“CAROL I” NATIONAL DEFENCE UNIVERSITY
CENTRE FOR DEFENCE AND SECURITY STRATEGIC STUDIES

STRATEGIC IMPACT

No. 1 [82]/2022

Open-access academic quarterly, nationally acknowledged
by CNATDCU, indexed in CEEOL, EBSCO, ProQuest,
WorldCat and ROAD international databases

“CAROL I” NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, ROMANIA

CONTACT ADDRESS
Șos. Panduri, nr. 68-72, Sector 5, 050662,
București, Romania
Phone: +4021.319.56.49; Fax: +4021.319.57.80
Website: https://cssas.unap.ro/index_en.htm
E-mail: impactstrategic@unap.ro

ISSN 1841-5784; ISSN-L 1841-5784; e-ISSN 1842-9904

CONTENTS

EDITOR'S NOTE

The first edition of 2022 (volume 82), is part of the regular theme of the journal and comprises six articles, the ***Book review*** rubric, as well as the traditional *Scientific Event*.

The journal opens with the rubric ***NATO and EU: Policies, Strategies, Actions***, which includes two articles. In the first, Major Engineer Teodora Zecheru, PhD, together with Brigadier General Professor Engineer Ghiță Bârsan, PhD, co-authored a topic on the European Directive on the intra-community transfer of defence-related products. The Directive introduced a new licensing system in order to encourage Member States to use general licenses for simple transfers of defence products between them. However, the Directive is proving difficult to apply. Next, our colleague, Senior Researcher Mirela Atanasiu, deals with the main threats to NATO member countries on the eastern border, as identified in official documents, before Russia's attack on Ukraine.

The ***Security and Military Strategies*** rubric hosts an article, written by Mr. Robert Zsakai, PhD, that deals with disaster management as a complex process, by stressing the fact that more attention should be paid to psychological assistance and psychic resilience improvement for the military.

Under the heading ***Geopolitics and Geostategies: Trends and Perspectives***, our intern Mihai Vlaicu assesses how the joint actions have given the Israeli Defence Forces an advantage in achieving the strategic objectives set by the Israeli Government, as well as whether the Momentum Plan, part of the doctrine of joint actions, is feasible or has vulnerabilities that can be remedied.

In this edition, in the rubric ***Information Society***, we have included two articles. The first, signed by Mrs. Oana-Cătălina Frățilă, brings to attention a topical issue, namely the opportunity represented by social networks for the process of recruiting human resources, from the perspective of information distributed by users; the paper reveals that although many intelligence services have official pages on social media, only a few of them share content. In the second article, Mr. Mihai Vlaicu highlights the main concepts and methods of use of information warfare, especially CEMA operations (cyber electromagnetic activities), by the armed forces of different nations and formulates some potential developments regarding the future of information operations.

In the ***Book review*** rubric, Mrs. Lavinia Moiceanu, PhD, brings to the attention of our readers the last volume of the trilogy "Civilization and Capitalism, 15th-18th Century", written by the French historian Fernand Braudel, entitled *The perspective of the world*.

In the ***Scientific event*** rubric, our colleague, Raluca Stan, presents the main conclusions following the Workshop on "National Adjustment of the Allied Multidomain Operations Concept", organized online by CDSSS, on March 25th, 2022.

Also, the edition includes the *Guide for Authors*, a recommended reading for those who wish to disseminate the research results in *Strategic Impact*.

For those who read for the first time *Strategic Impact*, it is an open-access peer reviewed journal, edited by the Centre for Defence and Security Strategic Studies and published with the support of "Carol I" National Defence University Publishing House, and, according to the National Council for Titles, Diplomas and Certificates (CNATDCU), the publication is a prestigious scientific journal in the field of military sciences, information and public order.

Strategic Impact is being printed in Romanian language for twenty-two years and in English for seventeen years, and approaches a complex thematic: political-military topicality; security and military strategy; NATO and EU policies, strategies and actions; geopolitics and geostrategies; information society and intelligence, military history. Readers may find in the pages of the publication analyses, syntheses and evaluations of strategic level, points of view which study the impact of national, regional and global actions dynamics.

Regarding international visibility − the primary objective of the journal − the recognition of the publication's scientific quality is confirmed by its indexing in the international databases CEEOL (Central and Eastern European Online Library, Germany), EBSCO (USA), Index Copernicus (Poland), ProQuest (USA) and, in addition, WorldCat and ROAD ISSN, but also its presence in virtual catalogues of libraries of prestigious institutions abroad, such as NATO and of universities with military profile in Bulgaria, Poland, Czech Republic, Hungary, Estonia etc.

Strategic Impact is printed in two distinct editions, both in Romanian and English language. The journal is distributed free of charge in main institutions in the field of security and defence, in the academia and abroad − in Europe, Asia and America.

In the end, we would like to encourage those interested to publish in our journal to prospect and evaluate thoroughly the dynamics of the security environment and, also, we invite the interested students, Master Students and Doctoral Candidates to submit articles for publication in the monthly supplement of the journal, *Strategic Colloquium*, available on the Internet at http://cssas.unap.ro/ro/cs.htm, indexed in the international database CEEOL, Google scholar and ROAD ISSN.

Editor-in-Chief, Colonel Florian CÎRCIUMARU, PhD
Director of the Centre for Defence and Security Strategic Studies

DOI: 10.53477/1842-9904-22-1

THE EUROPEAN DIRECTIVE ON TRANSFERS OF DEFENCE-RELATED PRODUCTS WITHIN THE COMMUNITY AND A NON-EXHAUSTIVE MODEL OF IMPLEMENTATION

Teodora ZECHERU, PhD*
Ghiță BÂRSAN, PhD**

The European Directive on the intra-community transfer of defence products from 2009 established mandatory steps to be taken in order to simplify the necessary documentation and to create a federated framework linking Member States' national approaches and regulations. The regulatory document emerged as a result of the need to distinguish between import-export and transfer operations and, further, to secure the defence-related supplies within the European Union. The Directive introduced a new licensing system, based on general, global and individual licenses, encouraging the Member States to use general licenses for simple transfers of defence products between Member States, while maintaining control over their key security interests. From the perspective of the new European Defence Fund, the application of the Directive is difficult and measures should be taken to secure a more uniform implementation at Member States' level, at least from the perspective of transfers associated with research and development and innovation.

Keywords: *Directive 2009/43/EC; intra-community transfer; essential security interest; EDTIB; defence industry; licensing.*

**** Major PhD Engineer Teodora ZECHERU is defence advisor and NADREP at the Permanent Delegation of Romania to NATO, Brussels, Belgium. E-mail: teodora.zecheru@dpa.ro***
***** Brigadier General Professor PhD Engineer Ghiță BÂRSAN is the Rector of the Land Forces Academy "Nicolae Bălcescu", Sibiu, Romania. E-mail: office@armyacademy.ro***

Preliminary considerations

Since the launch of the European Defence Technology and Industry Base (EDTIB) in 2007 (European Parliament A 2020), the Member States of the European Union (EU) have been constantly working to integrate their national defence industrial and technological bases so that it can ensure, first and foremost, the security of supply at European level. A stronger EDTIB may be possible through a more efficient and strengthened intracommunity industrial cooperation, the correlation of all the European regulations related to the defence industry and the establishment of terms of reference for the entire domain.

Prior to 2009, there were no Community regulations on the licensing of defence equipment between EU Member States. The European defence industry had to comply with national regulations separately, with each Member State having its own export control regime designed primarily to control the risks associated with exports of military equipment to non-EU countries. Moreover, the process of granting or refusing a license for transfers between European states and for exports to non-EU states was essentially the same, which meant that Community economic operators did not have legislative instruments at their disposal to benefit from the EU internal market. Thus, the introduction of *Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community (Text with EEA relevance)* (the ICT Directive) (European Commission 2009) intended to minimize the obstacles regarding the movement of defence equipment between European states. This Directive is therefore considered an important part of the strategy for the foundation of a valid European internal market for defence equipment and services, thus being included in the European Commission's defence package in order to liberalize the European defence trade process and, consequently, to promote the prominence of EDTIB.

1. Purpose of the ICT Directive

The ICT Directive is a significant step toward reducing barriers to intra-EU trade in defence products, encouraging the harmonization and simplification of the EU framework in terms of licensing and national procedures. Its aim was to simplify the terms of transfers of defence products within the EU, with a view to facilitating and accelerating the movement of military products in Europe to strengthen security of supply and the competitiveness of the European defence industry. Thus, the ICT Directive applies to all defence equipment suppliers for the Armed Forces of another Member State or to the suppliers or the sub-suppliers of a certified company established in another Member State. The Directive applies to

all commercial defence-related products, their transfers for maintenance or repair and also to products at the experimental model/demonstrator level. Defence-related products are defined as any of the products listed in the Annex of the ICT Directive, including energetic materials, chemical, biological, radioactive and related materials, ammunition, weapons, vehicles and military equipment, software and technology. Of all these categories included in the Annex, some products are very well defined, while others need to be addressed and interpreted in accordance with the provisions of other regulations and directives.

The general objective of the Directive was opening up of the internal market for defence products, to facilitate cross-border procurement (European Parliament B 2020), to build a EU-wide industrial base in the European defence and security sectors by introducing a standardized certification system for the defence industries, building trust between national governments and meanwhile complying with export control regulations.

The ICT Directive is a tool designed to standardize the regulations of EU Member States on the transfer or export of defence equipment and provides Member States' competent authorities with a regulatory framework that, in theory, should reduce the administrative burden on authorities and suppliers. Since its entry into force, the ICT Directive has proved to be a robust regulatory act, being amended only on delegated acts − in 2019 (European Commission 2019) and to update the List of Defence Products (European Commission 2021).

2. Types of Licenses

According to the ICT Directive, a company that intends to transfer defence equipment from one Community state to another needs a prior authorization (a license) from the authorities of the European state from which the product is to be transferred. However, the ICT Directive allows European states to exempt certain types of transfers from the licensing obligation under particular conditions. In addition to traditional individual transfer licenses, it introduces the general (GTL) and global transfer licenses.

According to Article 5 of the Directive, GTL can be granted *ex officio*. While some Member States have introduced constraints and require registration before the first use of a GTL, this requirement is not mandatory in the text of the Directive, allowing automatically the authorization for movements that meet the legal licensing requirements. Such licenses allow the suppliers to export their defence-related products to different recipients in various Member States without any supplementary request.

Where a Member State considers that, under certain conditions, transfers of certain types of military products to other Member States do not involve major

risks, it may adopt and publish a GTL (European Commission 2016) to authorize such transfers, allowing all national suppliers of such products to perform multiple transfers directly to other Member States under certain conditions, without the need for another individual license to be issued.

According to Article 5, paragraph 2 of the Directive, the conditions set for releasing a GTL may apply not only to the types of products covered, but also to the Member States to which those products may be transferred under license, to the purpose of transfers, *e.g.*, maintenance, demonstrations or exercises, or to recipients of products, *e.g.*, the armed forces or the contracting authorities (European Commission 2016) (European Commission 2018).

Regarding the global transfer license, according to Article 6 of the ICT Directive, such a license is granted on request to individual suppliers. With such a license, the supplier may deliver products to one or more recipients in other Member States. National authorities are responsible for determining the conditions under which transfers may be authorized under a global license and not individually (for transfers not covered by GTL). Global transfer licenses are particularly useful in a contractual framework that involves a regular flow of products between the supplier and the recipient.

The individual transfer licenses are described in Article 7 of the ICT Directive. Such a license is granted on request and allows a single shipment of a specified quantity of designated products only to one EU Member State in one or several shipments. It is used in all cases where licensing exemptions, GTL and global transfer licenses cannot be used.

3. Assessing the Level of Implementation of the ICT Directive

Regarding the ICT Directive implementation, there were performed extended assessments, which have proven its unequally application within the Member States. The challenges identified included the moderate advocacy of the new licensing options, an ambivalent approach to minimum congruity, the slow pace of defence companies' certification and a sudden shift in responsibility (and inherent risks) from the competent authorities towards individual economic operators. Thus, the ICT Directive has had a limited impact, without achieving its main objectives, in particular that of facilitating the movement of defence products on the EU market, and to have an efficient internal market, an enhanced security of supply and an improved competitiveness. In addition, it is still early to properly assess the impact of the ICT Directive on the development of EDTIB and on the European defence equipment market (European Parliament. SEDE. 2015) (European Commission 2016) (Brown, Teichler and Simmonds 2017)

In terms of efficiency, there are some positive effects on the national control systems, but they are very limited at EU level. In the meantime, GTL has not yet provided the expected benefits, and the cost/benefit balance of certification remains unclear. Thus, the application of the ICT Directive yet encounters three main obstacles: transfers are still perceived as a matter of national sovereignty with strong implications in export control policies, there are clear differences between EU Member States' control cultures and policies and there is a relative lack of Europeanization of transfer control communities.

4. An Application Model of the ICT Directive – the European Defence Fund

The global perspective on competitiveness, in particular transatlantic developments, plays an important role in trying to understand the issue of licensing, mainly from industry, but also from the governmental side. EU Member States have implemented the ICT Directive differently, so in addition to having to navigate among different regulatory practices on internal transfers, companies from the defence industry also have to deal with different re-export regulations. These issues create uncertainty on the market and represent a major concern when considering to ensure the industry competitiveness. The lack of regulations harmonization for both ICT and re-export creates a barrier to European cooperation both in development and production of major defence equipment. Consequently, there is a risk of precluding the European companies to cooperate in various types of projects. This apprehension applies to the recently introduced action, the European Defence Fund (EDF).

The European Commission initiated the EDF (Official Journal of the European Union 2021) to encourage the research and development among Member States in a collaborative manner in defence-related areas, and, consequently, to promote innovation and competitiveness for EDTIB (European Defence Agency 2020). The link between ICT and EDF is the common goal of promoting a strong EDTIB, although no changes to the ICT Directive have been planned so far as a consequence of EDF emergence. However, for the implementation of the basic objectives and principles, the dimensions of added value that could help to make decisions on EDF's research and development and innovation actions and technologies must be taken into account, namely:

– contributing to the support of EU resilience and European technological sovereignty/autonomy, by targeting strategic and industrial technology areas, in order to reduce dependence on non-EU sources, increasing EU autonomy and strengthening the security of supply. Thus, EDF supports the development of critical as well as disruptive technologies for defence applications and focuses on areas where defence research and development and innovation can be accelerated and

streamlined, thus contributing to the implementation of the European industrial strategy and the strengthening of EDTIB;

− alignment with the defence and security interests of the Member States and the EU, by funding research and development and innovation of defence products and technologies in line with the priorities set for obtaining defence capabilities;

− ongoing cooperation of Member States in the field of defence research and development and innovation, by directing funds to complex multinational actions, resulting in economies of scale, increased interoperability and greater efficiency for operational users;

− cross-border cooperation of small and medium-sized enterprises (SMEs), in view of the need for diverse and creative support in research and development and innovation programs, without the control of third countries.

Through the intermediary of its research and development programs, the EU intends to actively support critical defence technologies for defence applications. From the perspective of cooperation between Member States, the initiative to support defence-related research and development and innovation by funding is welcome, more specifically by cooperation and by directing budgets towards actions that would benefit from economies of scale, as they are too expensive, complex or too hazardous for a single actor. Supporting the defence industry by funding scientific research and collaborative development and innovation in the field of defence makes from the EDF an important tool that will be able to strengthen the industrial defence ecosystem for all categories of forces and, moreover, for joint forces.

Although the ambition to involve SMEs and industry in general in the EDF (European Commission 2022) is clearly expressed, they are reluctant to participate, questioning on potential legislative barriers, and consequently the potential cross-border cooperation may be hampered by policy differences as regards the granting of export licenses for commercial exploitation. In the case of export control, there are many situations in which the products that are subject to a transfer or an export are integrated into larger equipment and are then exported to various other destinations. In addition to the classic restrictions on the (re)export of the component as such (in certain states, or generally without the consent of the home-state), both from the perspective of the component manufacturer (intellectual property) and an export control authority in the state of origin, there are situations where re-export restrictions extend to the system or the sub-system in which the ICT component is integrated. The status of the component should be clearly identified in the end-user certificate or the end-user statement. The certification process of the integrating companies demonstrates exactly this ability of a manufacturer to comply with the re-export restrictions related to the components purchased from the Member States. From this perspective, the European Commission's recommendations on GTL have common minimum clauses on retransfer/export (re-export) in the case of final operations (to the Armed Forces and/or to certified companies).

Therefore, a harmonized EU export control strategy, as in the case of dual-use items, should prevent this from happening. And by the specificity of the direct approach of technologies and intracommunity cooperation, EDF can be seen as an additional step towards the creation of a more unified and open defence market. However, in the situation where the regulatory issues related to ICT and re-export are not sufficiently addressed, EDF itself risks not achieving its main objective, but instead only to serve as a mechanism for financing and consolidating the European defence industry in the short term, without ensuring a long-term return on investment for the EU Member States.

EDF can provide opportunities for the development of harmonized transfer licenses that smoothen collaborative projects. Additionally, the creation of an accurate EU transfer control community is a very promising medium-term effort to reconsider the national approaches and to advance a common culture of control. The EDF should thus be seen as a key initiative towards a more concerted political impetus from both the Member States and the EU to stimulate cooperation and consolidation in order to respond to the geopolitical trends facing the Union. The resurgence of the rivalry of the great powers means that only a market-approach to building a strong EDTIB is insufficient, and that the EDTIB is essential for the EU to maintain the same rate of progress with global technological developments.

5. NATO's Vision on Export Control

NATO's commitment to the defence and security industry was underlined after the 2012 Chicago Summit (NATO 2012), when heads of state and government recognized for the first time the relevance of the defence industry in Europe and the industrial cooperation within the Alliance as an essential condition for capabilities achievement. Building on the NATO Industrial Advisory Group (NIAG), one of the main dedicated groups in the Conference of National Armaments Directors (CNAD), and complementing the efforts of other relevant stakeholders (Allied Command Transformation and Agencies), NATO has been constantly working to improve its relationship with capability providers. For more than a decade, NATO has been considering the Transatlantic Defence Technological and Industrial Cooperation (TADIC) Forum, the NIAG studies (NATO 2013) and conferences, exploring options for addressing barriers in defence and technical and industrial cooperation, such as trade barriers and tariffs, intellectual property rights, competition, standardization and interoperability. Highlights from TADIC studies have informed the US export control reform and the recent US policy on conventional arms transfers.

At the NATO-Industry Forum (NATO's highest level of interaction with the defence and security industry), in 2021 (Allied Command for Transformation 2021), discussions were held on the adoption of innovation and it was emphasized that the

strategies adopted will influence the future geopolitical context and will pave the way for new legislation and regulations, the development of modern procurement procedures, the creation of advisory and consultation mechanisms, the extension of existing cooperation mechanisms or the identification of solutions to facilitate national involvement and contributions. NATO's overall relationship with the defence industry aims to support the acceleration and provision of capabilities, facilitating industry involvement even from the concept and development stage to enable the generation of "military requirements informed by industry advice". Thus, in recent years, the defence industry is increasing its' participation in earlier stages than the typical competitive/commercial level associated with procurement.

Furthermore, NATO encourages the Allies to take action on industrial policies and is currently focusing on the implementation of dual-use capability products through the intermediary of new initiatives, such as the NATO Defence Innovation Accelerator (DIANA) and the NATO Innovation Fund (NATO 2021), which also entail the establishment of a common legal framework in all NATO nations, including the modeling of sanctions regimes, the export control, the intellectual property or the foreign investment screening mechanisms.

Conclusions

The ICT Directive seems to be inefficient at some level, due to the fact that the transposition of the Directive itself has varied greatly among the EU Member States. The harmonization of ICT regulations at Member States level has not been achieved, as Member States do not apply the Directive in a federate manner. This has created uncertainty at the industry level on the modality to ensure the compliance with the various existing regulations for the same defence industry.

Consequently, it is clear that additional congruence is required to meet the ICT Directive objectives. Although charges and administrative-related burdens have been somewhat reduced and there are no reports of unreasonable increases in the costs associated with the certification process, there is a fear that the documentation requested by the competent authorities and the associated costs may change abruptly. In particular, this is a risk for the SMEs, partly due to the lack of information available and the lack of understanding by the SMEs on how and when to use the tools provided by the ICT Directive (European Commission 2022). There is also uncertainty on the usefulness of being certified, given that Member States have very different processes stemming from the ICT Directive disjoint implementation. The certification scheme's deficient application suggests that harmonizing the certification process is an important first step in achieving the ICT Directive objectives, and overall, it is difficult to argue that the ICT Directive has helped to create a functional and efficient single market, and the consensus is that, although a step has been made in the right direction, the goal of achieving EDTIB has not been met.

With the introduction of the EDF, the EU has taken important steps towards a more integrated European defence and the EU strategic autonomy. This strategic autonomy has a significant defence component, and a more effective common EDTIB needs to be created to support the development of European defence capabilities. This implies more competition and consolidation, including from the perspective of the ICT Directive. Given the priorities identified at EU level, addressing emerging challenges in the modern battlefield, defence catalysts and excellence in real confrontations to improve operational capabilities and support ambitious defence systems, the disruptive technological solutions and the information management may be considered key interdisciplinary activators. In order to benefit from these activators, it is necessary to first create the regulatory and implementation framework for the use of emerging technologies and autonomous systems, both from the perspective of international humanitarian law and lessons learned. Therefore, the cooperation of all EU Member States in defence is particularly important, so that these priorities are supported to develop and implement the results of the capability programs and to be able to talk in the near future about technological independence, interoperability and interchangeability at European level.

BIBLIOGRAPHY:

Allied Command Transformation. 2021. "NATO-Industry Forum". Accessed on March 5, 2022. https://www.act.nato.int/industryforum

Brown, Neil, Teichler, Thomas, and Simmonds, Paul. 2016. "Evaluation of Directive 2009/43/EC on the Transfers of Defence-Related Products within the Community. Final Report". Accessed on January 17, 2022. European Commission. Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs. https://op.europa.eu/en/publication-detail/-/publication/538beabd-92af-11e7-b92d-01aa75ed71a1/language-en/format-PDF/source-search

European Commission. 2009. "Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community". Accessed on March 3, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02009L0043-20211007

European Commission. 2016. "Commission Staff Working Document. Evaluation of the Transfers Directive Accompanying the document. Report from the Commission to the European Parliament and the Council on the evaluation of Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community". Accessed on March 3, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016SC0398R(01)&from=EN

European Commission. 2016. "Commission Recommendation (EU) 2016/2123 of 30 November 2016 on the harmonisation of the scope of and conditions for general transfer licences for armed forces and contracting authorities as referred to in point (a) of Article 5(2) of Directive 2009/43/EC of the European Parliament and of the Council (notified under document C(2016) 7711)". Accessed on March 3, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016H2123&qid=1648331850953

European Commission. 2016. "Commission Recommendation (EU) 2016/2124 of 30 November 2016 on the harmonisation of the scope of and conditions for general transfer licences for certified recipients as referred to in Article 9 of Directive 2009/43/EC of the European Parliament and of the Council (notified under document C(2016) 7728)". Accessed on March 3, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016H2124&qid=1648331942379

European Commission. 2018. "Commission Recommendation (EU) 2018/2052 of 19 December 2018 on aligning the scope of and conditions for general transfer licences for the purpose of exhibition as referred to in point (c) of Article 5(2) of Directive 2009/43/EC of the European Parliament and of the Council (notified under document C(2018) 8611)". Accessed on March 1, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H2052&qid=1648332017427

European Commission. 2019. "Regulation (EU) 2019/1243 of the European Parliament and of the Council of 20 June 2019 adapting a number of legal acts providing for the use of the regulatory procedure with scrutiny to Articles 290 and 291 of the Treaty on the Functioning of the European Union (Text with EEA relevance)". Accessed on March 2, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R1243&qid=1648332096265

European Commission. 2021. "Commission Delegated Directive (EU) 2021/1047 of 5 March 2021 amending Directive 2009/43/EC of the European Parliament and of the Council as regards the updating of the list of defence-related products in line with the updated Common Military List of the European Union of 17 February 2020". Accessed on January 24, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021L1047&qid=1648332170672

European Commission. 2022. "The Defence Transfers Directive - Handbook for SMEs". Accessed on February 25, 2022. https://ec.europa.eu/defence-industry-space/download-defence-transfers-directive-handbook-smes_en

European Commission. 2022. "Internal Market, Industry, Entrepreneurship and SMEs". Accessed on February 22, 2022. https://ec.europa.eu/growth/index_en

European Defence Agency. 2020. "Implementation of the EU Defence Package". Accessed on February 26, 2022. https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-(edf)

European Parliament. SEDE. 2015. "The impact of the 'defence package' Directives on European defence". Accessed on January 6, 2022. https://www.europarl.europa.eu/RegData/etudes/STUD/2015/549044/EXPO_STU(2015)549044_EN.pdf

European Parliament. 2020. "EU Defence Package: Defence Procurement and Intra-Community Transfers Directives". Accessed on January 15, 2022. https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)654171

European Parliament. 2020. "The EU's Defence Technological and Industrial Base – In-Depth Analysis". Accessed on February 1, 2022. https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2020)603483

NATO. 2012. "Chicago Summit Declaration". Accessed on February 22, 2022. https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

NATO. 2013. "Transatlantic defence technological and industrial cooperation (TADIC) - NIAGConsultancy Advice Study". Accessed on January 6, 2022. https://diweb.hq.nato.int/indrel/Shared%20Documents/Brochure_TADIC_SG154.pdf

NATO. 2021. "NATO Allies take the lead on the development of NATO's Innovation Fund". Accessed on January 5, 2022. https://www.nato.int/cps/en/natohq/news_187607.htm

Official Journal of the European Union. 2021. "Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092". Accessed on February 4, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0697&qid=1648332296124

Acknowledgement: The topic of this article was addressed during the 2021 Edition of European Session of Armaments Program Managers (SERA), under the auspices of the Institute for Advanced Studies in National Defence, Paris, France, as well as at the NATO-Industry Forum on November 16-18, 2021, Rome, Italy, attended by major Teodora Zecheru.

