of the analysis are provided to national intelligence centers. If the sample is of strategic importance, then for coordination with other NATO member states, the results of the analysis are transmitted to the general structures of the Alliance, in particular the NATO Intelligence Fusion Centre (NIFC), the NATO Communications and Information Agency (NCIA) and the Science and Technology Organization (STO).

During combat operations, the operation of captured or transferred enemy weapons and accompanying documentation is added to the TECHINT mission. Priority in the evacuation of captured munitions is given to radio-electronic systems and means of communication, ammunition and explosives, technical documentation (firing tables, logbooks,

Approaches to the study of captured enemy munitions used by NATO

Multidisciplinary approach (integration of different types of intelligence)

Phased approach:
– collection and initial assessment phase (detection and recovery of samples on the battlefield, initial inspection and assessment of threat or value);
– in-depth analysis;
– testing phase (testing samples in conditions simulating real combat situations);
– reporting and data sharing phase (compiling analytical reports and disseminating results to allies)

Reverse engineering:
– disassembling a sample into components to study their design, operating principles and materials;
– creating accurate technical models to identify strengths and weaknesses;
– using the data obtained to develop or upgrade your own weapons

Materials and manufacturing technology analysis:
– study of the materials from which the sample is made to identify unique alloys or manufacturing technologies and assess the enemy's industrial potential;
– materials analysis to identify technologies that can be applied to improve one's own samples

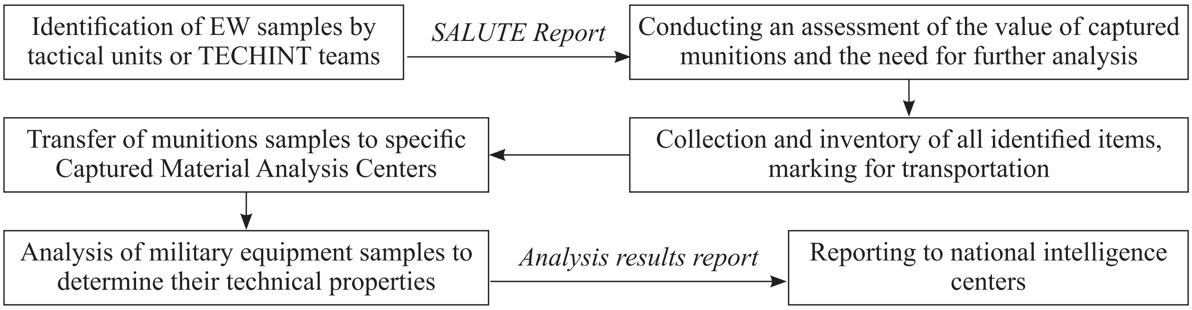
Functional analysis and modeling:
– studying the functioning of the sample in real conditions;
– modeling and simulation (using digital models to test the effectiveness of the sample in various scenarios and determine tactical advantages and disadvantages)

Comparative analysis:
– comparison of samples with known weapons samples available in NATO databases;
– analysis of innovations used in samples compared to existing analogues

Threat assessment and development of countermeasures:
– based on the analysis of possible threats to NATO forces;
– development of recommendations for improving protection against this type of weapon and using the vulnerabilities of the model to neutralize its effectiveness

International information sharing:
– dissemination of research results through NATO data sharing networks;
– allowing Allies to quickly integrate the knowledge gained into their defense strategies

F i g . 3. Approaches to the study of captured enemy munitions samples



F i g . 4. The process of moving TECHINT data from teams that captured EW samples to national intelligence centers

technical descriptions and operating instructions for munitions).

Data obtained through TECHINT is an important component of Joint Intelligence, Surveillance, and Reconnaissance (JISR). Within NATO, this concept involves the integration of different sources and types of intelligence to obtain a complete understanding of the battlefield situation and support decision-making at the operational and strategic levels.

TECHINT complements other types of intelligence, such as SIGINT (signals intelligence), IMINT (imaging intelligence), HUMINT (human intelligence) and provides deeper technical analysis, which increases the overall effectiveness of JISR and the speed of response to threats.

Data obtained through TECHINT also contribute to the formation of tactical and strategic lessons that are taken into account during exercises and operations, which is an integral part of the Lessons Learned processes. TECHINT results allow for the improvement of tactical techniques and the introduction of innovations in weapons models, which provides NATO with the ability to adapt to rapidly changing technological challenges [9, 10].

