BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

3/2019
JULY-SEPTEMBER

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, 2019

BULLETIN

OF
"CAROL I" NATIONAL DEFENCE UNIVERSITY

3 / 2019

SCIENTIFIC PUBLICATION HIGHLY ACKNOWLEDGED IN THE FIELD OF "MILITARY SCIENCES, INFORMATION AND PUBLIC ORDER" OF THE NATIONAL COUNCIL FOR ATTESTATION OF ACADEMIC DEGREES, DIPLOMAS AND CERTIFICATES, INDEXED IN INTERNATIONAL DATABASES EBSCO, CEEOL & GOOGLE SCHOLAR

PUBLICATION FOUNDED IN 1937

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, 2019

Cover: Andreea GÎRTONEA

The articles published in the Bulletin of ”Carol I” National Defence University, ISSN 2284-936X, L 2284-936X, are also found in full text – title, author, abstract, content and bibliography – in the Romanian version of the journal, ISSN 1584-1928.

EDITORIAL BOARD

1. HONORIFIC BOARD

Brigadier Gen.Prof. Gheorghe CALOPĂREANU, PhD	"Carol I" National Defence University
Lect. Codrin MUNTEANU, PhD	Ministry of National Defence
Brigadier Gen.Prof. Constantin Iulian VIZITIU	Military Technical Academy
Brigadier Gen.Prof. Ghiță BÎRSAN, PhD	"Nicolae Bălcescu" Land Forces Academy
Brigadier Gen.(Air) Prof. Gabriel RĂDUCANU, PhD	"Henri Coandă" Air Forces Academy
Commander Prof. Octavian TARABUȚĂ, PhD	"Mircea cel Bătrân" Naval Academy
Col.Prof. Valentin DRAGOMIRESCU, PhD	"Carol I" National Defence University
Col.Prof. Ion PURICEL, PhD	"Carol I" National Defence University
Col.Prof. Cezar VASILESCU, PhD	"Carol I" National Defence University
Commander Prof. Ioan CRĂCIUN, PhD	"Carol I" National Defence University
Col. Prof. Ioana ENACHE, PhD	"Carol I" National Defence University
Col.Prof. Constantin POPESCU, PhD	"Carol I" National Defence University
Lect. Florian BICHIR, PhD	"Carol I" National Defence University
Col.Prof. Doina MUREŞAN, PhD	"Carol I" National Defence University
Col.Prof. Daniel GHIBA, PhD	"Carol I" National Defence University
Col.Lect. Florin CÎRCIUMARU, PhD	"Carol I" National Defence University
Col. Prof. Marinel-Dorel BUŞE, PhD	"Carol I" National Defence University
LtCol.Assoc.Prof. Tudorel-Niculai LEHACI, PhD	"Carol I" National Defence University
Col.Lect. Liviu BALABAN, PhD	"Carol I" National Defence University
Cpt.Lect. Răzvan GRIGORAŞ, PhD	"Carol I" National Defence University
Inspector Carol Teodor PETERFY (Winner of the Nobel Peace Prize in 2013)	Organization for the Prohibition of Chemical Weapons – OPCW

2. SCIENTIFIC BOARD

Prof. Gheorghe CALOPĂREANU, PhD	"Carol I" National Defence University
Assoc.Prof. Iulian CHIFU, PhD	"Carol I" National Defence University
Prof. Daniel DUMITRU, PhD	"Carol I" National Defence University
Prof. Gheorghe MINCULETE, PhD	"Carol I" National Defence University
Prof. Teodor FRUNZETI, PhD	"Titu Maiorescu" Christian University
Prof. Gelu ALEXANDRESCU, PhD	"Carol I" National Defence University
Prof. Sorin TOPOR, PhD	"Carol I" National Defence University
Prof. Marian NĂSTASE, PhD	The Bucharest University of Economic Studies
CS II Alexandra SARCINSCHI, PhD	"Carol I" National Defence University
CS II Cristina BOGZEANU, PhD	"Carol I" National Defence University
Pavel OTRISAL, PhD	University of Defence, Brno, Czech Republic

Assoc.Prof. Elena ŞUŞNEA, PhD	"Carol I" National Defence University
Elitsa PETROVA, PhD	"Vasil Levski" National Military University Veliko Tarnovo, Bulgaria
Jaromir MAREŠ, PhD	University of Defense, Brno, Czech Republic
Lect. Cris MATEI, PhD	Center for Civil-Military Relationships, USA
Piotr GAWLICZEK, PhD	"Cuiavian" University in Wloclawek, Poland
Assoc.Prof. Piotr GROCHMALSKI, PhD	"Nicolaus Copernicus" University in Torun, Poland
Marcel HARAKAL, PhD	"General Milan Rastislav Štefánik" Armed Forces Academy, Liptovský Mikuláš, Slovak Republic
Lucian DUMITRESCU, PhD	Romanian Academy
Prof. Anton MIHAIL, PhD	"Carol I" National Defence University"
Prof. Constantin IORDACHE, PhD	"Spiru Haret" University
Prof. Gheorghe ORZAN, PhD	The Bucharest University of Economic Studies
Prof. Gheorghe HURDUZEU, PhD	The Bucharest University of Economic Studies

3. SCIENTIFIC REVIEWERS

Col.Prof. Ioana ENACHE, PhD
Col.Prof. Ion ANDREI, PhD
Col.Prof. Dănuț TURCU, PhD
Col.Prof. Dorin EPARU, PhD
Col.Prof. Filofteia REPEZ, PhD
Commander Prof. Florin NISTOR, PhD
Col. Associate Prof. Cristian-Octavian STANCIU, PhD
LtCol. Associate Prof. Daniel ROMAN, PhD
Col. Ștefan-Antonio DAN ȘUTEU, PhD
LtCol. Associate Prof. Tudorel-Niculai LEHACI, PhD
LtCol. Engineer Associate Prof. Dragoș BĂRBIERU, PhD
Mr Associate Prof. Marinel-Adi MUSTAȚĂ, PhD
Lecturer Florin BICHIR, PhD
Associate Prof. Diana-Elena ȚUȚUIANU, PhD

CONTENT

MIGRATION IN THE KREMLIN'S DISINFORMATION WAR

Magdalena CRIȘAN, PhD Student*

The migration crisis of 2015 was accompanied by a wave of disinformation and fake news related to migrants, meant to influence the public perception of the phenomenon, and which serves Russia's geopolitical interest: a divided European Union and split European societies with leaders whose legitimacy is called into question.

Keywords: disinformation; Russian propaganda; European Union; perception; migration; fake news.

In recent years, new forms of struggle for power and hegemony in international relations have been discussed. This fact leads not only to the adoption of new strategies, but also to the design and use of new weapons. Hybrid warfare, for example, implies among other types of technologies also the use of refugees as a weapon[1] . Kelly M. Greenhill asserts that the *"exploiting and manipulating outflows created by others"* can become a non-military weapon of effective *coercion* on the international stage, especially if the opponent is a state with a liberal democracy[2]. The aim of the constraint of the adversary is to generate an *"domestic conflict"* or /and *"public dissatisfaction"* in the target state, either by diminishing the capacity or by influencing a state's *willingness* to receive and integrate a number of migrants[3]. This second strategy, called *"political agitating"*, represents an efficient way to increase the gap between the pro and cons in a society, especially in the case of sensitive issues such as migration, which translates into a vulnerability of the leader of the target country, consequently, by a decrease in his ability to negotiate externally[4]. For weak actors, the transformation of migration into a weapon means reaching a political goal that *"would be utterly unattainable through military means"*, and for powerful actors *"it would have been too costly"*[5]. It is no secret that Russia wants to regain its place as a major global player, implying the control over its former spheres of influence in Europe, and uses therefor all means of warfare to achieve its goal. Because the West's military technology is superior to its own, Russia is betting on another strategy of *"warfare"*, with non-military means such as disinformation, manipulation campaigns[6], dissemination of fake news, whose purpose is *"shaping their (A/N population in European countries) opinions in favor of Russian objectives"*[7], a strategy that was applied also in 2015, when the migration crisis hit the European Union .

"The day has come when we all have to admit that a word, a camera, a photo, the Internet, and information in general have become yet another type of weapons, yet another component of the armed forces. This weapon can be used in a good and in a bad way", stated the Russian Defense Minister Serghei Shoigu in 2015[8]. So the battlefield is the mind of the people, the population of Western states, often neglected by the Western military strategies[9], and the aim is *"weakening the internal cohesion of societies and strengthening the perceptions of the dysfunctions of the Western democratic and economic system"*, shows the report of the Center for Strategic and International Studies in Washington, *"The Kremlin Playbook"*[10]. Altering perceptions and destroying cohesion are successfull only where there already are institutional deficiencies or issues that polarize public opinion. One such chink in EU's armour speculated by Russia is the migration crisis that started in 2015, when FRONTEX registered 1,8 million illegal border crossings into the EU[11], and when over 1.2 million migrants applied for asylum in several EU states, a figure twice as large as in the previous year[12]. Most of the asylum seekers in 2015 were Syrians, Afghans and Iraqis[13]. The wave of migration brought to light deficiencies of the European institutions

* ***"Carol I" National Defence University***
e-mail: *crisanmagda@yahoo.com*

and the institutions of the member states, which proved to be unprepared to handle such a large number of migrants, and stimulated populist and extremist political discourses. From the media point of view, the migration crisis resembles the military Operation Desert Storm of 1991, which through its broadcasting in real-time on CNN has captured the attention and influenced the public opinion[14]. In 2015, migrants coming from the sea or the Balkan route to Western Europe were intensely mediatized, flows being broadcast in real time on television and streamed live online. These images have stirred up concerns[15] and polarized opinions in the European Union[16]. Thus, the issue of migration is an extremely fertile ground for the Russian propaganda because it has the potential to split the EU, *"to disrupt European unity and shake EU citizens' confidence in European institutions"* and to question the legitimacy of some leaders of the member states[17]. And Russia's geopolitical interest is having a EU-polyphony of weak voices and weak states.

Fake news and Russian propaganda targeting migration

Media that makes pro-Russian propaganda proved to be *"in large part responsible for the dissemination of migration-related fake news"*[18]. There is plenty of scientific literature on the fake news phenomenon[19], and from the collection of definitions we draw out three essential aspects *"the low (A/N level) of facticity"*, *"the immediate intention to deceive"* and the attempt *"to appear like real news"*[20]. The type of discourse promoted by the Pro-Russian propaganda, accompanied by fake news, supports the one of the anti-immigration parties and aims to pit, completely false, the image of an *"ailing West"* and that of *"a stable and peaceful Russia"*, who keeps its traditions, values, identity[21]. And in its foreign policy strategy the Kremlin plays the cultural identity card. An official document on Russia's foreign policy from 2010 shows that *"it is increasingly evident, that the global competition takes on a cultural dimension. Among the fundamental games in the international arena the struggle for cultural influence becomes more intense"*[22]. "The Foreign Policy Concept of the Russian Federation" in 2008 underlines that "*Russia will seek its objective perception in the world, develop its own effective means of information influence on public opinion abroad, strengthen the role of the Russian mass media in the international information environment providing them with essential state support"* and that it will *"take necessary measures to repel information threats to its sovereignty and security"*[23]. The most prominent names in the propaganda media mentioned in the document above are Sputnik and Russia Today, whose news is also available in English, French, German, so that their content reaches the EU public directly. The European Union considers the Kremlin's disinformation tactic so dangerous that in 2015 it set up an East StratCom Task Force - as a part of the administration of the the European External Action Service -, whose aim is dismantling and combating the Kremlin's disinformation. An analysis of EUvsDisinfo, part of East StratCom activity, shows that from November 2015 to August 6, 2019, over 6,000 cases of disinformation cases sprout from Russia were identified, and migration is among top 10 topics of disinformation[24]. Another EUvsDisinfo document draws attention to Kremlin misinformation tactics, for example, different messages and different communication channels (eg face-to-face, social media, press) for different target audience categories, an unknown number of communication channels, and communicators[25]. These communicators may include diplomatic staff, secret services, so-called Kremlin-funded NGOs and blogs, trolls and bots on social media[26], and not least the Kremlin's propaganda media, which spread fake news and, *"stir up confusion"*[27].

The way in which disinformation works is basically the same: it artificially feeds the negative emotions, fear, anger, disgust, in a certain society, obtaining, for example, a wave of antipathy for the West, for a certain ethnic or sexual minority or an anti-immigration wave[28]. For example, the pro-Russian propaganda media supporting the anti-immigration discourse securitizes migration, transforming it into a threat to the security of European society by linking it with terrorism and increased crime, inducing a state of discomfort and fear among the population[29]. And a highly polarized society *"shaken by strong emotions will behave more irrationally and will be easier to manipulate"*[30] . The EUvsDisinfo plan to combat disinformation at EU level, launched in June

2019, notes that there is evidence for *"a continued and sustained disinformation activity by Russian sources aiming to suppress turnout and influence voter preferences"* in the European Union[31]. The same document shows that *"malicious actors using disinformation to promote extreme views and polarise local debates, including through unfounded attacks on the EU"*, and that this type of discourse was adopted by national actors from the member states[32].

The weapon of disinformation on migration issues

Claire Wardle, a social media expert, has identified several types of intentional disinformation, including invented content, false context, and manipulated content[33]. We must underline that disinformation mostly retains a grain of truth, it builds around a pre-existing problem, targets a public that is vulnerable to false information[34]. An example of disinformation by providing a wrong context and wrong connections is a Sputnik article on the increase in the number of sexual offences in Sweden, in which the author suggests, without having any evidence, that the Swedish open doors policy is to blame for it[35]. *"Whereas the Swedish political establishment is loath to acknowledge any possible link between immigration, crime and the population's growing feeling of insecurity, Sweden's handling of foreign-born felons has triggered concern"*, reports the article, suggesting that migrants are implicitly criminals[36] . After a month the message was taken over by British populist politician Nigel Farage, who wrote on Twitter that *"pro-rata Sweden"* is the country that *"has taken more young, male migrants than any other country in Europe"* and the result is that, *"Malmo is now the rape capital of Europe"*[37].

The article published by Sputnik and taken over by Farage does not inform that the Swedish law on sexual offences includes more offences since 2013, that unlike other European countries, in Sweden, ten rapes committed in ten days by a man on a woman are registered as being 10 different cases of rape; in addition, an allegation of rape, which was later found to be unfounded, remains in the Swedish sex offences statistics[38]. The number of sex crimes registered in 2015, when Sweden received a large number of migrants, is lower than the previous year[39]. We also have an example of disinformation by false allegations accompanied by real images: In 2017, after the London Bridge attack, the photo of a woman in hijab at the scene of the attack, which was described as ignoring the victims, was intensely speculated by Russian and anti-immigration propaganda. The Twitter account, with over 16,000 followers, @SouthLoneStar, whose owner described himself as a *"proud Texan and American patriot"*, the one who published the photo with the woman in hijab and made the false allegation, was dismantled as *''one of 2,700 accounts handed over to the US House Intelligence Committee by Twitter as a fake account created in Russia to influence UK and US politics"*[40]. Another disinformation from February 2018, built on false information and a digitally manipulated photography, targeted this time the Russian public. Several Russian news sites and a Russian social media platform reported on a flashmob organized by women in Germany, Sweden, Denmark and other European countries called *#sorry*, asking Muslim migrant rapists to forgive them because they provoked them through *"depraved behavior and clothing"*[41].This flashmob did not exist, and the photography in which a young woman from Europe appears holding a sign that says *"Sorry Mustafa"* is flagrantly edited. The real photo was taken in 2014, at an action aimed to support Ukrainian soldiers, and real the says: *"Cold? Think about those who are sleeping in the trenches"*[42]. An already well known example of fabricated content promoted by the Kremlin is the case of Lisa, a German teenager of Russian origin, who was reported to have been raped by migrants in 2016. The news, which stirred up emotions in Germany and gave Russian Foreign Minister Sergei Lavrov the opportunity to criticize Germany for hiding the case, initially appeared on an obscure site for Russian expats living in Germany and proved to be be fake[43]. Even the Russian President, Vladimir Putin, fell prey to fake news disseminated by the public television station Channel One Russia. The Russian leader said in the fall of 2016 that the Austrian court acquitted an Iraqi migrant who raped a boy because he didn't speak German and therefore did not understand the victim's verbal protest[44]. In fact, at the time Putin made this statement, the Iraqi migrant was in custody of the Austrian authorities[45].

Conclusions

Migration can become a weapon in the hands of actors aiming at destabilizing opponents, diminishing their bargaining power on the international stage. Russia is the proof, Kremlin is waging a war of disinformation, fake news, in Europe, whose purpose is to influence the perception of the population, weaken the unity of the European Union and deepen distrust in the institutions, democratic processes in the West. The migration crisis was a fertile ground for the Kremlin's disinformation campaign because in the EU and in the member States there were deficiencies in managing the large number of migrants, public opinion was beginning to polarize, and populist politicians felt entitled to keep their anti-immigration discourse. Russian propaganda has supported the anti-immigration discourse, fueling confusion and speculating on the discomfort and fear of citizens of European states. The practice of Russian propaganda consists in the securitization of migration, linking migrants with terrorism, criminality, thus a danger to the security of the member states and the physical security of its citizens. Through its disinformation war in the EU states, the Kremlin is trying to gain a better image for Russia, eager to become again a major global player, opposing the image of a migrant-ridden West, whose identity is in danger, the image of a Russia that defends its values, traditions and cultural identity, basically a model to follow. Russian disinformation, including in the topic of migration, is done through different channels, face-to-face, on social media sites or in the propaganda press, which includes Sputnik and Russia Today, which offer content in several languages spoken in EU countries. The messages of disinformation agents are different for different categories of target-audience, either instigating anti-Western feelings, or hatred towards a certain minority or migrants. Disinformation can take many forms, the common denominator is the intention to deceive and the content with low or zero facticity. We can come up against information out of context, other put in the wrong context, news in which the author intentionally makes wrong connections or we can simply have news completely fabricated. The European Union recognized the danger of Russian disinformation for the security of the EU and its member states and created mechanisms to dismantle and combat it. In nearly four years, 6,000 cases of misinformation in Russia have been identified, and migration is among the favorite topics.