DOI: 10.53477/1842-9904-22-2

SECURITY THREATS REFLECTED IN THE STRATEGIC DOCUMENTS OF NATO'S EASTERN MEMBER COUNTRIES

Mirela ATANASIU, PhD*

The aim of the paper is to identify and compare the main threats to the security of NATO member states situated on its Eastern border, as they are found in the strategic documents of NATO's Eastern border member states and in document "NATO 2030: United for a New Era" at organisational level. The analysis is limited to the threats identified as such, not to the security risks or vulnerabilities.

Thus, it is found that some of the former communist Eastern European countries, many of them part of NATO's Eastern border, have in common the reminiscent threat related to Russia's vicinity. However, NATO's Eastern countries also have specific perceptions of security threats. For some of these countries, a threat reassessment is needed in order to include the results in their national security strategies. The same update needs to be reflected in NATO's Strategic Concept, given the new challenges and the flare up of old ones.

Keywords: *NATO Eastern member states; the Russian Federation; threat; perception; Romania; security policies.*

Introduction

Since the end of World War II, the transatlantic organization has been the cornerstone of European and Euro-Atlantic security. For more than seven decades, NATO has confronted with multiple and dynamic threats, has succeeded to adapt,

**** Mirela ATANASIU, PhD, is Senior Researcher within the Centre for Defence and Security Strategic Studies, "Carol I" National Defence University, Bucharest, Romania, and also Associate Researcher within Doctoral School for Safety and Security Sciences, Obuda University, Budapest, Hungary. Email: atanasiu.mirela@yahoo.com***

and remains the most powerful political-military organization in the world, despite all the difficulties. Meanwhile, it has defended its members not only by military force, but also through an active contribution to improving the Euro-Atlantic and international security climate.

During the Cold War, NATO's role and purpose were clearly defined by the existence of the threat posed by the USSR. After the Warsaw Pact was abolished and the Soviet Union disintegrated, the traditional opponent of the Alliance disappeared. But the Alliance has reinvented itself. Thus, after the USSR fall in the 1990s, the Russian importance on the NATO agenda declined, and many of the Alliance's resources were redirected to other areas, such as global terrorism, Afghanistan and Iraqi conflicts, China deterrence, and the Middle East pacification.

However, when Russia restarted its military assault over the states considered to be part of its former influence area (Georgia – 2008, Ukraine – 2014, 2022), the former Soviet states in the vicinity started to feel threatened by its aggressive posture and started to ask more support from the Alliance in order to build in more security and deterrence on its Eastern Flank.

1. NATO's Overall Threats Evolution as Reflected in Its Policy Documents

The main mission of NATO members, stipulated in the 1949 Washington Treaty, is to unite their efforts for collective defence and for the preservation of peace and security, this standing as the organization's constant regardless of the future historical context or geopolitical context. Inside this founding document of the Euro-Atlantic Alliance, the single considered threat was a military attack as "such an act against one of its members was to be considered as an aggression against all NATO countries" (NATO 1949), in conformity with Article 5, and an response intervention to such an act is legitimated by Article 51 of the UN Charter,

The end of the Cold War changed the international relations system, as well as the nature and range of threats. With the collapse of the USSR, the 1991 Strategic Concept of NATO was presented in Article 7 that "The threat of a simultaneous, full-scale attack on all of NATO's European fronts had effectively been removed and thus no longer provided the focus for Allied strategy" (NATO 1991). In this specific Concept, as the direct military threat became defused and basically generally reiterated in Article 20.III "To deter and defend against any threat of aggression against the territory of any NATO Member State" (NATO 1991), similar to its presentation in Article 5 of the Washington Treaty, the risks, as significantly expressions to Member States security, have come to the forefront of the organization's political agenda as "multi-faceted in nature and multi-directional" (NATO 1991). These kind of expressions showed the need for NATO reconfiguration from its posture as entity

built to balance militarily the USSR threat to a more general approach of missions in times of peace, conflict or war. The focus was specifically shifted to the risks embodied by "ethnic rivalries and territorial disputes faced by many countries in Central and Eastern Europe". Of course, the worrying motives were plausible, as these countries were in the reorganizational path from communism to democracy.

The *1999 NATO Strategic Concept* maintained the same line of concerned threats against the Alliance: deterrence and defence in conformity with Articles 5 and 6 of the Washington Treaty and the unlikeliness of a large-scale conventional aggression. However, a new approach has emerged in relation to NBC weapons proliferation that could pose a direct military threat to the Member States of the transatlantic organisation's populations, territory, and forces, as was stipulated in Articles 35 and 53h of the respective Concept (NATO 1999). Article 3 emphasized "the new complex risks to Euro-Atlantic peace and stability, including oppression, ethnic conflict, economic distress, the collapse of political order, and the proliferation of weapons of mass destruction" (NATO 1999). Article 12 also included the encouragement of cooperation and dialogue with other states, including Russia, as a consequence of their relations defrost on the background of the *NATO-Russia Founding Act on Mutual Relations, Cooperation and Security* signing in 1997.

In 2006, in the *Comprehensive Political Guidance*, issued after the September 11, 2001 acts, the perception of threat suffered a real change as terrorism and the spread of weapons of mass destruction were seen to be the main threats to the Alliance's territory over the next 10 to 15 years. The risks were reflected in Article 2 of this Guidance to be emanating from instability due to "failed or failing states, regional crises and conflicts, and their causes and effects; the growing availability of sophisticated conventional weaponry; the misuse of emerging technologies; and the disruption of the flow of vital resources" (NATO 2006) exacerbated by potential access of terrorism to WMDs. In the same Guidance, asymmetric threats and risks are seen to damage the security environment in the next decade (NATO 2006).

In the *Declaration on Alliance Security* issued on April 2009, in the context of the NATO Summit, on the anniversary of 60 years of the organization, the aim of cooperating with Russia on common challenges was re-iterated, despite the Russian military intervention in Georgia (2008). As global threats were seen "terrorism, the proliferation of weapons of mass destruction, their means of delivery and cyber-attacks" (NATO 2009). It was stressed out that Alliance's security is strongly connected to other regions security.

In the 2010 NATO Concept "Active Engagement, Modern Defence", the Alliance came up with an updated understanding of the new geopolitical context that reinterpreted its 1949 Treaty. Article 5 remained the stronghold of the document, but

in addition deterrence of both nuclear and conventional capabilities were considered threats against Alliance's security. A wide range of threats returned on NATO's political agenda, thus, the focus of the document has shifted from many risks to many threats, and this reveals the unpredictable dynamic changes intervened in the security environment. Also, with regard to the threat of a conventional attack against NATO territory, from "highly unlikely" in the 1999 Concept, in 2010 became "low" and "cannot be ignored" (NATO 2010), according to Articles 7 and 8. The proliferation of ballistic missiles is seen as "real and growing threat", particularly from the part of "world's most volatile regions" (NATO 2010). Terrorism also remained on the list of direct threats, with its high potential to "acquire nuclear, chemical, biological or radiological capabilities", as well as "instability or conflict beyond NATO borders", potentially fuelled by transnational criminal activities (NATO 2010). Cyberattacks are seen as a growing threat to Euro-Atlantic critical infrastructures providing vital services (NATO 2010). Concept also stresses that "NATO poses no threat to Russia", and NATO-Russia cooperation is needed, and in this regard, in Articles 33 and 34, some areas of shared interests are listed "missile defence, counterterrorism, counter-narcotics, counter-piracy and the promotion of wider international security" (NATO 2010).

Since 2014, in response to Russian military intervention in Ukraine, NATO-Russia practical cooperation has been suspended. Some political documents were issued calling on the Russia's unlawful behaviour: Joint statement of the NATO-Ukraine Commission – December 2014, Warsaw Summit Communiqué – 2016, and the Brussels Summit Declaration – 2018. Moreover, in 2018, after some Russian actions (the use of Novichok[1] chemical agent, the development and launching of the 9M729 missile system − action infringing the Treaty on intermediary range nuclear and conventional forces[2] − and the deployment of military forces in the Ukraine vicinity near the Azov Sea and the Kerch Strait), NATO statements became sharper and some were followed by actions. Thus, it was decided "the expulsion of over 140 Russian officials by over 25 NATO Allies and partners" and the reduction of "the maximum size of the Russian Mission to NATO by ten people" (NATO 2018).

At the end of 2020, NATO 2030: United for a New Era, document resulted from the work of the Reflection Group assigned by NATO Secretary General, presents that "NATO's external security environment has changed dramatically since the 2010 Strategic Concept was published", therefore "the starting point must be to update

[1] In March 2018, former Russian spy Sergei Skripal, his daughter Yulia, and police officer Nick Bailey were poisoned with Novichok in Salisbury in March 2018.

[2] The Intermediate Nuclear Forces Treaty, signed in 1987, also known as the INF, required the USA and the USSR to phase out and permanently abandon their nuclear and conventional ballistic and cruise missiles, all with a range of 500 to 5,500 kilometers.

the 2010 Strategic Concept" (NATO 2020, 16, 12). Threats are better described than in the previous documents, and, this time, real solutions are set for them (Table no. 1).

Table no. 1: Threats and solutions identified in "NATO 2030: United for a New Era"

No.	Threat	Solution
1.	A direct Russian military action to the Euro-Atlantic area	- Dual-track approach of deterrence and dialogue addressing gaps in deterrence and defence system on NATO Eastern flank
2.	Increasing China's importance in the world	- Outlining a political strategy based on security interests for China
3.	Terrorism	- Enhancement of the fight against terrorism as part of the hybrid and cyber threats
4.	Pandemics	- Inclusion in NATO planning of exercises, deliberations and discussions on the resilience and management of health crisis
5.	Migration	- Boosting current partnerships in the South, namely the Mediterranean Dialogue (MD) and the Istanbul Cooperation Initiative (ICI)
6.	Cyber attacks	- Building a common policy framework for how NATO should assess, attribute, and respond to hybrid and cyber incidents in a crisis
7.	Climate change	- Raising awareness of the situation, early warning, and information sharing, including by considering the establishment of Centre of Excellence for Climate and Security.
8.	Hybrid attacks	- Developing political and non-political tools to counter hybrid activities, such as new approaches to attribution, deterrence in the hybrid domain, as well as tackling disinformation
9.	Emerging and disruptive technologies	- Organizing a digital summit of governments and private sector to identify gaps in collective defence cooperation in security-related AI strategies.

Later, in February 2021, on the transatlantic organizational level, in the "Food for Thought Paper: NATO 2030 − a Transatlantic Agenda for the Future", most of these threats were reiterated. Also, in the Communiqué of the Brussels Summit in June 2021, Russia's aggressive actions appear, together with terrorism in all its forms, state and non-state actors challenging the rule-based international order, cybercrime and China's growing influence, as the main threats to NATO security (NATO 2021). Following the launch of Russia's "special operation" in Ukraine, on February 28, 2022, the Heads of Defence of the 30 NATO Member States got together in an extraordinary meeting in the Military Committee of the organization, to discuss the situation created around Ukraine.

2. Common and Specific Threats against NATO Member-States in Eastern Europe[3]

As a new NATO Strategic Concept is not yet updated on the new security challenges, including the circumstances of the Russian Federation military aggression on Ukraine, we take as milestones the ones that are explicitly mentioned as such in *NATO 2030: United for a New Era* document (a direct Russian military action to the Euro-Atlantic area; China's growing importance in the world; terrorism; pandemic; migration; cyberattacks; climate change; hybrid attacks; emerging and disruptive technologies) in considering common and specific threats to NATO Eastern member countries−Bulgaria (BG), the Czech Republic (CZ), Estonia (EE), Hungary (HUN), Latvia (LV), Lithuania (LT), Poland (PL), Romania (RO), Slovenia (SI) and Slovakia (SK).

"Common" threats are considered the ones similarly identified as such in the aforementioned document and in the NATO Eastern members' strategic security documents. Also, by "specific" threats there are considered the ones presented in the security or defence strategies of the mentioned countries, but are not identified among the 9 threats explicitly considered in NATO 2030: United for a New Era.

Bulgaria has a security strategy issued ten years ago, but largely updated in 2018, wherein Article 9 states that "The risks and threats to the security of Republic of Bulgaria and of its citizens are largely identical or similar to what the EU or NATO member countries face", and also that "none of the neighbouring countries consider it a potential aggressor" (National Security Strategy of the Republic of Bulgaria 2011). In particular, the last quoted phrase, practically, expresses, that if Russia does not see it as an aggressor, thus, Bulgaria is not threatened by a Russian direct military action, but as the strategy's time horizon was 2020, it must be updated. In the Bulgarian Security Strategy there are identified some specific asymmetric threats, such as: proliferation of WMDs, regional conflict and trans-border organized crime (National Security Strategy of the Republic of Bulgaria 2011). Also, specific threats against international security are identified to be: failed states, unstable political and economic situation in third countries, crises related to energy security, Middle East instability (National Security Strategy of the Republic of Bulgaria 2011). Moreover, Bulgaria's 2018 version of the Strategy acknowledges hybrid threats, but without outlining means to counter them. Recently, since 2019, Bulgarian national security authorities have revealed information on a number of unauthorized uses of their own computer systems by Russian intelligence services (Kramer 2021) and, thus, the Bulgarian hybrid threat ranking and perception on Russia must have changed, which must be also included in a new updated security strategy.

[3] These are not all geographical *stricto sensu* East European countries, some, on case by case basis, are also considered to be part of the Central Europe (Hungary and Poland, for example).

Czech Republic's security strategy, issued in 2015, focuses on non-military threats, while the risk of direct military attack on the country remains low. However, a military threat and hybrid war manifestations are seen as possibility for other NATO member countries stemming from some states' aspirations of power (Security Strategy of the Czech Republic 2015, 3, 5, 10). Thus, in the document common threats are mentioned–international migration, terrorism, hybrid threats, cyberattack, pandemic –, and some specific asymmetric threats are identified: interruptions in strategic supplies of raw materials, increasing global inequality, regional conflicts, extreme violence, growth of interethnic and social tensions, organised crime ("serious economic and financial crime, corruption, human being trafficking and drug-related crime") (Security Strategy of the Czech Republic 2015).

Estonia in its 2017 National Security Concept sees as a main threat "Russia's increased military activity and aggressive behaviour". Also, there are seen global asymmetric threats as "economic instability, developments in the cyberspace, technology-related threats, radicalisation and terrorism, organised crime and corruption, migration flows" that can harm the security of the Estonian state (National Security Concept of Estonia 2017, 4, 5). Thus, there is a share of common and specific threats perceived in Estonian security document.

Hungary, although agrees in paragraphs 52 and 118 of its security strategy that "the forced acquisition of land with aggression has fundamentally changed our security environment", aims in its security strategic document "a pragmatic development of Hungarian-Russian relations and economic cooperation with Russia", while the idea that "the Alliance does not seek conflict or pose a threat to Russia" is strengthened (Hungary's National Security Strategy 2020). Approximately the same pragmatic relational approach is also presented towards China, but with the concern that "China's military and security policy aspirations need to be monitored in the longer term" (para 119). Migration and its collateral effects "cross-border threats … arms, drugs, human and organ trafficking" (Hungary's National Security Strategy 2020) are seen to be the most damaging to Hungarian internal security.

Latvia includes in its 2020 National Defence Concept an analysis of threats wherein Russia is seen as the source of the threat or potential threat of a traditional military attack or hybrid ("economic sanctions, suspension of energy supply, humanitarian influence, informative propaganda, and psychological influence, as well as cyberattacks …" (The National Security Concept 2020, 4). In fact, a wide part of the Concept relates Russia's "doings" as an aggressor state and its possible means of aggression in the future. As regards Latvian threats other than ones included in the aforementioned *NATO 2030* document, there are identified "foreign fighter phenomenon", and "internal threats caused by inhabitants, specifically youth, of Latvia … participating in military training camps located in other countries" (The National Security Concept 2020, 7).

Lithuanian 2017 National Security Strategy sees Russia as its major threat, many reasons of this affirmation being stated in the document's paragraph 8 "Aggression against the neighbouring countries, annexation of Crimea, the concentration of modern military equipment of the Russian Federation, its large scale offensive capabilities and their exercises near the borders of the Republic of Lithuania and other states, especially in the Kaliningrad Region …, cause international tensions and threaten world peace" as well as "Capacity of the Russian Federation to use military and economic, energy, information and other non-military measures … the ability to exploit and create internal problems of the states located in the Eastern neighbourhood of the Republic of Lithuania, as well as preparedness of the Russian Federation to use a nuclear weapon even against the states which do not possess it" (National Security Strategy 2017). Specific threats are identified as "economic and energy dependence, economic vulnerability … … social and regional exclusion, poverty … demographic crisis … corruption … organized crime … crisis of values" (National Security Strategy 2017).

The 2020 Security Strategy of ***the Republic of Poland*** identifies that "The most serious threat is the neo-imperial policy of the authorities of the Russian Federation, pursued also by means of military force" (National Security Strategy of the Republic of Poland 2020). Energy dependence on Russia and organized crime are also seen as threats.

Romania has a new and updated security strategy issued in 2020, wherein part of the main common threats considered in NATO 2030 document are present, except for the direct threat of China's emergence. There are also some elements specifically perceived as threats by Romanians, namely the "volatility of the security situation in the Western Balkans correlated with the limited prospects in resolving frozen conflicts in the region and conserving outbreaks of conflict in Southern Caucasus …", and MENA instability (Strategia Națională de Apărare a Țării pentru perioada 2020-2024 2020), which in NATO's document are identified as risks.

Slovenia has as security strategic document *The Resolution on the National Security Strategy*, issued in 2019. Military threats are considered possible for the first time since the end of the Cold War (Resolution on the National Security Strategy of the Republic of Slovenia 2019, 16). This resolution expresses very well the actual context NATO has to deal with: "In the East, we are facing a serious increase in military threats, while the South and South-East are facing instabilities and the possibility of threats being transformed into asymmetric threats" (Resolution on the National Security Strategy of the Republic of Slovenia 2019, 8). It is also noted that "armed conflicts and low intensity conflicts in crisis areas pose a threat to international peace and security", "the proliferation of conventional weapons … and dual-use items, is an important potential threat", "national security is threatened by serious and organized forms of crime" and "the escalation of tensions around

international trade relations, and the potential crisis of the Eurozone, pose a real threat of a new financial and economic crisis" (Resolution on the National Security Strategy of the Republic of Slovenia 2019). Threats to public safety as "increased attacks on human life and property; economic crimes; corruption; financial fraud; the falsification of documents and goods; counterfeit money; cyber and environmental crimes; and mass violations of law and order" (Resolution on the National Security Strategy of the Republic of Slovenia 2019, 28) are also considered.

The Defence Strategy of ***the Slovak Republic*** is the newest security/defence strategic document among those analysed. In paragraph 10, Russia is seen as a danger from the perspective of Ukraine sovereignty violation, as an escalation of power competition between states. Specific perspectives of threat are "erosion of arms and disarmament regimes", "spreading propaganda damaging the cohesion in NATO and the EU", and "extremism, including its penetration into the Armed Forces" (Defence Strategy of the Slovak Republic 2021).

In Table no. 2 is presented the summary of the main threats identified in *NATO 2030: United for a New Era* and whether they are reflected as such in the analysed security policy documents of each NATO Eastern member.

Table no. 2: "NATO 2030: United for a New Era" threats as reflected/ non-reflected in Eastern NATO member countries security strategies

Country / Threat[4]	BG	CZ	EE	HUN	LV	LT	PL	RO	SI	SK
No. 1	No	No	Yes	No	Yes	Yes	Yes	Yes	No	No
No. 2	No	No	No	No	No	No	No	No	No	No
No. 3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
No. 4	No	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes
No. 5	Yes	Yes	Yes	Yes[5]	Yes	Yes	No	Yes[6]	Yes[7]	Yes[8]
No. 6	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
No. 7	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
No. 8	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
No. 9	No	Yes[9]	No	No	No	Yes	Yes	Yes[10]	Yes	Yes

[4] No. 1 – A direct Russian military action to the Euro-Atlantic area; No. 2 – Growing importance of China in the world; No. 3 – Terrorism; No. 4 – Pandemic; No. 5 – Migration; No. 6 – Cyber attacks; No. 7 – Climate change; No. 8 – Hybrid attacks; No 9 – Emerging and disruptive technologies.
[5] Illegal immigration.
[6] Illegal migration.
[7] Illegal migration.
[8] Massive illegal migration.
[9] Proliferation of weapons of mass destruction and their means of delivery.
[10] Proliferation of weapons of mass destruction and their means of delivery.

3. Similarities/Differences in the Threat Perception of NATO's Eastern Border Countries

The Alliance was always focused on a set of common identified threats, but geographic position created differences in threat perceptions. The member countries situated on the Alliance's Eastern border have built a geopolitical axis from the Baltic Sea to the Black Sea. Both seas are in NATO's attention as they are situated in the buffer zone of Russian areas of influence, and they are also former communist countries.

Table no. 2 shows that, although all these countries were part of the former Soviet bloc, the Russian aggressive posture and its hybrid war worries some of these NATO countries more than the others. Thus, Bulgaria, the Czech Republic, Hungary, Slovenia and Slovakia do not express directly in their documents that Russia is a threat (although the hybrid threats from aggressive neighbours are highly mentioned in their documents), perception that diverges from the other Eastern Border States considering Russia as a real military and hybrid threat (the Baltic States, Poland, and Romania). Moreover, currently there is no perception consensus as regards the possibility of a military threat against them, which is reflected in their security and defence policy papers. Some countries stipulate in their strategies that Russia may be the initiator of a potential direct military threat on them (Estonia, Latvia, Poland and Lithuania), Slovenia sees possible a direct military threat on it, Hungary considers a military attack over any NATO member as possible, other countries see any military threat against them as low (Czech Republic) or this direct threat is not mentioned at all (Bulgaria, Slovakia), while Romania, in regard to paragraph 121 of its active security strategy, is more worried about "the perpetuation of imbalances on the size of the eastern flank and changes in the positions of others in relation to the Russian Federation, (that) have the potential to have negative influences on Romania's security situation" (Strategia Națională de Apărare a Țării pentru perioada 2020-2024 2020).