TECHINT is also linked to NATO's defense planning processes (NATO Defense Planning Process, NDPP), in particular:

TECHINT provides critical information for identifying technological threats that may arise from potential adversaries, which is taken into account in the NDPP when developing requirements for new weapons systems or modernizing existing ones;

data obtained through TECHINT is used in developing capability requirements, namely when determining the technological needs of the NATO defense system to effectively counter new threats.

Thus, TECHINT is integrated into numerous NATO processes, which allows the alliance to quickly adapt to new technological challenges. According to the above algorithm, various institutions and bodies are involved in S&TI, TECHINT and TE in NATO countries, in particular:

in the USA:

Defense Intelligence Agency (DIA) – conducting S&TI and TECHINT on the latest weapons and technologies of the enemy;

National Security Agency (NSA) – TECHINT related to electronic communications;

Central Intelligence Agency (CIA) – S&TI on assessing the scientific and technical capabilities of other states;

National Ground Intelligence Center (NGIC) – research on ground weapons (armored vehicles, air defense systems, artillery);

Naval Surface Warfare Center (NSWC) – research on naval weapons, captured ships, submarines and their systems;

Air Force National Air and Space Intelligence Center (NASIC) – research on aviation equipment, captured aircraft, drones and air defense systems;

in the UK:

Defense Intelligence (DI) – organization of military intelligence, including S&TI and TECHINT;

Government Communications Headquarters (GCHQ) – provision of technical intelligence in the field of cybersecurity and electronic intelligence;

Defense Science and Technology Laboratory (DSTL) – research on the technological complexity of captured weapons samples;

Intelligence, Surveillance and Reconnaissance (ISR) – implementation of TECHINT of captured equipment and its electronic systems;

Defense Equipment & Support (DE&S) – coordination of technical analysis of captured weapons;

In Germany:

Bundesnachrichtendienst (BND) – performance of S&TI tasks, in particular in the field of industrial and technological intelligence;

Amt für den Militärischen Abschirmdienst (MAD) – TECHINT;

Bundeswehr Technical Center (Wehrtechnische Dienststellen, WTD) – TECHINT;

Bundeswehr Geoinformation Center – study of navigation and communication systems of captured equipment;

In France:

Direction Générale de la Sécurité Extérieure (DGSE) – conduct of external intelligence, including S&TI;

Direction du Renseignement Militaire (DRM) – performing military intelligence tasks, including TECHINT;

Direction Générale de l'Armement (DGA) – conducting TE of captured weapons, their technological and combat capabilities;

Centre de Recherche et d'Études en Aérospatiale et Défense (CREAD) – research into aerospace systems and air defense;

in Canada:

Canadian Security Intelligence Service (CSIS) – conducting scientific and technical intelligence in the context of threats to national security;

Communications Security Establishment (CSE) – TECHINT in the field of information security;

Defense Research and Development Canada (DRDC) – research into captured equipment for the adaptation of new technologies;

Canadian Forces Intelligence Command (CFINTCOM) – S&TI of captured weapons systems.

A narrower and more practical TECHINT process focused on obtaining and using materials and technologies for further exploitation is Technical Exploitation [11, 12].

The term TE is used as a universal one, reflecting the full complexity of the approach and covering [12]:

analysis and assessment of the technical characteristics of EW samples;

development of countermeasures;

integration of results into future military operations;

potential use of captured samples in one's own interests.

The process of technical analysis involves the application of scientific methods to gain additional knowledge and understanding of information about material assets, which allows commanders and staffs to obtain reliable data about the operational environment. Material assets can include documents, electronic components and media, weapons, explosives and other relevant materials [12].

The main principles of technical analysis are as follows [11]:

clear, consolidated process management and control through the Joint Intelligence Staff (CJ2), coordination of technical operations activities with other personnel elements and units;

preservation of personnel lives (awareness of risks and weighing them against the value of information that can be obtained from operations activities);

preservation of material assets (using optimal documentation methods and procedures that are least invasive and destructive);

high-speed technical operation processes that allow for rapid dissemination of critical information and materials;

introduction of a methodology and system for sorting and prioritizing material assets based on their importance and the safety of personnel;

management of the organization's information resources by processing knowledge obtained by one or many different individuals and institutions for the purpose of exchanging information with NATO and other partners, archiving data.

Technical analysis is carried out at three levels [11, 12]:

field/tactical level, considered in [12];

theater level (operational);

strategic level (outside theater level).

TE tasks within the framework of defined capabilities at the strategic level are reflected in [11].