NOTES:

1 Kelly M. Greenhill, "*Strategic Engineered Migration as a Weapon of War"*, **Civil Wars**, vol. 10, no. 1, 2008, pp. 6-21, online DOI: 10.1080/13698240701835425, accesed at July 12, 2019.

2 Kelly M. Greenhill, *"Migration as a Weapon in Theory and in Practice"*, **Military Review**, noiembrie/decembrie 2016, online https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2016/, accessed at July 14, 2019, p. 25.

3 *Idem.*

4 *Ibidem*, p. 26 and p. 28.

5 *Ibidem*, p. 27.

6 Russian officials P. A. Doulnev and V. I. Orlyansky assessed in 2015 that the enemy must be defeated or at least made economically, politically vulnerable before the war itself begins, including by manipulating public opinion. P. A. Doulnev, V. I. Orlyansky, *"Basic Changes in the Character of Armed Struggle in the First Third of the 21st Century"*, Journal of the Academy of Military Science, nr. 1 (2015): 46, cited in Lt. Col. Timothy L. Thomas, *"Russian Forecasts of Future War"*, Military Review, Army University Press, May-June 2019, online https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Thomas-Russian-Forecast/, accessed at July 2, 2019.

7 Timothy P. McGeehan, *"Countering Russian Disinformation"*, Parameters 48(1), Army War College, 2018, online https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/8_McGeehan_CounteringRussianDisinformation.pdf, accessed at May 2, 2019, p. 50.

8 *"Shoigu: Information becomes another armed forces component"*, **Interfax**, March 28 2015, online http://www.interfax.com/newsinf.asp?id=581851, accessed at April 20, 2019.

9 "Civil society presents a fundamental blind spot in the American military understanding of warfare", which is why it was turned into a weapon by opponents like Russia or China. Buddhika B. Jayamaha, Jahara Matisek, *"Social Media Warriors:Leveraging a New Battlespace"*, **Parameters**, vol. 48, nr.4, Army War College, 2018-2019, p.11.

10 H. Conley, J. Mina, R. Stefanov, M. Vladimirov, *''The Kremlin Playbook. Understanding Russian Influence in. Central and Eastern Europe",* CSIS Europe Program CSD Economic Program, October 2016, p. X.

11 The number of illegal crossings is not the same with number of illegal migrants. "Risk Analysis for 2017", FRONTEX, februarie 2017, Warsaw, online https://frontex.europa.eu/assets/Publications/Risk_Analysis/ Annual_Risk_Analysis_2017.pdf, accessed at July 3, 2019, p.18.

12 "Record number of over 1.2 million first time asylum seekers registered in 2015", Eurostat Press Release, March 4, 2016, online https://ec.europa.eu/eurostat/documents/2995521/7203832/3-04032016-AP-EN.pdf/790eba01-381c-

4163-bcd2-a54959b99ed6, accessed at July 13, 2019.

13 *Idem.*

14 Philp Seib, *''Effects of Real-Time News Coverage on Foreign Policy"*, Journal of Conflict Studies, volum XX, nr. 1, primăvara 2000, online https://journals.lib.unb.ca/index.php/jcs/article/view/4309/4920, accessed at 2 June, 2019.

15 The percentage of Europeans who consider migration a challenge for the EU increased by the end of 2015 by 33% compared to June 2013. While citizens of countries such as Germany and Sweden, target of the migrant wave, consider that in the context of migrant crisis migrants on the labor market are needed (72% respectively 77%). In states like Hungary, Czech Republic, Slovakia, Poland less than 40% agreed with this. *"Parlemeter 2015 – Part I The main challenges for the EU, migration, and the economic and social situation"*, European Parliament, Brussels, October 14, 2015, online http://www.europarl.europa.eu/pdf/eurobarometre/2015/2015parlemeter/eb84_1_synthese_analytique_partie_1_migration_en.pdf, accessed at December 2, 2018, p. 10 and p. 34.

16 Support for a common migration policy has declined in 23 Member States from spring to fall 2015, and in 9 states even with 10%. Standard Eurobarometer 84, *"Europeans' views on the priorities of the European Union"*, Comisia Europeană, toamnă 2015, online https://bit.ly/2UjGxfs, accessed at January 12, 2019, p. 45.

17Attila Juhász, Patrik Szicherle, *'"The political effects of migration-related fake news, disinformation and conspiracy theories in Europe"*, Friedrich Ebert Foundation, Political Capital Policy Research and Consulting Institute, 2017, online https://www.politicalcapital.hu/pc-admin/source/documents/FES_PC_FakeNewsMigrationStudy_EN_20170607.pdf, accessed at May 3, 2019, p. 4.

18 *Idem.*

19 Part of the many definitions of fake news: Figure 1 "Overview of characteristics in fake news definitions", in Jana Laura Egelhofer, Sophie Lecheler, *"Fake news as a two-dimensional phenomenon: a framework and research agenda"*, Annals of the International Communication Association, 43:2, 97-116, online DOI: 10.1080/23808985.2019.1602782, accessed at November 2, 2018, p. 3.

20 Edson C. Tandoc Jr., Yheng Wei Lim, Richard Ling, *"Defining Fake News", Digital Journalism*, *6*(2), pp.137–153, 2018, online DOI: 10.1080/21670811.2017.1360143, accessed at March 15, 2019, pp. 147-148.

21 Attila Juhász, Patrik Szicherle, *op.cit.*, p.4.

22 Document of the Russian Federation from 2010, *"Basic Guidlines Concerning the Policy of the Russian Federation in the Sphere of International-Humanitarian Cooperation"*, cited in Marcel H. Van Herpen, *''Putin's Propaganda Machine: Soft Power and Russian Foreign Policy"*, Rowman & Littlefield, Lanham Maryland, SUA, 2015, p. 28.

23"The Foreign Policy Concept of the Russian Federation", Russian Federation Presidency, January 12 2008, online http://en.kremlin.ru/supplement/4116, accessed at June 3, 2019.

24 *"Figure of The Week: 6000+"*, EUvsDisinfo, August 6, 2019, online https://euvsdisinfo.eu/figure-of-the-week-6000/, accessed at August 7, 2019.

25 "The Strategy and Tactics of the Pro-Kremlin Disinformation Campaign", EuvsDisinfo, June 27 2018, online https://euvsdisinfo.eu/the-strategy-and-tactics-of-the-pro-kremlin-disinformation-campaign/, accessed at August 23, 2018.

26 *Idem.*

27 In a paper from 2012, S. G. Chekinov and S. A. Bogdanov, officers of the Russian General Staff Academy assess that in preparing a future war ''The attainment of information superiority and the use of the mass media will stir up chaos and confusion in an adversary's government and military management and control systems". S. G. Chekinov and S. A. Bogdanov, *"Initial Periods of War and their Impact on a Country's Preparations for Future War",* Military Thought, nr. 11 (2012): 16, cited in Lt. Col. Timothy L. Thomas, *"Russian Forecasts of Future War"*, Military Review, Army University Press, May-June 2019, online https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Thomas-Russian-Forecast/, accessed at 2 July, 2019.

28 Russian military strategists believe that the influence of the will, emotions, behavior, psychology and morals of the opponent plays a fundamental role in the fight. Valeriy A. Kiselev, *"For What Kinds of Conflict Should the Armed Forces of Russia Prepare?",* Military Thought, nr. 3 (2017): 37, cited in Lt. Col. Timothy L. Thomas, ''Russian Forecasts of Future War", Military Review, Army University Press, May-June 2019, online https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Thomas-Russian-Forecast/, accessed at July 2, 2019.

29 Attila Juhász, Patrik Szicherle, *op.cit.*, p. 7.

30 *"The Strategy and Tactics of the Pro-Kremlin Disinformation Campaign", op.cit.*

31 "Action plan against desinformation. Report on progress", EU vs Disinfo, European Commission, June 2019, online https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf, accessed at July 1, 2019, p. 2.

32 *Idem.*

33 Claire Wardle, "*Fake News. It's complicated"*, February 16 2017, First Draft, online https://firstdraftnews.org/fake-news-complicated/, accessed at May 17, 2019.

34 *"The Strategy and Tactics of the Pro-Kremlin Disinformation Campaign"*, *op.cit.*

35 *"More Swedish Women Haunted by Fears of Rape»*, **Sputnik**, January 11 2017, online https://sputniknews.com/europe/201701111049464215-swedish-women-rape-fears/, accessed at March 23, 2019.

36 *Idem.*

37 *"Reality Check: Is Malmo the 'rape capital' of Europe?"*, February 24 2017, **BBC**, online https://www.bbc.com/news/uk-politics-39056786, accessed at February 14, 2019.

38 Attila Juhász, Patrik Szicherle, *op.cit.*, p.12; "*Reality Check: Is Malmo the 'rape capital' of Europe?"*, *op.cit.*

39 *"Reality Check: Is Malmo the 'rape capital' of Europe?"*, *op.cit.*

40 "Anti-Muslim online surges driven by fake accounts", **The Guardian**, November 26 2017, online https://

www.theguardian.com/media/2017/nov/26/anti-muslim-online-bots-fake-acounts, accessed at April 10, 2019.

41 *"Fake Russian Story Stokes Anti-Immigrant Fears"*, **StopFake**, February 8 2018, online https://www.stopfake.org/en/fake-russian-story-stokes-anti-immigrant-fears/, accessed at December 15, 2018.

42 *Idem.*

43 Jakub Janda, *"The Lisa Case: STRATCOM Lessons for European states"*, Security Policy Working Paper, No. 11/2016, Federal Academy for Security Policy, online https://www.baks.bund.de/de/node/1577, accessed at May 23, 2019.

44 *"Putin-Kritik an Österreich: Schuldgefühl Migranten gegenüber»*, **Die Presse**, November 2 2016, online https://diepresse.com/home/ausland/aussenpolitik/5111245/PutinKritik-an-Oesterreich_Schuldgefuehl-Migranten-gegenueber, accessed at January 23, 2019.

45 *Idem.*

BIBLIOGRAPHY

Conley H., Mina J., Stefanov R., Vladimirov M., *"The Kremlin Playbook. Understanding Russian Influence in. Central and Eastern Europe"*, CSIS Europe Program CSD Economic Program, October 2016.

Egelhofer Jana Laura, Lecheler Sophie, *"Fake news as a two-dimensional phenomenon: a framework and research agenda"*, Annals of the International Communication Association, 43:2, pp. 97-116, online DOI: 10.1080/23808985.2019.1602782, accessed at November 2, 2018.

Greenhill Kelly M., *"Migration as a Weapon in Theory and in Practice"*, **Military Review**, noiembrie/decembrie 2016, online https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2016/, accessed at June 14, 2019.

Greenhill Kelly M., "*Strategic Engineered Migration as a Weapon of War"*, **Civil Wars**, vol. 10, no. 1, 2008, pp. 6-21, online DOI: 10.1080/13698240701835425, accessed at July 12, 2019.

Janda Jakub, *"The Lisa Case: STRATCOM Lessons for European states"*, Security Policy Working Paper, No. 11/2016, Federal Academy for Security Policy, online https://www.baks. bund.de/de/node/1577, accessed at May 23, 2019.

Jayamaha Buddhika B., Matisek Jahara, *"Social Media Warriors: Leveraging a New Battlespace",* Parametres, vol. 48, no.4, Army War College, 2018-2019.

Juhász Attila, Szicherle Patrik, *"The political effects of migration-related fake news, disinformation and conspiracy theories in Europe"*, Friedrich Ebert Foundation, Political Capital Policy Research and Consulting Institute, 2017, online https://www.politicalcapital.hu/pc-admin/source/documents/ FES_PC_FakeNewsMigrationStudy_EN_20170607.pdf, accessed at May, 2019.

McGeehan Timothy P., *"Countering Russian Disinformation"*, Parameters 48(1), Army War College, 2018, online https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/8_McGeehan_CounteringRussianDisinformation.pdf, accessed at May 2, 2019.

Seib Philp, *"Effects of Real-Time News Coverage on Foreign Policy"*, Journal of Conflict Studies, volum XX, no. 1, spring 2000, online https://journals.lib.unb.ca/index.php/jcs/article/view/4309/4920, accessed at June 2, 2019.

Thomas Timothy L., *"Russian Forecasts of Future War"*, Military Review, Army University Press, mai-iunie 2019, online https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Thomas-Russian-Forecast/, accessed at July 2, 2019.

Tandoc Jr. Edson C., Lim Yheng Wei, Ling Richard, *"Defining Fake News", Digital Journalism*, *6*(2), pp.137–153, 2018, online DOI: 10.1080/21670811.2017.1360143, accessed at March 15, 2019.

Van Herpen Marcel H., *"Putin's Propaganda Machine: Soft Power and Russian Foreign Policy"*, Rowman & Littlefield, Lanham Maryland, SUA, 2015.

Wardle Claire, *"Fake News. It's complicated"*, February 16 2017, First Draft, online https://firstdraftnews.org/fake-news-complicated/, accessed at May 17, 2019.

Press articles

"Shoigu: Information becomes another armed forces component", **Interfax**, March 28 2015, online http://www.interfax.com/newsinf.asp?id=581851, accessed at April 20, 2019.

"More Swedish Women Haunted by Fears of Rape", **Sputnik**, 11 ianuarie 2017, online https://sputniknews.com/europe/201701111049464215-swedish-women-rape-fears/, accessed at March 23, 2019.

"Reality Check: Is Malmo the 'rape capital' of Europe?", February 24 2017, **BBC**, online https://www.bbc.com/news/uk-politics-39056786, accessed at February 14, 2019.

"Anti-Muslim online surges driven by fake accounts", **The Guardian**, November 26 2017, online https://www.theguardian.com/media/2017/nov/26/anti-muslim-online-bots-fake-acounts, accessed at April 10, 2019.

"Fake Russian Story Stokes Anti-Immigrant Fears", **StopFake**, February 8 2018, online https://www.stopfake.org/en/fake-russian-story-stokes-anti-immigrant-fears/, accessed at December 15, 2018.

"Putin-Kritik an Österreich: Schuldgefühl Migranten gegenüber", **Die Presse**, November 2, 2016, online https://diepresse.com/home/ausland/aussenpolitik/5111245/PutinKritik-an-Oesterreich_SchuldgefuehlMigranten-gegenueber, accessed at January 23, 2019.

Online pages of institutions

The European Border and Coast Guard Agency frontex.europa.eu

European Commission ec.europa.eu

European Parliament europarl.europa.eu

EUvsDisinfo, site of combating Russian disinformation, part of the East StratCom Task Force euvsdisinfo.eu

Fact-checking organization to combat fake news stopfake.org

THE PHYSIOGNOMY OF JOINT MULTINATIONAL OPERATIONS

LtCol. Associate Professor Alexandru HERCIU, PhD*

In general, the doctrine for joint multinational operations establishes the set of notions and principles of employing the Romanian armed forces in the joint multinational operations. It presents the multinational operations to which Romania can participate as part of an alliance, coalition or other agreed commitment and highlights the joint organizational formations needed to coordinate land, air, maritime and special joint security operations (defense) in a multinational environment.

It provides the necessary military guidance in the exercise of authority by commanders in the military theater of operations, directing the force-generation activity, planning, transferring authority, and executing the joint multinational operations. It is compatible with the doctrines of multinational operations of the armed forces of Western NATO member states.

In this context, the present paper aims to analyze the characteristics and physiognomy of the joint multinational operations in which forces belonging to the Romanian Army can participate in the context of alliance or coalitions, given the specificity of the current operational environment.

Keywords: joint operations; multinational operations.

Introduction

The reality highlighted by the recent conflicts demonstrates that in the current security environment, military operations have a joint and multinational character, and conventional actions intertwine with unconventional and asymmetric ones. Whether we are talking about state adversaries, non-state actors, or a combination of them, in a potential hybrid conflict, they will use a wide range of asymmetric activities to exploit the vulnerabilities of their opponent. This category includes terrorist, insurgent, separatist, and organized crime actions as part of a dynamic and diversified mix. The military phenomenon analysts expressed this mixture in the concept of „hybrid conflict". Engaging capabilities specific to each type of operation will occur under the influence of a set of factors, conditions, circumstances, and particular stress factors that define the current security environment. It includes belligerents and neutral actors, the physical environment, and the information (virtual) environment.

***"Carol I" National Defence University**
Land Forces Department within Command and Staff College
e-mail: *herciu_alexandru12@yahoo.ro*

Theoretical aspects regarding joint multinational operation

Military operation

The military operation represents all the combat actions carried out by military formations in order to achieve goals at different levels of military art: tactical, operational, or strategic. By adopting the definition provided in AAP-6, NATO's Glossary of Terms and Definitions, the Romanian doctrinal provisions define the operation as a "military action or the execution of a strategic, tactical mission specific to a category of forces, training, or service forces; the process of conducting a fight, including the movement, support, attack, defense, and maneuvers necessary to accomplish the objectives of a battle, operations, or campaign."[1]

Some earlier publications state that the operation represents all the combat operations carried out by operational formations and tactical units following a unique plan. The aim of these operations is considered to be the accomplishment of an operational or strategic purpose and consists, as a rule, of a series of battles coordinated in time and space, based on a unitary concept.[2]

Joint operation

The "joint" adjective is used to describe the coordinated framework of military activities. These activities involve at least two different branches of the army, components or services.

The joint operation is defined as: "all the land, air and maritime actions carried by a group consisting of forces or elements and means belonging to several services of armed forces in the appropriate environment specific to each of them in a defined geographic area, in a unitary concept and under the unique command of an joint operational command for the purpose of achieving strategic objectives."[3]

A more comprehensive definition of the joint operation stipulates that the effort focuses on the synchronization of forces and capabilities provided by the "land, maritime, air, space, cyberspace, special operations and other functional forces"[4] component, one or some of which to predominate at a particular stage of the operation.