Strategic documents of NATO Member States on its Eastern border show that they face high uncertainties resulting from the frozen conflicts in Moldova, Georgia, open conflicts[11], but also the systemic crises in the Middle East and North Africa generating illegal migration, cross-border crime, extremist tendencies and terrorism. These concerns are mainly expressed in the security strategies of Romania, Bulgaria, Slovakia and Slovenia.

Similarities. As a hard-line similarity identified in almost all analysed security strategies, it is shown that internal and external security threats blend and transit one each over, therefore their differentiations are blurred. Phenomena such as terrorism,

[11] Obviously, given that the security and/or defence strategies of the states are renewed in a few years, the consequences of the Russian-Ukrainian war have not yet been integrated into them.

migration, organized crime, cyber-attacks, and hybrid attacks are perceived as internationalized and transnational. Also, some of the Eastern NATO countries have similar threat perceptions on different areas, for example, both Bulgaria and the Czech Republic believe that emerging asymmetric threats can be imported in their territories from relatively distant regional conflicts.

Similarity also exist between some countries threat perception related to the proliferation of WMDs, namely Bulgaria, the Czech Republic, Estonia, Lithuania, or Romania. For some states (Estonia, Lithuania, and Slovenia) corruption is considered a threat. Thus, as for the mentioned states these are sets of similarities, compared to other countries they constitute commonly or specifically perceived differences.

Regarding migration, in their strategic documents, Hungary, Romania, Slovenia and Slovakia share the same opinion that illegal migration is a threat, not all migration, while Poland is the only country not counting migration as a threat, but rather as a risk.

Particular differences of threat perception are found in each national strategy and are reflected in the specific national perception over an express phenomenon seen as threat in that presented form only by a single country:

- for Bulgaria, "piracy and abduction of commercial fleet crews around Africa and South Asia" (National Security Strategy of the Republic of Bulgaria 2011), stated in Article 38 of its Strategy to be an important threat;
- for the Czech Republic, interruptions of strategic raw material supplies is a real threat;
- for Hungary, the threat of an armed attack "covered by Article 5 of the North Atlantic Treaty" (Hungary's National Security Strategy 2020), is presented as a possibility in its Strategy, in paragraph 51, without naming a possible aggressor;
- for Estonia, economic instability is a threat;
- for Latvia, internal threats caused by its inhabitants, participating in military training camps located in other countries are identified;
- for Lithuania, "the development of unsafe nuclear energy projects nearby the borders of the Republic of Lithuania" (National Security Strategy 2017) is seen as threat in paragraph 14 of its Strategy;
- for Poland, energy dependence on Russia is seen as threat against its national security;
- for Romania, the economic crisis caused by the COVID-19 pandemic is seen in its Defence Strategy as a severe threat;
- for Slovakia "extremism, including its entry into the Armed Forces" (Defence Strategy of the Slovak Republic 2021) is an actual threat expressed in its Strategy, in paragraph 10;
- for Slovenia, threats to public safety are urgent.

Conclusions

The main threats identified in the security program documents of NATO border member countries are residual, arising from the legacy left by the Cold War termination, as these states were within the sphere of influence of the USSR. Russia, even before the recent events in Ukraine, was perceived as a threat both in terms of military tensions that were seen as having the potential to generate violent conflicts in the region, including the direct military threat of some NATO Member States, and from the perspective of its hybrid warfare manifestations.

Although all these states fear Russia, which is seen in the way they have designed their security strategies, not all expressly show this in writing. For example, Hungary has expressed its wish for cooperation with Russia and China as emerging powers on the international stage, Bulgaria states that is not threatened by a Russian direct military action because it does not consider Russia as an aggressor, Latvia openly expresses that Russia is the source of the threat or potential threat of a traditional military or hybrid attack.

Currently, the security strategies of NATO's Eastern border countries show that they face growing uncertainties, mainly from the frozen conflicts in Moldova, Georgia and Ukraine (thawed in 2022), but also from the open conflicts in the Middle East and North Africa, generating another set of perceived threats, such as: illegal migration, cross-border crime, extremist trends and terrorism.

Some NATO Member States in Eastern Europe have obsolete security strategies to varying degrees because they do not reflect important events that have taken place, or are taking place, in the international arena: Russian military aggression on Ukraine since 2014 and 2022, the migration and refugee crisis of 2015-2016, the emergence of Islamic terrorism with the terrorist attacks taking place in Europe and the current COVID-19 pandemic.

BIBLIOGRAPHY:

2021. *Defence Strategy of the Slovak Republic*. https://www.mosr.sk/data/files/4291_defence-strategy-of-the-slovak-republic-2021.pdf.

2020. *Hungary's National Security Strategy.* 23 04. https://magyarkozlony.hu/dokumentumok/6c9e9f4be48fd1bc620655a7f249f81681f8ba67/letoltes.

Kramer, Mark. 2021. "A Weak Link in NATO? Bulgaria, Russia, and the Lure of Espionage." *Davis Center for Russian and Eurasian Studies, Harvard University.* 1 April. https://daviscenter.fas.harvard.edu/insights/weak-link-nato-bulgaria-russia-and-lure-espionage.

2017. "National Security Concept of Estonia." *Republic of Estonia, Ministry of Defence.* https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf.

2017. *National Security Strategy.* https://kam.lt/wp-content/uploads/2022/03/2017-national-security-strategy.pdf.

2011. "National Security Strategy of the Republic of Bulgaria." *Republic of Bulgaria. Ministry of Energy.* https://www.me.government.bg/en/themes/bulgaria-s-national-security-strategy-904-0.html.

2020. *National Security Strategy of the Republic of Poland.* https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf.

NATO. 2010. "Active Engagement, Modern Defence." *North Atlantic Treaty Organisation.* 19 Nov. https://www.nato.int/cps/en/natohq/official_texts_68580.htm.

—. 2021. "Brussels Summit Communiqué." *North Atlantic Treaty Organisation.* June 14. https://www.nato.int/cps/en/natohq/news_185000.htm.

—. 2009. "Declaration on Alliance Security." *North Atlantic Treaty Organisation.* 04 April. https://www.nato.int/cps/en/natohq/news_52838.htm.

—. 2020. "NATO 2030: United for a New Era." *North Atlantic Treaty Organisation.* 25 November. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

—. 2006. "North Atlantic Treaty Organiaation." *Comprehensive Political Guidance.* 29 Nov. https://www.nato.int/cps/en/natohq/official_texts_56425.htm.

—. 2018. "Statement by NATO Secretary General on further decisions following the use of a nerve agent in Salisbury." *North Atlantic Treaty Organisation.* 27 March. https://www.nato.int/cps/en/natohq/news_153223.htm.

—. 1991. *The Alliance's New Strategic Concept.* 07-08 Nov. https://www.nato.int/cps/en/natohq/official_texts_23847.htm.

—. 1999. "The Alliance's Strategic Concept." *North Atlantic Treaty Organisation.* 24 April. https://www.nato.int/cps/en/natohq/official_texts_27433.htm.

—. 1949. *The North Atlantic Treaty, Washington D.C.* . 4 April. https://www.nato.int/cps/en/natohq/official_texts_17120.htm.

2019. *Resolution on the National Security Strategy of the Republic of Slovenia.* https://www.gov.si/assets/ministrstva/MO/Dokumenti/ReSNV2.pdf.

2015. "Security Strategy of the Czech Republic." https://www.vlada.cz/assets/ppov/brs/dokumenty/security_strategy_1.pdf.

2020. *Strategia Națională de Apărare a Țării pentru perioada 2020-2024.* https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

2020. *The National Security Concept.* https://www.mod.gov.lv/sites/mod/files/document/NDK_ENG_final.pdf.

DOI: 10.53477/1842-9904-22-3

ASSESSMENT OF PSYCHOLOGICAL CHALLENGES AND TREATMENT POSSIBILITIES IN MILITARY PERSONNEL

Robert ZSÁKAI, PhD*

Disaster management is a very complex phenomenon, which is not only the task of an organization, rather a common aim of the government, social organizations and civilians. Disaster relief, prevention, response and recovery are complex processes where cooperation between countries and international bodies is essential. Breaking with previous conventions has made the system more open, thus they can monitor the effects of disasters from several aspects. In addition to social and economic damage prevention, this paper's aim is to clearly stressing the fact that more attention should be paid to psychological assistance and psychic resilience improvement of military personnel.

Keywords: *stress; psychological assistance; resilience; disaster management; defence forces.*

Introduction

The news often informs us about various disasters and their consequences. Disasters have an impact on the life of those living in the affected area and, most certainly, on the life of the various military and helping personnel who act during disaster management. Civilized societies are usually based on solidarity, thus helping and assisting the people in need is a basic characteristic in most societies. Nevertheless, psychic reactions and mental load can arise during such assistance

**** Second Lieutenant Robert ZSÁKAI, PhD, is Platoon Commander within Air Operation Command and Control Center, Garrison Support Command, Veszprém, Hungary. E-mail: info@zsrobert.com***

processes that can even affect the relief efforts of the action bodies rescue personnel. It would be beneficial to survey whether staff of professional action bodies are aware of their appropriate reactions for each mental load, and how could their psychological endurance be further strengthened?

From the perspective of the intervention staff, a given mental load or problem can even disrupt an intervention process of the whole action body. The increasing number of research results in the psychological sciences have broadened people's knowledge of various difficult social phenomena, as well as natural and civilizational disasters. The law of 1935/12th Article, regarding aerospace defence in Hungary, established the Hungarian Air Defence Spaces Protection as the legal predecessor of civil protection. The activities of the groups involved in this kind of defence date back a long time. Throughout history, of course, these groups have had various names, but what they still have in common is that their success depended not only on the technological level of the age or their application, but on the most important factor of all time: the human factor! Their most important aim has been to save human lives. Disaster protection has increasingly evolved into a system of regulated defence, which has also meant protecting the values of society. The tasks of national defence forces and disaster protection are similar, however, the cause and timing of a given event point to the differences, because if an action is called an act of war in the case of a war, it can be human activity in the case of protection against natural disasters during peacetime.

The Fundamental Law of Hungary[1] designates the basic tasks of the Military of Hungary, as well as that it participates in the prevention of disasters, on the basis of Defence Act and the Disaster Protection Act. Task of disaster protection sector are regulated by a decision of the Minister of Defence[2]. In the life of the intervention personnel of both organizations, it may become necessary to treat mental loads in order to avoid psychosomatic diseases. As unpredictability increases, people's sense of vulnerability also increases. Anxiety, the emergence of fears increasingly proves that people should not be left permanently in a state of doubtfulness. The catastrophic and panic processes also require the complex assistance of mental crisis management. The growing number of disasters poses a constant challenge to national governments, the military, and disaster management organizations. The role of authorities during an emergency situation is key in the management and coordination of assistance, as they have a legal duty to take care of those involved. The need for the supportive power of international and national humanitarian organizations is also being strengthened.

[1] The Fundamental Law of Hungary, Article 45 about The Hungarian Defence Forces
[2] 23/2005. (VI. 16.) Military of Hungary, decision about disaster management, prevention and action for military personnel

Scientific results have expanded people's knowledge of various social phenomena, natural and civilizational disasters. Rapidly evolving technology increases the chances of preparation, thus improving prognosis and also the effectiveness of defence. The professionals who perform the primary intervention appear on the spot as the first contact during disasters. While they carry out their professional work, they are under considerable psychological pressure, thus they are often unable to provide psychosocial support to others.

Revealing the causes of psychological trauma, its aspects, and helping to treat and endure the difficulties of crisis situations is a psychology matter. The intervention forces, the soldiers are also exposed to extreme level of stress, hence it would be necessary to monitor their mental health as well. In addition to their professional training, the intervention staff should be aware of the degree of their mental level and preparedness to prevent the development of depression, possibly post-traumatic stress disorder (PTSD). Thus, it becomes necessary to apply the possibilities of psychosocial support to disaster management tasks as well. The role of assistants helping in treatment is increasing, but the requirements for the assistants are not yet formulated.

Stress Resources and Treatment Possibilities

It is important to monitor the most important milestones during the development of mental assistance and to compare its possibilities and applied methods with its current situation to be suitable for future expectations as well.

The staff of the defence bodies needs psychological support, which is provided primarily by the psychologists of the defence organization in Hungary. However, the capacity is not sufficient for full support in several cases, thus investigating and improving psychological support has become essential. The mental preparedness and carrying capacity of the helper is an inevitable part of all support activities. Rescue forces are living in permanent stress, their adrenaline levels are usually high, which can have negative long-term effects. Thus, stability of the psychological and immune system of the primary intervention personnel is necessary.

Three groups of stressors can be divided into three subgroups:

1. Psychological stressors (social interactions, failures, conflicts, frustration, etc.);
2. Physical stressors (strong vibrations and sound effects, heat effects, injuries, sensory dimming, etc.);
3. Social stressors (severe family and social crises, major social changes, economic crises).

Stress-related changes and reaction can also be divided into three groups:

1. Psychic reactions, which can be:
   a. affective (emotional);
   b. cognitive, and
   c. motivational reactions.

2. Physiological (physical).
3. Behavioural reactions.

Stress is our body's response to different types of workload. The differences between eustress and distress are the triggers, the causes of stress stimulus. In many cases, it is not possible to determine the different effects of stressors. Eustress can be, for example, a new challenge, the excitement of the workplace, a long vacation, anything that fills us with positive excitement. The distress is the opposite of these, which tend to cause anxiety and fear, such as disasters, pandemics, hopelessness, financial difficulties, divorce, etc.

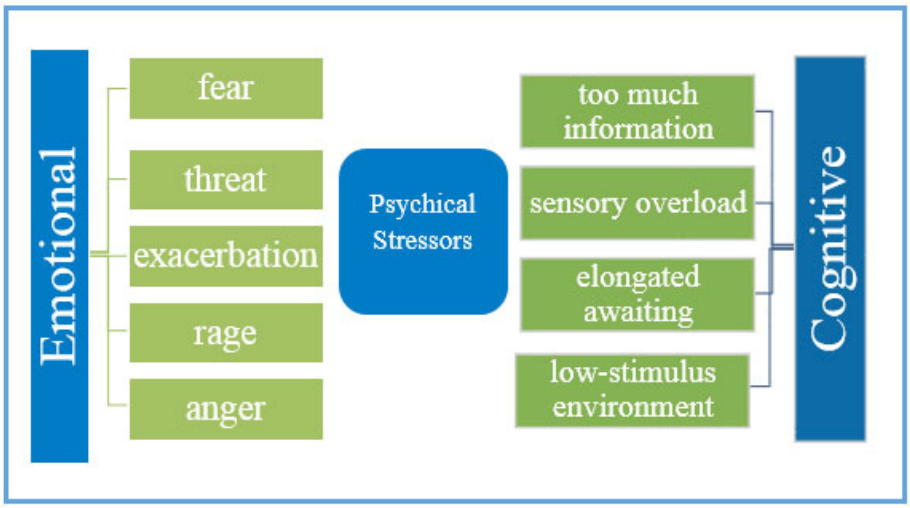

Figure no. 1: Emotional and cognitive causes of stress

To reduce the impact of the stress phenomenon, preventive measures are needed even before the stressor appears. Prevention in this case may include immediate treatment as well. Prevention aims to reduce the intensity of the effects of a stressor on an individual (Jones 1995).

One of the possible ways of prevention is the appropriate use of psychological measuring tools during the selection, as well as the regular psychological control and support of new employees. Furthermore, the process of training can be included in the prevention toolbox. This encompasses both professional (e.g., learning and using new technical tools), and psychological (e.g., reducing anxiety caused by ignorance) training. Preventive measures also include recognizing and treating the stress symptoms. Knowledge of the temporal aspects of stress reactions helps professionals to select appropriate tools and therapeutic methods for successful treatment (Barna n.d.).

Staff of national defence and disaster management organisations can frequently cope with fear and anxiety, but for several person's mental stability does not return to its balance because their psychic resources have been damaged because various stress reactions. In their case, crisis intervention is necessary (Pavlina – Komar, II. 2007). Crisis intervention is an immediate action that takes place within 72 hours of a crisis, when contacting relatives and family members is also part of the process. Rapid assistance helps prevent mental injuries and post-traumatic stress following a crisis. The focus is on resolving stress and fears, reducing acute symptoms, creating the opportunity to find mental balance. The feeling of fear occurs during a disaster when one is in trouble, and this process brings physiological changes that help to survive. However, it does not always lead to successful activity, because it can increase some ineffective escaping behaviour as well (Dr. Zellei 2000). Fear can be crippling for both body and mind. Fear can be felt towards real things, while the object of anxiety is a non-existent thing. Anxiety can occur suddenly and can often last for years.

Persons working in the field of assistance/protection are in especially difficult situations when struggling with some anxiety, and negative life situations because of the nature of their work, can affect their living. Since it is a negative feeling, we try to get rid of it, but it is almost impossible without mental treatment. Therefore, the fear of anxiety itself triggers another anxiety in us. This fact was articulated by anxiety specialist Tim Box in an interview [3]. He then put it this way about treating anxiety: "the biggest problem in treating anxiety is that we count it as a disease, even though anxiety is an emotion that is present in every person's life, to varying degrees, of course."

During mass disasters, rescue forces are also affected by psychological effects that would normally require psychological training to diagnose and treat. We hypothesize that stress effects affect their lives, thus there might be diseases in which there is a link between their health status and the experienced stress. The helping, protective and rescue forces perform a hard work in extreme conditions that is physically and mentally stressful. Their preparedness is provided by a combination of three important areas: professional knowledge, physical condition/fitness and mental preparedness. These must be established in the previous period, during trainings. During their work, they must be provided not only with the minimum care necessary for their existence and work, but because of the hostile and unhealthy conditions in many cases, their security must also be ensured. An important performance limiting factor is inadequate task allocation and inadequate timing (Hornyacsek 2011). In the following, we have summarized the results of research in a stress map and assigned those organizational and task-specific community resilience components that can be defined as effective protective factors.

[3] Tim Box: How to stop feeling anxious about anxiety, TedTalks, TedXFolkstone, Interview 14. 10. 2019. https://www.youtube.com/watch?v=ZidGozDhOjg&list=LL&index=5 downloaded in 01. 05. 2021.

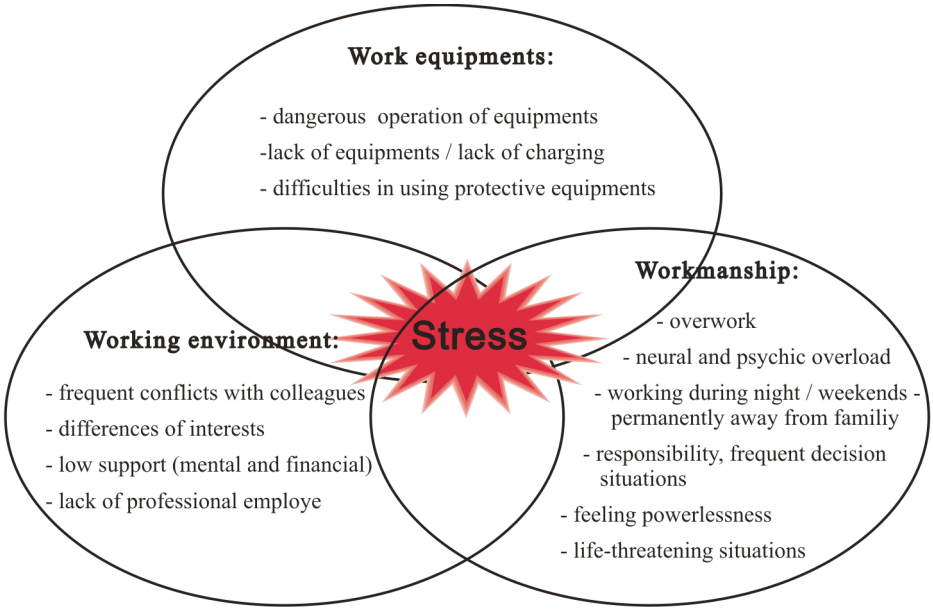

Figure no. 2: Stress map of the staff of defence bodies

Staff of defence bodies usually work together on phenomena that is much larger than their own tasks. Collectives, communities can thus achieve much greater results than individuals, but the individuals are needed to operate collectives. Therefore, workers can reasonably expect from both their leaders and vulnerability-reducing factors such as clothing, equipment, etc., to receive the appropriate support and protection. Experiencing and treating emergencies are processes that involve increased mental load, even extreme stress, and, in some cases, trauma. Extreme stress is a level of stress when the heart rate and blood pressure are close to the physiological limit, when cognitive functions, such as perception, are reduced, and inadequate emotional and behavioural reactions can occur. Thus, "paralysis of action", panic reactions, or symptoms of catastrophic syndrome[4] are typical (Urbán and Péter 2016).

[4] Catastrophic syndrome: Psychic and social problems what victims of crises and disasters usually experienced. Professionals of crisis management distinguish specific phases of the syndrome: pre-impact (restlessness and anxiety accompanying the threat), impact (disaster occurs and the community organizes rescue efforts), post-impact (often referred to as the "honeymoon phase" because it is characterized by high-energy struggle and mutual cooperation) and disappointment (when individuals face long-term consequences caused by a disaster).

Coping with stress is a complex process for which many psychological models exist. The definition of resilience goes back to Block (1969), who examined the factors of mental resistance. The concept of resilience has become very popular and widely used in recent years. In addition to not having a generally accepted definition, a number of different fields of research started to apply. The term "resilience" originated from the natural sciences, where it is defined as the ability of an object to return to equilibrium after disturbance (Bajayo, 2010). It is also widely used in the social sciences and psychology, where it refers to a similar human to reach the equilibrium after tilt over (Devaney 2014).

Experiencing a crisis situation can tilt an individual over of the stage of mental equilibrium and thus in many cases can cause mental illness, which can even lead to a pathological stage. According to the classic analytical interpretation, the ego is constantly struggling with the threat of the perceived world, while prevention can work unconsciously. Coping is a conscious struggling process, a struggle that constantly controls environmental effects to reduce fear. In examining what makes an individual more resilient than another, current psychological research concludes that certain protective factors that strengthen and/or maintain the resilience of one person (and a group) exist. The conditions for maintaining resilience can be distinguished into three main groups: the family, the individual and the environmental protection factors.

The main goal of resilience research in Hungary is prevention. In terms of health psychology, the role of protective factors responsible for the development of psychosomatic illnesses is mapped. An increase in resilience can only be expected from the combined effect of several components. Although post-disaster intervention by governmental and humanitarian organizations can trigger resilience development, long-term knowledge requires ongoing collaboration between organizations, communication between organizations and also with the public, development programs, project-based funding, and widespread dissemination of results (Sáfár 2018).

International Federation of Red Cross and Red Crescent (IFRC) provides perhaps the most accurate definition: "community resilience is the ability of communities exposed to disasters, crises, vulnerabilities to anticipate, prepare for, mitigate, adapt to, and recover from the effects of shocks and stress, without risking their own long-term plans and aims" (IFRC 2014).

The resilience of the community in the field of military services is largely determined by more favourable working conditions, supportive environment, and favourable group cohesion. Extraordinary situations have a particularly detrimental effect, but the common, ordinary effects should not be neglected either. In the defence field, such ordinary effects can be the constant readiness, the extreme load of wearing uniforms and protective clothing, and the peculiarities of the command system, during which the worker may find himself frustrated. It is not easy to process workplace mobbing, possible restrictions on personal freedom, and so on.