Thus, the S&TI, TECHINT and TE processes are determined by different tasks of military technical intelligence, in particular:

S&TI focuses on the analysis of scientific and technical aspects of potential threats, which includes the study of technologies, scientific research, engineering developments and technical capabilities of the enemy and covers the processing of a wide range of scientific and technical information and the analysis of scientific and technical innovations that are important for national security;

TECHINT includes various aspects of technical intelligence, from the study of technological systems to innovations, with a special emphasis on military and strategic applications in order to assess the potential and vulnerability of enemy technologies, as well as develop countermeasures strategies;

TE focuses on the in-depth analysis of specific physical objects or materials in order to obtain detailed technical information about them for operational and strategic use [12]. An important task that is solved in the course of S&TI, TECHINT and TE is the formation of relevant reports based on the results of research. At the moment, there is no standard document in NATO that would regulate the structure of reports developed based on the results of research [12].

However, a typical list of technical intelligence reports and their content can be presented as follows [8]:

1. SALUTE (size, activity, location, unit/uniform, time and equipment) report.

This report is compiled by tactical units or TECHINT teams and is used to quickly report on the capture of enemy materials.

The SALUTE report contains data on:

the number and type of captured enemy EW samples;

the circumstances of the capture;

the location (coordinates) of the capture;

the presence of camouflage, tactical signs, markings, inventory number and series on the sample;

the unit that captured the EW sample;

the date and time the EW sample was discovered;

additional equipment and ammunition that was captured together with the EW sample.

2. Preliminary technical report (PRETECHREP) – a preliminary technical report.

PRETECHREP contains the following data:

the type of captured equipment and its quantity;

date and time of capture;

location (coordinates) of capture;

unit that carried out the capture and circumstances of capture;

enemy formation from which it was captured;

brief description of the captured munitions with serial numbers;

important technical characteristics and photographs;

time of sending the Report;

current location of the captured munitions.

Also, when forming PRETECHREP, the report must include data on all radio frequencies of communication equipment, serial markings of equipment and combat damage caused by the captured munitions.

3. Complementary technical intelligence report (COMTECHREP) – Additional technical intelligence report.

COMTECHREP contains a more detailed description of the captured munitions than PRETECHREP and informs Research Centers and tactical units about the significant detailed technical information received.

Thus, the Report contains data on:

the design of the sample (dimensions, materials, production technology), key components, schemes or drawings;

unique or innovative technical solutions;

comparison with similar systems of our own production or samples of allies;

evaluations of functional characteristics obtained from test results;

evaluations of the effectiveness of the sample in combat conditions;

identified vulnerabilities and shortcomings;

the potential for using the enemy's technologies in our own defense sector;

proposals for creating our own technologies based on captured ones, or improving existing ones;

analysis of the enemy's technological base;

possibilities for creating countermeasures or using technologies to modernize our own systems.

4. Multi-service complementary technical intelligence report (MULTI-SERVICE COMTECHREP) – multi-service additional technical intelligence report.

This report is submitted as soon as possible and is used to report on all items that are not related to explosive ordnance.

The following is an example of a multi-service COMTECHREP:

date and location of the sample (map coordinates);

type of equipment captured and its quantity;

origin of the sample;

description of the sample with external features;

condition of the equipment;

technical characteristics of immediate tactical significance (additional details);

recommendations for disposal;

nameplates with photographs;

other information;

tasks of the TECHINT collection group performing this initial analysis;

time of sending the report.

5. Complementary technical intelligence report – type B (COMTECHREP – TYPE B) – Complementary technical intelligence report – type B.

COMTECHREP – type B is used to report on detected explosive ordnance. This report should be as complete and detailed as possible.

The table of contents should include the following elements:

date and location of capture;

country of manufacture, designations and identification marks;

description;

overall length including fuse and dimensions of tail, blades, control surfaces and fittings measured in various states;

maximum diameter of each element;

description of shape, design and internal configuration (streamlines);

span of blades and control surfaces;

number, relative position and dimensions (width, length) of control surfaces;

thickness of hull (nose, skids, main body);

type and materials of hull and control surfaces;

color and marking (nose, main body, tail and blades;

weight (with fuel and empty);

nature of filling, e.g. submunitions or solid charge;

method of application, e.g. spray or airburst;

description of warhead (if any), material and its geometric dimensions;

type of missile guidance system and methods of its stabilization in flight;

values of frequencies used for targeting;

description of non-contact detonator (if any);

electronic countermeasure system and equipment for scattering dipole reflectors (if any);