This definition is more comprehensive because it is not limited to the physical nature of the action but also takes into account other components involved in the operation, such as the information one.

Consequently, we believe that the process of analyzing the joint operation can only be achieved in the context of understanding the new physiognomy of modern military conflicts. The new trends involve their deployment in an extended operational environment – where the social environment is a fundamental segment – and include an extremely active information component.

Under these circumstances, the actions carried out involve the integrated and united involvement of all categories of forces intersecting, overlapping, complementing each other.

The joint operation runs over a specified period within the physical boundaries of a geographical area called the joint area of operation, where the commander of the joint force plans and executes an operational level mission.[5]

Reference military publications[6] include Special Operations Forces (SOF) as one of the components of the joint operation.

Therefore, the components of the combined operation are the following: the land component; the air component; the maritime component; and the special operations component.

The joint operation has a predominantly offensive character and is directed at the strategic and operational centers of gravity of the opponent. The synchronization and coordination of forces and activities within the joint operation shall be ensured permanently in the process of operations, during its planning, preparation, execution, and evaluation phases.

The success of joint operations is assured by the merged effort of all services and components of the force or the combined effort of at least two of them, operating under a single command.

Integrated operation

The integrated operation is the military action in which civilian and military structures are coordinated with the most diverse roles and positions, which can contribute – by engaging in the specific field of activity – to resolving the conflict and achieving the goals of the military operation. Therefore, the integrated action implies, in our opinion, a conjugation of the individual effort of the entities to achieve a common goal, resulting from putting together the multiple individual goals.

The joint peculiarity requires, first of all, an identification of all actors operating in the operational security environment, their motivations/interests, the influences and resources of each of them to coagulate the energies of those entities. These actors can be conventional military forces; unconventional military forces; asymmetric, neutral or undecided opponents; international bodies; International Organizations (IOs); Non-governmental organizations (NGOs); local and national institutions and authorities; Media; economic agents; private security companies; and the civilian population.

Secondly, the integration process involves a different approach of each actor and finding an appropriate way of communication and interaction between the joint multinational force operating in the theater of operations and that entity. This can be a critical challenge for the joint force commander, a situation that can be overcome by the excellent knowledge of all the actors, the connections and relationships between them and the proper use of communication and negotiation skills. Besides, integration calls on the commander to mediate and harmonize relations between certain actors who may be adversely affected in the context of interpersonal relationships but who are equally beneficial to the military.

Last but not least, we consider that the integration process is continuous and dynamic and must be considered at all stages of the conflict before the armed confrontation arises, during and

after the military operations, in close correlation with the evolution of the operational environment.

Another aspect that deserves to be mentioned is that military operations have acquired a joint facet across the spectrum of the conflict and at all levels at which they place.

We strongly believe that the integration process must be understood and addressed within all its aspects: structural, cognitive, information, and logistic. Thus, the organizations, the common understanding of reality, the activities carried out, and the resources made available and shared can be channeled, based on the outlined operational design, in order to achieve the overall goals of the operation. This requires a thorough and sustained effort to coordinate all the integrated components during the planning, preparation, execution, and evaluation of the military operation, especially in the context of hybrid conflicts, which we consider to be quintessential for this type of operation.

Multinational operation

Nowadays, the vast majority of military operations are carried out within a multinational framework due to the need for visibility of political consensus and the legitimacy of military action. Cooperation within the multinational operation is carried out with both traditional members and partners within the alliances and with less familiar members in coalitions of states.[7]

The multinational operation is a military operation involving forces from at least two nations acting together to carry out a mission. The "multinational" adjective describes both the participation of national elements in the constitution the force and their engagement in activities and operations. Within NATO, for the multinational operation, both the "combined force" and the "multinational combined force" are used to describe an operation carried out by force composed of two or more nations that act together and which include elements of at least two services of the army. [8]

Peculiarities of the joint operation carrie out in a multinational context

"The military structures of the future will be conceived and trained to carry out complex military actions in a joint context, often with a multinational, modular structure that can be adapted in short time to the mission and the particular conditions."[9]

The concept of joint operation is not entirely new to the Romanian military theory and practice. Known in recent decades as the "air-land battle", the concept has been studied only from the perspective of the defender: the Romanian armed forces were considered the part that was supposed to counteract hostile joint military action. Operational and strategic level actions in the Romanian Army over the last twenty years have been a model in this respect. The regulations in force required the conception or execution echelons to create a tactical, operational or strategic framework in which the planned actions, regardless of the branches of the army or services, have to be integrated.

From a historic point of view, joint actions of two or more categories of forces have taken place since the first division of the armed forces (infantry and cavalry), to which artillery and battleships were later added. However, they were complementary or mutually supportive military actions and not considered to be *joint* military actions.

Two events preceded the official discussion of the concept of *joint* military action.

The first was the Falkland/Malvinas War (1982), in which modern British royal military forces had to face the more arduous Argentine army, but with the considerable advantage of the land on its side. The lack of air protection of the British maritime convoys by the Royal Air Forces (RAF) produced significant human and equipment losses and quickly constituted an almost destabilizing factor.

The second example was the US Grenade Rescue Mission in 1983, in which the incompatibility of communications, combat procedures and even maps weakened the intensity of air operations. As a result of the lessons learned from these conflicts, in 1986 the US Congress approved the so-called *Goldwater-Nichols Act*, which was the cornerstone of the future integration of US forces and the creation of United States Joint Forces Command (USJFCOM) on October 7, 1999.

Following the American model, in the same year, the British Government approved the establishment of a Permanent Joint Headquarters in Northwood, London (PJHQ) and the transformation of the military colleges of force categories into a single Joint Services Command and Staff College

(JSCSC). This is a British military academic establishment providing training and education to experienced officers of the Royal Navy, Army, Royal Air Force, Ministry of Defence Civil Service, and serving officers of other states.[10]

From the semantic analysis of the syntagm "integrated character", by associating the meaning of the two notions, it is clear that this is a distinctive feature, which is the specificity of military action "harmonized in one"[11]. In other words, the integrated nature of military actions expresses the degree of harmonization and synchronization of all elements that make up an active system such as battle, operation, or campaign. That meant all forces and means, regardless of the type and branches of the army or services they are part of.

The integrated character of military actions is a feature of operations, the emergence of which was determined by the multiplication of the action couples that it composes, being a natural consequence of the increase in the number of branches of the army and the organization of modern armies by different services. At the same time, these features are reasonable consequences of the evolution of the war phenomenon, as a result of the development of science and technology. This trend has continuously increased in complexity, resulting in a continuous amplification of the connections between the composing elements.

The joint operations are inevitably important components (campaigns, battles or operations) of the war, knowing that the war has an extensive range of expression, far exceeding the sphere of violent confrontation. Thus, the emergence of the joint concept of operation is a consequence of the evolutionary-historic process of military art. The current acceptance of the phrase "joint operation" embraces its multiple and complex aspects, defining in principle the sum of the military actions, and not only, carried out at operational, strategic and tactical levels. The force is composed of several categories of forces of the modern armies, under a single leadership, after a unitary conception and having a single objective/mission.

By proceeding to a translation of the theoretical and practical issues, it is worth noting that this integrated character involved a considerable increase in the importance of cooperation between the forces participating in the integrated military actions in order to accomplish the purpose of the operation. As a result, the provisions of the specific rules, forms, and methods of cooperation, in order to jointly carry out combat missions, began to appear in the content of the fighting regulations of each branch of the army and service category.

The need to interconnect the specific mode of accomplishing one's missions with that of other branches of the army appeared not only within a category of forces that usually act in the same environment and against the same opponent but also between branches of the army belonging to different services of the military. In the same manner, one can analyze the character of inter-categories of army forces of recent military actions, a peculiarity that expresses the functional relations between at least two services within the operations that can be of strategic but also an operational level.

Within the strategic sphere, the joint feature of operations is implicit, due to the participation, as a rule, of both, services and branches of the army. In the same context, the integrated nature is revealed mainly in the strategic level operations, but one should not exclude the possibility of its materialization also at the operational level, as in the case of setting up joint level gatherings. Of course, these come from tactical or operational formations belonging to several services.

By deepening the analysis, the integrated character of inter-armed forces and inter-categories of army forces can be highlighted and will have to be achieved at all stages of the preparation and conduct of military actions. During the preparation of the military actions, the realization of integrated inter-branches and inter-services has a special significance and must be found in each of the activities that take place at the level of the JFC.

As such, developing the concept of the use in operation, tailoring forces and means must originate from a thorough analysis of the missions, the adversary, space, and the available time. A correlation and interconnection of the missions' variables must be carried out in the first stage of the operations process, according to the potentialities of the forces and means available and on the corresponding character of the actions of different branches of the armies and services.

The finality of these concerns will be the focus of efforts to achieve the goals of the joint operation by highlighting all the elements that give the unitary character to the armed struggle in

general. All these elements of conception will be materialized in a single, unitary operation plan, based on which orders and provisions are emitted for all subordinate structures.

It is also important to remark that, in a similar integrative perception, the logistic dilemmas will be solved, revealed in a separate plan, even if the material assurance responsibilities will still belong to other structures not directly involved in military actions. A real synchronization and interconnection, the complementarity and synergy of military actions will be displayed, especially during the conduct of the joint operations.

Harmonizing the efforts of all participating units to achieve the objectives of the joint operations, will be achieved through the unique management of the actions and their permanent coordination. The basis for achieving this desideratum, which confers the integrity of operations, will be to organize and maintain permanent cooperation.

The joint operations are planned and executed on three levels: strategic, operational, and tactical. A joint operation is a set of military actions taken simultaneously on land, in the air, and sometimes also on the sea (river), on the high seas and the broad front, by groups of operational level forces. At this level, operations are prepared and conducted based on a unitary concept and a singular plan in one or more operational areas including objectives of political, economic and military importance, the maintenance or release of which allows for the partial achievement of the war.

In the perception of some advanced western armies, the purpose of the successful joint operation is consistently pursuing *"... the simultaneous engagement and hitting of the enemy on the entire depth of the battlespace. As a consequence, the opponents' fighting formation will be blocked and consequently its reactions are slowed down, desynchronized, and ultimately paralyzed"; in that way; it will "create the necessary conditions for the continued successful offensive actions". The Romanian doctrines subsequently implemented this valuable idea.* [12]

The current joint actions require an appropriate doctrine and capable forces to act together, in a joint and integrated manner. They need to complement and rely on each other in all phases of engaging. In order to lead a joint force capable of acting in a short time, the commander of the Force Command must have at his disposal appropriate technical support, adapted to the type of operation and the requirements of the modern combat space. Without an integrated command, control, communication and information system capable of integrating the information flow and assisting the staff in the decision process, it will not be possible to create the optimum conditions for a joint force command.

The intervention of the international community can provide a satisfactory response to solving crises through specific means of the strategic level. These means are replicated by political, diplomatic, information, and economic tools. The use of power tools in joint multinational operations is the last resort. The integrated action of forces in multinational combined operations is the result of the establishment of alliances or coalitions among nations. This alignment provides the necessary framework for the achievement of common goals and objectives, taking into account the diplomatic realities, constraints, limitations, and objectives of the member countries, of the participating or contributing countries.

The Alliance is an agreement concluded based on formal agreements between two or more states, with medium and long-term political and military objectives, aiming at achieving common interests and goals, as well as promoting the national values of its members.

The coalition is an ad hoc political and military arrangement between two or more states, designed to carry out joint actions. In the context of a coalition, multinational action takes place outside the links established within the Alliance and refers to unique situations or long-lasting cooperation in a specific area, that is, where a common interest is identified.

The coalition warfare involves addressing and solving the following vital issues: creating a multinational military force under the aegis of the ruling nation; the establishment of multinational governing bodies; coordination of political, economic, military, technical-scientific efforts; as well as achieving logistic compatibility and infrastructure development.

Multinational joint operations are those military actions involving two or more states with military forces of different sizes belonging to several services, under political control and single command and for which a single objective has

been established. Multinational quality reflects the political need to seek international consensus and legitimacy of military action.[13] NATO must always be ready to work with traditional members and partners, but also with other, less familiar forces, in a coalition. Mutual trust is essential when working in a multinational environment.

The primary purpose of a multinational operation is to direct the military effort to achieve the common goal. Multinational operations are unique. Each national commander is responsible in front of the commander of the multinational force, in front of his national chain of command and, last but not least, is responsible for carrying out the entrusted mission.[14]

Within NATO, Multinational Combined Joint Operations are those operations involving armed forces from two or more countries and involve at least two categories of armed forces. The Allied Joint Operation concept refers to operations involving forces belonging only to NATO member countries.[15]

The following types of armed forces can participate in such operations:

a) Command Forces – those forces that are still in peacetime under Operational Command or NATO Operational Control;

b) Allocated Forces – provided for actions under NATO control;

c) The forces that are foreseen for future NATO-led actions (Assigned Forces) – will strengthen the forces initially committed. To carry out these operations, NATO uses different models for organizing multinational units.

The joint action of the forces in the multinational joint operations is the result of the establishment of alliances or coalitions between nations which provide the necessary framework for the fulfillment of common goals and objectives. These coagulations generally take account of the diplomatic realities, constraints, limitations, and objectives of the member countries, or contributions.[16]

In case military operations are to be carried out along with Allied forces, in the framework of joint multinational operations, the efficiency of the Romanian Armed Forces is dependent on a number of factors, of which the most important we consider to be: the goals pursued by each member of the Alliance (the coalition); the battle doctrine; the level of training; the interoperability of the equipment, the means of striking and other equipment; cultural differences; language; mutual trust; the teamwork.

In cooperation with allied forces, national goals can be harmonized based on a common strategy. If they are expressed callously by each member without concessions, then, instead of uniting them and contributing to the cohesion of the coalition, they will highlight the differences of interest. The commonality of the goals pursued ensures the functionality of the coalition, as the emphasis on common elements can reduce dysfunctions while maintaining its operational character.

Besides the common goals pursued in the multinational joint operations, one of the fundamental problems that give the contents of the cooperation with the allied forces is the compatibility of the Romanian doctrines with those of the partners. The compatibility that we must remember must be achieved within all functional operating systems/ battlefield operating system of military action (combat functions), namely: intelligence, maneuver, fire support, force protection, logistics, and command and control.

Achieving compatibility between the doctrines of the Romanian and Allied forces is of vital importance for the physiognomy and the outcome of the operations, influencing the choice of forms and procedures of struggle adopted by the partners, the goals proposed in the joint actions and the dynamic equilibrium of the forces. If these aspects were not taken into account, the actions of the whole force could be damaged by the occurrence of inequalities and fractures, operations suffering from conceptual and action incompatibility. At the same time, it should be borne in mind that not all differences between doctrines have a subjective determination due to the differences existing in the supply of weapons systems and combat techniques.

Eliminating the adverse consequences due to the existing differences between the battle doctrines could be achieved by: the support for the weaker partner, so that its units are brought in terms of fighting capacity to the level closest to that of the most potent partner; differentiated assignment of responsibilities and missions among Allies, depending on the real operational capabilities of each of them.

Along with the compatibility of battle doctrines, we consider that one of the factors contributing to the success of joint operations is the relatively close level of training of the committed and allied forces.

It will be influenced by: the degree of professionalization of partner forces; the compatibility of the doctrine; the degree of integration of training systems; and the technical level of the specific endowment.

Achieving the goals pursued in the military actions carried out in cooperation with allied forces and the achievement of the compatibility of battle doctrines are to a great extent dependent on the interoperability of the technique, the striking means and the various equipment used. The commander of the joint multinational forces will have to solve the problems due to the inevitable differences between the weapon systems, equipment, and devices used by the forces participating in the joint actions against a potential aggressor. These are much greater in cooperation with other forces than those traditional ones, formed in the ad-hoc coalition.

Moreover, even within the recognized, permanent, alliances, there still remain a large number of incompatibilities that will have to be overcome.

Conclusions

In the actual context of hybrid conflicts, the typology of actions in terms of the dangers, risks, and threats, presents a shift from the traditional to the unconventional ones, and especially the asymmetric ones. They tend to generalize and to manifest itself throughout the conflict and throughout its spectrum.

They will also express themselves in the future by coordinated action, especially in real and figurative conditions of night and visibility, with no precise, distinct fingerprint, which will lead to an intense and constant fighting rhythm on the part of the opposing force.

In order to achieve this imperative, it will constitute a conglomerate that is carefully proportional to the types of structures and forces that are capable of engaging the hybrid opponent on each component distinctly but at the same time coordinated to maintain the continuity and rhythm of operations.

From this point of view, the armed forces must be prepared to execute a wide range of missions in a joint and multinational context, in different regions and in a complex operational and consequently uncertain environment. They will face a variety of hybrid threats and simultaneous combinations of types of activities that will change and adapt at all times.

This requires anticipating, identifying, and understanding the goals of a wide variety of involved actors, even from the planning stage of the joint operation, to integrate, coordinate, and synchronize their efforts.

Understanding the complexity of the hybrid operating environment is a significant challenge for the commander and the staff of the joint multinational force.

In the context of the hybrid conflict, operations are conducted through the joint, integrated action of branches of the army, specialties, and services. Their engagement takes place in a complex operational environment in which a multitude of entities – institutions, authorities, international organizations, non-governmental organizations, nations – can influence positively or negatively the conduct of military operations.

NOTES:

1 *** *Doctrina Armatei României*, Bucureşti, 2012, *Anexa nr. 1*, p. 136.

2 *** *Lexicon militar*, Editura Militară, Bucureşti, 1980, p. 474.

3 *** *Doctrina Armatei României*, Bucureşti, 2012, *Anexa nr. 1*, p. 136.

4 *AJP-3(B), Allied Joint Doctrine for the Conduct of Operations*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), March 2011, p.ix.