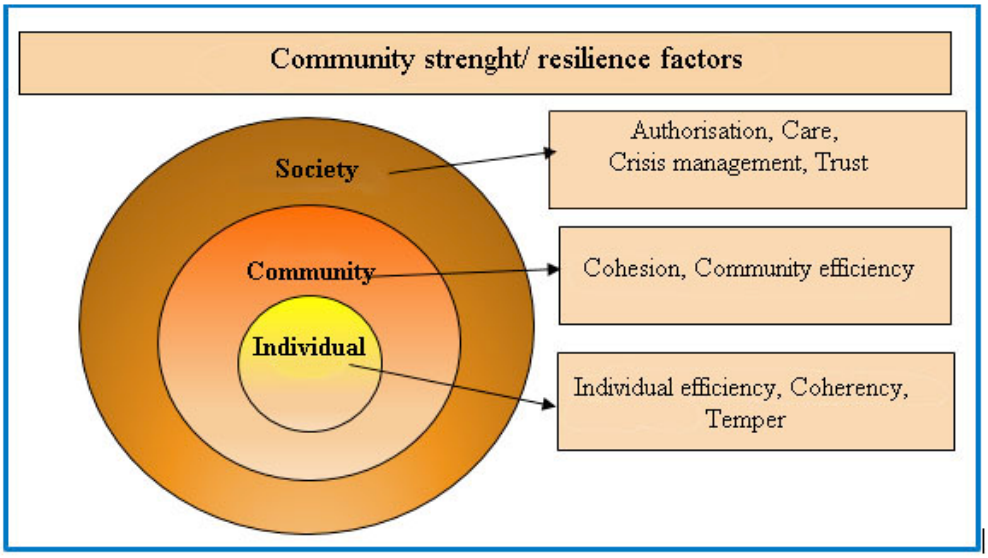

Figure no. 3: Resilience factors in different levels of community

Psychological and emotional support is necessary to maintain the mental health of all workers, helpers. Efforts should be made to minimize the effects of stress events and the symptoms of post-traumatic events. Workers should not be stigmatized when they are more affected by a stressful event or less able to treat it.

To help increase resilience, a leader should strive to ensure the opportunity for the members of the intervention team to share their experiences and feelings, either immediately or later after a stressful event. The potential sight of cadavers and the feeling of powerlessness constantly reminds the individual that he had suffered a negative phenomenon. Sight of several serious emotions, crying, breaking up families involve extreme levels of stress. The issue of mental assistance is a great opportunity, because if the mental health of the rescue staff decreases, the management of the problem, disaster, crisis and mitigation of its consequences would be endangered.

It should be an important task for the direct commander to monitor the reaction of the participants during the intervention event. Emotionally, intelligent leaders can handle their destructive thoughts and remain calm even in depressing situations. They can adapt quickly to the situation and also to the rapid changes. They cannot live life routinely, but should constantly upgrade their qualities or learn new coping techniques for stress treatment. If necessary, they should pick person(s) most affected by the stressful event out from the situation.

In our accelerated world, mental loads of the increasing challenges and the diversity of disasters are accumulating at an growing rate. Finding solutions for more and more distressing problems await leaders and disaster management commanders,

who need their mental, physical, and emotional renewal to do this. Thinking as a team-work, strengthening the cohesion also requires caring for personal and emotional aspects and competencies. Well-resonant leaders know exactly when to go into the details and when to just listen. New conversational techniques, or the ability to empathize can also help understand workers' mental state, thus commanders need to be increasingly open to this area as well. They would be able to encourage their employee, teammates, comrades even more when paying attention to mental assistance. There should be a natural need in the leader to bring hidden or silenced things to the surface from their subordinates, which can strengthen the trust. At the same time, today's leaders should also be aware of performance-oriented, highly ambitious individuals often report exhaustion, possibly burnout, which needs to be monitored as they can reduce the efficiency of their work. Unfortunately, these are not individual cases, their number is growing every day.

The mental balance of the intervention personnel should also be monitored, because if their mental balance suffers, they would feel emotionally and mentally threatened and hopeless, and they easily can fall into an "emotional vortex". They often realize they cannot overcome these psychological difficulties on their own. Fear is a very important emotion for the body's defence as it can trigger instinctive survival reactions. Fear exists in the life of all of us and can have both negative and positive effects. Jenő Ranschburg distinguishes between preventive (expected) fear and post-event panic, and has experimentally demonstrated that if the individual has the opportunity to experience the impending danger in time, he/she will acquire preventive activities more quickly and carry them out more effectively (Ranschburg 1983). Helpers have a big role in this process: anyone can be a helper who can be involved in treating the mental load, or can tip the person out of hopelessness. The main aim of mental assistance should be the acceptance of the experienced trauma and the same time giving hope and help starting the idea of redesign. Honesty, encouragement, empathy is needed for mental and emotional assistance. Additionally, a basic requirement is to not promise something we may not be able to fulfil, because it can deepen depression and give space to mistrust.

Several studies emphasized the important role of pro-activeness from helpers. There is a consistent conclusion that helpers should not wait for people who have suffered a disaster to seek help, as their current mental stage may not allow them to behave actively. People who have experienced a crisis or trauma often have narrowed focus and can concentrate on the given problem[5]. Generally, nowadays it is yet unusual to share our mental and psychological problems with an outsider, which can often seem ridiculous. Some people have the anxious felling that this behaviour is a sign of weakness, as well as an indication that an individual is unable to cope with their own situation. This should be changed in the collective minds of society.

[5] Interview with lieutenant colonel Péter Kovács (16.04.2014), who is the lead psychologist of Directorate for National Disaster Protecion Organization.

The lifestyle and direct environment of humans in the 21th century involves many positive things and situations, but unfortunately also can be a cause for constant concern. Nowadays, the emergence of epidemics, the constant struggling with disasters or terrorism are all problems that people must face (Besenyő 2017). The SARS-CoV2 pandemic has made everyday life especially difficult. Anxiety, fears, feelings of helplessness are becoming an increasing mental load on us. Doctors, health workers, soldiers and staff of disaster management forces on the front lines have a great responsibility. During their work, they may be affected by so high mental loads that are usually observed, for example, in the primarily intervention personnel during natural disasters or in war zones. The need of daily constant preparedness, fears, the proximity of deaths, and feelings of powerlessness can also trigger emotional trauma that can lead to serious mental problems.

Important aspects of mission tasks are to guarantee regional security and to cooperate with governments. It is also crucial to protect the civilian population and guarantee the security of international civilians. Soldiers delegated to missions are expected to be able to carry out their activities effectively even when employed in conditions other than those at home. For this, already gained experience is essential either as a subordinate or as a leader. Participation in team practice was previously an essential requirement, but this is no longer a significant part of practice. Impeccable health, physical and mental stability are essential for excellent and rapid situational awareness and decision-making (Besenyő, Participation of Hungary in African Operations between 1989-2019, 2019)

Conclusions

It can be stated that in order to successfully cooperate in all disaster-stricken areas, the intervention personnel work together with the civilians and non-governmental organizations. It can also be increasingly demonstrated that effective preparation reduces the extent of damage caused by disasters. Rapidly evolving technology can increase the level of preparation, however, a sense of vulnerability becomes perceptible. It can reinforce feelings of danger, unpredictability, anxiety, and fear, which may require the use of complex mental assistance. After examining the methods of psychosocial assistance, it is clear now that various methods are suitable for proper mental assistance both at the individual and community level. The mental treatment of disasters has various individual psychological and social effects. There are cases where the assistance staff/helpers also need help so that integrative collaboration between humanitarian organizations can provide a higher level of psychosocial and mental assistance and care. That is why it would be worthwhile to process and treat our experience, make them available and incorporate as soon as possible during the practices and preparations.

BIBLIOGRAPHY:

Jones, D. F.: Psychiatric Lessons of War, in: F. D. Jones et al. (eds.), War Psychiatry. – In. TMM Publications, Washington, D. C., 1995. pp. 1–33.

Barna, Boglárka: Psychological Methods of the Treatment of Combat Stress Based on Modern Armed Struggles. http://real.mtak.hu/104397/1/HSZ_2019_3-9_Barna_145-162.pdf, downloaded: 2021. 03. 21.

Hornyacsek, Júlia: The New Understanding of the Civil Protection and Recommentation on its Use woth the Help of the Example of the Events of Hurricane Katrina in New Orleans. Engineer Military Bulletin of University of Public Service (Hungary), 2011. vol. XXI. issue 1-4, pp 371-393.

Urbán, Nóra, PÉTER, László: A stresszel szembeni rugalmas vészreagálás (reziliencia) katonai aktualitásai. – In. Hadtudományi Szemle, 2016. vol. IX. issue 1. pp. 294-303.

Devaney, Lee (ed.): Community Resilience in Urban Areas. British Red Cross (Participants: Denmark, Hungary, Netherlands, United Kingdom), Budapest, 2014.

Sáfár, Brigitta: Deployment of standardized emergency response units in large scale emergencies. Engineer Military Bulletin of University of Public Service (Hungary), ISSN 2063-4986, 2018. vol28 issue 3, pp 164-173

Ranschburg, Jenő: Félelem, harag, agresszió (Fear, anger, agression). Budapest Textbook Publisher, 1983. p. 33.

Besenyő, János: Low-cost attacks, unnoticable plots? Overview on the economical character of current terrorism, Strategic Impact, 62/2017: (Issue No. 1) pp. 83-100. (2017), https://www.ceeol.com/search/article-detail?id=531307

Besenyő, János: Participation of Hungary in African Operations between 1989-2019, Óbuda University, Safety and Security Sciences Doctoral School, Budapest, 2019, pp. 97-100.

DOI: 10.53477/1842-9904-22-4

DEVELOPMENTS WITHIN THE DOCTRINE OF JOINT ACTIONS OF THE ISRAELI DEFENCE FORCES

Mihai VLAICU*

This paper has as its main focus the way in which the Israeli Joint warfighting doctrine has evolved in time, since the creation of the Jewish state, as well as the particularities and methods of improving the next stage of this type of doctrine, as outlined in the Momentum Plan released by the Israeli Defence Forces (IDF). The aim of the research is to assess whether the joint warfighting actions have given the IDF an edge in accomplishing the strategic objectives designed by the Israeli political leadership, as well as whether the next planned iteration of the Israeli joint warfighting doctrine, the Momentum Plan, is feasible and whether it has any vulnerabilities to address. The main methodological methods used in this paper are the case study of the conflicts where the IDF used joint warfighting actions as its main method of conducting operations, as well as the observation of actions that could prevent the Momentum Plan from achieving the desired results.

Keywords: *joint operations; anti-access/area-denial (A2/AD); combined arms; multi-domain battle (MDB);cross-domain maneuver (CDM); Momentum Plan.*

Introduction

Since the dawn of time, military organizations have tended to create specialised formations, based around different types of weapon systems, and develop their doctrine around the combined action of these formations.

Although it can be argued that the actions of the military in the First World War constitute the first examples of combined arms operations, due to the fact that

**** Mihai VLAICU is a Master Student in the field of Security and Diplomacy within the National University of Political Studies and Public Administration (SNSPA), Bucharest, Romania. E-mail: vlaicumihai10@gmail.com***

the air arms of most belligerents evolved during the interwar period, World War II can be considered the first war in which all categories of armed forces, air, land and sea, operated under equal terms, due to the technological advance achieved in the interwar period. The existence amongst the ranks of the first Israeli servicemen of individuals that have previously served in the armies of various nations during WWII (Israel Ministry of Foreign Affairs, 1999) has been a major influence in the IDF's acceptance and development of its own joint warfighting doctrine since 1948 (Israel Defence Forces 2017).

From the very beginning, the State of Israel was surrounded by hostile states, because of the cultural, religious and social differences between the Jewish and Arab populations (Kaplan 2012). At the same time, from a geographic stand point, it can be observed that the territory of Israel has reduced dimensions, thus making defence in depth actions on the ground infeasible and requiring for the IDF to use all its resources in order to deter possible adversaries (Allison 2016) or reach a quick, favourable outcome to any conflict.

1. Evolution of the Israeli Military Doctrine

The first clear demonstration of the usage of multiple domain missions is the Suez Canal War of 1956. The adequate supply of tanks, AFVs and artillery meant that IDF had to undergo a significant change in terms of methods of carrying out combat actions by Israeli Armed Forces (Brower 2018). Armoured formations, founded during the previous war, were brought to adequate level of manning and equipment, which led to their placement in the first echelon of frontline troops. Due to the manoeuver to fires ratio that was thus in their favour, the Israeli Ground Forces became a military structure that placed greater emphasis on offensive operations. Even more so, the IDF began to create and deploy specialised infantry formations, ranging from airborne to mechanised units, designed to function, either as the avant-garde or as units attached to the armoured forces, supported by specialised, and in some cases mobile, artillery units, establishing in this way the usage of combined arms formations in the land domain. The Paratrooper Brigade conducted its first combat drops during this conflict, proving that the IDF had the capability to conduct airborne operations in an efficient manner (Ginsburg 2015). Remarkable to the organisation of the Israeli airborne formations of the time was the inclusion of armoured and artillery sub-units in their order of battle, thus giving the whole formation the ability to execute combined arms manoeuver (Gawrych 1990).

In the aerospace domain, due to the purchases of new aircraft, planes were able to complete missions in the proximity of ground forces, thus ensuring air defence and close support of allied troops.

Lessons learned in the 1967 Six-Day War, mainly that of close tactical and operational coordination between the ground and air forces, were highlighted in the early stages of the 1973 Arab-Israeli War. The 1967 war had multiple results in the local political balance. Thus, Israel's decision to go to war through a surprise attack led to the refusal of France, Israel's main arms supplier at the time, to continue to provide the military equipment and related maintenance services required to the Israeli armed forces. Israel's exit from the sphere of influence of France (Bass 2010) led to the formal introduction of this state into the sphere of influence of the United States, due to its acceptance to take over the duties of Israel's main supplier of military equipment (Bowen 2017). Thus, the 1973 war became the first official war, through third states/proxies, between the two superpowers, the Soviet Union and the United States, in the Middle East. As is well known today, the first attempts of the IDF to push back the Syrian and Egyptian forces on both fronts were dominated by armoured advances, aided by Close Air Support missions, fact that the Arab forces pre-empted, due to its similarity to the IDF actions during the 1967 War (Israel Ministry of Foreign Affairs n.d.). The two most important factors that helped the Israeli forces to rally were the excessive deployment of Egyptian forces, besides their AAA coverage, as well as the fact that a number of Syrian AAA (anti-aircraft artillery) units have not completed the relocation of their equipment in time to provide coverage for their ground assets, facts that were used by the IDF to their advantage, through the usual air-land attacks. From this point of view, this conflict illustrated that air units cannot win wars on their own, requiring constant coordination between these troops and ground forces in order to stack their effects and enable commanders to manoeuver. The naval forces played a strategic role during the 1973 War, due to the fact that their deployment helped ensure the continued supply of IDF with ammunition and equipment. The Naval Forces, like the IAF (Israeli Air Force), have helped maintain Israel's ability to strategically hit targets, either inside the Arab territories (Israel Ministry of Foreign Affairs n.d.) that were previously considered safe by Arab leaders.

The end of the 1973 War brought no major changes in doctrine. The fact that Israel has managed to defeat the two most important opposing countries twice in less than ten years, eventually reaching a peace agreement with one of them, has strengthened Israel's prestige and managed to prevent any major attacks on its territory.

Although the 1978 attempt of IDF to launch a military operation in Lebanon faltered because of the lack of American support (Middle East Monitor 2019), the 1982 Invasion of Lebanon which has unclear motives, perhaps being more accurately described as the first Israeli War motivated mostly by internal politics (Oren 2017). More importantly, because of the uncertainty that was present among the majority of the political leadership of the time, the commanders could not be briefed accurately

with a conclusive set of objectives and timetables in which to achieve them (Oren 2017). At the same time, extra pressure was put on the commanders due to the fact that reserve units had to mobilise for the invasion of a country, a measure that proved to be unpopular, reducing the morale and the combat effectiveness of the troops (Rubin 1982), involving Israel into what its leadership envisioned as a limited war (Anton and Iordache 2007).

Although Operation "Mole Cricket 19" became the best-known operation during this conflict, rightly so given the fact that the IAF used drones for the first time in order to supress Syrian air defence batteries in the Bekaa Valley, other operations such as the amphibious landing carried out by IDF north of Sidon can provide even now a valuable blueprint for combined arms actions at the operational level due to the fact that the amphibious landings of ground assets was supported with a diversionary one, mainly consisting of interdiction missions carried out by missile boats of the Israeli Navy and IAF aerial assets (McLaurin 1989).

Furthermore, as a new element to the IDF doctrine, the IAF has deployed attack helicopters both in close air support missions for ground forces or in hunter-killer roles against mechanised or motorised assets of the Syrian and Lebanese forces (Israel Defense 2014).

More importantly, the 1982 War brought to IDF's attention the fact that it needed to adapt its' operating procedures to the urban terrain. The IDF excelled in the rural areas of the region, due to the fact that the majority of the population and resources were placed in those areas. Even the reclaiming of Jerusalem did not prove to be a challenging experience for the IDF as a whole. The Lebanese Conflict proved to be exactly that. The IDF came face to face with an enemy force who, besides its unwavering devotion to their religion, had the support of the local population, had knowledge of the operational battle-space, as well as the fact that it could be used as a deniable proxy force by its adversaries. Israel has also faced an important adversary, Israeli public opinion, due to the fact that the IDF presence in Lebanon was seen as an occupation and, more importantly, it was interpreted as a waste of lives and resources to achieve unclear goals.

The hit and run attacks and ambushes of Hezbollah and its proxies became a common fact, the emergence of IEDs (Improvised Explosive Devices) as an important tool in the insurgent's arsenal, as well as the introduction of missile attacks has shown the form of the actions that insurgents would take in the next series of conflicts, actions that IDF had to adapt in order to degrade or prevent them.

Since the conflict, IDF have had to adapt to the fight against unconventional opponents, whilst maintaining conventional war-fighting capabilities.

In the air field, the IAF adapted and used aerial means that could have considerable time on station, UAVs (Unmanned Aerial Vehicles), helicopters and SIGINT (Signals intelligence) aircraft gaining more attention due to the fact that operations, now known as targeted killings, had the following requirements:

– attacks on enemy structures or combatants was meant to be precise, in order to prevent collateral damage;

– the attacks were to be carried out at stand-off distance, that did not endanger the crew or the aircraft (Israel Defence 2014);

– The continuous fusion of data from sensors was to be achieved due to the requirement of maintaining awareness of the targets and of the surrounding battle-space (Sadot n.d.).

The IDF started developing tactics in order to prevent the usage of low tech methods by the insurgents, such as improvised artillery attacks or UAVs, either through adapting the tools for ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) used during targeted killing operations, or by deploying and adapting air defence and aerial assets to intercept the aforementioned kind of attacks.

In the maritime field, the Israeli Navy started increasing its manpower, due to the fact that it needed to enact interdiction operations against smuggling attempts by Hamas, PLO (Palestine Liberation Organization) or Hezbollah affiliated groups.

The ground domain is the one in which the IDF could be said to have developed largely due to the 1982 War and subsequent Intifadas. The need for the Land Forces to operate in heavily populated urban areas, where the majority of the inhabitants are hostile towards Israeli units, led to these structures to develop procedures, equipment and tactics specific to riot control after high profile incidents (Shipler, 1982). At the same time, the urban experience gained by the Land Forces during this conflict led to the widespread adaptation of one of Merkava Main Battle Tank's principles, that of being able to take infantryman into combat, to IDF's substantial tank reserves, creating heavy Armoured Fighting Vehicles (Markowitz 2018).

At the same time, due to the fact that, in addition to the early stages of the 1982 War, up to 2006, the IDF were mainly involved in low-intensity conflicts, naturally led to an over-emphasis on counter-insurgency tactics and operations, whilst the combined arms doctrine was placed on a secondary level of importance.

The 2006 War could be considered the last great moment the IDF learnt valuable lessons in the combined arms operations. The emergence of Hezbollah as a prototype of what would later be known as a hybrid force created multiple difficulties for the Israeli armed services.

For the first time since the 1982 war, the IDF faced a challenge, both for its frontline troops and, even more importantly, in the depth of its own perimeter, an asymmetric formation, Hezbollah, proving that it had the means and the will to stop Israeli strikes and to disrupt the Israeli mobility operations.

The IDF's answer was to start a endowment program aimed at counteracting the threats posed by Hezbollah's actions. In the field of land forces, Active Protection Systems, adapted to Soviet systems, were put into production and distributed

massively to armoured, mechanised and even motorised formations (Markowitz 2018). Heavy AFVs, previously introduced during the 1982 War, were modernized due to the need to operate in an urban environment, where ambushes by heavily armed infantry formations were common occurrences. At the same time, the Land Forces started introducing elements of "network-based warfare", such as the Tsayad system, meant to offer commanders a more accurate assessment of the battlefield and to increase the level of coordination between troops (Defense Industry Daily 2007).

One of the most important lessons by the IDF is the one regarding missile defence. Although a number of systems, such as David's Sling, Iron Dome or the Arrow series, were developed during the 2006 Lebanon War, the frequency and complexity of Hezbollah's missile attacks had given the impulse needed for these systems to be tested and implemented faster (Rapaport 2010).

Also, Land Forces recognised the importance of applying the lessons learned in the conventional conflict to the fight against unconventional forces, one of these being the control of the territory, mainly rural, through the establishment of checkpoints meant to control the flow of personnel and equipment (Matthews 2008), a practice taken over by the Israeli Border Police.

2. The Momentum Plan-Adaptation to Change

The mass development of anti-access/area-denial technologies by a number of countries, such as Russia and China, has determined the Western military community, the Israeli included, to take actions in order to either prevent the establishment of such systems and, in the case of deployment by a potential adversary force, to degrade, deny or destroy the respective system in order to allow friendly forces the ability to manoeuvre in the depth of the adversary's battle-space. The use of A2/AD (Anti-Access/Area Denial) systems is not new, given that during the Cold War, all sides developed and deployed surface-to-air and surface-to-surface missile systems, a fact taken into account during the period's military planning.

The present tendency to plan for the neutralization of this systems can be viewed through the prism of the "great power competition" that takes place nowadays, as well as the military's need to find a potential adversary in order to stay relevant for funding.

The US Armed Forces, with the US Land Forces at the forefront, have taken steps to update the end of Cold War strategy of the AirLand Battle, adapt the new (to a certain extent) cyber and space elements, by creating the MDB/CDM (Multi Domain Battle/Cross-Domain Manoeuver) (South 2019). These armed forces consider that the first operating procedure would apply with tactical and operational means, whilst allowing operational and strategic level commanders to employ Cross Domain Manoeuver, using the effects of multiple types of formations in order to

achieve the desired effect of manoeuvring in the opposing force's strategic depth (South 2019). Thus, it can be argued that this type of actions are an update to the combined arms tactics used in the previous century.

Israel is firmly placed in the style of Western military thinking, making adoption of the MDB/CDM for the IDF almost a fact. Considering that the main countries actively deploying the A2/AD types of systems, Russia and China, are traditional suppliers of ammunition for potential Israel opponents, such as Syria, Hezbollah and Iran, offer the rationale behind the IDF's call for a new type of overarching set of principles and tactics (Bethel, 2016).

The IDF's variant of the MDB/CDM has been called the Momentum Plan, due to the fact that it calls for "strong manoeuver capabilities" (Frantzman, 2020) and "temporary breaches" (Ortal 2020), using "through the concentration of strike capabilities and through advanced ISTAR capabilities (Ortal 2020). What differentiates the Momentum Plan from MDB/CDM is that IDF plan takes into account the need for destroying enemy assets firing at friendly civilian objectives, promoting thus a whole-of-government approach regarding warfare (Ortal 2020).

One of the main characteristics of the Momentum Plan is the establishment of "expose and destroy companies", small formations meant to attract enemy fire in order to provide friendly ISTAR objectives the opportunity to locate, fix and destroy the opposing force formation (Shaham 2021).

A unit created around the principles of the Momentum Plan was established in 2019, under the name Unit 888. The latest publicly available information with regards to this unit was presented in 2020, stating that the unit will consist of servicemen from the infantry, engineers, armour and aviation weapons, with the planned integration of transfer of servicemen coming from the intelligence and communications branches of service, for the start of the first training activities of the unit (i24NEWS 2020).

Conclusions

The IDF has, from its very beginning, been a force that used to the fullest the concepts of combined arms formations, in order to enable breakthrough of the opposing side's frontlines and rapid manoeuver for the achievement of envelopment and eventual surrender.