description of seeker and its design;

diameter of fairing and dimensions of seeker antenna (if any);

dimensions (internal and external) of waveguides in the homing head, as well as waveguides and/or antennas in the wings or hull, description of the technology used;

shape and dimensions of the torpedo, method of movement and propeller data;

system detonation, fuze system (nose, tail or cross) and details of the triggering mechanism;

type of suspension, with details of devices used, such as electrically operated shrouds or release mechanisms;

other information (including an estimate of the time required to prepare the object for shipment to a technical intelligence center or designated industrial facility for detailed analysis);

name of the officer in charge of the technical team conducting the investigation;

time of notification;

time required to complete the investigation;

preliminary set of photographs to be sent with the report.

6. Nine line unexploded ordnance/improvised explosive device spot report – Nine line report on the detection of explosive objects (unexploded ordnance / improvised explosive devices).

In the event of the detection of mines, explosives or other explosive objects, a report must be made to the tactical operations center in the following format:

date and time of detection of the object;

reporting organization (unit identification code) and location of the detected object;

means of communication (radio frequency, call sign, contact person and telephone number);

type of munition (dropped, launched, installed or thrown), dimensions of the danger area (if known), number of objects, details of size, shape, color and condition (intact or damaged);

presence of chemical, biological, radiological or nuclear contamination;

equipment, facilities or other assets that are at risk in the event of an explosive object being detonated;

description of the current tactical situation (the impact of the presence of an explosive object on the task);

description of the measures taken to protect personnel and equipment;

recommended priority for the response of demining technicians or engineers.

7. Detailed technical report (DETECHREP) – detailed technical report.

Information about the structure of the report is not available in open publications, since it is usually classified. However, in the USA, such a report is prepared at the Center for Military Equipment Operations (CMEC) with the assistance of scientific and technical information (S&TI) analysis personnel and is sent to the units responsible for organizing the examination (S&TI) and its abbreviated version – to the units directly conducting combat operations.

8. Technical intelligence summary – a summary report of technical intelligence.

This report is formed on the basis of the results of the analysis of several captured samples of munitions that affect tactical operations within a certain theater of operations. Information for the report comes from preliminary technical reports (PRETECHREPs) and technical communication reports (COMTECHREPs), which are collected over a period of time or from a large technical information collection facility.

9. Technical intelligence report (TIR) – Technical intelligence report.

A TIR is a critically important report that is sent to the highest levels of the intelligence hierarchy and is always classified. The report is based on information from preliminary technical reports (PRETECHREPs), additional reports (COMTECHREPs) and detailed technical reports (DETECHREPs).

Thus, it can be stated that the results of S&TI, TECHINT and TE are of critical importance for ensuring national security, technological leadership and competitiveness of the state, as well as for adapting to rapidly changing challenges.

The main areas of use of these results include:

assessment of threats and potential of the enemy (analysis of military technologies, weapons, tactics and strategies of the enemy);

integration of identified modern technologies into promising weapons;

creation of technologies for protection against enemy weapons;

determination of priorities for the development of new weapons systems and technologies;

assessment of technical achievements of other countries to predict the development of critical technologies in the world and the formation of key directions of technological development of the state.

Given the content of the reports, it can be concluded that their formation requires the use of an interdisciplinary approach, in particular, the involvement of specialists from various fields: engineers, analysts, cryptographers, electronics specialists and others. Also, the reports should integrate data from various sources: intelligence, technical tests, open sources (OSINT), etc.

Currently, research is being conducted to improve the structure of S&TI, TECHINT and TE reports, in particular, in [12] the structure of a TE report at the strategic level is proposed.

It should be noted that Ukraine has not yet created an effective system of intelligence agencies and research institutions, like the leading NATO countries, which complicates the conduct of S&TI, TECHINT and TE in the conditions of armed aggression of the russian federation against Ukraine.

At the same time, the key factor influencing the effectiveness of S&TI, TECHINT and TE tasks is the coordination of actions of personnel, teams and units.

Thus, during the Martial Vision exercises, it was established that the absence of a coordination group with TE (Technical Exploitation Coordination Cell) creates an «information vacuum» regarding technical exploitation within J2, which requires the formation of a command and control (C2) system for technical exploitation with support for all relevant processes [13].