5 *AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012, p. 2-J-1.

6 *AJP-3(B), Allied Joint Doctrine for the Conduct of Operations*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), March 2011, pp. 1-10.

7 *AJP-3(B), Allied Joint Doctrine for the Conduct of Operations*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), March 2011, pp. 1-10.

8 *AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012, p.2-C-9, 2-M-10.

9 Gl. dr. Mureşan Mircea, Gl. bg. (r) dr. Ţenu Costică, Col. (r) dr. Stăncilă Lucian, *Operaţiile întrunite în războiul viitorului*, Editura UNAp, Bucureşti, 2005, p. 11.

10 Information vailable on www.Joint_Services_Command_and_Staff_College accesed on 27 July, 2019.

11 *Dicţionarul explicativ al limbii române*, Editura Academiei, Bucureşti, 1984, p. 119.

12 AJP-3.2, *Allied Joint Doctrine for Land Operatios*, Edition A, Version 1, 2016, pp. 1-12, art. 0134.

13 AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, Edition C, Version 1, 2019, pp. 2-6.

14 JP 3-16, *Multinational Operations*, 2013, p. II-3.

15 AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, Edition C, Version 1, 2019, pp. 1-7.

16 *Ibidem*, p. 12.

BIBLIOGRAPHY

*** *The explanatory dictionary of the Romanian language*, Academia Publishing House, Bucureşti, 1984.

*** *The Doctrine of the Romanian Army,* Bucharest, 2012.

*** *Military Lexicon*, Military Publishing House, Bucharest, 1980.

*** AAP-6, *NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012.

*** AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, Edition C, Version 1, 2019.

*** AJP-3 (B), *Allied Joint Doctrine for the Conduct of Operations,* North Atlantic Treaty Organization, NATO Standardization Agency (NSA), March, 2011.

*** AJP-3.2, *Allied Joint Doctrine for Land Operatios,* Edition A, Version 1, 2016.

JP 3-16, *Multinational Operations*, 2013.

Gl.dr. Mureşan Mircea, Gl.bg. (r) dr. Tenu Costică, Col. (r) dr. Stăncilă Lucian, *The Operations in the Future War*, UNAp Publishing House, Bucharest, 2005.

www.Joint_Services_Command_and_Staff_College

SOCIETAL SECURITY IN THE CURRENT CONTEXT

Octavian Victor Mihail DIMA, PhD Student*

Starting from the idea that modern security is no longer strictly a matter of state and military threats, the Copenhagen School has developed an extended security concept based on security sectors and securitization theory. In this context, it has developed a special security sector, called societal security, to address the conservation capacity of a society by preserving its identity, spiritual values and perennial character. From this perspective, contemporary societal security is the subject of a variety of risks and threats, among which those due to the process of regionalization and European integration occupy a central place. This article is focused on introducing the societal security concept and analyzing its mining in the current european geopolitical context.

Keywords: societal security; identity; security sectors.

Introduction

Societal security is a concept developed by the Copenhagen School of Security Studies which focuses on the ability of a society to preserve itself by preserving its essential character. The concept emerged in the 1990s with the end of the Cold War and was developed in the context of the integration of states into the European Union. This paradigm minimizes the role of state power in guaranteeing security by confronting threats, in order to bring to the fore issues regarding the identity of communities and societal dynamics. Taking into account these aspects, this article presents the concept of societal security and analyzes its significance in the current geopolitical context.

What is societal security?

The end of the Cold War, which culminated in the collapse of the Soviet Union and the emergence of new states, followed by sustained efforts for continued integration into the European Union, has prompted specialists and policy makers to rethink the paradigm of independent state and military security.[1] The new world order required a re-conceptualization of Europe and European security, which could no longer be based on the old understanding of security, as an arrangement between states. For this reason, security concerns were closely marked by questions about social identity, national values, free movement of persons or cross-border crime. The concept of societal security, developed by the specialists of the Copenhagen School, is in the context of these concerns.[2] The security of the company refers to: "the ability of a company to persist in its essential character under changing conditions and possible or real threats"[3].

In Ole Waever's view, the concept of social security represents, "the ability of a society to survive in its essential characteristics under fluctuating circumstances and in the face of possible or present threats"[4]. If until now the state was the object of the military, political, economic and environmental dimensions of security, in the case of societal security, the object of study is the society whose essential characteristic is that of national identity.

Characteristics of societal security

In his book *Security: a new framework for analysis*, Barry Buzan et al. formalizes the broader understanding of security by introducing five sectors, each governed by distinctive characteristics and dynamics and conceptualized around reference objects and actors (ie, military, environmental, economic, societal and political). The security of the society represents the survival of a community as a cohesive unit; its reference object is the large-scale collective identity that can function

* *"Carol I" National Defence University*
e-mail: *dimavictor2000@yahoo.com*

independently of the state[5].

Societal insecurity arises when a society fears that it will not be able to live on its own and comes from: migration (influx of people will overcome or dilute the identity of a group, for example the need to define Britishness), vertical competition (integration of a group into within the framework of a larger organization, for example Euroscepticism regarding the future of the EU), nationalist-separatist claims and horizontal competition (the community is obliged to integrate more influential identities in their own groups, for example the French cultural exceptionalism that is defended by American influences).

The security of the society is not related to a territory, as is the security of the state, for example in the territory inhabited by Kurds, the security problems of the state and the society are largely divergent and conflict.[6]

From a sociological perspective, the concept of societal security embodies a certain vision of security that considers security as an independent phenomenon. Thus, the security of the society is not a threat, nor an opportunity but is both a center and a base, on the basis of which the reliability and certainty of the collective life could be built. This means that security is considered to be based on collective life – the lives of ordinary people – instead of looking at differences and insisting on disagreement between groups and states, which is a key factor in determining threats and identifying friends or foes. Security as a social phenomenon does not need military solutions or even soft solutions. In other words, the security of society cannot be assimilated with power, on the contrary, it must be seen as a mechanism for transforming social ties. Finally, societal threats and opportunities can only be considered as deterrence or impetus. In other words, the ultimate goal of societal security is the comfort and understanding of the beauty of collective life - not an interest for the government, not the elimination of enemies, not facing the perceived threats to the nation.[7]

The current context of societal security

The security of a society is endangered when a threat is perceived to it regarding its identity and its survival as a community. The overlap between the state and society has led analysts to consider societal identity as a value to be defended and thus to promote the concept of identity security, as a basis for societal security. In the acceptance of the Copenhagen school there are two types of societies that participate in shaping the specific identity of the human being, respectively the ethno-national communities and the religious communities. In this context, the problem arises of identifying the actors who should have the competence to provide security. If, traditionally, the security provider is the state, through its political-institutional bodies, in the case of societal security, the state faces certain difficulties. Sometimes, the actions of the state can generate insecurity in the societal sector, and attempts to influence the identity are not always effective, they can have negative consequences, provoking strong manifestations against the oppressive tendencies of the state. In order to identify threats to the identity of a state, we must establish the values around which the community coagulates, in this case the nation, including objective factors such as the national language, territory and other identifying elements specific to the state concerned.

Barry Buzan identifies three major types of threats to societal security:

a) Migration – when a people receives a percentage of foreigners too high their identity can be affected by the modification of their social composition;

b) Horizontal competition – the cultural and linguistic characteristics of a society can be affected by the influence of neighboring cultures with clear effects on the identity of the respective people;

c) Vertical competition – sometimes integrationist or secessionist projects cause people to stop identifying as Z people (eg Catalonia, Kosovo etc.).

In addition to the three types of threats at present, three more threats to societal security are identified, namely:

a) Depopulation has an ambivalent character and is therefore mentioned separately. Depopulation has an ambivalent character because it does not represent a real threat to the identity of a society, but, first of all, to the individuals, who are the bearers of the identity of a nation. It becomes a threat to societal security when it threatens to destroy society;

b) Discrimination;

c) Terrorism.

In the context of integration in the European Union, the identity of the states is becoming more and more important as the borders are almost disappearing. "In a united Europe, those national societies that succeed in preserving their moral and identity bases will enjoy security."[8] According to the analysis provided by the Copenhagen school, it can be said that the integration into superstate structures of the European Union type can be interpreted as a renunciation of national identity and sovereignty, causing phenomena circumscribed to the vertical competition. Not only does the renunciation of the identity held in favor of a supranational identity correspond to such dynamics, but also the exacerbation of subnational identities of minorities. In this regard we refer to the multitude of speeches that have as their subject the autonomy or even secession of some regions of some European Union countries after the Brexit in the United Kingdom of 2016.

Conclusions

Starting from the new paradigm of contemporary security, this article is nothing more than a justification for the need to place great attention on its societal dimension. According to the opinions of many specialized analysts in this sector, the biggest changes occur and, therefore, it is necessary to understand much better what are the response mechanisms of the society to security threats which are varied and especially difficult to anticipate. We consider that it is possible to speak of a dilemma of the societal security, in the sense that the effects of the threats to society's security are really difficult to stop and the effects are in the long term.

In an identity conflict the parties tend to treat the threats as aiming at their very existence and survival, and such wounds close very hard. The knowledge of this sector is not an easy one, especially given the inherent multidisciplinarity, but also the need to develop the most suitable analysis tools. Although the concept of social security should have a unitary academic approach, it is nevertheless difficult to imagine a unique theory that corresponds in the same approach to all societies in the European Union.

The effort to have a unitary construction of the social security, which encompasses these specificities, is of the utmost importance to imagine a stable European Union adapted to the current needs of its citizens. However, the dynamics specific to the societal dimension, including the risks and threats of insecurity, are constant concerns of the politico-social factors even if their approaches are not identical or related to the same societal level.

Migration, population aging, horizontal competition, vertical competition, depopulation, discrimination and terrorism have a long-term societal impact that must be integrated into the socio-economic policies of the European Union, and these, in turn, must be implemented by all Member States. It is clear that all these problems can be solved only through cooperation between the Member States and calls for serious discussions to establish clearly what is the national-European border in the fight for the defense of the traditional values specific to each state and implicitly the national identity.

NOTES:

1 P. Bilgin, *Individual and Societal Dimensions of Security*, International Studies Review, 2003, available on Internet at: https://www.academia.edu/393273/_2003_Individual_ and_Societal_ Dimensions_of_Security, retrieved 15.08.2019.

2 *Ibidem,* p. 211.

3 Ole Wæver, *Identity, Migration and the New Security Agenda in Europe*, 1993, p. 23.

4 Barry Buzan, *Societal Security, State Security and Internationalization*, în Weaver, Ole, Buzan, Barry, Kelstrup, Morten, Lemaitre, Pierre, *Identity, Migration and the New Security Agenda in Europe*, Pinter, London, 1993, p. 213.

5 Wæver Buzan & de Wilde, *Security a new Framework for Analysis*, Lynne Rienner Publishers, 1998, p. 22.

6 *Ibidem,* p 119.

7 Manijeh Navidnia, *Societal Security*, Iran, Tehran: Research Institute of Strategic Studies (Rahbordi), 2009, pp. 69-83.

8 Ionel Nicu Sava, *Studii de securitate*, Centrul român de studii regionale, Bucureşti, 2005, p. 252.

BIBLIOGRAPHY

Buzan Barry, Hansen Lene, *The Evolution of International Security Studies*, Cambridge University Press, Cambridge, 2009.

Buzan Barry, *Popoarele, statele şi frica*, Editura Cartier, Chişinău, 2005.

Buzan Barry, Waever Ole, De Wilde Jaap, *Security: a new framework for analisys*, Lynne Rienner Publishers Inc, London, 1998.

Buzan Barry, *Societal Security, State Security and Internationalization*, în Weaver, Ole, Buzan, Barry, Kelstrup, Morten, Lemaitre, Pierre. *Identity, Migration and the New Security Agenda in Europe*, Pinter, London, 1993.

Chifu Iulian, Nantoi Oazu, Sushko Oleksandr, *Securitate societală în regiunea trilateralei România-Ucraina-Republica Moldova*, Editura Curtea Veche, Bucureşti, 2008.

Sava Ionel Nicu, *Studii de securitate*, Centrul român de studii regionale, Bucureşti, 2005.

Stoica Ionel, *Tentaţia migraţiei: necesitate şi oportunitate într-o lume globalizată*, Editura Militară, Bucureşti, 2011.

Ştefănescu Simona, Velicu Anca, *Naţional şi/sau european? Reprezentări sociale ale identităţii în societatea românească actuală*, Editura Expert, Bucureşti, 2006.

Strategia Naţională de Apărare a Ţării pentru perioada 2015-2019, disponibil http://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf

SOME DYSFUNCTIONAL ELEMENTS IN THE MANAGEMENT OF HEALTH FACILITIES WITH BEDS WITHIN THE OWN SANITARY NETWORK OF THE MINISTRY OF NATIONAL DEFENCE

LtCol. MD Ionuț RĂDULESCU, PhD Student*

Public health facilities with beds are, in our opinion, the most complex medical organizational entities within the Romanian social health insurance system. Their management often raises particular issues and significant challenges, considering that in these veritable "temples" of medicine basically all existing types of medical assistance are provided: preventive/ prophylactic, emergency, primary/ family, outpatient clinic, hospital and even recovery and rehabilitation.

Keywords: military health facilities; criteria; performance; value; indicators; assessment; board of directors; interim commander.

Schematically approaching the management and/or coordination system of health facilities with beds within the own sanitary network of the Ministry of National Defence, we can state that, according to the incident national/republican[1] regulatory and specific[2] frameworks, it consists of the following five distinct structural and organizational entities: board of directors, a commander named through interview/examination, organized by the board of directors, directing committee, medical council and ethical council.

Basically, according to art. 176 paragraph (4) from *Law no. 95/2006 regarding Health Reform, republished*, the commander chosen by passing the interview/examination for the position of General Manager concludes a management contract with the Ministry of National Defence, represented by the National Defence Minister, for a period of maximum 3 years. However, the management contract can be ended before the deadline after the annual or whenever needed assessment. The aforementioned assessment is performed based on the general performance criteria, determined by the order of the Health Minister, as well as on the specific performance criteria and the shares established and approved through executory act of the heads of ministries or institutions with their own sanitary network.

Simultaneously, paragraph (7) of the law article mentioned above states that the optimal values of the performance indicators of the hospital activity are established and approved by the order of the Health Minister. This aspect can constitute, in our opinion, an important malfunction considering that in the case of specific performance criteria, these and the optimal values of the performance indicators, respectively, are established non-uniformly and in an uncorrelated manner by different institutions, situated in separate fields.

For the implementation and application of the provisions of art.176 paragraph(4) from the aforementioned law, the Health Minister issued an order[3] which states that the evaluation activity discussed above is done annually, until the 30th of April of every year for the previous year, taking into account a number of 17 performance criteria. We also consider that this is of a dysfunctional nature, as the 17 performance criteria do not have afferent predicted levels/values. Thus the assessment is done, in our opinion, in an arbitrary, unwise and subjective manner as well as in an inaccurate and flawed one, solely by reference to self-assumed values and established by the person assessed for the indicators in question, in the content of the concluded management contract.

In order to justify what was previously stated, we formulate the hypothetical case of a commander of a military hospital who, owning a

** Joint Logistics Command*
e-mail: *drionut2002@yahoo.com*

high level of "institutional ambition", has self-set in the management contract high values/levels of performance criteria, with increased percentages of achievement, of 70%, 80% or even more. Paradoxically, but as true and plausible as possible, in the case of failing to achieve these high "targets", the Annual Assessment of Activity Commission of this commander, named by the Minister of National Defense, may, and is actually required by the "letter of law" to propose the termination of his management contract and his release from office.

Likewise, in this sense, there was also issued an order by the Minister of Health[4] that states the framework-model for the management contract of health facilities with beds within the public healthcare network, also applicable in the case of military hospitals. This contains, distinctively, a list of 28 indicators of performance, grouped into 4 different categories, as follows: performance indicators of the activity of the public hospital manager, service usage indicators, financial and economic indicators and quality indicators, respectively. As a malfunction of this normative act, we underline the fact that this norm does not unequivocally establish clear levels/values for these performance indicators, making it even harder to correctly and fairly evaluate them.

Therefore, on the basis of what was discussed above, including the military hospitals, yearly, an assessment committee named by the Minister of National Defence evaluates the activity of their commanders, based on two types of performance criteria. Some of them are general, applicable to any public hospital and others are specific to the military institution. The two categories of criteria mentioned and their share are established by order of the Minister of National Defence[5].

Analyzing carefully the norms that are opposed to the activity in question, we can state that, even if there are established a series of criteria/indicators of performance used in the assessment of the heads of public hospitals within the Romanian social health insurance network, the Ministry of Health has not issued, until the present day, a rule to establish clearly, concisely, coherently and in an unitary manner optimal levels and/or values, in digital, percentage, interval etc. form, which is a serious and concerning problem, in our opinion.

However, it needs to be mentioned that, in 2007, the Ministry of Health had tried to normalize this situation, by issuing a Minister Order which solved the issue strictly temporarily, only for that year[6]. The order in question contained the national average values of the performance indicators of hospital management, accomplished in 2006 and it specifically mentioned the fact that those digital values are the basis of establishing the levels of performance indicators for every public hospital in 2007, not at all for a multiannual period of time.

All the dysfunctional aspects previously stated can generate cases in which, on their deadline of termination, the management contracts of the commanders of military hospitals may not contain specifically fixed values/levels of some general performance criteria/indicators, common with those used by other public hospitals in Romania.