The evolution of the environments in which the units of the IDF have thought enable this organisation to assimilate a number of new technologies and tactics, remaining, even after this most recent conflict, at the forefront of military innovation and achieving its aim of protecting the Israeli nation.

Although the Momentum Plan aims to provide a rapid victory, integration with joint forces such as the United States, and synergy between the various categories of forces, shows planners that they have to consider a number of facts.

Firstly, the fact that electronic countermeasures in place by the opposing force could degrade or deny the IDF of its' informational superiority and, more importantly, the use of networked, precision-focused systems, countermeasures such as those used in the conflict in Ukraine.

Secondly, the concept of "expose and destroy companies" could prove to be flawed. Recent examples that should be kept in mind are the usage of remotely-operated weapons by ISIS (Islamic State in Iraq and Syria) in the Middle East, the deployment of similar systems by Hamas or Hezbollah meaning that IDF subunits would expose themselves to a volley of accurate and constant level of fire, in order to achieve the destruction of what amounts to a little more than a robot in a building. Although jamming could be an answer used by the IDF, pattern recognition software readily available on the Internet could negate this countermeasure.

Thirdly, the Momentum Plan focuses on the delivery of blows by all three categories of IDF forces, thus giving the Land Forces ample freedom of deployment in regions such as Gaza or Lebanon. However, whilst the MDB/CDM take into consideration the appearance of a peer competitor, the Momentum Plan excludes this, focusing on unconventional opponents with access to highly sophisticated weaponry, thus not taking into account the appearance of an equal competitor for Israel, such as Turkey, which could maximize the usage of aerial and naval means to degrade or destroy Israeli troops. The recent tensions in the Eastern Mediterranean Sea between Turkey and the other NATO members, such as Greece and Turkey, may provide examples of growing Turkish influence in the region, which could interfere with the economic and political activities of the state of Israel, leading to the need to adapt the IDF in order to combat possible aggressive actions by conventional state actors.

Lastly, the usage of joint warfare actions by the IDF has enabled this organization to achieve considerable advantages over its adversaries in both urban and rural areas. At the same time, the 1982 and 2006 wars in Lebanon have proven to be conflicts where the IDF faced initial, doctrinal difficulties and were able to identify and remedy them, proving a considerable level of adaptability that could be applied if the Momentum Plan needs to be further developed.

BIBLIOGRAPHY:

Allison, G. (2016). *Why ISIS fears Israel*. Retrieved 05 15, 2015, from https://www.belfercenter.org/publication/why-isis-fears-israel

Anton, S., & Iordache, G. (2007). General Considerations Regarding Military Actions Carried out in the Current Security Environment. *UNAP Bulletin, Nr.1*, p. 39.

Brower, K. S. (2018). *The Israel Defense Force, 1948-2017*. Retrieved 05 15, 2021, from The Begin-Sadat Center for Strategic Studies: https://besacenter.org/wp-content/uploads/2018/06/150-MONOGRAPH-Brower-IDF-1948-2017-WEB-UPDATED.pdf

Defense Industry Daily. (2007). *Tadiran Wins $205.M Follow-On for Advanced Radios*. Retrieved 05 15, 2021, from https://www.defenseindustrydaily.com/tadiran-wins-205m-followon-for-advanced-radios-02973/

Gawrych, D. G. (1990). *Key to the Sinai: The Battles for Abu Ageila in the 1956 and 1967 Arab-Israeli Wars.* Retrieved 05 15, 2021, from United States Army University Press: https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/key-to-the-sinai.pdf

Ginsburg, M. (2015). *59 years after last combat use, why do Israel's paratroopers need new chutes?* Retrieved 05 15, 2021, from https://www.timesofisrael.com/59-years-after-last-combat-use-why-do-israels-paratroopers-need-new-chutes/,

i24NEWS. (2020, 03 01). *IDF unveils new, revolutionary multi-faceted combat unit*. Retrieved 03 19, 2022, from https://www.i24news.tv/en/news/israel/diplomacy-defense/1577894720-idf-unveils-new-revolutionary-multi-faceted-combat-unit

Israel Defence Forces. (2017). *War of Independence*. Retrieved 05 15, 2021, from https://www.idf.il/en/minisites/wars-and-operations/war-of-independence/

Israel Defense. (2014). *The End of the Cobra Era*. Retrieved 05 15, 2021, from Israel Defense: https://www.israeldefense.co.il/en/content/end-cobra-era2014

Israel Ministry of Foreign Affairs. (n.d.). *The Yom Kippur War (October 1973)*. Retrieved 05 15, 2021, from https://mfa.gov.il/mfa/aboutisrael/history/pages/the%20yom%20kippur%20war%20-%20october%201973.aspx

Kaplan, R. D. (2012). *The Revenge of Geography.* New York: Random House Trade Paperbacks.

Markowitz, M. (2018). *Israel's Heavy Armored Personal Carriers*. Retrieved 03 19, 2022, from https://www.defensemedianetwork.com/stories/israels-heavy-armored-personnel-carriers/

Matthews, M. M. (2008). *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War.* Retrieved 05 15, 2021, from United States Army University Press: https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/we-were-caught-unprepared.pdf, 2008

McLaurin, R. (1989). *The Battle of Sidon.* Retrieved 05 15, 2021, from Defense Technical Information Center: https://apps.dtic.mil/dtic/tr/fulltext/u2/a217091.pdf

Middle East Monitor. (2019). *Remembering the Israeli withdrawal from south Lebanon*. Retrieved 05 15, 2021, from https://www.middleeastmonitor.com/20190613-remembering-the-israeli-withdrawal-from-south-lebanon/

Oren, A. (2017). *With Ariel Sharon Gone, Israel Reveals the Truth About the 1982 Lebanon War*. Retrieved 05 15, 2021, from https://www.haaretz.com/israel-news/with-sharon-gone-israel-reveals-the-truth-about-the-lebanon-war-1.5451086

Ortal, E. (2020). "Momentum" Multi-Year Plan: A Theoretical Framework. *Dado Center Journal, Nr28-30*.

Rapaport, A. (2010, 07). *The IDF and the Lessons of the Second Lebanon War.* Retrieved 05 15, 2021, from Begin-Sadat Center: https://besacenter.org/wp-content/uploads/2010/07/MSPS85En.pdf

Rubin, T. (1982). *Israeli Army breaks ranks over its role in Lebanon fighting*. Retrieved 05 15, 2021, from https://www.csmonitor.com/1982/1005/100538.html

Sadot, U. (n.d.). *A Perspective on Israel*. Retrieved 05 15, 2021, from Center for New American Security: http://drones.cnas.org/reports/a-perspective-on-israel/

Schimdt, A. (2016). Countering Anti-Access/Area Denial Future Capability Requirements in NATO. *Joint Air Power Competence Centre Journal, Nr.23*, pp. 69-77. Retrieved from https://www.japcc.org/countering-anti-access-area-denial-future-capability-requirements-nato/

Shaham, U. (2021). *IDF establishes 'expose and destroy' companies for the modern battlefield*. Retrieved 05 15, 2021, from https://www.jpost.com/israel-news/idf-establishes-expose-and-destroy-companies-for-the-modern-battlefield-664495

South, T. (2019). *This 3-star Army general explains what multi-domain operations mean for you*. Retrieved 05 15, 2021, from https://www.armytimes.com/news/your-army/2019/08/11/this-3-star-army-general-explains-what-multi-domain-operations-mean-for-you/

United States Army Maneuver Center of Excellence. (n.d.). *Maneuver Self Study Program.* Retrieved 03 19, 2022, from 2018: https://www.benning.army.mil/mssp/Combined%20Arms%20Operations/

United States Army Training and Doctrine Command. (2018). *TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations 2028.* Retrieved 03 19, 2022, from https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf

United States Army Training and Doctrine Command. (2020). *AFC Pamphlet 71-20-2 Army Futures Command Concept for Brigade Combat Team Cross-Domain Maneuver 2028.* Retrieved 03 19, 2022, from https://api.army.mil/e2/c/downloads/2021/01/05/79256d9f/20200814-afc-pam-71-20-2-afc-concept-for-bct-cross-domain-maneuver-final.pdf

United States Department of Defense. (2021). *DOD Dictionary of Military and Associated Terms.* Retrieved 03 19, 2022, from United States Department of Defense Joint Chiefs of Staff: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

DOI: 10.53477/1842-9904-22-5

PRESENCE OF INTELLIGENCE SERVICES ON FACEBOOK

Oana-Cătălina FRĂȚILĂ*

This study is based on the need to demonstrate the opportunity that social networks represent for the recruitment of human resources in terms of information that is constantly shared by users. We chose to focus on intelligence services because they are more reluctant than the other structures empowered to ensure national security in terms of social media activity.

Through this analysis we discovered that although many intelligence services own official pages on social networks, there are few intelligence services that share content on them. Of the 12 Facebook pages analyzed, we identified posts with content related to human resources recruitment only on the pages of four intelligence services.

***Keywords**: intelligence services; Facebook; recruitment; human resources; posts; users.*

Introduction

The present study aims at identifying the need for intelligence services to use social networks in the process of recruiting human resources. Many of the military organizations, including the intelligence services, are publicly present on social media. In order to achieve the objective, we will analyze the work carried out on social networks by the most important intelligence services in the world. Through this research, we aim to establish whether they are intelligence services that use social networks as a means of attracting human resources and how they do so.

**** Oana-Cătălina FRĂȚILĂ is a PhD Student at the "Mihai Viteazul" National Intelligence Academy, Bucharest, Romania. E-mail: fratila.catalina@animv.eu***

1. Choice of Reference Group

The first step in conducting the research was to identify the social network that in question, and the second step was to establish the intelligence services we will analyze. In order to achieve this, we have set a criterion to help us objectively choose the social network and a criterion on the basis of which to objectively choose the intelligence services. When choosing the social network, we will consider the number of users, and in the case of choosing intelligence services, we will identify the latest research in which the classification of the best information services in the world has been carried out.

Since we cannot carry out research on all existing intelligence services, and also we do not have the necessary tools to achieve a new ranking of them, we will look for a classification made by other researchers of the intelligence services that have established themselves worldwide over time. Through a single search of the phrase *best secret services in the world* on the search engine, we identified several articles in the foreign press in which the classification of the secret services in the world was made. The most recent list was made in June 2021, by Anuj Tiwari of the India Times (Table no. 1). Being the newest classification, we will include the results of this research in the reference group of intelligence services taken into consideration in the present study. We cannot confirm the validity of the data in the identified classification, but our research is not influenced by this, nor is it intended to classify the best intelligence services. It is important to choose objectively the intelligence services whose activity in the online environment we will follow.

For the choice of the social network that we will use in this research, we have taken into account the number of active users. According to the information identified on the Data Reportal website, Facebook is the social network used by most people (DataReportal 2021). Since its emergence, Facebook has been the most used social network, globally, this being the reason for its inclusion in this research. Notwithstanding, intelligence services are also officially present on other social networks, presumably Twitter and Instagram.

Facebook is a social network that allows users to create an online profile through which to interact with other users. Through their profile, users can get involved in various online activities, such as: sharing photos, posting comments, sharing the location or distributing personal information (Padyab, and Others 2016). A large amount of information can be shared on Facebook, all that matters is how willing users are to share their personal data with other users.

Therefore, Facebook's features show the intelligence services could use this social network to identify or attract potential candidates. The activity that potential candidates perform on Facebook can determine their compatibility or incompatibility with the specifics of the intelligence services. Their posts, the people who are on their

list or the likes they make, help to sketch a candidate profile which can be compared to the profile sought by the intelligence services. Intelligence services may also use Facebook to send messages aimed at attracting potential candidates.

Table no. 1: The best information services in the world
Source: (Tiwari 2021)

Central Intelligence Agency (CIA), USA
Research and Analysis Wing (RAW), India
Mossad, Israel
Inter-Services Intelligence (ISI), Pakistan
Secret Intelligence Service (MI6), UK
Main Intelligence Agency (GRU), Rusia
Ministry of State Security (MSS), China
National Investigation Agency (NIA), India
National Security Agency (NSA), USA
Federal Security Service (FSS), Rusia
Bundesnachrichtendienst (BND), Germania
Intelligence Bureau (IB), India
General Directorate for External Security (DGSE), Franța
Federal Bureau of Investigation (FBI), USA
Australian Secret Intelligence Service (ASIS), Australia
Canadian Security Intelligence Service (CSIS), Canada

The next step in our research was to verify the existence of a Facebook page associated with each previously identified intelligence agency. To achieve this, we have introduced the name of each intelligence service, in part, on the social network Facebook, both in English and in the official languages of the countries of origin. As a result of the searches, we identified official pages on Facebook for twelve intelligence services out of the 16 previously identified. The results of the searches performed on Facebook are shown in Table no. 2.

The four intelligence services for which we have not identified official pages on Facebook come from: Australia, Canada, India and Russia. Canada and Australia each have one service in the list identified, instead India owns three, and Russia owns two, therefore Australia and Canada are no longer the subject of our research. The best services in the world with official Facebook pages belong to the following countries: USA, India, Israel, Pakistan, UK, China, Russia, Germany and France.

Table no. 2: List of intelligence services that have official Facebook pages
Source: (Tiwari 2021)

Central Intelligence Agency (CIA), USA
Research and Analysis Wing (RAW), India
Mossad, Israel
Inter-Services Intelligence (ISI), Pakistan
Secret Intelligence Service (MI6), UK
Ministry of State Security (MSS), China
National Security Agency (NSA), USA
Inter-Services Intelligence (ISI), Pakistan
Federal Security Service (FSS), Rusia
Bundesnachrichtendienst (BND), Germania
General Directorate for External Security (DGSE), Franța
Federal Bureau of Investigation (FBI), USA

2. Research Methodology

Our research was based solely on public social media posts shared by intelligence services. All the information obtained complied with the terms and conditions imposed by social networks. We also mention that in the research we used only public information, posted by the intelligence services, without asking them for additional information. The intelligence services have nothing to do with the conducted research (McCulloh, and others 2020).

Most of the activities conducted by the intelligence services are secret, which is why there have been situations in which citizens misunderstood the need for secrecy of activities and accused the intelligence services of lack of transparency in the execution of missions. To eliminate this aspect, some intelligence services have decided to take advantage of the opportunity offered by social networks and be publicly present in the online community. This can be an *indicator* of the importance that social networks have for intelligence services. In terms of quantity, we have determined that most intelligence services are publicly present in the online environment, having official pages on the social network Facebook. The next stage of the research was to qualitatively analyze their presence on Facebook, and this we did, using content analysis as a research method. The analysis involved tracking the posts shared on the Facebook page of each intelligence service, in part. We distributed the identified posts in three categories: recruiting human resources,

promoting the institution, and informing the citizens. The category of interest in this research is the category of posts related to the recruitment of human resources, but we found it useful to quantify all posts so we could observe, compared to the other categories, the attention paid to this stage. To categorize the posts, we considered the message that the post was sending.

To determine the time frame that we will have as a benchmark in the research, we considered the event that caused changes worldwide. Initially, we had planned to follow the activity of the intelligence services on the social network Facebook during a year (July 2020 – July 2021), but we considered that there is a possibility that the coronavirus pandemic will change the data obtained and the importance of the role of social networks for intelligence services. So, we decided to frame the study between the time of the outbreak of the pandemic and the time of the research (July 2021). The next step in conducting the research was to check each official page of each service and to quantify the posts from each month of the established period. We analyzed each post to identify its message, and later placed the post in one of the established categories.

3. Analysis of the Activity of the Intelligence Services on the Social Network Facebook

Central Intelligence Agency (CIA), USA

The CIA joined the social media community in 2014. The intelligence agency became visible in the online environment to be close to the citizens, given the agency's activity has the citizen at its core. The first social network in which the CIA appeared was Twitter, and the first post was meant to amuse the followers: "We can neither confirm nor deny if this post is the first" (Crilley and Pears 2021), but also to convey the message that from that moment on they will be present in the online environment, publicly. The status of posts shared on the CIA's official Facebook page between December 2019 and July 2021 is shown in Table no. 3.

Inter-Services Intelligence (ISI), Pakistan

ISI was founded in 1948, with the main purpose of facilitating the distribution of information between the armed forces, naval forces and air forces. Following the introduction of the name of this service in the search box of Facebook, several pages have been aidentified. We checked these pages to pinpoint the one belonging to ISI. The first criterion taken into consideration was the option that shows the verified pages, but none of the pages were checked, so the next criterion we had in mind was the existence of the link that connects the Facebook page to the official website of the service. This is how we identified the Facebook page on which we carried out the research of the posts, and their situation is shown in Table no. 4 (Banerji 2011).

Table no. 3: CIA activity on Facebook
Source: (Tiwari 2021)

Month and year	Informing citizens	Promotion of the institution	Recruitment of human resources
July 2021	7	6	9
June 2021	9	5	10
May 2021	6	8	7
April 2021	8	10	6
March 2021	8	9	7
February 2021	11	11	4
January 2021	11	7	3
December 2020	10	4	8
November 2020	7	7	10
October 2020	11	8	8
September 2020	10	13	8
August 2020	9	9	9
July 2020	8	9	10
June 2020	6	5	7
May 2020	8	18	7
April 2020	15	10	11
March 2020	10	17	9
February 2020	6	10	8
January 2020	6	6	11
December 2019	13	11	8

National Security Agency (NSA), USA

This American intelligence service owns a page on the social network Facebook on which posts were distributed every month during the analyzed period. The purpose of the posts differs from month to month, as we can see in Table no. 5, that is, there are months in which posts predominate that have the role of either informing citizens or promoting the work of the NSA, and there are months in which posts with reference to the recruitment of human resources predominate.

Table no. 4: ISI activity on Facebook
Source: (Tiwari 2021)

Month and year	Informing citizens	Promoting the organization	Recruitment of human resources
July 2021	2	1	0
June 2021	3	2	1
May 2021	6	5	1
April 2021	3	1	0
March 2021	0	1	0
February 2021	4	4	0
January 2021	5	9	0
December 2020	0	0	0
November 2020	0	0	0
October 2020	0	0	0
September 2020	0	0	0
August 2020	0	0	0
July 2020	0	0	0
June 2020	0	0	0
May 2020	0	0	0
April 2020	0	0	0
March 2020	0	0	0
February 2020	0	0	0
January 2020	0	0	0
December 2019	0	0	0

Federal Bureau of Investigation (FBI), USA

The FBI is the last foreign intelligence service for which we conducted the research on the Facebook page. The number of posts to inform citizens is much higher than the number of posts are meant to promote the institution and the number of posts that have the role of recruiting human resources. The status of posts, for each month, is shown in Table no. 6. Posts with content about recruiting human resources may be in the form of information related to certain institutions in which schooling for the FBI is conducted, or they may be direct calls to citizens to fill vacancies.

Table No. 5: NSA's facebook activity
Source: (Tiwari 2021)

Month and year	Informing citizens	Promoting the organization	Recruitment of human resources
July 2021	4	3	8
June 2021	6	6	10
May 2021	2	2	1
April 2021	4	5	4
March 2021	3	9	10
February 2021	5	4	4
January 2021	0	6	3
December 2020	7	8	8
November 2020	6	4	4
October 2020	8	8	10
September 2020	3	1	7
August 2020	3	2	9
July 2020	5	3	9
June 2020	3	5	5
May 2020	3	3	8
April 2020	5	2	4
March 2020	5	10	8
February 2020	6	11	15
January 2020	3	3	10
December 2019	6	1	13

4. Inactive Information Services Present on Facebook

Of the intelligence services identified as the best and being present on the social network Facebook, there are a few that do not use this social network for sharing posts. We followed their activity during the researched period, and we presented the situation of each intelligence service in this subchapter.

One of the intelligence services that does not have activity on the Facebook page is RAW (The Foreign Intelligence Agency of India). This intelligence service did not provide much information to citizens about the work they carry out, and so there were many assumptions about the actions in which RAW was involved (Shaffer 2015). Although RAW created a Facebook page, only two posts were shared in 2013,

the same year in which it was created, and since then the activity on this page has stopped. During the time we conducted the research, no posts were shared. We could not conduct an analysis of the work carried out on Facebook of this service, which is why we stated that RAW agents do not follow the recruitment of human resources through the social network Facebook. While entering the Facebook community was an attempt for RAW to be more visible to citizens, this attempt was abandoned shortly after the initiation.

Table no. 6: FBI Activity on Facebook
Source: (Tiwari 2021)

Month and year	Information to citizens	Promotion of the institution	Recruitment of human resources
July 2021	61	7	2
June 2021	61	14	7
May 2021	69	29	25
April 2021	98	13	38
March 2021	96	15	26
February 2021	87	5	20
January 2021	113	4	16
December 2020	87	13	19
November 2020	53	12	15
October 2020	71	13	14
September 2020	68	10	12
August 2020	92	12	15
July 2020	87	11	9
June 2020	67	14	13
May 2020	59	9	7
April 2020	101	15	16
March 2020	87	14	11
February 2020	99	17	15
January 2020	85	14	9
December 2019	88	16	13

We continued with the analysis of the Facebook page of the Israeli intelligence service. In the case of Mossad, the situation is similar to that of RAW, which means that only one post was shared this year, on July 21, and the post prior to it was shared in 2019. This year's post was aimed at presenting the Facebook page and

guiding citizens to address the intelligence service through it, assuring them that it is a very secure means of communication. Therefore, within Mossad, the social network Facebook is not used to recruit candidates.

For The Secret Intelligence Service (MI6), the foreign intelligence service of the United Kingdom, a page was created on the social network Facebook in August 2019, but there has been no activity on this page since then until the time of this research. Although MI6 leaders acknowledge that social media offers the opportunity to find out valuable information, they did not focus on creating a page that would attracts citizens.

The Chinese intelligence service, The Ministry of State Security (MSS), has a Facebook page created in 2015, but no posts have been shared since then. A single post appears on this page describing the mission of the service. We have identified the Facebook page of this information service using Chinese, although the English translation also appears on the name of the page.

The Russian intelligence service, The Federal Security Service of the Russian Federation (FSS), created an official Facebook page in November 2019, just before the outbreak of the pandemic. On the day the page was created, several posts were shared, but subsequently we did not identify any other activities, apart from a single post at the beginning of 2021, specifying the ways in which possible terrorist acts can be reported. Therefore, the FSS Facebook page does not track the recruitment of human resources.

The German intelligence service, The Bundesnachrichtendienst (BND), is not active on Facebook. Although there is a Facebook page related to this intelligence service, there is no recorded activity. Therefore, the recruitment of human resources through the social network Facebook by the German intelligence service is not pursued.

The French intelligence service, The General Directorate for External Security (DGSE), is present on the social network Facebook, but the Facebook page does not imply the existence of a profile yet presupposes that there is a way for other persons to be able to mention that they have visited that service. For this reason, we affirm that DGSE is not one of the intelligence services that uses Facebook to recruit new employees.

5. Interpretation of Results

Drawing a parallel to a research conducted by Landon-Murray in 2015, where the work carried out by the US intelligence services for a fixed period was tracked, we note that there are both differences and similarities between the activity conducted by the intelligence services on social networks in 2015, compared to the activity carried out by them in 2021.

In 2015, CIA was the American intelligence service that shared the most posts on Facebook (Landon-Murray 2015), but according to our research, in 2021, FBI is the U.S. service mostly active on Facebook. In the same study conducted in 2015, it was shown that the NSA predominantly distributes on its Facebook page posts that have the role of recruiting human resources (Landon-Murray 2015). At the time of our research, as can be seen in Figure no. 2, posts that have content related to the recruitment of human resources continue to predominate on the NSA's Facebook page.

The research carried out showed us that from the list of the best intelligence services in the world, during the research period, it is the FBI that shared the most posts on Facebook, followed by CIA, NSA and ISI. Instead, NSA is the intelligence service that has shared the most posts related to human resource recruitment compared to other types of posts.