The specified system should provide [13]:

coordination and centralized management of all stages of technical exploitation, starting from the collection and identification of collected materials suitable for analysis and ending with the analysis of the obtained results;

effective interaction between different units and performers;

rapid dissemination and coordination of information;

adoption of coordinated decisions and ensuring optimal allocation of resources;

processing of results in accordance with the priority of tasks and established security protocols;

increasing the reliability of the classification of collected materials;

reducing the risks of duplication of efforts or loss of important data (all participants have access to up-to-date information and commanders and analysts can quickly respond to changes in the situation).

Such centralized management should be implemented within a single information space. At the same time, the integration of all source data used in conducting S&TI, TECHINT and TE is proposed to be implemented by using network-centric cognitive IT tools built on the principles of ontology engineering. The ontology structure will allow reflecting specific aspects of the specified information environment by creating information descriptions based on an object-oriented formalization procedure and descriptions of interpretative functions that control the process of supplying an information resource and will also simplify information processing [14].

Also, effective implementation of tasks for conducting scientific and technical expertise of enemy weapons (weapon fragments) is possible through the use of large language models [12] and ontological engineering methodology [15]. At the same time, to ensure the efficiency, reliability and standardization of the analysis process within the framework of S&TI, TECHINT and TE, there is a need to develop an appropriate scientific and methodological apparatus (SMA) for the technical analysis of enemy munitions samples.

The specified SMA should ensure:

unification of processes, in particular the use of unified approaches to data collection, processing and interpretation;

increasing the reliability of research by minimizing errors in the process of data collection and analysis;

implementing transdisciplinary approaches to processing the results of munitions analysis [16];

increasing the efficiency of research by prioritizing tasks and optimizing the expenditure of time, human and material resources.

It is precisely on the development and implementation of the specified SMA that further scientific research will be directed.

REFERENCES

1. NATO AJP-2. Allied Joint Doctrine for Intelligence, Counter-intelligence and Security. Ed. A. Version 2. February 2016. 90 p.
2. Joint Doctrine Publication 2-00 (JDP 2-00), Intelligence, Counter-intelligence and Security Support to Joint Operations. Ed. 4. The Ministry of Defence of UK. August 2023. 181 p.
3. Changing role of Military Scientific and Technical Intelligence (S&TI). [Online]. Available at: https://idstch.com/security/changing-role-of-military-scientific-and-technical-intelligence-sti/. (Accessed 09 January 2025).
4. Air Force Doctrine Publication 2-0, Intelligence. Ed. 4. U.S. Air Force. June 2023. 37 p.
5. The Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms. U.S. Army. February 2013. 506 p.
6. NATO Glossary of Terms and Definitions (English and French), AAP-06. NATO Standardization Office. November 2019. 299 p.
7. Joint Publication 2-0, Joint Intelligence. U.S. Army, October 2013. 143 p.
8. TECHINT, Multi-Service Tactics, Techniques, and Procedures for Technical Intelligence Operations. FM 2-22.401/NTTP 2-01.4/AFTTP(I) 3-2.63. U.S. Army. June 2006. 84 p.
9. The NATO Lessons Learned Handbook. Ed. 4. NATO, Joint Analysis and Lessons Learned Centre. June 2022. 58 p.
10. Joint Intelligence, Surveillance and Reconnaissance. [Online]. Available at: https://www.japcc.org/chapters/c-uas-joint-intelligence-surveillance-and-reconnaissance/. (Accessed 09 January 2025).
11. NATO AIntP-10. Ed. A. Version 1. Technical Exploitation. NSO. September. 2015. 64 p.
12. Slyusar, V.I., Sotnyk, V.V. & Chepkov, I.B. (2024). “Metodolohiia doslidzhen system ozbroiennia: teoretychni ta praktychni aspekty” [Weapon systems research methodology: Theoretical and practical aspects], Weapons and Military Equipment. № 3 (43). Pp. 3—8. https://doi.org/1034169/2414-0651.2024.3(43).3-8.
13. Slyusar, V.I. (2024). “Zvit za rezultatamy uchasti predstavnykiv Zbroinykh Syl Ukrainy u zasidanni Hrupy tekhnichnoho analizu NATO (NTEG, AC/343) (10–11 hrudnia 2024 r. u shtab-kvartyri NATO, m. Briussel, Belhiia)” [Report on the results of the participation of representatives of the Armed Forces of Ukraine in the meeting of the NATO Technical Exploitation Group (NTEG, AC/343) (December 10-11, 2024 at NATO Headquarters, Brussels, Belgium)]. K.: CSRI AME AFU. 9 p.
14. Holovin, O.O. (2018). “Yedynyi informatsiinyi prostir – osnova efektyvnoi realizatsii pryntsypiv prohramno-tsilovoho planuvannia rozvytku ozbroiennia ta viiskovoi tekhniky” [Single information space as a basis of effective implementation of the principles of program-target planning for the development of armaments and military equipment], Science and technology of the Air Forces of Ukraine. № 2(31). Pp. 41—46. https://doi.org/10.30748/nitps.2018.31.04.
15. Chepkov, I.B., Stryzhak, O.E., Sotnyk, V.V. & Potapov, H.M. (2022). “Naukovo-metodychnyi aparat doslidzhennia trofeinykh zrazkiv ta ulamkiv ozbroiennia ta viiskovoi tekhniky rosiiskoi federatsii” [Scientific and methodological apparatus for the study of trophy samples and fragments of weapons and military equipment of the russian federation], Weapons and Military Equipment. № 1 (33). Pp. 12—22. https://doi.org/1034169/2414-0651.2022.1(33).
16. Holovin, O.O. (2019). “Zastosuvannia metodolohii transdystsyplynarnykh ontolohii v informatsiino-analitychnii systemy pidtrymky protsesiv osnashchennia ozbroienniam ta viiskovoiu tekhnikoiu” [Application of methodology of transdisciplinarity ontology in information-analytical system for support processes with equipping of armament and military equipment], Systems of Arms and Military Equipment. № 3(59). Pp. 17—24. https://doi.org/10.30748/soivt.2019.59.02.