With regard to the assessment of the activity performed by the commanders of the health facilities with beds within the own sanitary network of the Ministry of National Defence, there were introduced some particular elements, of specificity, in line with the specific tasks, activities, responsibilities and obligations, respectively *The specific performance criteria for the annual or whenever needed evaluation of the activity of commanders of health facilities with beds within the sanitary network of the Ministry of National Defence, on the basis which the management contract can pe prolonged or terminated before the deadline* approved by *The order of the Minister of National Defence no. M.68/2013.*

Analyzing this last norm, we estimate, as the first dysfunctional aspect, the fact that it has not undergone any change and/or additions since its issue in 2012, until now, while the regulated field has experienced an increasing dynamism during this period. At the same time, the rule states that the assessment of these criteria is done by "analyzing the size of each criterion" and consequently being given, by the evaluator, a score of 0 to 5 points, without having set up, as it should have been normally and naturally, reference levels or values for the evaluation. For example, the "performing functional tasks" indicator is provided in the order with three dimensions to be evaluated , namely "prioritizing actions and correlating them with available resources", "how to address identified issues and performing specific tasks" and "the impact of decisions on how to perform specific functional duties", but no standard reference is

indicated. As active military officers, the military commanders of military units with beds are subject, each year, to a professional evaluation process specific to the military body for the purpose of drawing up an annual service assessment, an activity established by order of the minister[7]. The purpose of service assessment is precisely the evaluation of professional competence, moral quality and prospects for military personnel development. It should be mentioned that among the objectives of this annual service assessment activity we may include the improvement of the efficiency of the military structures by evaluating the individual professional performances, the efficient use of military cadres and their classification according to the requirements of the positions, the professional training and the performances obtained, and, last but not least, the awareness of the evaluated military personnel regarding the importance of the way of fulfilling the functional attributions and the ways to improve the professional performance and skills.

Logically and systematically following the above, we can state that in the case of the commanders of the military sanitary units with beds in the sanitary network of the Ministry of National Defence, they are unnaturally subject to two independent annual evaluation processes, which nevertheless have a number of counterproductive overlapping elements that are also time consuming. Thus, the first annual evaluation process ends in January for the previous year, with the annual service appreciation, and the second one is held later, until April for the previous year, finalizing with the awarding of a general mark represented by the mark obtained in the assessment of the general performance criteria in the management contract, in conjunction with the rating obtained in assessing the fulfillment of the specific performance criteria.

A hard, if not impossible to comply with and apply provision is the one stipulated in art.4 paragraph (4) of the *Order of the Minister of National Defence no. M.68 / 2013*, namely taking into account, when drawing up the annual service assessment of the nominated commanders, as military cadres in service, the overall rating established as a result of the assessment for the commanders of sanitary units. The "chronological fracture" is, in our view, extremely obvious, scheduling in January an activity that was supposed to be carried out in April in the same calendar year.

Another dysfunctional element, for health facilities with beds within the network of the Ministry of National Defence, is the application of the provisions of *Law no. 95/2006 on Health Reform*, republished, with the subsequent amendments and additions, regarding the suspension of the labor contract of the manager of the sanitary unit with beds and the members of the steering committee, incompletely harmonized, in our opinion, with the provisions of the military cadre status regulated by *Law no. 80/1995 on the status of military cadres*, with subsequent amendments and additions. Thus, in the case of termination before the deadline of the mandate of the commander of the military sanitary unit with beds, the Minister of National Defense "empowers" by order, according to art.4 paragraph (4) from *The order of the Minister of National Defense no.M129/2009 on the management of health facilities with beds within the sanitary network of the Ministry of National Defence,* with the subsequent amendments and additions, at the proposal of the head of the Medical Directorate or, as the case may be, of the chief / commander of the structure coordinating the sanitary unit with beds, an interim commander for a period of up to 6 months, during which the interview for the job is held. In this case, the interim commander does not conclude a management contract for the period in which he temporarily runs the sanitary unit with beds. A similar process applies to the other members of the Board of Directors.

We assume that in these situations, the purpose for which the management contract has been established is not achieved, since, in the case of the provision of the interim, by the empowered persons, there is no obligation to conclude these contracts and, implicitly, the obligation to meet the general and specific performance indicators. Furthermore, during these interim periods, the evaluation of the manager's activity cannot be carried out, as according to art. 1 paragraph (2) of *The Order of the Minister of Public Health no.112/2007 regarding the performance criteria on the basis of which the management contract can be extended or may terminate before the deadline*, with the subsequent amendments and additions, the evaluation of the activity of the public hospital manager for the previous calendar year shall be

made by 30th of April of the following year. Only the managers who have the management contract during the validity period and who have run the public hospital for a period of at least 6 months in the assessed year can be assessed.

Conclusions

The optimization of the management of health facilities with beds in the own sanitary network of the Ministry of National Defence requires intensive, focused and concerted effort carried out rhythmically, constantly and rigorously, especially for the conceptual /doctrinal harmonization with the republican/ national incident normative framework. At the same time, the systematization, unification and coordination of specific/departmental norms in the field should not be overlooked either.

NOTES:

1 *** *Law no. 95/2006 regarding Health Reform, republished,* with subsequent amendments and additions, cap. 3.

2 *** *Order of the Minister of National Defence no. M.129/2009 regarding the management of medical facilities with beds within the sanitary network of the Ministry of National Defence,* with subsequent amendments and additions, art. 1 line (2), art. 7 line (1), art. 18 line (1), art. 21 and art. 25 line (1).

3 *** *Order of the Minister of Public Health no. 112/2007 regarding performance criteria on the basis which the management contract can be prolonged or terminated before deadline,* with subsequent amendments and additions, art. 1 line (2).

4 *** *The order of the Minister of Health no. 1384/2010 regarding the approval of the model-framework of the management contract and the list of performance indicators of the activity of the manager of the public hospital*, with subsequent amendments and additions, art. 1 line (1).

5 *** *Specific performance criteria for the annual or whenever needed evaluation of the activity of commanders of health facilities with beds within the sanitary network of the Minister of National Defence, on the basis which the management contract can be prolonged or terminated before the deadline,* approved by *The order of the Minister of National Defence no. M.68/2013*, Annex no. 4.

6 *** *The order of the Minister of Public Health no. 1567/2007 regarding the approval of national average values for performance indicators of the hospital management,* Annex no. 1.

7 *** *Methodology of making service assessments for military cadres in the structures of the Ministry of National Defence, in peacetime approved by the Order of the Minister of National Defence no. M.122 /2014,* with the subsequent amendments and additions, art. 3 line (1).

BIBLIOGRAPHY

*** *Law No. 95/2006 on Health Reform, republished,* with the subsequent amendments and additions.

*** *Law no. 80/1995 on the status of military cadres,* with the subsequent amendments and additions.

*** *Order of the Minister of National Defence no. M.129 / 2009 on the management of sanitary units with beds from the sanitary network of the Ministry of National Defence,* with the subsequent amendments and additions.

*** *Order of the Minister of Public Health no. 112 /2007 regarding the performance criteria on the basis of which the management contract can be extended or terminated before the deadline,* with the subsequent amendments and additions.

*** *Order of the Minister of Health no. 1384 /2010 regarding the approval of the framework model of the management contract and the list of performance indicators of the public hospital manager activity,* with the subsequent amendments and additions.

*** *The specific performance criteria for the annual or whenever necessary assessment of the activity of the commanders of sanitary units with beds in the sanitary network of the Ministry of National Defence under which management contracts may be extended or terminated before the deadline* approved by *the Order of the Minister of National Defence nr. M.68 /2013.*

*** *Order of the Minister of Public Health no. 1567 /2007 regarding the approval of the national average values of the hospital management performance indicators.*

*** *Methodology of making service assessments for military cadres in the structures of the Ministry of National Defense, in peacetime* approved by *the Order of the Minister of National Defense no. M.122/2014,* with the subsequent amendments and additions.

THE USE OF COMPLEXITY IN SOCIETAL SECURITY STUDIES

Professor Ioan CRĂCIUN, PhD*
Octavian Victor Mihail DIMA, PhD Student**

Societal security, as developed by the Copenhagen School of Security, is an extremely important area of the broader contemporary security concept which, in addition to military issues, also takes into account a number of other threats coming from the fields such as political, economic, societal or environmental ones. In the study of contemporary societal security, a number of concepts specific to the theory of complex systems, such as complexity, self-organization, the threshold of chaos, etc., have been borrowed, substantially enriching the hermeneutics of security discourse on the basis of non-mechanistic interpretations of social systems. This article aims to show that in the study of societal security the use of tools specific to the study of modern complex systems has produced quite interesting results, which could give a new meaning to the research in this field. At the same time, the paper presents some conclusions regarding the methodology of analysis specific to the science of complexity applicable to the field of societal security.

Keywords: societal security; complexity science; systemic thinking; security in a systemic context.

Introduction

Systemic thinking has had a significant impact in many fields of study and research, among which the field of international relations and, in particular, that of Security studies, has occupied an important place. Thus, the concepts of complexity have been used in the study of military conflict and war by a number of analysts such as Quincy Wright or Pitrim Sorokin, and other analysts such as Lewis F. Richardson or Frederick Lanchester have applied these concepts, especially game theory elements, in the study of national / military security. In the study of international relations, elements of complexity theory were used by Morton A. Kaplan and Karl W. Deutsch[1] and, later, Barry Buzan, together with other specialists of the Copenhagen School, applied such elements in contemporary Security studies. Thus, they developed the *extended security concept* proposed by this school, based on five distinct areas of analysis (political, economic, military, social and environmental) and introduced the *theory of securitization*[2] as the basis of a new post-Cold War security paradigm.

Over time, elements of complexity theory have become extremely important in the study and research of new military threats, and especially non-military threats to contemporary security. In this context, the main purpose of this article is to show that in the study of contemporary conflicts, terrorism, transnational crime, migration or uncontrolled degradation of the environment, the use of tools specific to the study of complex modern systems has produced quite interesting results, which could give new meaning to research in this field. However, there are also situations in which the use of methodologies derived from the research of complex systems for security studies has been questioned by the insufficient understanding of the concepts of the social sciences or of the theories specific to the complex systems. Given these difficulties, in this article, we aim to identify some of the possible answers regarding how we should understand and overcome the conceptual barriers in applying the concepts of complex systems theory in contemporary security studies.

** "Carol I" National Defence University*
e-mail: *craciun64@gmail.com*
*** "Carol I" National Defence University*
e-mail: *dimavictor2000@yahoo.com*

Using complexity in the social sciences

In sociology, social complexity is a conceptual framework used for the analysis of society and the current use of the term *complexity* refers specifically to social theories that treat society as a complex adaptive system. This aspect motivates the fact that both the social complexity and its emergent properties are central recurring themes

not only for the study of the historic evolution of social thinking, but also for the study of social changes[3]. In addition, social complexity theory offers a medium-level theoretical platform for setting working hypotheses[4] in the study of social phenomena at micro and macro level, the concept of social complexity being methodologically neutral.

The first uses of the concept of complexity in the social and behavioral sciences having as theoretical basis the theory of the complex systems was found in the studies regarding the modern organizations and in those regarding the management studies[5]. However, in management studies, especially, complexity has often been used in a metaphorical manner rather than in a qualitatively or quantitatively theoretical way[6]. However, by the mid-1990s, complexity was incorporated in the field of social sciences, concomitantly with the adoption of study and research tools similar to those generally used in complexity science. In 1998, the first specialized online publication called the *Journal of Artificial Societies and Social Simulation* was created, followed by numerous other high-profile publications that contributed to the promotion of complexity theory in the social field. On the other hand, these concerns have been connected with other theoretical traditions specific to the social domain such as constructivist epistemology and the philosophical positions of phenomenology, postmodernism and critical realism.

As we have already shown, social complexity is a neutral theoretical notion, which means that it can be used in both local and global approaches to sociological research. In this context, the research methodologies are determined according to the level of analysis established by each researcher or according to the level of description or explanation required by the research hypotheses[7].

At the micro level, methods as content analysis, ethnographic observations or other qualitative research methods may be appropriate. More recently, highly sophisticated quantitative research methodologies have been developed that can be used in sociological researches both at the micro and macro level. Such methods include, but are not limited to, bifurcation diagrams, network analysis, nonlinear and computational modeling, including cellular, socio-cyber-type programming and other social simulation methods.

Theoretically, social complexity can be applied to any research that deals with social interaction or the results of such interactions, especially when these interactions can be measured and expressed as continuous or discrete data. A common criticism often cited about the usefulness of complexity science in sociology is the difficulty of obtaining adequate data[8]. However, the application of the concept of social complexity and the analysis of such complexity has begun and continues to be a continuous field of research in sociology.

Can complexity be used in security studies?

The new realities since the end of the Cold War led to an extension of the unrealistic concept of security due to the wider range of potential threats that the world had to face. Deepening the agenda of security studies has required the use of different security references that the state, both at lower levels, up to the individual, transposed into the concept of *human security*, and at higher levels, up to the global level, transposed into the concept of *international* or *global security*, regional and societal security being intermediate references of this interpretation. This parallel extension and deepening of the concept of security was proposed by the constructivist approach associated with the researches of the Copenhagen School[9]. These features make up the core of the security concept and can be used as a starting point for identifying systemic attributes of contemporary security[10].

In order to preserve and develop the analytical properties of the concept of security in a systemic sense, we propose a compromise approach, which we call eclectic. It combines, at least at the declarative level, the objective value of the extended neorealist security concept with the in-depth constructive idea of security viewed as compelling discourse[11]. In this eclectic approach, following the interpretation of Buzan and his collaborators in Copenhagen School, security refers to the following sectors: military, economic, political, environmental and societal, and the basic concepts used are those of existential threat and securitization. Any public problem, presented as an existential threat, can be securitized, as it requires emergency measures and justifies actions outside the normal procedural limits. Security is a self-referential practice, because a certain problem becomes a *security matter*, not necessarily because there is a real existential threat, but because the

problem is described as a threat[12]. Opposite to the concept of securitization is *desecuritization* which can be defined as a process in which a factor, called a threat, is perceived/described as one that is out of date and, therefore, no longer requires extraordinary measures after a persuasive discourse which had previously been presented with the need to impose such measures[13].

The proposed approach helps to identify a stratagem of compromise between the unrealistic approach of predictability of objective threats and the constructivist approach of denying any possibilities for predicting security. Solving this dilemma can be found by abandoning the mechanistic and linear visions of social processes and adopting visions based on complex systems theory. Instead of refining extrapolations, computer models, scenarios and forecasts, emphasis is placed on learning mechanisms that lead to prediction-making, as happens in management[14] or to refinement methods applied in forecasts as is the case with studies about the future[15].

These assessments allow us to conclude that this scientific corpus called complexity can be successfully applied in the security studies which we intend to further explore.

Applying complexity in security theory and practice

Security specialists along with policy makers in this area have high expectations for complexity research. Specialists and decision-makers in the military field are placed in the same margin of expectations. For this reason, it has often been attempted to adapt complexity-specific methods to all levels and situations of a military nature and not only, that is, in post-conflict situations or in so-called emergency situations.

Expanding and deepening the concept of security contributes to increasing the real or perceived complexity of the world we live in today. Therefore, traditional state-centric security studies, oriented on the cause-effect linear approach, even if they were based on scientific models (including those borrowed from early systemic thinking such as: stability, polarity or hegemonic stability), had to be replaced with new approaches based on systemic thinking in which security studies use complex systems concepts such as analogies, metaphors or mathematical models. Thus, nowadays, there are more and more analysts who think that only in a limited number of cases can the mechanistic concepts of the functioning of social systems be applied. Therefore, a number of concepts specific to the theory of complex systems, such as: complexity, self-organization, chaos threshold has been taken up in security analyzes. In most of these approaches it is not clearly specified, for example, what is really chaotic but, of course, such metaphors are valuable heuristic tools. Therefore, as we have already stated, the notions taken from the study of complex systems have substantially enriched the hermeneutics of security discourse on the basis of non-mechanistic interpretations of social systems.

Thus, the reality indicates that between the research of the complex systems and the contemporary security policy, there have been increasingly close links. On the other hand, the scientific community offers analyzes/works that fall within the same coordinates. We support this claim with a few examples: Holland, J. D., *Hidden Order. How Adaptation Builds Complexity*, Basic Books (New York), 1995, Kauffman, S. A., *The Origins of Order: Self-Organization and Selection in Evolution*, Oxford University Press (New York/ Oxford), 1993, Prigogine, I., *End of Certainty*, The Free Press (New York), 1997, and so on.

The need to understand these concepts has determined the evolution and development of research in the field. Thus, the specific debates have undergone a constant expansion and have concentrated on explaining the extent to which these new terms allow the correct / exact description of the specific social phenomena. In this context, many opinions have emerged, to which we also rally, which support the validity of these concepts, as well as many criticisms of them. On whose side the truth remains, it remains to be proven, but what is certain is that such terms significantly enrich the language of social discourse regarding contemporary security policies and strategies.

Therefore, research in the context of complex systems has offered a new approach to contemporary security analysis. Thus, new possibilities for explaining/predicting the security phenomena at the macro level have emerged, starting from the behavior of the elements at the micro-system level. A good example of this strategy is the *Sugarscape*[16] project, part of a larger project, the

2050 Project, developed by the Santa Fe Institute, in collaboration with the World Resources Institute, and the Brookings Institution. The project involves identifying the conditions for a sustainable global system in the next century and for developing policies to help achieve such a system[17].

Conclusions

All the aspects shown so far demonstrate that complexity studies have become an indispensable part of the epistemology of contemporary security theory and even a useful tool for security policy. The use in security studies of mathematical models, analogies and metaphors related to complexity has broadened the epistemological foundations of research in this field. This does not mean, however, that complexity studies have directly responded to all expectations of security studies in terms of prediction, explanation of causal effects, normative approach, resilience and (always limited) improvement in the ability to influence social phenomena.

The applications of complexity in security discourse demonstrate two essential shortcomings. First, there are too high expectations from security theory and policy and, on the other hand, we notice incorrect use of concepts and abuses. Security specialists, analysts and politicians often treat complexity-related approaches as a new, modern element and with some sense of the magic of contemporary security language. Similarly, researchers familiar with the methodology of complexity reduce social phenomena to very simple models, irrelevant to the reality we live in. In our opinion, references to non-linearity, self-organization and chaos allow for a deeper understanding of all social phenomena. However, in security oriented research they have a special significance because they offer an answer regarding the need for prediction and normative, action-oriented studies.