ISI does not have a lot of activity on Facebook, and regarding posts for recruitment purposes, ISI shared only one post in May 2020 that referred to the possibility of being part of the ISI community. Since then, there have been no posts that attract candidates to the service, which is why we can deduce that this way of recruitment is not a priority for this intelligence agency.

The efficiency of the recruitment of human resources by the FBI in the online environment is a topic that has been addressed in other researches. For example, the results of a research in which a case study on the FBI was conducted showed that organizations that post messages on social networks to recruit human resources can identify more people to meet the requirements, and the financial implications are much lower when using social networks as a tool for recruiting human resources (McCulloh, and others 2020).

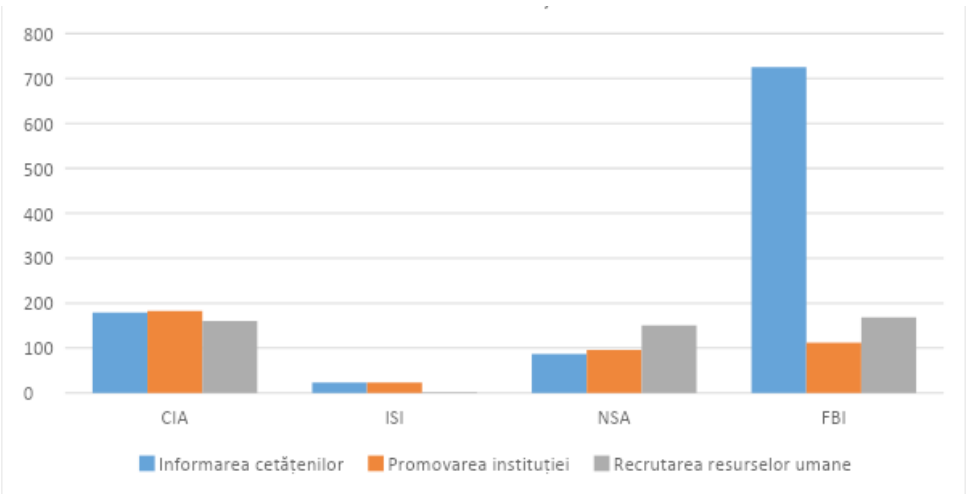

Figure no. 1: Posts shared on Facebook by foreign intelligence services

Conclusions

Researching intelligence services' posts shared on Facebook pages has helped us understand they are taking advantage of the opportunities offered by social networks. The large number of social media users and the increased time they spend online determine the need for intelligence services to be part of the social media community.

Although we have analyzed the activity on the social network Facebook of some intelligence services, from several states, we can see that only the US intelligence services are focused on the distribution of posts aimed at recruiting human resources. Moreover, of the twelve intelligence services that are officially present on Facebook, only four are active, and of the four, three are American intelligence services, the fourth being Pakistani.

Thus, the conclusion that can be drawn from the research is that, at international level, although the need for intelligence services to be officially present on Facebook has been identified, most intelligence services do not use this social network to attract potential candidates.

BIBLIOGRAPHY:

Banerji, Rana. 2011. "Pakistan: Inter Services Intelligence Directorate (ISI) An Analytical Overview." *Journal of Defence Studies* 1-27.

Crilley, Rhys, and Louis Pears. 2021. "'No, we don't know where Tupac is': critical intelligence studies and the CIA on social media." *Intelligence and National Security* 599-614.

DataReportal. 2021. *GLOBAL SOCIAL MEDIA STATS.* https://datareportal.com/social-media-users.

Landon-Murray, Michael. 2015. "Social Media and U.S. Intelligence Agencies: Just Trending or a Real Tool to Engage and Educate?" *Journal of Strategic Security* 67-79.

McCulloh, Ian, Nathan Ellis, Onur Savas , and Paul Rodrigues. 2020. "Assessing e-Recruiting on Social Media: FBI Case Study." *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. Washington: DOI:10.1109/ASONAM49781.2020.9381351. 742-747.

Padyab, Ali, Tero Päivärinta, Anna Ståhlbröst, and Brigitta Bergvall-Kåreborn. 2016. "Facebook Users Attitudes towards Secondary." *Thirty Seventh International Conference on Information Systems.* Dublin. 1-20.

Shaffer, Ryan. 2015. "Unraveling India's Foreign Intelligence: The Origins and Evolution of the Research and Analysis Wing." *International Journal of Intelligence and CounterIntelligence*, 04 06: 252-289.

Tiwari, Anuj. 2021. *These Are The World's Most Powerful Intelligence Agencies.* 06 12. Accessed 02 17, 2022. https://www.indiatimes.com/trending/social-relevance/most-powerful-intelligence-agencies-542516.html.

DOI: 10.53477/1842-9904-22-6

INFORMATION OPERATIONS CONDUCTED BY ARMED FORCES – CONCEPTS, METHODS AND POTENTIAL DEVELOPMENTS

Mihai VLAICU*

The increased level of integration of electrical and electronic-based devices and systems in the military field has led to the development of better methods of using information in real time, but at the same time has introduced new vulnerabilities to exploit, degrade and deny the information flow between military units and/or different types of weapon systems. The purpose of this paper is to identify key concepts and methods of using information warfare, specifically, CEMA (Cyber Electromagnetic Activities) operations by the armed forces of various nations (the United States of America, People's Republic of China and Israel) and to formulate several potential developments with regards to the future of information operations.

Keywords: *information operations; cyber operations; electronic warfare; Cyber Electromagnetic Activities (CEMA).*

Introduction

Basically, information warfare is a concept that has been used for centuries, in order to discredit or deceive an adversary's forces or population (Nick-Brunetti-Lihach 2018). However, with the acceleration of technological progress that characterizes the 20th and 21st centuries, information warfare has been expanded in order to integrate new methods, based on electronic or electromechanical devices. The first types of these devices were computers based on vacuum tubes, such as

**** Mihai VLAICU is a Master Student in the field of Security and Diplomacy within the National University of Political Studies and Public Administration (SNSPA), Bucharest, Romania. E-mail: vlaicumihai@gmail.com***

Colossus (Crypto Museum n.d.), based on electrical circuits (Ellsbury 1998). Thus, it can be argued that from its very inception, the cybernetics domain has intertwined with the electrical domain, the research and development (R&D) efforts being poured into one of those having a considerable amount of importance on the R&D efforts of the other. One of the things that needs to be clarified is that the aforementioned device was used by organisations focused on military intelligence processing (in this case, the Government Code and Cypher School(GC&CS) (Marsh 2019), the military being thus the primary customer of electronics-based information processing technology.

The development of the transistor has given ways for electronics to become miniaturized, cheaper, more energy-efficient, more modular, and most importantly, able to transmit, receive and manage a growing level of data, in a multitude of formats. Some of the well-known transistor-based innovations in the electronics domain that were and still are important in the cyber domain, are the integrated circuit and the programmable logic device (Dobriceanu 2012), the development of the information-based society being impossible without multiple principles developed in electrical engineering.

The proliferation of integrated circuits has led to their integration in security and military oriented organisations, these types of institutions often being at the forefront of technological development in electronics. This integration manifested itself in many ways, from computers to satellite-based systems. One of the common traits in the adoption of these devices in the military field, irrelevant of their type, is the measure-countermeasure cycle, the military of one nation introducing precision guided munitions, while the armed services of another developing and implementing principles and methods for degrading the efficiency of, or completely disabling, the aforementioned type of weapon systems. It should be noted that, although largely overlooked, computer networks are also a type of weapon systems, even though their effects could be interpreted mostly as non-kinetic. Thus, the information field started being acknowledged as an equal part of military operations (Kozloski 2009). Information operations are an evolving type of concepts, with different armed services having different interpretations of these actions.

The methodology used has been that of researching the development of cyber and electromagnetic capabilities of three case studies (US military forces, Iran and Israel), and the development of prospective studies, with regards to countering the mass usage of these capabilities, in the case of a large scale conflict between superpowers.

1. United States Armed Forces

Some of the first armed forces to take the lead in information warfare are those of the United States. By itself, this is an unsurprising fact, considering:

- that most of the innovations described in this paper were developed in the U.S.;

- one of the agencies of the U.S. Department of Defense, the Advanded Research Projects Agency, developed the first type of computer network in the world and proceeded to integrate it into the armed services (Norman n.d.).

The United States Armed Services are the first to introduce the concept of information operations, being mentioned in JP 3-13, as the "integrated employment of electronic warfare, computer network operations, psychological operations, military deception and operations security" (Joint Chiefs of Staff 2006). For the purpose of this paper, emphasis will be placed on the first two types of actions.

According to JP 3-12, cyber operations consist of three main categories (Joint Chiefs of Staff 2018):

- offensive (OCO);
- defensive (DCO);
- administrative (DODIN).

Firstly, the US Armed Forces, in contrast with the other examples in this paper, postulate the fact that cyber administrative duties, related to the processing of information into data and data dissemination is a type of action different from defensive actions.

Secondly, the reason for such a difference in this military system must be considered. Some of the first orders regarding the organizing of the military structure responsible with conducting cyber operations may present a valuable clue. Thus, military cyber offensive capabilities and DoD networks defence capabilities were allocated to the U.S. Cyber Command (United States Strategic Command 2018), cyber and signals intelligence operations, cryptographic activities and national cyber defensive actions were delegated to the National Security Agency (National Security Agency Central Security Service n.d.), whilst maintaining the developing DoD information processing and communications infrastructure remained under the leadership of the Defense Information Systems Agency (Defense Information Systems Agency n.d.).

Offensive cyber operations carried out by the US Armed Forces, or as they are more commonly known computer network operations, are conducted through multiple organisations, the most important of which is the US Cyber Command. This Command, although designated as a unified combat command (United States Cyber Command 2018), is actually composed of the cyber command of each service (United States Cyber Command n.d.), being responsible for creating the framework and distributing resources for the subordinate commands to execute specific operations. For the purpose of this paper, it should be mentioned the fact that although mostly known for the strategic level, offensive actions taken against various non-state actors, US Cyber Command has also the mission, per USCYBERCOM Announcement Message to "planning Operational Preparation of the Environment (OPE), and as directed, executing OPE or synchronizing execution

of OPE in coordination with the Geographic Combatant Commanders (GCC)." (National Security Agency Central Security Service n.d.). As such, the US Cyber Command is tasked with executing military, tactical and operational level cyber offensive operations against designated targets, in close coordination with kinetic, military operations conducted during a war.

It should be noted that, although at the level of the GCC and the armed services, cyber and electronic operations are to be employed in an unified manner (Joint Chiefs of Staff 2006), the organizational chart of the organizations supporting joint electronic warfare from JP 3-13.1 (Joint Chiefs of Staff 2006) or through that of the US Cyber Command (United States Cyber Command n.d.) shows the fact that these types of operations are not to be conducted from the same military unit or agency of the DoD, thus raising questions regarding the level of coordination that these types of operations would be characterized of, during an interstate, declared conflict.

Electronic warfare is one of the oldest types of electronics based military actions, its foundation being laid in the Second World War, with the development of radar type systems and of electronic countermeasures in order to degrade the capabilities of these weapons. As described in ATP 3-36, electronic warfare "involves the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy" (Headquarters, Department of the Army 2014). As already mentioned, EW is associated with two other types of operations, "cyberspace operations and spectrum management operations" (Headquarters, Department of the Army 2014), forming a distinct type of operations being known as "cyber electromagnetic activities." (Headquarters, Department of the Army 2014). In one other publication, FM 3-12, the U.S. Army reinforces the degree of connectivity between electronic and cyber types of operations, cyberspace being defined as a multitude of "networks that make information globally available through wired and wireless connections" (Headquarters, Department of the Army 2017), whilst electronic warfare being described as having "effects by affecting devices that operate in and through wired and wireless" (Headquarters, Department of the Army 2017), both of these types of actions operating, thus, through the same media. From these examples, it can be concluded that there is a consensus, at least among United States Army senior command staff, on the integrated usage of cyber warfare, electronic warfare, and spectrum management types of actions. The United States Armed Forces can be considered the first to realize the potential of bringing together cyber and electronic warfare operations into a single, general operational domain.

In contrast with the conduct of cyber operations, electronic warfare operations are not employed by a single command or military unit, being distributed across the United States Armed Forces. Also to be noted is the fact that most electronic operations conducted by these armed services were mainly directed towards degrading or denying adversary forces of communication and coordination, electronic defence measures are mainly composed of encrypted communications.

The platforms used by the US military for conducting information operations, in general, and CEMA type of operations, in particular, are varied, ranging from air assets such as EC-130 or EA-18G to land based forces such as Terrestrial Layer System. One fact to be taken into consideration is that whilst the first two types of platforms are used mainly in electronic warfare and signals intelligence (SIGINT) type of operations, the latter, composed of two distinct subsystems, the TLS-EAB and TLS-BCT, is created with the main purpose of integrating cyber and electronic operations. Thus, the stated objectives of the TLS system-of-systems are the provision of "defensive electronic attack" (Pomerleau 2020) and of "radio frequency-delivered cyber effects" (Pomerleau 2020), representing, in itself, the integration of principles in the aforementioned publications, bringing the first such merger of cyber and electronic warfare actions at the operational level. To be noted that the two aforementioned types of operations could be used to infiltrate, degrade or destroy the components of an adversary's weapon systems', ranging from avionics to electronic fuse.

One of the earliest implementations of CEMA-type operations took place during the 1991 Desert Storm and Desert Shield operations. Even though the airstrikes conducted during this campaigns remained representative of US involvement in the Gulf, they were preceded by a significant level of electronic warfare actions directed against Iraq's air defence systems (Mann 1994), thus diminishing their level of effectiveness in the early hours of military operations. One of the key issues, overlooked by CEMA operations was the usage of the BLU-114/B bomb by the United States Armed Forces in order to destroy Iraq's electrical power grid (BBC News 2003). The usage of a weapon of this sort, in conjunction with the use of electromagnetic pulses, would most likely affect a future adversary's capability to wage war.

However, the cyber component of the US Armed Forces was not used until recently during a military conflict or in conjunction with kinetic military operations against another state. Thus, in 2019, with an increased level of tension between the United States and Iran, President Donald Trump ordered the armed forces to conduct cyber operations against a series of Iranian military and paramilitary targets (Hanna 2019). Although it is one of the first direct examples of a state using cyber weapons in order to destroy targets of another state, it was conducted as a stand-alone measure.

As a conclusion, the United States has a capable military system that could execute CEMA activities in order to degrade or destroy an adversary's military capabilities. Although employed, at the time of writing this paper, as stand-alone measures, electronic and cyber operations conducted by the US Armed Forces have proven to be effective, integration of these methods being planned for the near future.

2. People Liberation's Army

The "Shock and awe" campaign led by the coalition forces in the First Gulf War had a long-lasting effect on the military and political elites in the People's Republic of China, leading to emphasis being placed on "informatizing" the formations of the People's Liberation Army. The military and, overall, the national strategy used in the last 20 years, is available to be discovered through informal publications, such as Unrestricted Warfare, by colonels Qiao Liang and Wang Xiangsui, or the "Challenge of Information Warfare", by Major General Wang Pufeng. The overarching theme of these papers is the fact the PRC does not necessarily make a clear distinction between tactical, operational and strategic use of information warfare, thus continuing the concept of "people's war", developed by Mao Zedong. However, in both of these papers there are elements that show a logical evolution of the comprehension of "information warfare" as a concept.

First of all, general Pufeng sees Information Warfare as "offensive" (Pufeng 1995) and "defensive" (Pufeng 1995). In the first category, he places actions that could be regarded, in our time, as non-kinetic elements of C4 ISTAR such as "information reconnaissance" (Pufeng 1995) or "electronic interference" (Pufeng 1995), or as kinetic ones, such as "information suppression by using counter radiation guided missiles to destroy air defence radar stations" (Pufeng 1995) or "information attack by using precision guided-warheads to attack pre-set targets" (Pufeng 1995). While the first and second type of actions could be presented as elements of information warfare, the third and fourth are mainly kinetic actions which do not, by themselves, constitute parts of information warfare, precision-guided munitions being a part of warfare since, at least, World War I. With regards to defensive information warfare, the general uses actions such as "counter reconnaissance" (Pufeng 1995), "multiple-communication methods" (Pufeng 1995), "resist viruses" (Pufeng 1995) in order to describe IW, elements that could be classified as part of modern-day information operations, together with the more ambiguously termed "information counterattack" (Pufeng 1995). One of the facts that should be remembered is that this paper was published in 1995, four years after the US-led Coalition removed the Iraqi Armed Forces from Kuwait, this period of time being a possible reason for why the PLA did not have a clearly defined concept regarding information warfare.

A remarkable leap forward is represented by "Unrestricted Warfare", published in 1999. This paper shows a clear cognitive evolution, presenting "weapons" that are nowadays associated with information operations such as "computer logic bombs, network viruses, or media weapons" (Liang and Xianqsui n.d.) as information weapons. Even more interesting is the fact that it acknowledges the importance of CEMA operations, regarding "the network space" (Liang and Xianqsui n.d.) as being formed from "electronics technology, information technology and the application of

specific designs." (Liang and Xianqsui n.d.). Another aspect of this paper is that it illustrates the willingness of the PLA, at the turn of the century, to combine various types of warfare in order to achieve the CCP's and its goals, acknowledging the fact that every one of these combinations are "all determined based upon a specific target" (Liang and Xianqsui n.d.). This last quote is particularly important because it illustrates modern Chinese military thinking. Thus, in sharp contrast with NATO and US military thinking, in which almost every crisis is met with a mixture of information warfare and, accordingly, precision strikes, the PLA understands the fact that in every situation, whether considering, for example, the South China Sea or Central Asia, it deals with a different type of opponent, with a different set of tools and, ultimately, mentality to counteract. In essence, this approach represents the most capable and adaptable implementation of information warfare, using all available systems to disrupt, degrade or destroy an opponent's information and decision-making cycle.

One of the most important contributions to the development of information warfare in the PRC was that of Major General Dai Qingmin, who introduced the concept of Integrated Network Electronic Warfare. By itself, INEW can be perceived as the Chinese equivalent of CEMA activities, the differentiating factor between the two being the fact that whilst the second one ensured a balanced approach with regards to the conduct of military operations, the first one places emphasis on offensive actions (Krekel, Bakos and Barnet 2009). INEW must, at the same time, be seen in context. Western military thinking since the early 2000s has attached increasing importance towards the development and deployment of network centric warfare doctrines, systems and tactics. As such, Chinese military thinkers acknowledged this fact and, besides applying the concept for their own forces, developed possible avenues in order to counteract its advantages. NCW is built around the concept of shooters and sensors (Thales Group n.d.), the information and data from each platform being shared amongst the other deployed troops. In order to ensure its proper usage, the military force that uses this kind of doctrine has to ensure the security and integrity of its information sharing and processing capabilities, the Chinese thus, correctly, observing the fact that the most efficient method of countering this type of actions is by using CEMA activities, such as intercepting and jamming data links and exploiting any kind of vulnerabilities in the information security architecture of the adversaries' systems.

One of the turning points of recent Chinese military and strategic history is, without a doubt, the ascension of Xi Jinping to power. Whether considering the purges in the ranks of the PLA that took place under his leadership (BBC News 2017), the replacement of Jiang Zemin's Three Represents with his Four Comprehensives policy (Reuters 2015) and by placing his thought in the PRC Constitution, amongst the line of thought of other important Chinese autocrats, such as Mao Zedong and

Deng Xiaoping (Phillips 2017), Xi Jinping's ultimate goal is to ensure both his status as China's leader and the country recognition as a great power. In order to achieve both of this tasks, Xi Jinping recognized the importance of reforming the armed forces, initiating a purge in the ranks of military officers perceived as affiliated with the Jiang Zemin group and modifying the structural organization of the PLA.

Relevant to the subject of this paper, is the 2015 integration of the PLA's cyber, space and electronic warfare capabilities under the control of one organisation, the PLA Strategic Support Force (Ni and Gill 2019). The PLASSF has been created with regards to PLA's continued efforts to create a "smart force", but, in the same time, its potential could be more than that. One answer regarding its purpose could be by observing the basis and development of a similar organisation from abroad, in this case, the US STRATCOM. Until 2009, STRATCOM was the functional combatant command tasked with maintaining the US's main capabilities of strategic deterrence, the nuclear triad, the cyber capabilities and the space warfare capabilities. PLASSF is responsible for the main PLA units focused on cyber warfare, space warfare and electronic warfare, being the nucleus of a possible counterpart of the 2000-level STRATCOM, focused on providing an adequate level of deterrence for the PRC.

The PLASSF branch responsible for conducting cyber and electronic warfare capabilities is the Network Systems Department (Ni and Gill 2019), thus representing the importance granted by the PLA leadership towards creating a synergy of the service's CEMA capabilities.

PRC's alleged hacking actions were largely directed towards acquiring classified military and industrial secrets from foreign computer networks. The fact that the PLA has not taken part, recently, in any military conflicts abroad presents researchers of the topic with the open question of assessing this organization's cyber warfare capabilities during an open conflict, against another state's army.

While the military cyber capabilities of the PRC have been more documented, so far less emphasis has been placed on PLA's electronic warfare capabilities. One of the things to be noted is the fact that also, in this area, China's possible strategy closely matches US' doctrine and developments, with emphasis being placed on China's geographical location. Electronic warfare variants of JH-7 and J-16 aircraft platforms have been developed and could emphasise that the PLA plans to use EW capabilities in a tactical, potentially limited, role in a future, regional conflict.

3. Israel Defense Forces

Israel's approach to information warfare has to be seen in the light of its geopolitical situation. Israel has two types of opponents:

− state-based, with no direct border with Israel, such as Iran and Turkey;

− hybrid organisations that occupy territories directly bordering Israel, such as Hamas and Hezbollah.

After years of civil warfare, Syrian territory hosts Russian and Iranian military units. Also, in Syria, a significant number of Turkish and American military assets regularly conduct military operations. In the South and East, Egypt and Jordan have a balanced approach with regards to Israel, maintaining cooperation with the Jewish state on security related issues.

Other two important sources of instability are represented by the presence of Hamas and other militias on Palestinian Administration's territory and by the fact that the militant Shiite group Hezbollah continues to maintain its stronghold in Lebanon. The potential for cooperation between these two groups has increased recently, with cooperation ranging from political statements (Al Jazeera 2008) to sharing military equipment in order to test and degrade Israel's national security (Ahronheim 2018).

Although well known for their missile attacks towards Israeli territory, in recent years, both groups have diversified their methods of action, mainly in the information field. Both Hamas and Hezbollah have official, active cyber methods of promoting their causes among their members and possible adherents, mobilizing groups (Keyser 2018) (Martinez 2019) in different countries in order to attack Israel's perceived aggression against their interests. Information operations conducted by both these groups, in the past, have had two types of goals:

- extracting information, either from human or technical sources, through either infiltrating social media profiles or groups of interest (Perper 2018) or hacking into the live feeds of various information systems used by the Israeli government (The Times Of Israel 2016);

- manipulating Israeli public perception, conducted through defacing cyberattacks, DDoS, Zero-day or viruses (Shamah 2015).

One of the most notable characteristics of the actions of these groups is represented by the fact that, they have so far not used electronic warfare against Israeli targets or Israeli society. One possible explanation is that an electronic operation is much harder to conceal than a cyber-operation, IDF having the ability to trace back and destroy an EW target with a dedicated anti-radiation missile, a type of weapon that does not have an equivalent for a cybernetic target, the IDF having to use joint operations in order to track in real time and hit an opponent's cyber formations (Groll 2019).

On the other hand, Israel's strategic conflict with Iran (and, in the future, with Turkey) is largely limited, based on proxy forces and information operations. Iran has been the alleged source of a growing number of cyber operations against the Israeli society (AFP 2021) (Deutsche Welle 2022). Israel is also alleged to have deployed cyber weapons on multiple occasions, such as Stuxnet (The Times of Israel 2020) and the 2020 explosions which took place in Iranian strategic targets (The Times of Israel 2020).

The Israeli military-political leadership has used a different approach than the United States with regards to information warfare, establishing information

warfare, in particular, CEMA capabilities, both in the combat support forces and the intelligence services of the IDF. However, Israel has chosen to place emphasis on the development of cyber warfare and signal intelligence capabilities, with less information available to its electronic warfare capabilities.