Головін О. О., Палій В. Л.

ОРГАНІЗАЦІЙНІ АСПЕКТИ СИСТЕМИ ТЕХНІЧНОЇ РОЗВІДКИ ОЗБРОЄНЬ І ВІЙСЬКОВИХ ТЕХНОЛОГІЙ У КРАЇНАХ НАТО

Вивчення та науково-технічний аналіз зразків (фрагментів) озброєння та військової техніки противника є невід'ємною частиною підтримки обороноздатності держави та є критично важливим для ефективної оборони і стримування в сучасних умовах. В статті розглянуто організацію систем науково-технічної та технічної розвідок, технічної експлуатації країн НАТО, а також проведено аналіз підходів до проведення таких досліджень. Показано мету кожного з процесів, їх складові та результати, які мають бути отримані.

Встановлено, що ключовим фактором, який впливає на ефективність виконання завдань S&TI, TECHINT і TE, є координація дій персоналу, груп і підрозділів, що потребує формування системи управління технічної експлуатації з підтримкою всіх відповідних процесів. Наведено типовий перелік та зміст звітів, які формуються за результатами проведення відповідних досліджень.

Визначено, що в сучасних умовах ефективне впровадження в Україні підходів НАТО до науково-технічного аналізу зразків (фрагментів) ОВТ противника потребує розробки відповідного науково-методичного апарату проведення досліджень. Показано, що результати досліджень мають критичне значення для забезпечення національної безпеки, технологічного лідерства та конкурентоспроможності держави, а також для адаптації до швидко змінюваних викликів.

Ключові слова: *науково-технічна розвідка (S&TI), технічна розвідка (TECHINT), технічна експлуатація (TE), озброєння та військова техніка*

Відомості про авторів:

Головін Олексій Олександрович
доктор технічних наук
старший науковий співробітник
Заступник начальника Центрального
науково-дослідного інституту озброєння та військової техніки Збройних Сил України
м. Київ, Україна
https://orcid.org/0000-0003-4662-4559
e-mail: a_a_golovin@ukr.net

Палій Віталій Любомирович
старший науковий співробітник науково-дослідного відділу розвитку зенітних систем та комплексів науково-дослідного управління розвитку озброєння та військової техніки Повітряних Сил Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України
м. Київ, Україна
https://orcid.org/0009-0008-0458-3289
e-mail: azov0474@gmail.com

Information about the authors:

Holovin Oleksii
Doctor of Technical Sciences, Senior Research
Deputy Chief of Central Scientific Research Institute of Armament and Military Equipment of Armed Forces of Ukraine
Kyiv, Ukraine
https://orcid.org/0000-0003-4662-4559
e-mail: a_a_golovin@ukr.net

Palii Vitalii
Senior Fellow at the Central Scientific Research Institute of Armament and Military Equipment of Armed Forces of Ukraine
Kyiv, Ukraine
https://orcid.org/0009-0008-0458-3289
e-mail: azov0474@gmail.com

The article was received by the editorial board on 15.01.2025.