Therefore, we must pay greater attention to both the efficiency and the legitimacy of the applications of complexity in the theory and practice of contemporary security. Due to the ideas associated with the diversified complexity, the epistemology of security studies has been enriched with tools useful in analysis and research. The new social phenomena specific to the information society have received names that facilitate their understanding, as well as the processes of social communication that target them. The employment of terms such as stability, turbulence, non-linearity, self-organization, chaos, etc. used in security studies reinforce the argument of using complexity theories to explain and model contemporary security phenomena. Although the complexity studies offer the final argument of the impossibility of elaborating in-depth forecasts in security research, they nevertheless offer concrete methods for improving the predictive capabilities either by using mathematical models, or by using analog and metaphorical applications or heuristic stimulation.

NOTES:

1 C. Mesjasz, *Applications of Systems Modelling in Peace Research*, Journal of Peace Research, 25/1988, p. 3, available on Internet at: http://journals.sagepub.com/doi/10.1177/002234338802500319, accessed at 14.05.2018.

2 B. Buzan, O. Wver, J. de Wilde, *Security. A New Framework for Analysis*, Lynne Rienner Publishers (Boulder-London), 1998.

3 Eve Raymond, Sara Horsfall, Mary E. Lee (eds.), *Chaos, Complexity and Sociology: Myths, Models, and Theories.* Thousand Oaks, CA: Sage Publications, 1997.

4 Lee Freese, *Formal Theorizing*, în Annual Review of Sociology, 6/1980, pp. 187-212.

5 Douglas L. Kiel, *Managing Chaos and Complexity in Government: A New Paradigm for Managing Change, Innovation and Organizational Renewal.* Jossey-Bass: San Francisco, 1994, available on Internet at: http://infra-eu.cinecardz.com/l8u3t4q5dhyf/04-santina-waelchi-iv/read-9780787900236-managing-chaos-and-complexity-in-government-a-ne.pdf, accessed at 12.05.2018.

6 Eve Raymond & co., *op.cit*.

7 Niklas Luhmann, *The Differentiation of Society,* New York, NY: Columbia University Press, 1982.

8 Stewart, Peter, *Complexity Theories, Social Theory, and the Question of Social Complexity*, in Philosophy of the Social Sciences, 31(3), 2001, pp. 323-360, available on Internet at: http://journals.sagepub.com/doi/abs/10.1177/004839310103100303, accessed at 12.05.2018.

9 B. Buzzan, et comp., *op. cit.*

10 C. Mesjasz, *Complex Systems Studies and the Concepts of Security*, în Kybernetes, 35/2006, pp. 3-4, available on Internet at: https://www.emeraldinsight.com/doi/full/10.1108/03684920610653755, accessed at 15.05.2018.

11 B. Buzzan, et comp., *op. cit.*

12 *Ibidem.*

13 O. Wver, *Securitization and Desecuritization*, in Lipschutz, R. D., (ed.), On Security, Columbia University Press (New York), 1995, available on Internet at: https://www.scribd.com/doc/95165611/Securitization-and-Desecuritization, accessed at 14.05.2016.

14 K. van der Heijden, *Scenarios. The Art of Strategic Conversation*, John Wiley & Sons (New York), 1996.

15 J. C. Glenn, T. J. Gordon, *2006 State of the Future*,

The Millennium Project, American Council for the United Nations University: Washington, D.C., 2006.

16 This project attempts/intends to apply computer-based modeling techniques to study complex social phenomena (breeding, seasonal migration, interaction with the environment, trade, disease spread, population dynamics and more). The overall goal is to develop a computerized solution that allows the study of different types of human activities from an evolutionary perspective.

17 J. M. Epstein, R. L. Axtell, *Growing Artificial Societies. Social Science from the Bottom Up*, MIT Press (Cambridge, MA), 1996, p.177. available on Internet at: https://mitpress.mit.edu/books/growing-artificial-societies, accessed at 19.08.2019.

BIBLIOGRAPHY

Buzan B., Wver O., de Wilde, J., *Security. A New Framework for Analysis*, Lynne Rienner Publishers (Boulder-London), 1998.

Epstein J. M., Axtell R. L., *Growing Artificial Societies. Social Science from the Bottom Up*, MIT Press (Cambridge, MA), 1996, available on Internet at: https://mitpress.mit.edu/books/growing-artificial-societies.

Eve Raymond, Sara Horsfall, Mary E. Lee (eds.), *Chaos, Complexity and Sociology: Myths, Models, and Theories*. Thousand Oaks, CA: Sage Publications, 1997.

Freese Lee, *Formal Theorizing*, in Annual Review of Sociology, 6/1980.

Glenn J. C., Gordon T. J., *2006 State of the Future*, The Millennium Project, American Council for the United Nations University: Washington, D.C., 2006.

Heijden van der K., *Scenarios. The Art of Strategic Conversation*, John Wiley & Sons (New York), 1996.

Kiel L. Douglas, *Managing Chaos and Complexity in Government: A New Paradigm for Managing Change, Innovation and Organizational Renewal.* Jossey-Bass: San Francisco, 1994, available on Internet at: http://infra-eu.cinecardz.com/l8u3t4q5dhyf/04-santina-waelchi-iv/read-9780787900236-managing-chaos-and-complexity-in-government-a-ne.pdf.

Luhmann Niklas, *The Differentiation of Society.* New York, NY: Columbia University Press, 1982.

Mesjasz C., *Complex Systems Studies and the Concepts of Security*, în Kybernetes, 35/2006, pp. 3-4, available on Internet at: https://www.emeraldinsight.com/doi/full/10.1108/03684920610653755.

Mesjasz, C., *Applications of Systems Modelling in Peace Research*, Journal of Peace Research, 25/1988, p. 3, available on Internet at: http://journals.sagepub. com/doi/10.1177/002234338802500319.

Stewart Peter, *Complexity Theories, Social Theory, and the Question of Social Complexity*, in Philosophy of the Social Sciences, 31(3), 2001, available on Internet at: http://journals.sagepub.com/doi/abs/10.1177/004839310103100303.

Wver O., *Securitization and Desecuritization*, în Lipschutz, R. D., (ed.), On Security, Columbia University Press (New York), 1995, available on Internet at: https://www.scribd.com/doc/95165611/Securitization-and-Desecuritization.

INTEGRATED SOFTWARE PLATFORM FOR MALWARE ANALYSIS OF MOBILE TERMINALS

LtCol. Eng. Associate Professor Dragoș-Iulian BĂRBIERU, PhD*
Col. Ștefan-Antonio Dan ȘUTEU, PhD**
Associate Professor Elena ȘUȘNEA, PhD***

Beyond the marketing of IT companies, in the context of escalating cyber-attacks that affect organizations around the world, cyber security solutions have become the primary element in protecting IT infrastructures and devices. The proliferation of Intelligent Mobile Devices and Cloud Technologies, the Internet of Things requires new technological solutions, implemented both at hardware and software levels, to combat threats. This paper summarizes the Integrated Software Platform for Malware Analysis of Mobile Terminals which aims to integrate various software technologies to protect mobile devices.

Keywords: malware analysis; cyber security; mobile terminals.

Introduction

The malware applications analysis for mobile terminals is a difficult process due to the diversity of mobile platforms and existing security mechanisms, the frequency of occurrence of operating system versions and the use of malware code protection techniques. In the context of the national and international situation shaped by security trends, there has been a need to develop a software platform integrating, in a unitary manner, various open-source and commercial malware analysis solutions for mobile telephony. Most cyber actors are adapting to an existing environment, but information and technology supremacy is achieved through innovation, as Vice Admiral Arthur K. Cebrowski says: "I realized that military competition wasn't about how fast one could align with reality, but how fast one could leap over it and create a new reality"[1].

Cyber security and security in general are closely linked, as security comes from most cyber-attack and defense methods and techniques. The 7 stages of the Cyber Kill Chain[2] presented by the Lockheed-Martin Corporation are identical to the stages of an attack against a person or group of people. The static analysis of malware can be seen as an investigation to establish a person's psychological profile. Although it is more cost-effective than dynamic analysis, a program can hide a malicious code by encryption or different methods, just as a person can cheat at a personality questionnaire. Dynamic analysis involves executing a program and tracking all parameters to identify suspicious activities in a controlled environment.

The honeypot concept, the techniques to check if the environment where you are acting is secure are similar to real life when a person is under the magnifying glass of a detector in a safe environment or designed for sure by the one who wants to track down certain events. The attacks such as distributed denial of service can be related to the intoxication of an opponent with false information that consumes time and resources until they are exhausted. The rapid development of information and communications technology and "easy Internet access have not only yielded indisputable benefits but also it brings some vulnerabilities to security environment"[3]. Hybrid warfare through various third parties is mirrored today in the world of the Internet, using various proxy technologies and specialized hacking groups. Regardless of present or future technologies, patterns that are limited in number can be identified, but the manifestation is

*_Security and Defence Faculty_
e-mail: *oldboy@yahoo.com*
**_Command and Staff Faculty_
e-mail: *dan-suteu.antonio@unap.ro*
***_Security and Defence Faculty_
e-mail: *susnea.elena@unap.ro*

inexhaustible. These patterns are not characteristic of present days, but have their roots in our species' history and are forms of attack and defense, many of which are borrowed from biology. Camouflage and mimicry are weapons from the animals' arsenal and can secure victory against a possible opponent[4]. We believe that cyber space, much more diverse through intrusion and protection manifestations, operates a limited set of existing patterns in biology as well, resulting from the long evolutionary process.

Malware uses different camouflage techniques. It can be installed in the distribution chain, so a user cannot see any changes to the device activity that often occurs after a program has been installed. Compromising the signal processor inevitably leads to interception of telephone calls and messages, but using existing correlations between DSP and CPU, attackers can get extensive capabilities on applications running on the mobile terminal. By offering free apps or apps from unofficial stores, people can insert malicious codes. The control flow obfuscation procedure prevents the dynamic analysis of malware. Using encryption algorithms will lead to the inability to disassemble and decompile the code of an application.

Detecting the malicious behavior of mobile terminals involves 3 types of analysis: static analysis involves disassembling and decompiling an application to identify malicious code, dynamic analysis tracks different parameters and events in a sandbox-controlled environment to identify suspicious behaviors, the hybrid analysis combines the two types of analysis briefly presented above. Malicious code detection typically uses a signature list, and if this process fails, artificial intelligence algorithms or manual analysis can be used. The approach to malware behavior from a machine learning perspective involves a series of steps: "selecting the initial set of data (training set), as a rule, an equal number of safe and malicious applications from which some features are extracted"[5]. Based on some feature selection methods, it selects the most relevant to build a model using a classification algorithm. In the test phase, the model is checked to evaluate the accuracy using different metrics. Choosing features is not a random process. The range of classification algorithms is diverse, with approaches based on statistics, neural networks and kernel-based methods. The most common classification algorithms are Naive Bayes, K-Neares Neighbors and Vector Machine Support.

Vulnerabilities can be of two types, preinstalled or generated by the complexity of the internet. Preinstalled vulnerabilities can be installed by a producer or in the distribution chain. It is almost impossible to check and test each piece of code.

Software development platforms, such as GitHub, could provide tools to check for various errors in the code in the future, in order not to be exploited by attackers.

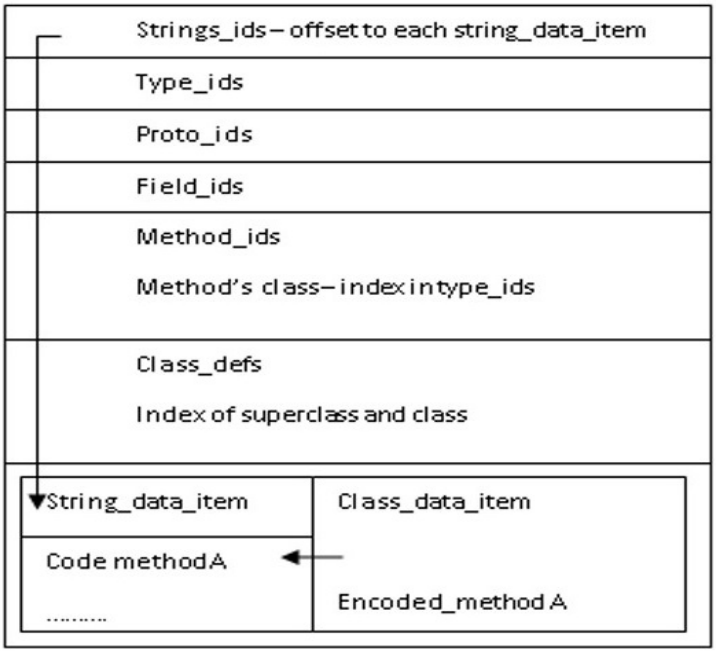


Figure 1. *Structure of a dex file*

The methods of hiding malware code are diverse and depend on the operating system features of the mobile terminal[6]. For example, the structure of a file (Figure 1) with the dex extension has areas assigned to Header, String_ids, Type_ids, Proto_ids, Fields, Methods, Classes and Data.

A class is found in the *class_defs matrix* in the form of an index that points to another index in the string *strings_ids*, the latter being connected to *string_data_item* that can return the class name. Each class defined in the code area is described by a class_data_item structure that contains its variables and methods. The methods are declared as a structure with the name encoded_method.

This structure consists of: *flag access* – such as method (public, private, protected, etc), *offset code* - the address where the method code is located from the beginning of the file *.dex* and *method_idx_diff* - an increment index for each method in the structure method_ids. To hide a method, the first step is to manipulate the *encoded_method* structure to reference another method, recalculate the SHA1 checksum, modify the .dex file header and package the application. Handling the *encode_method* structure involves a value for *method_idx_diff*, which can be 0 and the change of address that accesses the method code.

The camouflage technique used in cyberspace is identified by methods such as encryption, oligomorphism, polymorphism and metamorphism[7]. Semi-polymorphic or oligoorphic malware uses different encryption algorithms at each infection. The major difference between oligomorphism and polymorphism is that the latter can use an unlimited number of encryption algorithms. Metamorphism completely changes the malware code and does not use encryption algorithms. The mimicry type techniques can be identified in methods of obfuscation of the code. The most common methods of obfuscation are the use of junk code, variable permutation and replacement substitution, code transposition, and big code loop. When malware resides in hardware, the analysis process is much more difficult.

Integrated software platform for malware analysis of mobile terminals

In the first stage of development of malware software for mobile terminals, a series of necessary steps were identified. The first step involves identifying common and less common ways to infect mobile terminals with different security reports, and defining taxonomy by certain features such as attack vectors, source, targets, vulnerability exploited, threat type, etc.

In the second step, open-source or commercial applications were tested to choose solutions that meet security requirements. Various research projects and scientific papers were studied that relate to the detection of suspicious behavior and a customized firmware concept was proposed to improve the operating system. Among the tested solutions we could mention the Cellebrite UFED Pro Series, Cellebrite UFED Field, Cellebrite UFED Analytics, Oxygen Forensics, BlackBag Technologies, Forensic Toolkit, EnCase Forensic Software, Belkasoft Evidence Center, Autopsy, Computer Aided Investigation Environment, Mobile Security Testing Live Environment, MOBILedit, etc. A series of malware detection frameworks were installed and/or tested, such as: MODELZ[8], Andromaly[9], MADAM[10], ComDroid[11] and ProfileDroid[12]. The analyzed frameworks use different features of mobile terminals. MODELZ analyzes the power consumed by the battery when running different applications and based on these features identifies a signature. In my opinion, the main drawback of this analysis is the need to implement an external device to acquire the history of energy consumption in a precise way. The authors test on an external oscilloscope, Agilent Infinium 54851-A, and suggest building an inexpensive external circuit based on an Atmel AVR microcontroller. The Andromaly Framework uses an application installed on the mobile device that exploits various parameters such as CPU usage, number of Wi-Fi packs, number of processes running, battery level to deduce the normal operation of the device. The number of tracking features is 88.

The use of artificial intelligence algorithms for grading on a large number of features extracted from the mobile terminal, some of them redundant or irrelevant, suffers from several issues, such as: inefficiency of the learning algorithm, overuse, reduced generality, increasing model complexity and time execution. In our opinion, the application that implements classification algorithms should not run on mobile devices because they are often restricted by data storage and processing capabilities,

as well as battery power. The process of detecting malicious behavior becomes cumbersome when some malicious activities are of short duration and do not provide sufficient data to detect or engage the model, there is no possibility of accessing an unlimited database of malicious applications to increase the accuracy of algorithms, malicious behavior of an application is generated by multiple attack vectors, so a classification is difficult and the small number of malicious applications used as inputs generates an imbalance problem. The major disadvantage of the MADAM framework, though it uses 13 features and has been tested on real mobile devices, is that the mobile terminal has to be rooted. This framework monitors system calls, running processes, memory and CPU usage, called phone numbers, Bluetooth and Wi-Fi functionality, incoming or outgoing SMS, idle and activity times, key presses. The Droid Detective Framework[13] proposes an analysis based on the grouping of permissions for malware detection. After permissions are extracted, their occurrence frequency will be calculated when grouped (permission grouping starts from a permission to a group of 6 permissions) on safe and malicious applications. The group of permissions that indicates malicious behavior is identified for applications that use the features: ACCESS_NETWORK, READ_PHONE_STATE, INTERNET, READ_SMS, and WRITE_SMS. A number of authors[14] propose using several classification algorithms to improve the accuracy of malware detection. Multiple sets of features in the learning phase are used: API functions, permissions and commands of the SO. The algorithms used are: Decision Tree, Simple Logistic, Naive Bayes, Partial Decision Tree and Ripple Down Rule learner. The total number of selected features is 179, of which 125 permissions and 54 API functions and OS commands. As an input data set, the McAfee database with 2925 malicious applications and 3938 secure applications was used. To evaluate the performance of the classification algorithms, the 10-fold cross validation method is used (involving partitioning the 10-part initial set, 9 training on one and testing one, repeating the procedure, and checking the accuracy). RIDOR and PART have the best detection rate. Authors have a complete approach because they use sets of different features simultaneously with varied classification algorithms. The way to select the relevant features is not specified.