The offensive cyber capabilities of the IDF have been placed within the competence of the Intelligence Corps (Stavridis 2019), its most well-documented unit being Unit 8200 (Stavridis 2019). Publicly available data on Unit 8200 presents the fact that, besides conducting cyberattacks, it also conducts signal intelligence tasks (spacewatch.global 2017), collecting data about the electronic communications and electronic signatures of potentially hostile Armed Forces, the unit being oriented towards employing CEMA capabilities in the case of a conflict.

The organisation tasked with the cyber-defence of the IDF is the Cyber Defense Directorate (Israel Defence Forces n.d.).

Conclusions and potential developments

All of the countries that were part of the case studies of this paper have developed their capabilities to a considerable level, where these can be used effectively both during peace and wartime. At the same time, the methods these countries have used for the development of their CEMA-centric information operations have been different, the US, China and Israel developing institutional frameworks in order to sustain and develop separately these capabilities.

The increased level of integration of electronic equipment in the military will increase exponentially in the coming years, and its effects on information warfare could be classified in the short-term, with an emphasis on the integration of EW, EMSO and cyber operations in order to gather intelligence or conduct remote hacking of an adversary's systems; increased use of cell phone simulators in information attacks targeting military and paramilitary personnel, in order to obtain intelligence or cause them to question orders; the continued pace of adapting existing weapon systems to, together with the design and use of new weapon systems focused around, concepts such as data/information exchange, will lead to vulnerabilities in the electronic field, more specifically, a system's ability to perceive the battlefield and share data with other platforms will be severely diminished, in case of a joint, sustained CEMA attack; in the medium term, the increased level of importance granted to EW and EMSO warfare will, most likely, determine either a communication "arms race", based on A.I., or the reintroduction of traditional methods of war communications, such as couriers, in case of long-term, strategic-level military operations; further research and development where the focus will be placed on the production, (wireless) distribution and storage of electricity, in order to combat the effects of an adversary's usage of electromagnetic impulse-effect or BLU-114/B type weapons.

BIBLIOGRAPHY:

AFP. 2021. *Iran-linked hackers attack Israeli targets: company.* 12 16. Accessed 04 11, 2022. https://www.france24.com/en/live-news/20211216-iran-linked-hackers-attack-israeli-targets-company.

Ahronheim, Anna. 2018. *Report: Hezbollah is helping Hamas build rocket factories, training camps.* Report: Hezbollah is helping Hamas build rocket factories, training camps.

Al Jazeera. 2008. *Hezbollah, Hamas chiefs meet to discuss Israel-Arab ties.* https://www.aljazeera.com/news/2020/9/6/hezbollah-hamas-chiefs-meet-to-discuss-israel-arab-ties.

BBC News. 2017. *Charting China's 'great purge' under Xi.* Accessed 10 18, 2020. https://www.bbc.com/news/world-asia-china-41670162.

—. 2003. *Fact file: Blackout bombs.* http://news.bbc.co.uk/2/hi/americas/2865323.stm.

C.M. Melliar-Smith, M.G. Borrus, D.E. Haggan, T.Lowrey, A.S.G. Vincentelli, W.W. Troutman. 1998. "The transistor: an investitor becomes big business." *Proceedings of the IEEE,Vol.86, Nr.1.* IEEE. 86-110.

Crypto Museum. n.d. *Colossus Birth of the digital computer.* https://www.cryptomuseum.com/crypto/colossus/index.htm.

Defense Information Systems Agency. n.d. *Our work, DISA 101.* https://disa.mil/About/Our-Work.

Deutsche Welle. 2022. *Apparent cyberattack on Israel disables government websites.* 03 14. Accessed 04 11, 2022. https://p.dw.com/p/48TT7.

Dobriceanu, Mircea. 2012. *Sisteme cu Microprocesoare.* Craiova: Editura Universitaria.

Ellsbury, Graham. 1998. *The Enigma Machine Its Construction, Operation and Complexity.* http://www.ellsbury.com/enigma2.htm.

Groll, Elias. 2019. *The Future Is Here, and It Features Hackers Getting Bombed.* https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/.

Hanna, Andrew. 2019. *The Invisible U.S.-Iran Cyber War.* https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war.

Headquarters, Department of the Army. 2014. "ATP 3-36 (FM 3-36) Electronic warfare techniques." *Headquarters, Department of the Army.* http://www.bits.de/NRANEU/others/amd-us-archive/atp3_36%2814%29.pdf.

—. 2014. "Field Manual 3-38 Cyber electromagnetic activities." *Federation of American Scientists.* https://fas.org/irp/doddir/army/fm3-38.pdf.

—. 2017. "FM 3-12 Cyberspace and electronic warfare operations." *Berlin Information-center for Transatlantic Security.* http://www.bits.de/NRANEU/others/amd-us-archive/FM3-12%2817%29.pdf.

Israel Defence Forces. n.d. *C4I and Cyber Defense Directorate.* https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate/.

Joint Chiefs of Staff. 2006. "Joint Publication 3-13 Information Operations." *HSDL.* https://www.hsdl.org/?view&did=461648.

—. 2018. "JP 3-12 Cyberspace Operations." *Berlin Information-center for Transatlantic Security.* http://www.bits.de/NRANEU/others/jp-doctrine/jp3_12%282018%29.pdf.

—. 2006. "JP 3-13 Information Operations." *HSDL.* https://www.hsdl.org/?view&did=461648.

—. 2006. "JP 3-13 Information Operations." *Joint Chiefs of Staff.* http://www.bits.de/NRANEU/others/jp-doctrine/JP3_13.1%2812%29.pdf.

Keyser, Zachary. 2018. *The under-reported use of Hezbollah's Internet recruitment tactics.* https://www.jpost.com/middle-east/the-under-reported-use-of-hezbollahs-internet-recruitment-tactics-606682.

Kozloski, Robert. 2009. "The Information Domain as an Element of National Power." https://www.hsdl.org/?view&did=232244.

Krekel, Bryan, George Bakos, and Christopher Barnet. 2009. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." *National Security Archive.* Accessed 10 18, 2020. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.

Liang, Qiao, and Wang Xianqsui. n.d. *Unrestricted Warfare.* 1999: PLA Literature and Arts Publishing House.

Mann, Edward. 1994. "Desert Storm: The First Information War?" *Aerospace Power Journal, Volume 8, Nr.1*, 9-15. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-08_Issue-1-Se/1994_Vol8_No4.pdf.

Marsh, Allison. 2019. *The Hidden Figures Behind Bletchley Park's Code-Breaking Colossus.* Accessed 10 18, 2020. https://spectrum.ieee.org/the-hidden-figures-behind-bletchley-parks-codebreaking-colossus.

Martinez, Hector. 2019. *Hashtaggers For Hezbollah? How Social Media Fundraising Can Skirt The Rules.* https://www.bellingcat.com/news/2019/08/27/hashtaggers-for-hezbollah-how-social-media-fundraising-can-skirt-the-rules/.

National Security Agency Central Security Service. n.d. *Mission & Values.* https://www.nsa.gov/about/mission-values/#:~:text=The%20National%20Security%20Agency%2FCentral,order%20to%20gain%20a%20decision.

—. n.d. "Mission & Values." *National Security Agency Central Security Service.* https://www.nsa.gov/about/mission-values/#:~:text=The%20National%20Security%20Agency%2FCentral,order%20to%20gain%20a%20decision.

Ni, Adam, and Bates Gill. 2019. "The People's Liberation Army Strategic Support Force: Update 2019." *China Brief, Volume 19, Nr.10.*

Nick-Brunetti-Lihach. 2018. *Information Warfare Past, Present and Future.* https://www.realcleardefense.com/articles/2018/11/14/information_warfare_past_present_and_future_113955.html.

Norman, Jeremy. n.d. *ARPANET Splits into ARPANET and MILNET.* https://www.historyofinformation.com/detail.php?id=976.

Perper, Rosie. 2018. *Hamas reportedly created a fake dating app to lure Israeli soldiers and steal security information.* https://www.businessinsider.com/hamas-fake-dating-app-scam-israeli-soldiers-honeypot-glancelove-2018-7.

Phillips, Tom. 2017. *Xi Jinping becomes most powerful leader since Mao with China's change to constitution.* Accessed 10 18, 2020. https://www.theguardian.com/world/2017/oct/24/xi-jinping-mao-thought-on-socialism-china-constitution.

Pomerleau, Mark. 2020. "US Army to upgrade bigger units with new electronic warfare gear." *C4ISRNET.* https://www.c4isrnet.com/electronic-warfare/2020/10/01/us-army-to-upgrade-bigger-units-with-new-electronic-warfare-gear/.

Pufeng, Wang. 1995. "The Challenge of Information Warfare." *China Military Science.* https://irp.fas.org/world/china/docs/iw_mg_wang.htm.

Reuters. 2015. *After the 'Three Represents', China pushes 'Four Comprehensives'.* 2020 10. Accessed 18. https://www.reuters.com/article/us-china-doctrine-idUSKBN0LU0A620150226.

Shamah, David. 2015. *Official: Iran, Hamas conduct cyber-attacks against Israel.* https://www.timesofisrael.com/official-iran-hamas-conduct-cyber-attacks-against-israel/.

spacewatch.global. 2017. *ISRAEL'S CYBER WARFARE OUTFIT-UNIT 8200 GETS NEW COMMANDER.* https://spacewatch.global/2017/04/israels-cyber-warfare-outfit-unit-8200-gets-new-commander/.

Stavridis, Virginia. 2019. *Six Cybersecurity Questions Answered by the 8200 Unit.* https://www.cybintsolutions.com/six-cybersecurity-questions-answered-by-the-8200-unit/.

Thales Group. n.d. *Sensor to Shooter.* Accessed 10 18, 2020. https://www.thalesgroup.com/en/sensor-shooter.

The Times Of Israel. 2016. *Hezbollah: We hacked into Israeli security cameras.* https://www.timesofisrael.com/hezbollah-we-hacked-into-israeli-security-cameras/.

The Times of Israel. 2020. *Israel's alleged Natanz strike 'as complex as Stuxnet', a major blow to Iran.* https://www.timesofisrael.com/israels-alleged-natanz-strike-as-complex-as-stuxnet-a-major-blow-to-iran/.

United States Cyber Command. 2018. "Achieve and Maintain Cyberspace Superiority." *United States Cyber Command.* https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf.

—. n.d. “Components.” *United States Cyber Command.* https://www.cybercom.mil/Components.aspx#:~:text=Components&text=United%20States%20Army%20Cyber%20Command,the%20same%20to%20our%20adversaries.

—. n.d. *Components.* https://www.cybercom.mil/Components.aspx#:~:text=Components&text=United%20States%20Army%20Cyber%20Command,the%20same%20to%20our%20adversaries.

United States Department of Defense. 2020. “United States Department of Defense Electromagnetic Spectrum Superiority Strategy 2020.” *United States Department of Defense.* https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF.

United States Department of Defense-Joint Chiefs of Staff. 2021. “DOD Dictionary of Military and Associated Terms.” *Joint Chiefs of Staff.* https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

United States Strategic Command. 2018. *JP 3-12 Cyberspace Operations.* https://nsarchive.gwu.edu/dc.html?doc=2692108-Document-6.

THE PERSPECTIVE OF THE WORLD

by Fernand BRAUDEL*

The Perspective of the World is the third volume of Fernand Braudel's trilogy *Civilization and Capitalism 15th-18th Centuries*, where the author brings a deeper perspective of the European economy, sociology and geography. A reputed French historian of the past century, Fernand Paul Braudel (1902-1985) earned a special place in the complex study of history due to the multiple and nuanced aproaches of his works. The volume *The Perspective of the World* was published in 1979 with the entire trilogy, and represents an economic history of four centuries, which combines the analysis of the European time and space from a political, cultural and social perspective. The context of the publication of the trilogy is rather complex: the Cold War was at its peack, the arms race between the United States and the USSR marked the European time and space, the war in Afghanistan was starting and the European Monetary System was being established.

The beginning of the book analyses the divisions of space and time in Europe, observing how the economy was covering the space in different ways and layers.

**** Fernand BRAUDEL, The perspective of the world, Meridiane Publishing House, 1989, Bucharest.***

Sixteenth-century Europe was, in the author's view, a world-economy near the Mediterranean Sea. The first chapter describes the Mediterranean as a united economic space during the domination of the Spanish Empire under Charles V and the Ottoman Empire before the conquest of Constantinople. The civilizations that marked the Mediterranean space at that time were the Greek submitted to the Turks, the Muslim based in Istanbul and the Christian based in Florence and Rome. In order to exist, a world-economy needed its space with boundaries that give it a sense, this space involves a centre that is a city, a dominant capitalism and a hierarchy (this space is a sum of particular economies, where only the centre is relatively rich).

According to the author, the trends of the world-economies were the following: the slowly varying space, a dominant capitalist city, the succession of the cities' suppremacy, the hierarchy of its zones and its density. The variation of the space was given by the amplitude of trade for which the borders were exceeded. Passing the limits (often geographical limits such as the sea or the mountain) of an economy brought a bigger loss than the earning for which the limit is crossed. Cultural, religious or financial boundaries were surpassed by the advantages generated by commerce. In the centre of the world-economy, there was a dominant capitalist city having "satellite cities surrounding the pole, from a bigger or smaller or more or less respectful distance, associated or in complicity and rather serving their secondary role. Their activity goes hand in hand with the activity of the dominant city: they guard around it, they direct the business flow towards it, they redistribute and guide the goods that the dominant city sends to them, they hang on its credit or they bare it." (Braudel 1989, 22) The primacy of cities was a phenomenon of succession; the dominant cities did not remain permanently dominant, they substituted each other in the urban hierarchy. The more or less total urban dominations depended on the varying economic power; political power was irregular too (because money may prove stronger than it). The succession of domination reveals the weapons for domination: navigation, trade, industry, credit, political power or political violence.

The author achieved a hierarchy of the various zones from the proximity of the cities, the various zones around the center looked to the cities forming a whole, and the accumulation of resources was an important factor in the hierarchy. The economy that was superior in the hierarchy encompassed production through the control of collection, storage and organization of distribution, conducted its flow of activity especially through credits (Braudel 1989, 35). The big city was dominating its abstract field, which was a zone where fairs and villages lacked.

The spatial plan of the world-economy meant an overlapping of zones tied among each other at different levels. The three categories of areas are: a small centre, rather developed zones of secondary level and the marginal zones. The qualities and characteristics of society, economy, technique, culture and public order were

shifting from one zone to another. Neutral zones were those lying near the developed economies, but which maintained an archaic existence.

A world-economy reveals itself as a huge coverage with an infrastructure proper for its development. It has density, depth, means of defence and efficient force at its centre and at the regions around its centre. The latter may not be well connected to the decision-making centres either. The world-economy is described by the author as an order facing other orders, which is not isolated and in whose space many other entities worked together. The economic order and the international division of labour were showing, in Bradel's view, a modern age where economic priority became more and more pressing: *it oriented, troubled, and influenced other orders*.

Between the 15th and 18th centuries, the territorial state did not have the force to fill in all the social spheres, and therefore economy left it behind. England was the first European example of national economy in the 18th century, marking the moment when the territorial state became more powerful than its economy. At the beginning of the time period analyzed by Braudel, the state-cities Venice and Amsterdam, as trade cities lying at the crossroads between trade routes, were developing and thriving becoming important economic centres in the European world-economy. The monarchic order appears nearby the developed centre, an order that canot rule without bourgeoisie, that it moderately encouraged (an example in this case would be much later France during Napoleon's rule, where Foreign Minister Charles-Maurice de Talleyrand-Périgord was himself a representative of the relationship between monarchy and bourgeoisie at his time). The empire was a form of world-economy too, described by the author as an archaic organization which represented the triumph of the politics over economics.

According to Braudel, during the time of the pole-cities, society was developing slower than the economy, the fight among the social classes was a fight for priority and fast adaptation to the economic trend. Economy imposed the rhythm through the control of the tasks and of the work. But the economy was controlled by its basic needs at its turn. That is why no economic pattern completely matched everywhere, because the basic needs were different. Cultures and civilizations represent other orders as well, orders which organize the space and represent other economies. Colonialist Europe is described as an example of world-economy. A world-economy may overlap with a civilization, but not entirely. Culture competes economy in time, and religious values are at the core of each civilization.

The differences between a world-economy and a universe-civilization are shown through examples, such as Genoa and Venice versus Florence between the 13th and 15th centuries. Genoa and Venice were economic poles although their creation of culture did not mark their time, while Florence created Renaissance; in the 17th century, Amsterdam was economicly triumphant, but Rome was the cultural centre of Europe. This reality of the 17th century envisaged today's case of the United

States, which is a world economic power, but not a cultural centre. The economic changes that occurred at the centre reached out to the marginal area or to the centres of other world-economies. Braudel synthetizes the economy of the 16th century by describing it as a "transmission belt", the centre was imposing the price and created the trend in other centres in order to impose itself there as well. Such an example is 17th century Amsterdam, which was the centre of the world after the effects of the Black Plague had diminished the influence of Spain, Italy and the Mediterranean Sea, in general. Starting from 1809-1810, England had overtaken the European supremacy, and France gained its supremacy after the Napoleon was overthrown.

The second chapter analyzes the advantages that centre-cities had because they assured themselves their development through the roads, markets and money they accumulated. In today's terms, the access road, the bank, and the coin are the facilities they were after and that created cities. Currency represents the main pillar of the European trade revolution that started in urban areas, connected by the need for exchange, defence and administration (Braudel 1989, 113). Unlike Western Europe, the East did not have such developed trade facilities, the East still had a barter economy in a time when the West already had currency and credit.

The beginning of the European world-economy was marked by two trade poles – the Netherlands and Italy, the North and the South. One cannot precisely say when exacly did the the Netherlands overtook trade supremacy in Europe, but the Hanseatic League, signed in 1396, had an essential role in the development of trade in the North Sea area. The other commercial pole, the South with Genoa, Venice and Pisa, flourished after the Crusades, which brought the Mediterranean to the attention of the traders. After that, China's opening to the trade outside its borders brought the Black Seat to the attention of the European merchants in the XVIIIth century (Braudel 1989, 133). In the XVth century the most important trade point was in Venice, the European West depended upon it while the East was still facing invasions and could not reach the economic development of the West, so the East remained the marginal area of the European world-economy. During its best time, Venice was a labour economy dominated by money and administration, and Genoa was its competition as Europe's financial pole and the first city that used gold for its exchange market from Anvers. The financial domination of Genoa was so powerful, that there is this idea that Italy's unity was achieved by Genoa with the support of the Bank of Italy. Portugal, very developed at that time, suffered because it was not at the centre of the European world-economy, although it had a very developed monetary system. Lisbon remained an important trade centre, outpaced by Anvers which, in the XVIth century was reaching the peak of its capitalist development. In the XVII-th century the North overtook the European commercial power because the industrial activity of Venice was slowing down and the industries from the north starting with that of Amsterdam were thriving. The role of Genoa also decreased because the European

incapacity "to support a financial circulation that was disproportionate to the cash flow and the volume of production" (Braudel 1989, 219).

In the third chapter Amsterdam is described as the last imperialist commercial city. Having the biggest European fleet, the Low Countries gained respect during both peace and war, behaving like a true centre of a world-economy. Moreover, the ties of the Dutch with the Asian commercial routes brought them to the global commercial elite. The Dutch were thus participating to priviledged exchange circuits keeping their monopole on the source of commerce and diversifying the tastes of their final clients, thus raising the demand and the offer on the market in order to finally control the price and the profit. But what brought the decline of Amsterdam as a trade pole in the XVIIIth century came from inside the Dutch society and because of the decrease of trade relations with India. The upper social classes, the financial and cultural elites, embraced the French culture and became socially and culturally enstranged from the lower classes. This rift at the level of the Dutch society also produced other rifts at the level of professions and crafts, thus having a decisive impact including on the Dutch maritime power. The Dutch labour force was more expensive, more expensive than the French one, could not keep up with the active production which lacked the support to go on. From marginal zones spared by the Dutch, England and France turned into important trade centres which slowly and constantly developed at the expense of the Dutch. In the same time, the trade of the Baltic Sea region especially the Swedish trade, not as strong as the trade of Amsterdam, developed too but the Dutch competition kept it behind until the XVIIIth century. Sweden could not control the whole Baltic Sea and was not a merchandise intermediary either, that was why it could not defeat the Dutch trade. The Low Countries were enjoying the attraction of the inferior and submitted economies, the exchanges, capital and credits necessary to dominate. When England put an end to this domination in the XVIII-th century by creating its influence on the trade routes with Asia, especially with India, the British impetus could no longer be impeded by the Dutch, especially because of the internal shortcomings faced by the latter, but also because England's public debt in the XVIIIth century was not higher than the double of its GDP and because England was constantly depeloping despite all adversities. France, at its turn, took advantage more from its geographic conditions than Amsterdam and England. Moreover, France's network of roads and rivers encouraged and unified trade and thus facilitated the flow of cash. But "the abundness of space", as Braudel calls the vast and advatangeous expanse of the French territory, after the territorial conquests impeded its economic development in the XIXth century and encouraged the emergence of two poles of power- Paris and Lyon. France was to reach the finalization of its commercial network when the telecommunication lines would know an important development, after the trend set

by the already developed United States. Then New York took the place of London and Paris as centre of a world-economy.

The author further engages in the analysis of the passing from the status of centre of a world-economy to the national markets. The development of a national economy takes place at the core or nearby the centre of a world-economy. The XVIIIth century was oposing the world-economy of Amsterdam to that of England, a city versus a state. The Industrial Revolution made the difference between states and cities even bigger. The national economy was achieved through a series of political, economic, geographic factors and was encompassing various spaces connected among them. This became the main administrative organization starting from the XVIIIth century, after the Dutch decline.

A national market means power and unity and a peasantry that produces enough to feed the cities as well is a success of the agricultural policy. Because the national market is not only a product of economy, but first of all a political product. These premises were important in Europe, but not in the United States where the foundations were laid on an urban basis. This type of development had a major role in the defence of the local colonies from the attacks of the European colonialist powers. Braudel compares the administration of the national market/economy to the accountancy of a firm. According to him, a national accountancy has three variables and three dimensions: patrimony, national income and the income per capita are the variables, and the dimensions are production, incomes and spendings. Such is the analysis at the national level that Braudel achieves for England and France as centres of world-economy of the XVIIIth century. What he meant was to analyze the factors (let us call them national accountancy factors) which contributed to the economic development that the two countries reached after the decline of Amsterdam.

Marginal zones were not thus named because of any economic delay, they were characterized by a larger freedom in comparison to the centre. Moreover, the marginal zones were the key of the access to the centre. They were not as developed as the centre, but they had a strong defensive role and they were guiding the access routes towards the centre. Braudel used the example of Lille which took advantage of its geographic positioning in order to develop its craftsmaship, its relationship with the centre and the trade with the Low Countries. The centre was described by Braudel as a prisoner of the marginal zones. But the centre was also an important factor in establishing an economic flow for the intensively circulated marginal zones had the tendency to follow the economic development of the centre.

The fifth chapter is a socio-economic analysis of the other regions of the world such as the New World, Asia, Russia, Africa and the Extreme Orient, but it also contains an emphasis on the factors that made the United States a global economic centre. Starting from the progress of the United States, the economic globalization with its centre in the United States became more and more clear.

The demographic boom and the eagerness for business from the colonies gave the United States a powerful economic boost in comparison to the economic state of Europe in the XVIIIth century. In the XVIIth century New England thrived due to its fishery businesses of the puritans who had already been named "the Dutch of America" (Braudel 1989, 41). Their businesses flourished and brought about prosperity, economic growth, demographic progress, leading to the discontent of the European economic centre because of the competition and development built across the Atlantic. The colonies were trying to become independent from the centre and conflicts emerged because Spain, France, England and the Low Countries wanted to maintain their influence over the colonies, which produced raw materials, for these colonies to remain marginal zones of the European world-economy, and the colonies wanted to use their economic advantages for their own purposes. Freedom from the European powers came sooner in the North of the New World, the South would overtake complete power later in 1940. Latin America gained independence from the Spanish and Portuguese colonizers even later, it remained a marginal zone of the European world-economy for a longer time.