An interesting approach[15] is to analyze the permissions required by the application during execution and those in the manifest file. A permission that is not required in the initial phase may be required later. The idea is that there may be a difference between the required permissions and those used by the application. The bottom line is that malware requests more permissions than secure applications.

It is possible to build a classifier based on the set of lower level instructions using the N-gram model[16]. As a working procedure, the application is disassembled to generate smali type files. Each file contains a class of related methods in the Dalvik bytecode format. Disassembling an application is performed with the apktool utility (Figure 2). The instructions of each method are extracted from the resulting files into a string and their occurrence frequencies are calculated. Each Dalvik bytecode format has 1-byte size. The instruction number is 256 at 130, of which 218 instructions are used. There are 218 possibilities to arrange these instructions. The unique n-opcode number is calculated by the formula: N = X - (N - 1), where X is the number of instructions in the application and N represents the number of instructions in a pair. Thus, a 10-instruction method has 10 pairs of 1 instruction, 9 pairs of 2 instructions, 8 pairs of 3 instructions, etc.

Classification of malware can be done after a small set of instructions[17], respectively 6 instructions. These are: move, jump, packed-switch, sparse-switch, invoke, if. The initial premise is based on two questions: are the features chosen to distinguish between malicious and secure applications?

Furthermore, does the combination of the chosen features bring added value to the case when they are individually approached in malware analysis? The scientific contribution can be summarized as follows: the uniqueness of the chosen characteristics with good results using few resources for malware analysis. The significant difference that identifies malware is given by the move and jump instructions. The if and invoke instructions do not bring significant differences. The basic idea is that malware does not implement an application logic as complex as secure applications.

Due to the fact that iOS is closed, the security challenges are fewer. It allows revocation/ providing the identification of mobile terminals technical features, to include installed applications,

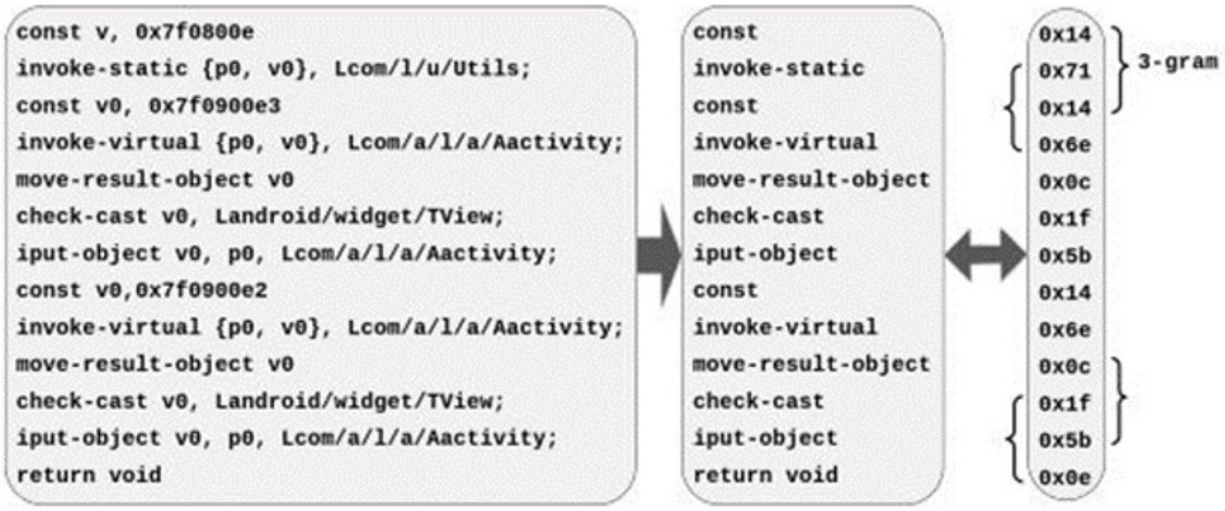


Figure 2. *Extract from a smali file the instructions and generate the 3-gram vector*

acceptance of dynamic permissions, executes ARM binary code that is difficult to disassemble, packing content is a tedious process with dex files. One of the attack vectors is the use of private API calls in applications.

The platform architecture was modularly designed so that it can integrate forensic software tools without compatibility issues (Figure 3). Each module performs specialized tasks as follows:

Web Central Platform

1. User Interface Module – This module performs management activities for the investigation cases, producing both dynamic and static security reports and, assigning risk scores for mobile terminals based on specific analysis and evaluation.

2. Authentication /Authorization Module. This module manages the authentication privileges for defined users as well as the access to the Web Central Platform.

3. Parameterization Module. This module manages the nomenclatures and provides the means to configure the parameters of the Web Central Platform.

4. Data Collection Module. The module gathers and disseminates the data, the results of analyses as well as contamination indices and specific mobile terminal applications.

5. Forensic Management Module. The module manages the forensic work tools and procedures, collecting mobile terminal artefacts and supporting the forensic analysis process for web services.

6. Monitoring Module. This module performs as a push Agent, analysing and evaluating all the applications installed on the mobile terminals, producing lists of suspicious applications and subsequently loading those suspicious programs as well as loading alerts, status and key performance indicators. This module is designed to enlarge the spectrum of malware threats identification by monitoring the behaviour of the mobile terminal installed applications and transmitting the results obtained to the central application responsible for Data Collection and Analysis.

7. Reverse Engineering Module. This module features reverse engineering capabilities, performing uploads and downloads of specific programs to be analysed as well as the analysis products.

8. Online Behaviour Integration Module. This module is directly connected to the Online Behaviour Analysis Module, to which it transmits the updated AI/ML algorithms, and from which it receives the results of online behavioural analysis for further processing.

9. Online Behaviour Analysis Module. The module features a web administrative interface, providing various capabilities such as Proxy, SSL Termination, VPN, Wireless Access Point, USB and Ethernet. The module records the traffic data produced when the mobile terminal is connected to

the Web Central Platform through Wi-Fi. Through network analysis, the module provides intrusion prevention services, runs AI/ML algorithms, detects applications anomalous behaviour caused by malware and transmits those traffic anomalies to the Online Behaviour Integration Module for further processing. Lastly the module profiles the mobile terminal in correlation with the default configurations and recorded traffic, acquiring lists with web sites classified as hazardous, accessing and integrating online threat intelligence sources.

mobile applications, manages alerts, supports the detection of malware based on signature lists, profiles the mobile terminal, correlating the default configuration with the installed applications.

12. Reverse Engineering Applications Module. Through a Sandbox type system, this module is designed to provide static and dynamic analysis of mobile terminals. It submits JSON/HTML reports to the web central platform, assesses the results of analysis, and identifies automatically the behaviour of specific malware.

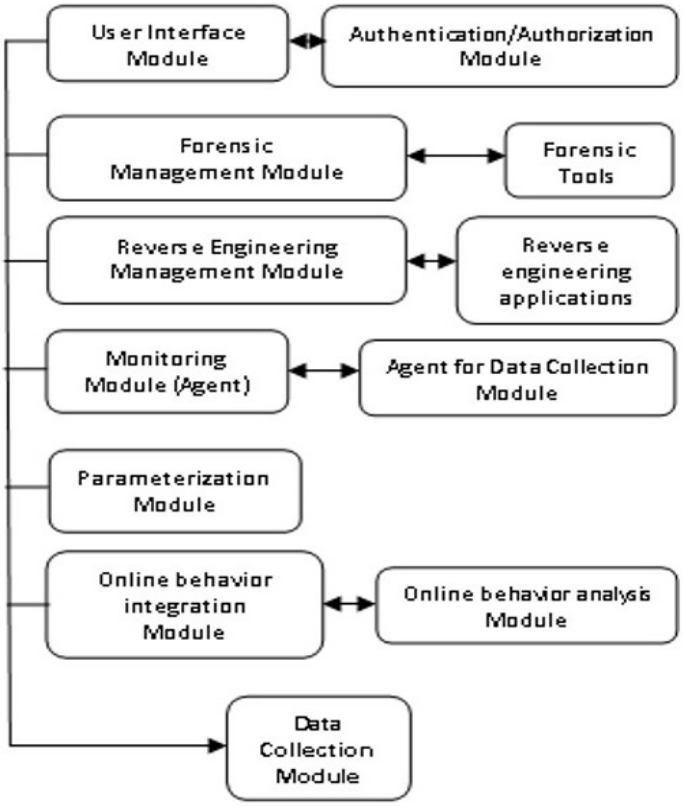


Figure 3. *Integrated software platform architecture*

10. Forensic Tools Module. The module displays a user-friendly interface. It enables parallel extraction and analysis from multiple mobile terminals and performs various tasks such as the physical and logical extraction of data, subsequent analysis of data, report configuration for data extraction, advanced analysis of mobile applications, as well as password and file recovery functionalities.

11. Agent for Data Collection Module. The agent gathers data and mobile applications, monitoring several security features. Thus, it collects key performance indicators, comparing hashes received from apps stores with hashes of installed

The Proxmox KVM server virtualization server was used for the necessary functionalities on which the virtual machines that support various services and applications are created. Virtual machines use Docker containers that are orchestrated by Kubernetes. LXD, which is a new generation system, has been used to handle containers and provides API REST services.

Using containers allows the creation of micro-services – applications are thus decoupled and can be installed and managed dynamically. The virtual machine VM3 is responsible for the PostgreSQL database for running the torsim-database service. The Apache Kafka and Elasticsearch tools are

Table 1. *Fluxes between applications and services*

No	Applications and services		
	Service/application	*Virtual machine*	*Role*
1	nginx	VM 1	The Front end receives requests from customers
2	torsim-proxy	VM 1	The application's graphical interface and secure services receive requests from the front end (nginx)
3	torsim-bro-logtail	VM 2	It takes the traffic recorded by the car and saves it in a queue from Kafka
4	torsim-message-processor	VM 1	It takes requests from torsim-proxy
5	MobSF, CuckooDroid	VM 1	It takes requests from torsim-proxy
6	torsim-adb	VM 1	The torsim-adb API takes requests from torsim-proxy
7	Torsim-database	VM 3	The torsim-database API receives requests from torsim-adb and torsim-proxy
8	PostgreSQL	VM 3	It takes requests from the torsim-database container
9	Elasticsearch	VM 3	It takes requests from the torsim-message-processor
10	Kafka	VM 3	It takes requests from the torsim-message-processor

also installed in this virtual machine. For the forensic functionality, the ADB utilities – Android Debug Bridge and MOBILedit – were used. The torsim-adb service encompasses the ADB client, communicating with the ADB server installed on the laptop, and communicating with the ADB deamon on the mobile terminal. At the moment, integration with MOBILedit is done at the procedural level, MOBILedit manually runs and the desired ratio is obtained, which then loads into the central platform. In order to intercept the traffic generated by the mobile devices, the Bro utility sends the intercepted packets into a Kafka message queue, which is then taken over by the torsim-message processor service and sent to Elasticsearch. For Trafficking Analysis and Malicious Behavior, Mail trail Maltese Traffic Detection System is used. The Mail trail application uses public lists of trusted and malicious sites, information from reports of various antivirus products, custom lists where signatures can be domain names, IPs, HTTP User-Agent header value, and heuristic mechanisms that can help detection of malware unknown yet. On the virtual machine VM 1 CuckooDroid is installed, an extension of Cuckoo Sandbox, an open source software used to analyze suspicious files with capabilities in static and dynamic analysis of Android apps. The MobSF framework also enables static and dynamic analysis of mobile applications. A Docker container was used for the Static Analysis MobSF application, and the integration with the central platform was done through the MobSF API, so applications can be submitted for analysis and both the PDF report and the JSON format are obtained. The latter is used to store scan data in the database and to be displayed in the web interface. An important step was testing the platform by verifying all the parameters introduced and obtaining the right reports in malware analysis. Agent mode is still in the development phase and will be supported by Android and IOS and a number of artificial intelligence algorithms on different features. In our opinion, an algorithm that tracks malicious behavior only on the basis of

permissions has a low efficiency. The agent must run on no rooting phones and track the required permissions for applications installed before and during running applications. The following artifacts can be tracked: accessing network and sensitive data such as contact list and location, receiving and transmitting SMS, clipboard data, access to different hardware components, number of clicks during the user's intense activity period correlated with the period of inactivity. The agent can be integrated with the public API and made available by VirusTotal to check the authenticity of the apk package by comparing the application's hash with the site's database. Check the application configuration files to identify the version of the application, the hardware resources it will require, the permissions to be assigned, the components and the list of dangerous permissions. The existence of suspicious character strings in the application may be an indicator of the presence of a malware infection. Entropy detects if there are encrypted areas.

Conclusions

New advances in Artificial Intelligence – Machine Learning have allowed the emerge of a new stage in evolution of cyber security. Continuously improving the possibilities of identifying and combating future threats is a viable solution to the fight against malware. Literature studied during the project period included only algorithms from supervised learning. Various mobile terminal security software solutions have been tested and hardware and software infrastructure built. The research project is not completed, following the testing phase of malware applications selected by project experts.

Acknowledgment

This work was possible with the financial support of the Executive Agency for Higher Education, Research, Development and Innovation Funding – UEFISCDI / Romanian Ministry of National Education, under the project number PN-III-P2-2.1-SOL-2016-05-0070 with the title "Integrated Software Platform for Malware Analysis on Mobile Terminals".

NOTES:

1 James R. Blake, "Transforming military", Praeger Security International, May 2007.

2 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

3 Elena Şuşnea, Adrian Iftene, "The Significance of Online Monitoring Activities for the Social Media Intelligence (SOCMINT)", Conference on Mathematical Foundations of Informatics MFOI'2018, Institute of Mathematics and Computer, Chisinau, Moldova, pp. 230-240, 2018.

4 Reza Hedayat, Lorenzo Cavallaro, *The Devil's Right Hand: An Investigation on Malware-oriented Obfuscation Techniques*, Computer Weekly, August 2016.

5 Dragoş Bărbieru, Alexandru Stoica, "Malware Analysis on Mobile Phone", The International Scientific Conference eLearning and Software for Education, Vol. 4, 11-15, "Carol I" National Defence University, Bucharest, pp. 11-15, 2018.

6 https://fortiguard.com/events/755/2013-10-25-playing-hide-and-seek-with-dalvik-executables

7 Babak Bashari Rad†, Maslin Masrom ††, Suhaimi Ibrahim, *Camouflage in Malware: from Encryption to Metamorphism,* IJCSNS International Journal of Computer Science and Network Security, Vol.12, No.8, August 2012.

8 Hannsang Kim, Member IEEE, Kang G. Shin, Padmanabhan Pillai, *MODELZ: Monitoring, Detection and Analysis of Energy-Greedy Anomalies in Mobile Handsets,* IEEE Transactions on mobile computing, Vol. 10, July 2011.

9 Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer, Yael Weiss, *"Andromaly": a behavioral malware detection framework for android devices*.

10 Gianluca Dini, Fabio Martinelli, Andrea Saracino, Daniele Sgandurra, *MADAM: a Multi-Level Anomaly Detector for Android Malware*, Computer Network Security: 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2012, St. Petersburg, Russia, October 17-19, 2012.

11 Chin E., Felt A. P., Greenwood K., and Wagner D.: "Analyzing inter-application communication in Android". Proc. 9th Int. Conf. On Mobile Systems, Applications, and Services (MobiSys '11). ACM, Washington, DC, USA, June 2011, pp. 239-252.

12 Wei X., Gomez L., Neamtiu I., and Faloutsos M.: "ProfileDroid: multi-layer profiling of android applications" Proc. 18th Int. Conf. On Mobile Computing and Networking (Mobicom '12), ACM, Istanbul, Turkey, August, 2012, pp. 137-148.

13 Shuang Liang; Xiaojiang Du, *Permission-combination-based scheme for Android mobile malware detection,* IEEE International Conference on Communications (ICC), June, 2014.

14 Suleiman Y. Yerima, Sakir Sezer, Igor Muttik, *Android Malware Detection Using Parallel Machine Learning Classifiers*, Eighth International Conference on Next Generation Mobile Apps, Services and Technologies, December, 2014.

15 Xing Liu, Jiqiang Liu, *A Two-Layered Permission-Based Android Malware Detection Scheme*, 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, April, 2014.

16 BooJoong Kang, Suleiman Y. Yerima, Sakir Sezer, Kieran McLaughlin, International Journal on Cyber Situational Awareness, Vol. 1, No. 1, 2016, pp. 231-255.

17 Gerardo Canfora, Francesco Mercaldo, Corrado Aaron Visaggio, *Mobile malware detection using op-code frequency histograms*, 12th International Joint Conference on e-Business and Telecommunications (ICETE), July, 2016.

BIBLIOGRAFIE

Babak Bashari Rad, Maslin Masrom, Suhaimi Ibrahim, "Camouflage in Malware: from Encryption to Metamorphism", *IJCSNS International Journal of Computer Science and Network Security*, vol. 12, No. 8, August, 2012.

Bărbieru Dragoş, Stoica Alexandru, "Malware Analysis on Mobile Phone", *The International Scientific Conference eLearning and Software for Education*, Vol. 4, "Carol I" National Defence University, Bucharest, 2018.

Blake R. James, *Transforming military*, Praeger Security International, May, 2007.

Canfora Gerardo, Mercaldo Francesco, Visaggio Corrado Aaron, "Mobile malware detection using op-code frequency histograms", *12th International Joint Conference on e-Business and Telecommunications (ICETE)*, July 2016.

Chin E., Felt A.P., Greenwood K., Wagner D., "Analyzing inter-application communication în Android", *Proc. 9th Int. Conf. On Mobile Systems, Applications, and Services (MobiSys '11). ACM*, Washington, DC, USA, June, 2011.