At the end of the fifth chapter other regions are being analysed and compared to Europe as economic centre. Africa was a marginal zone and a strategic communication tie with India from the first colonies. Russia was a world-economy itself, an autonomous zone with its own commercial network and intense trade exchange with China, Iran and Central Asia. Once the European trade network grew, the merchandise and the European tastes were permeating Russia marking its development and its opening to new trade routes and engaging it into its own Industrial Revolution.

The Ottoman Empire, as a world-economy itself, encompassed a very large territory. The Black Sea was to the Ottoman Empire as important as India was to Spain (Braudel 1989, 126). The Black Sea was very well secured by the empire because it assured its commerical circularity, it was "indispensable to the supplying of Istanbul and to the arming of the Turkish fleets" (Braudel 1989, 136). The economic centre of the Ottoman Empire was reestablished in Istanbul around 1750, as the empire had had multiple economic centres before that (Cairo, Aleppo, Alexandria etc) because of its large territory which imposed this multipolarity. But the economy of the empire could not compete with the European world-economy.

Although the author does not mention the situation of the Romanian Principalities, we will stop at this subject in order to detail their state, as a parallel with the events that marked the European world-economy. The Romanian Principalities were lying near the Black Sea, dominated by the Ottoman Empire and frequently attacked by invading troops between the XVth and the XVIIIth centuries, the Romanian Principalities were a marginal zone of a world-economy, they do not reach the economic level they strive to. Venice, centre-city in the XVth century, had signed a peace treaty with the Ottomans in 1479 in order to be able to continue and defend its trade. In 1484

the Romanian Principalities lost two important citadels Chilia and Cetatea Albă to the Ottomans, those were two very important citadels to the Romanian defence at the Black Sea. During this time, the Romanian art and culture developed and formed a new characteristic stage even to the Romanian political and military objectives at that time. During the XVIth century the Ottoman domination in the Romanian territories grew stronger, but "the exterior commerce of the Romanian Principalities - which maintain their own customs system- is oriented especially during the second half of the XVIth century- to the Ottoman market. Romanians need to sell mostly, and generally at lower prices than those of the international markets, products such as wheat, sheep, butter, honey. Muntenia and Moldova become the supplying spot of Constantinople, the larder of the kingdom, as it was said at the time. The commercial inventory remained excess…" (Giurescu C.C. 1972). And so would remain until the XVIIIth century, to new political and economic pressures exerted by the Istanbul and the Phanariot leaders, whose reign would end a century later.

The most extended world-economy studied by the author is that of the Extreme Orient made of Islam, India and China. The Extreme Orient had a rather closed and complementary commerce, as its countries were trading among them. Asia is the fourth world-economy analyzed in the book. Asia was a more densely populated land than Europe and was supplying European markets with most of their luxury products. The Asian colossus was a coherent space due to its coin in spite of all ‚indispensable assymetries' between the centres (Surat, Bengal etc) and its marginal zones. From the beginning of the Moghul Empire in the XVIth century, the commerce of the region thrives due to crafts and intense trade with various fabrics, and its lying by the Indian Ocean made it an attractive commercial destination. But in the XVIIIth century its economy marked a downfall and India was overtaken by the British during a time when India had to face many hostile factors, such as the competition of the European merchandise, the effects of the Industrial Revolution, the interferences of foreign forces, its own capitalist organization based on castes which impeded economic development but favoured the accumulation of capital, and the despotic states that India consisted in. India did not have an industrial capitalism, but rather its own form of progress by traditional means. It was a major commercial joint without marking the centre of any world-economy, but rather by counting on its faraway commerce. India was sharing the Extreme Orient with China, the two giants were enclining the trade balance to Malacca peninsula during their flourishing times. A domination of India was impossible without Malacca, a major connection between the Pacific and the Indian oceans. And that is a reality today,too, if we observe the importance of the Malacca Strait to the global trade and defence. Controlled by the United States, this strait or better said avoiding it and the creation of an alternative route controlled by China would be the basis of the Chinese investment project from the region of the Kra Thailand canal.

At the end of the volume the author compares the Industrial Revolution to growth. Started in England in the second half of the XVIIIth century, the Industrial Revolution expressed itself as economic and social progresses. The goods on the market, technique, industries, production, all then knew the development that turned England into an economic centre that imposed the pace of growth in Europe and across the ocean, in the New World. Agriculture was the only field that could not keep up with the English demographic progress; growth needed consistency. The revolution of the cotton, iron, of the loom, of the steam machines, the successful division of labour, all contributed to the progress of the English society and economy, finalized by the faraway trade. This development attracted the hostility of other countries competing in the commercial sectors where England dominated.

Observing today's world in the terms of Fernand Braudel, we might say that the shorter terms of stability in between global crises may be indicators of the more and more frequent clashes among the centres of the actual world-economies. The Covid pademic represents one factor of confrontation among the centres of world-economies. China's speed to announce its getting out of the pandemic was a manner to assure the continuity of its economy, in competition with that of the United States strongly damaged by the effects of the virus. Every state that was confronted to the pandemic was put in the situation to weigh and balance its healthcare challenges in order to minimize loss. Thus, the pandemic pointed out like an X-ray to the central zones, the medium zones and the marginal zones of the world as a whole, but also the relationships among them.

Without diminishing the role and amplitude of Braudel's masterpiece, we note some aspects which result from the structuralism presented by the author in the reviewed volume. The subtle, but general idea, exposed in the volume is that the international economic and political environment and the geographic determinism are the factors which prevail in the development of a state or pole-city if we are to refer to the European economy before the XVIIIth century, as Braudel studied it. We will further try to bring other perspectives as counterarguments to this thinking.

Once we look at the actual Chinese ascension, for example, from this perspective of the centre of a world-economy, we observe the manner in which it dominates certain sectors of the international trade. But the Chinese ascension takes place in spite of its geographical conditions and characteristics which are unfavourable to the economic development that China enjoys nowadays. Moreover, China's industrial products and its soft power component fill in the vacuums of political and economic power that emerged in various places of the world, by contracting time and space with the infrastructures that were built on the territories of many countries. But in the view expressed by the military strategist Edward Luttwak in *The Rise of*

China vs The Logic of Strategy, the shortcomings that China is confronted to are: the erronated belief that the world is shaped by the Chinese ascension, premature Chinese assertiveness, the so-called ‚autism' of the Chinese internal structures, the historical reminiscences of China's conduct and the resistance that many countries developed against China (Australia, Norway, Indonesia etc). Edward Luttwak opposes strategic thinking to the determinist factors proposed by Braudel. Opposite to this perspective, Braudel's structuralism would not have counted on the Chinese ascension in the given conditions, considering also its geographical characteristics, but it has been happening especially since Deng Xiaoping. Paradoxically or not, it has been happening under the leadership of the Chinese Communist Party.

Another approach beside the two already mentioned is studied by J.R. McNeill and William H. McNeill in their book *The Human Web*. We are not making a concept of their theory, but rather mention it as a different approach regarding the way in which economic development influenced space, time and humans in time. The two authors propose the perspective of the human web in order to explain the way how economic networks developed and created international trade as we see it today. In their view, humans generated networks, exchanges they needed, influencing time and space and contracting them for their own use. Although Braudel does analyze the influence of the networks generated by various economic contexts, they do not have priority in his view, but the capitalist structure- the coverage that evolves from urban to national and transnational through its mechanisms and subtleties. Like the approaches presented here, there are various other points of view to look at the history of the global economic system and capitalism, even under the socio-economic wrapping presented by Braudel. This shell of the economic development may well present itself under other forms than the structuralist one, even leaving aside the historic, social, economic and political phenomena generated by the pandemic.

Moreover, Braudel's approach is not singular, because the socio-economic history of capitalism was also studied by other authors. We mention here Immanuel Wallerstein, Karl Marx, Max Weber. While Karl Marx was the promoter of the economic structuralist thinking, Max Weber emphasized the role of ethics to the capitalist development. Nevertheless, the uniqueness of Braudel's book comes from the definition, hierarchization and classification of the economic cycles from the perspective of the inherent civilization and from the synthesis of the development and transformation of the world-economies from basis to top, from pole-city to developed state and transnational joint.

How are Braudel's writings relevant today then? His analysis of the historic times from the beginnings of capitalism and their impact on civilization cannot be contested. Capitalism with all its aspects cannot be put aside, just as Braudel's writings on the history of capitalism and its influence on the structures of daily

human life cannot be neglected. The depth and attention given to historic, social and economic phenomena which accompany the capitalist development make *The Perspective of the World* a genuine source of knowledge.

Conclusion

The contributions of the book to its field are remarkable. The analogy of the world's economic chronologies, the pedagogic way to emphasize the historical and economic the impact of capitalism on the human life, all these bring a particular light on economic history and transformation between the XVth and the XVIIIth century. The modern trends reached by the book are obvious, especially when we remember that the author studies capitalism from its beginnings. The circulation of resources, of humans and of money are observed by Braudel both in particular and in general, at micro- and macro-economic level, in the history that wraps them without entirely revealing their mistery, in the societies where they develop without suppression.

Which trend do we live now? This is one of the book's greatest questions. In 1979, at the end of the second volume, the author stated that the world was engaging in a crisis whose time lapse and nature were unfamiliar to him. Are the economic asymetries between centre and marginal zones still relevant today? They certainly are, and not only them, but also the struggles among them. If we look again at the pandemic context for example, but not only in its context, we may observe the efforts that states made in order to preserve their economies, in order to have access to scarce resources because of the lack of deliveries or the lack of production. Conquering another world-economy, let us say, is more and more defined by the conquest of the space and time allocated to reach it and cross it. Mobility and knowledge continuously compete against the physical field (like land and sea) in order to become more evident in the advance of technology and virtual space. Just like during the Industrial Revolution, but in a more advanced stage, these abstract notions are trends dictated by the economic centres of the world, global waves that the medium and marginal zones are trying to keep up with. But the global interconnections that appeared in the meantime impose the need for adaptation, flexibility and mobility among the global economic centres just as among the marginal zones. The way in which China has been struggling and still struggles to assure the Covid vaccine deliveries to marginal spaces such as Africa, the focus on conflicts from marginal zones, may reveal a bigger interest for addition, for the merging of the centre with the marginal zone. If during the Cold War one spoke of spheres of influence, from Braudel's perspective we may look at today's context from the perspective of the options and struggles of the economic centres in order to mark a marginal zone where they would impose themselves and that they would merge with themselves.

BIBLIOGRAPHY:

Bourcier de Carbon, P., Biraben, J.-N., Fernand Braudel — Civilisation matérielle, économie et capitalisme, XVe-XVIIIe siècle, *Population*, An 1981, pp. 428-429, https://www.persee.fr/doc/pop_0032-4663_1981_num_36_2_17191?q=le+temps+du+monde

Braudel, F., *Timpul lumii,* vol. I, II, Editura Meridiane, București, 1989

CIA Factbook, China, https://www.cia.gov/the-world-factbook/countries/china/#geography

Enciclopedia Britannica, https://www.britannica.com/biography/Fernand-Braudel

Frankopan, P., *The Silk Roads*, Bloomsburry, Londra, 2015

Gibbon E., *Istoria declinului și a prăbușirii Imperiului Roman*, Editura Minerva, București, 1976

Giurescu C. C., Giurescu, D. C., *Istoria românilor din cele mai vechi timpuri și până astăzi*, Editura Albatros, București, 1972

Hofstede G., Hofstede G. J., Minkov M., *Culturi și organizații. Softul mental. Cooperarea interculturală și importanța ei pentru supraviețuire*, Humanitas, București, 2012

Luttwak, E., *The Rise of China vs The Logic of Strategy*, The Belknap Press of Harvard University Press, Massachusetts, 2012

McNeill J. R., McNeill W. H., *The Human Web. A Bird´s-Eye View of World History*, Norton Company, New York, 2003

China's Growing Influence in the Developing World, *Belt and Road News*, 23 January 2019, https://www.beltandroad.news/2019/01/23/chinasgrowing-influence-in-the-developing-world/Tarle, E. V., *Talleyrand*, Editura Cartea Rusă, București, 1960

Tocqueville Alexis de, *Despre democrație în America*, Humanitas, București, 2017

Lavinia MOICEANU, PhD*

* ***Lavinia MOICEANU, PhD, is a graduate of the Geneva School of Diplomacy and International Relations, Geneva, Switzerland. E-mail: lavi.moiceanu7@gmail.com***

WORKSHOP

"National Adjustment of Allied Multi-Domain Operations Concept"

March 25th, 2022

The Centre for Defence and Security Strategic Studies held on Friday, March 25th, 2022, the online workshop on the *National Adjustment of Allied Multi-Domain Operations Concept.*

As the multi-domain operation is a concept less familiar to the public, however having the potential to capture the interest of the military and civilians engaged in the national or allied defence system, the scientific event created the opportunity to identify some aspects regarding the need for development and implementation, of the allied concept of multi-domain operations, at the Romanian Army level.

The event was addressed to experts, academia, researchers, PhD students, MA students, and students from national and international military and civil education and research institutions. The event was attended by representatives from the Operations Directorate, Strategic Planning Directorate, Joint Forces Command, Institute for Political Studies of Defence and Military History, "Henri Coandă" Air force Academy from Brasov, the Faculty of Command and Staff within "Carol I" National Defence University, as well as other institutions belonging to the National System of Defence, Public Order and National Security. Noteworthy is the active participation of Romanian representatives from the Multinational Joint Headquarters (COM MN JHQ) in Ulm, Germany and from the Supreme Headquarters Allied Powers Europe (SHAPE-NATO HQ) in Mons, Belgium, which brought an undeniable added value to the event.

The proposed topic shaped the scientific framework for notable lectures and wide-ranging debates, the main conclusions being:

- presentation of the development stage of the MDO concept at NATO and Member State level;
- analysing the need to implement the MDO allied concept in the Romanian Army;
- defining the operations and action areas within the Future Operating Environment (FOE);

Event photo: Workshop
"National Adjustment of Allied Multi-Domain Operations Concept"

•definition of multi-domain operations in an inter-institutional and multinational context;

•debating the fundamental MDO principles;

•determining the role, place and missions of national power mechanisms within the MDO;

•identifying a possible force structure for multi-domain operations;

•strengthening the role and place of emerging technologies in the way forces operate for multi-domain operations.

•establishing the main differences between the combined and multi-domain levels;

•describing the new operations areas entailed at the Allied level − outer space and cyberspace.

Encompassing the scientific level of debates, the origin of the participants and the results achieved, the workshop provided real support to the educational process. In addition, the event's success was highlighted by the attendee's assessments of the way the event was organized and conducted reflected in the interest shown in participating in the centre future scientific events. The scientific manifestations can be found by accessing the link: https://cssas.unap.ro/ro/manifestari.htm

Also, between June 08-10, 2022, we invite you to attend the Conference on "The Complex and Dynamic Nature of the Security Environment", an integral part of the *International Scientific Conference Strategies XXI,* organized at the "Carol I" National Defence University. This year's CDSSS panel, entitled "*Defence and Security Studies*", is developed in four sessions as follows:

1. Concepts and Theories in Security and Defence;
2. Resilience and Good Governance;
3. Strategic Areas of Interest – Global Trends;
4. Armed Forces and Society.

Conference administrative information and organisational details are posted on the new Strategies XXI website, URL: https://www.strategii21.ro/

GUIDE FOR AUTHORS

We welcome those interested in publishing articles in the bilingual academic journal *Strategic Impact*, while subjecting their attention towards aspects to consider upon drafting their articles.

MAIN SELECTION CRITERIA are the following:

- ✓ **Compliance with the thematic area of the journal – security and strategic studies** and the following topics: political-military topical aspects, trends and perspectives in security, defence, geopolitics and geostrategies, international relations, intelligence, information society, peace and war, conflict management, military strategy, cyber-security;
- ✓ **Originality** of the paper – own argumentation; novelty character – not priorly published;
- ✓ **Quality of the scientific content** – neutral, objective style, argumentation of statements and mentioning of all references used;
- ✓ **A relevant bibliography**, comprising recent and prestigious specialized works, including books, presented according to herein model;
- ✓ **English** language shall meet academic standards (British or American usage is accepted, but not a mixture of these). Romanian authors shall provide both Romanian and English versions of the text.
- ✓ **Adequacy to the editorial standards adopted by the journal.**

EDITING NORMS

- ✓ **Article length** may vary between **6 and 12 pages** (25.000 – 50.000 characters), including bibliography, tables and figures, if any.
- ✓ **Page settings**: margins - 2 cm, A 4 format.
- ✓ The article shall be written in **Times New Roman font, size 12, one-line spacing.**
- ✓ The document shall be saved as Word (.doc/.docx). The name of the document shall contain the author's name.

ARTICLE STRUCTURE

- ✓ **Title** (centred, capital, bold characters, font 24).
- ✓ **A short presentation of the author**, comprising the following elements: given name, last name (the latter shall be written in capital letters, to avoid

confusion), main institutional affiliation and position held, military rank, academic title, scientific title (PhD title or PhD Candidate – domain and university), city and country of residence, e-mail address.

- ✓ A relevant **abstract**, not to exceed 150 words (italic characters)
- ✓ 6-8 relevant **keywords** (italic characters)
- ✓ **Introduction / preliminary considerations**
- ✓ **2 - 4 chapters** (numbered, starting with 1) (subchapters if applicable)
- ✓ **Conclusions**.
- ✓ **Tables / graphics / figures**, if they are useful for the argumentation, with reference made in the text. They shall be also sent in .jpeg /.png/.tiff format as well.

In the case of tables, please mention above "**Table no. X**: Title", while in the case of figures there shall be mentioned below (e.g. maps etc.), "**Figure no. X:** Title" and the source, if applicable, shall be mentioned in a footnote.

Nota Bene: Titles of works shall be mentioned in the language in which they were consulted, with transliteration in Latin alphabet if there is the case and, preferably, translation in English language of the titles.

REFERENCES

It is academic common knowledge that in the Abstract and Conclusions there shall not be inserted any references.

The article shall have footnotes and bibliography, in the form seen below. Titles of works shall be mentioned in the language in which they were consulted, with transliteration in Latin alphabet if there is the case (e.g. in the case of Cyrillic, Arabic characters etc.). Please provide English translation for all sources in other languages.

The article will comprise in-text citation and bibliography (in alphabetical order), according to The Chicago Manual of Style[1], as in examples below:

BOOK

Reference list entries (in alphabetical order)

Grazer, Brian, and Charles Fishman. 2015. A Curious Mind: The Secret to a Bigger Life. New York: Simon & Schuster.

Smith, Zadie. 2016. Swing Time. New York: Penguin Press.

In-text citation

(Grazer and Fishman 2015, 12)

(Smith 2016, 315–16)

[1] URL: https://www.chicagomanualofstyle.org/tools_citationguide/citation-guide-2.html

CHAPTER OF AN EDITED BOOK

In the reference list, include the page range for the chapter. In the text, cite specific pages.

Reference list entry

Thoreau, Henry David. 2016. "Walking." *In The Making of the American Essay*, edited by John D'Agata, 167–95. Minneapolis: Graywolf Press.

In-text citation

(Thoreau 2016, 177–78)

ARTICLE

In the reference list, include page range for the whole article. In the text, cite specific page numbers. For article consulted online, include a URL or the name of the database in the reference list entry. Many journal articles list a DOI (Digital Object Identifier). A DOI forms a permanent URL that begins https://doi.org/. This URL is preferable to the URL that appears in your browser's address bar.

Reference list entries (in alphabetical order)

Keng, Shao-Hsun, Chun-Hung Lin, and Peter F. Orazem. 2017. "Expanding College Access in Taiwan, 1978–2014: Effects on Graduate Quality and Income Inequality." *Journal of Human Capital* 11, no. 1 (Spring): 1–34. https://doi.org/10.1086/690235.

LaSalle, Peter. 2017. "Conundrum: A Story about Reading." *New England Review* 38 (1): 95–109. Project MUSE.

In-text citation

(Keng, Lin, and Orazem 2017, 9–10)

(LaSalle 2017, 95)

WEBSITE CONTENT

Reference list entries (in alphabetical order)

Bouman, Katie. 2016. "How to Take a Picture of a Black Hole." Filmed November 2016 at TEDxBeaconStreet, Brookline, MA. Video, 12:51. https://www.ted.com/talks/katie_bouman_what_does_a_black_hole_look_like

Google. 2017. "Privacy Policy." Privacy & Terms. Last modified April 17, 2017. https://www.google.com/policies/privacy/

Yale University. n.d. "About Yale: Yale Facts." Accessed May 1, 2017. https://www.yale.edu/about-yale/yale-facts

Citare în text

(Bouman 2016)

(Google 2017)

(Yale University, n.d.)

NEWS OR MAGAZINE ARTICLES

Articles from newspapers or news sites, magazines, blogs, and like are cited similarly. In the reference list, it can be helpful to repeat the year with sources that are cited also by month and day. If you consulted the article online, include a URL or the name of the databases.

Reference list entries (in alphabetical order)

Manjoo, Farhad. 2017. "Snap Makes a Bet on the Cultural Supremacy of the Camera." *New York Times*, March 8, 2017. https://www.nytimes.com/2017/03/08/technology/snap-makes-a-bet-on-the-cultural-supremacy-of-the-camera.html

Mead, Rebecca. 2017. "The Prophet of Dystopia." *New Yorker*, April 17, 2017.

Pai, Tanya. 2017. "The Squishy, Sugary History of Peeps." *Vox*, April 11, 2017. http://www.vox.com/culture/2017/4/11/15209084/peeps-easter

In-text citation

(Manjoo 2017)

(Mead 2017, 43)

(Pai 2017)

For more examples, please consult The Chicago Manual of Style.

SCIENTIFIC EVALUATION PROCESS is developed according to the principle *double blind peer review*, by university teaching staff and scientific researchers with expertise in the field of the article. The author's identity is not known by evaluators and the name of the evaluators is not made known to authors.

Authors are informed of the conclusions of the evaluation report, which represent the argument for accepting/rejecting an article.

Consequently to the evaluation, there are three possibilities:

a) the article is accepted for publication as such or with minor changes;

b) the article may be published if the author makes recommended improvements (of content or of linguistic nature);

c) the article is rejected.

Previous to scientific evaluation, articles are subject to an *antiplagiarism analysis*.

DEADLINES:

Foreign authors will send their articles in English to the editor's e-mail address, **impactstrategic@unap.ro**.

We welcome articles all year round.

In the case of foreign authors, if the article is accepted for publication, an integral translation of the article for the Romanian edition of the journal will be provided by the editor.

NOTA BENE:

Authors are not required any fees for publication and are not retributed.

By submitting their materials for evaluation and publication, the authors acknowledge that they have not published their works so far and that they possess full copyrights for them.

Parts derived from other publications should have proper references.

Authors bear full responsibility for the content of their works and for ***non-disclosure of classified information*** – according to respective law regulations.

Editors reserve the right to request authors or to make any changes considered necessary. Authors give their consent to possible changes of their articles, resulting from review processes, language corrections and other actions regarding editing of materials. The authors also give their consent to possible shortening of articles in case they exceed permitted volume.

Authors are fully responsible for their articles' content, according to the provisions of *Law no. 206/2004 regarding good conduct in scientific research, technological development and innovation*.

Failing to comply with these rules shall trigger article's rejection. Sending an article to the editor implies the author's agreement on all aspects mentioned above.

For more details on our publication, you can access our site, http://cssas.unap.ro/en/periodicals.htm or contact the editors at impactstrategic@unap.ro

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE

Layout editor: Gabriela CHIRCORIAN

The publication consists of 100 pages.

"Carol I" National Defence University Printing House
Şoseaua Panduri, nr. 68-72, sector 5, Bucureşti
E-mail: editura@unap.ro
Tel: 021/319.40.80/215

17/12.07.2022 C. 133/2022