Dini Gianluca, Martinelli Fabio, Saracino Andrea, Sgandurra Daniele, "MADAM: a Multi-Level Anomaly Detector for Android Malware", *Computer Network Security: 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2012*, St. Petersburg, Russia, October, 17-19, 2012.

Hannsang Kim, Member IEEE, Kang G. Shin, Padmanabhan Pillai, "MODELZ: Monitoring, Detection and Analysis of Energy-Greedy Anomalies în Mobile Handsets", *IEEE Transactions on mobile computing*, Vol. 10, July, 2011.

Hedayat Reza, Cavallaro Lorenzo, "The Devil's Right Hand: An Investigation on Malware-oriented Obfuscation Techniques", *Computer Weekly*, August, 2016.

Kang BooJoong, Yerima Y. Suleiman, Sezer Sakir, McLaughlin Kieran, *International Journal on Cyber Situational Awareness*, Vol. 1, No. 1, 2016.

Shabtai Asaf, Kanonov Uri, Elovici Yuval, Glezer Chanan, Weiss Yael, *Andromaly: a behavioral malware detection framework for android devices*.

Shuang Liang, Xiaojiang Du, "Permission-combination-based scheme for Android mobile malware detection", *IEEE International Conference on Communications (ICC)*, June, 2014.

Şuşnea Elena, Iftene Adrian, "The Significance of Online Monitoring Activities for the Social Media Intelligence (SOCMINT)", *Conference on Mathematical Foundations of Informatics MFOI'2018*, Institute of Mathematics and Computer, Chisinau, Moldova, 2018.

Wei X., Gomez L., Neamtiu I., Faloutsos M., "ProfileDroid: multi-layer profiling of android applications", *Proc. 18th Int. Conf. On Mobile Computing and Networking (Mobicom '12). ACM*, Istanbul, Turkey, August, 2012.

Xing Liu, Jiqiang Liu, "A Two-Layered Permission-Based Android Malware Detection Scheme", 2nd *IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, April, 2014.

Yerima Y. Suleiman, Sezer Sakir, Muttik Igor, "Android Malware Detection Using Parallel Machine Learning Classifiers", *Eighth International Conference on Next Generation Mobile Apps, Services and Technologies*, UK, Oxford, December, 2014.

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

https://fortiguard.com/events/755/2013-10-25-playing-hide-and-seek-with-dalvik-executables

AN ANALYSIS OF NATO AND EU MARITIME STRATEGIES

Commander (N) Valentin-Cătălin VLAD, PhD Student*

In the context of the upgrading or initiation of NATO or European Union's maritime strategies, ensuring, maintaining and promoting the security, stability and prosperity of the Euro-Atlantic maritime space must be at the forefront of the process of streamlining and harmonizing transatlantic maritime security due to the fact that the Alliance and the Union have assumed similar values and interests and have targeted the same vital maritime space - the Euro-Atlantic maritime space.

In this respect, the analysis of NATO and the European Union's maritime strategies is the key element of understanding the vision, ambition and interest of the two organizations in order to determine the convergence elements on which to build a complementary action course to support Euro-Atlantic maritime security.

Keywords: Euro-Atlantic maritime security; maritime security strategies; regional cooperation.

Introduction

The evolution of the global security environment in recent years has been triggered by an increase of challenges and threats raised especially from the maritime space, for which the Euro-Atlantic community has reassessed and declared its maritime security priorities and interests through their own maritime strategy security.

In this regard, Mrs. Federica Mogherini – High Representative for Foreign Affairs and Security Policy – said that the EUMSS is the way the European Union *"is reaffirming its role as a global maritime security provider. It promotes international cooperation, maritime multilateralism and the rule of law at sea, in line with the strategic priorities identified in the EU Global Strategy"*[1].

Through the Allied Maritime Strategy (AMS) and the EU Maritime Strategy (EUMSS), both NATO and the EU aimed at countering threats to Euro-Atlantic and international maritime security, such as illegal migration, piracy, cross-border crime, terrorism, arms trafficking and prohibited material and, on the other hand, to exploit the credibility and legitimacy gained from recognition by the United Nations for their decisive contribution to the success of major operations or actions conducted in recent years to ensure international maritime security in the the Mediterranean Sea, the Aegean Sea or the Gulf of Aden – "Ocean Shield" (OOS), "Atalanta", "Unified Protector" (OUP), "Sophia", "Active Endeavor" (OAE) / "Sea Guardian" (OSG) to Combat Illegal Migration in the Aegean Sea (AEG).

ROU NAVY
e-mail: *valentin.vlad@navy.ro*

Fundamentals of the Euro-Atlantic maritime strategies

Under the motto that *"sea matters"*[2], the EU developed and adopted for the first time in 2014 the European Union's Maritime Safety Strategy[3] (EUMSS), centered mainly on securing its own maritime security and, above all, on promoting and capitalizing its statute as relevant actor for regional and international security based on the legitimacy offered by the international legal framework.

The EUMSS has as course of action the initiation and development of the maritime security cooperation with key international players in a comprehensive interinstitutional and multi domain approach to the main European sea basins – the Baltic Sea, the Black Sea, the Mediterranean Sea, the North Sea, the Ocean Atlantic, Arctic and international waters.

The regional focus of the EUMSS subscribes to Taylor's[4] theory of avoiding the globalization of a security community, which is why it can be said that the strategy has a conceptual foundation that will enable it to be effectively implemented on the four directions defined by the interinstitutional approach, functional integrity, the respect for rules and principles, and maritime multilateralism.

Through the four directions of action, the European Union aims to credibly and legitimately engage and relate to all its military and civilian structures in a joint effort, both domestically and internationally, in order to ensure maritime and international maritime security.

Thus, the multilateralism of maritime security cooperation with relevant international actors such as North Atlantic Treaty Organization (NATO), United Nations (UN) or International Maritime Organization (IMO) complement each other with the functional integrity that assures the assertion and enforcement of the rights and jurisdiction offered to the Union by the international legal framework.

Following the provisions of the Allied Strategic Concept[5] NATO adopted its Maritime Allied Strategy[6] (AMS) on March 18, 2011 having as a goal to secure the Euro-Atlantic maritime space through interinstitutional and cross domain cooperation with relevant regional and international actors and in full consideration to international legitimacy.

As in the case of the Union, NATO as a promoter of values, rights and freedoms guaranteed by international law aims to subscribe to regional and international efforts to ensure maritime security.

Thus, through NATO's Allied Maritime Strategy, NATO aims to achieve Euro-Atlantic and international maritime security by acting for collective discouragement and defense, crisis management and maritime security through cooperation in full compliance with international law, agreements and treaties (UN Charter, International Convention on the Law of the Sea).

In essence, the defining elements that create the basis of the two maritime strategies are represented by respect for international values, rights and freedoms as promoted by the Charter of the United Nations, but above all that, the fact that NATO and the European Union are open to cooperation and point to each other as the main partners in ensuring, maintaining and guaranteeing Euro-Atlantic and international maritime security, stability and prosperity.

Also, NATO and EU's orientation towards regional cooperation is seen as the key element of the process of making Euro-Atlantic and international maritime security more efficient, and as I have emphasized earlier, it subscribes to Taylor's theory that the universality of a security community is impossible[7].

Common elements of AMS and EUMSS

In order to talk about the efficiency of the Euro-Atlantic maritime security process it is necessary to bring NATO and EU maritime strategies to the same common conceptual and action denominator.

According to the provisions of their own maritime strategy, NATO and the EU aim at deterring threats, ensuring collective defense, crisis management and maritime security, namely risk management, conflict prevention and crisis response. This highlights common strategic visions focused on ensuring Euro-Atlantic and international maritime security and this is absolutely natural, given that the Alliance and the Union promote and defend the values and interests of 22 states that are found among both organizations.

Thus, shared elements defining the common denominator of these two strategies are mutual trust and respect, consideration of international maritime legislation, individual and collective values and rights, interest in comprehensive regional maritime cooperation, global ambition, common maritime space of interest (Euro-Atlantic) and in particular the fact that they target more than 75% of maritime capacities belonging to the same states (22 out of 29 NATO members are also EU members – 76%).

Asserting their willingness to promote and defend their interests on a global basis under international legitimate conditions confers NATO and the EU the breadth of United Nations (UN) agreed and accredited maritime actors as real benchmarks for international maritime security, stability and prosperity.

In this respect, NATO and EU interest in developing regional security communities at the level of the main Euro-Atlantic maritime basins fits perfectly into the provisions of the UN Charter[8] and becomes the center of gravity of the process of making Euro-Atlantic and international maritime security more effective through regional cooperation because its considerations and exploitation of the opportunities and vulnerabilities belonging to each sea basin.

This approach exploits the consideration of states and regional and international actors relevant to international laws and treaties, fosters their acceptance, support, empowerment and involvement in the joint effort to ensure international maritime security.

Thus, if we are to referring to Russian Federation as the second world maritime power, it declares in

its new Maritime Doctrine[9] the intention to promote and defend its global maritime interests in a comprehensive approach based on the development of modern maritime capabilities that allow it to be present at regional and international level under conditions of full international legitimacy.

The same orientation on legitimate regional maritime cooperation is shared by the main maritime power of the world, the United States, through its own maritime strategy tailored around the vision of the former US Naval Forces commander, Admiral Jonathan William Greenert: "*The reality of today is that we have to think about the global network of navies. All it takes is a willingness to cooperate – there's no commitment, you don't have to join an alliance, anyone can plug-and-play. There's a mission for everybody whether it's humanitarian assistance and disaster response, counterterrorism, counter transnational organized crime, or counter piracy*" [10].

However, the conceptual common denominator of the two Euro-Atlantic Maritime Strategies (AMS, EUMSS) focused on comprehensive regional maritime cooperation has not always been complemented by an unity of effort to implement their provisions from a variety of causes attributable to lack of joint strategic vision and actions' complementarity between NATO and the EU, which has not rarely witnessed rivalries, indecision, precipitation or reorientation that tense the transatlantic historical link, marked by numerous declarative episodes[11] [12] between the main European leaders Angela Merkel and Emmanuel Macron and the President of the United States of America, Donald Trump.

Thus, *"the times in which we (Europeans) could completely depend on others (UK and US-NATO) are, to a certain extent, over"*[13] and Europe must *"take its fate into its own hands"*[14] resonates negatively with the fact that the EU military *"is not an army against, and it can be a good complement to NATO"*[15] in which United Kingdom and US represent two maritime powers whose nuclear capabilities are complemented by that of France, which remains singular in the hypothesis of crediting Mrs. Merkel's vision, to ensure strategic nuclear deterrence against any threats of symmetric or asymmetric nature that could jeopardize Euro-Atlantic security and stability.

All this debate has generated the lack of a complementary strategic vision of the NATO-EU binomial and has led the eastern flank states, faced with increasing economic and security challenges and threats, to initiate and develop cooperation communities such as the Three Seas Initiative[16] (3SI) or Bucharest 9[17] (B9).

This direction was the proof of understanding the need to make Euro-Atlantic strategies more effective through regional focus, but also the puzzling of small European states regarding the perception of a common Euro-Atlantic vision that respects existing political-military or political-economic arrangements.

However, it should be noted that at least until this moment the declarative disagreement did not break the transatlantic link, and NATO continued to benefit from the unmatched support of the United States[18] and form a firm stand-on with respect to the collective security guarantees of its members by increasing its presence and support on the eastern flank, especially as a result of the evolution of the geopolitical situation after the events in the Black Sea Basin after 2014.

It is also worth noting the effort that the European Union has put forward and continues to make to ensure Euro-Atlantic and international maritime security against illegal migration or piracy in the Aegean Sea, the Mediterranean Sea or the Gulf of Aden.

Conclusions

Reducing the operational effort of NATO and EU Member States maritime capabilities and articulating a common Euro-Atlantic strategic response is the essence of the process of streamlining NATO and EU maritime strategies and in this respect defining Euro-Atlantic conceptual and actionable complementarity and adopting a possible model of security through maritime cooperation that exploits the theories of security communities initiated and developed by Wagenen, Deutsch, Adler, Barnett, Taylor, Cohen or Mihalka has to cover the agenda of NATO and EU leaders.

Only this way will the relationship between NATO[19] and the European Union get the dimension of unity and will be able to capitalize on the strength of the historic transatlantic link and the advantages of political-military instruments on the one hand and political-economic instruments on the other.

As a result, the adoption of a maritime security model through regional cooperation based on NATO-EU complementarity would ensure the valorization of the conceptual common denominator and implicitly the timely, credible and

legitimate implementation of the two Euro-Atlantic maritime strategies for the benefit of Euro-Atlantic and international maritime security.

In conclusion, the Allied Maritime Strategy and the Maritime Security Strategy of the European Union promote convergent conceptual visions on maritime security and the efficiency of the Euro-Atlantic and international maritime security process must be framed on the coordinates of the doctrinal and action complementarity of the NATO-EU binomial.

NOTES:

1 Maritime security: EU revises its action plan, EU, 26 June, 2018, accessed at https://www.consilium.europa.eu/en/press/press-releases/2018/06/26/maritime-security-eu-revises-its-action-plan/, accessed at 20 April, 2019.

2 European Union Maritime Security Strategy (EUMSS), UE, 2014, p. 2, accessed on https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT, accessed at 22 April, 2019.

3 *Ibidem*.

4 Michael Taylor, Community, Anarchy and Liberty, New York, Cambridge University Press, 1982, pp. 167-168.

5 NATO Strategic Concept, NATO, 2010, accessed at https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf, accessed at 24 April, 2019.

6 Alliance Maritime Strategy, NATO, 2011, accessed on https://www.nato.int/cps/ ua/natohq/official_texts_75615.htm, accessed at 24 April, 2019.

7 Michael Taylor, *op.cit.*, pp. 167-168.

8 Carta ONU, 1945, cap. VIII, accessed at https://www.un.org/en/sections/un-charter/chapter-viii/index.html, accessed at 26 April, 2019.

9 Maritime Doctrine of the Russian Federation, Russian Maritime Studies Institute (US Naval War College translation), 2015, pp. 7-8, accessed at https://dnnlgwick.blob.core.windows.net/portals/0/NWCDepartments/Russia%20Maritime%20Studies%20Institute/Maritime%20Doctrine%20TransENGrus_FINAL.pdf?sr=b&si=DNNFileManagerPolicy&sig=fqZgUUVRVRrKmSFNMOj%2FNaRNawUoRdhdvpFJj7%2FpAkM%3D, accessed at 29 April, 2019.

10 A Cooperative Strategy for 21st Century Seapower, US Navy, March, 2015, p. 5., accessed at http://www.navy.mil/local/maritime/150227-CS21R-Final.pdf, accessed at 03 May, 2019.

11 Angela Merkel: EU cannot completely rely on US and Britain any more, The Guardian, 2017, accessed on https://www.theguardian.com/world/2017/may/28/merkel-says-eu-cannot-completely-rely-on-us-and-britain-any-more-g7-talks, accessed at 04 May, 2019.

12 Trump demands NATO countries meet defense spending goals 'immediately', CNBC, 2018, accessed at https://www.cnbc.com/2018/07/11/trump-demands-nato-countries-meet-defense-spending-goals-immediately.html, accessed at 05 May, 2019.

13 Angela Merkel: EU cannot completely rely on US and Britain any more, The Guardian, 2017, accessed at https://www.theguardian.com/world/2017/may/28/merkel-says-eu-cannot-completely-rely-on-us-and-britain-any-more-g7-talks, accessed at 04 May, 2019.

14 *Ibidem*.

15 Merkel joins Macron in calling for EU army to complement NATO, Politico, Bruxelles, 2018, accessed at https://www.politico.eu/article/angela-merkel-emmanuel-macron-eu-army-to-complement-nato/, accessed at 05 May, 2019.

16 Inițiativa celor trei mări, accessed on URL: http://three-seas.eu/, accessed at 11 May, 2019.

17 Declarație comună a miniștrilor de externe din statele Formatului București 9 (B9), MAE, 2017, accessed on https://www.mae.ro/node/43571, accessed at 11 May, 2019.

18 SNMG-1 and SNMCMG-1 Conduct Change of Command, NATO, 2019, accessed at https://mc.nato.int/media-centre/news/2019/snmg1-conducts-change-of-command.aspx, accessed at 18 April, 2019.

19 Relations with the European Union, accessed at URL: https://www.nato.int/cps/en/ natohq/topics_49217.htm, accessed at 18 May, 2019.

BIBLIOGRAPHY

*** *A Cooperative Strategy for 21st Century Seapower: Forward, Engaged, Ready (CS21R),* accessed at http://www.navy.mil/local/maritime/150227-CS21R-Final.pdf.

*** AAP 6, *NATO Glossary Of Terms And Definitions* (English And French), Edition 2013.

*** A "comprehensive approach" to crises, NATO, 2016, accessed on https://www.nato.int/cps/en/natolive/topics_51633.htm.

*** A comprehensive approach, NATO, 2009, accessed at https://www.nato.int/summit2009/topics_en/19-comprehensive_approach.html.

*** A Cooperative Strategy for 21st Century Seapower, US Navy, March 2015, accessed at http://www.navy.mil/local/maritime/150227-CS21R-Final.pdf.

*** A framework for enhanced international maritime security cooperation and awareness, CJOS COE, 2011, accessed at http://cjoscoe.org/docs/MSA_Strategic_Framework_V1.0.pdf.

*** A Global Strategy for the European Union's Foreign and Security Policy, EU, 2016, accessed

at http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

*** Allied Joint Doctrine (AJP-01), NATO, 2017, accessed at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602225/doctrine_nato_allied_joint_doctrine_ajp_01.pdf.

*** Allied Maritime Strategy – A theory for success?, Kiel International Seapower Symposium Conference Report, 2018, accessed at https://www.kielseapowerseries.com/files/ispk/content/KISS18/KISS2018_final_Web.pdf.

*** Alliance Maritime Strategy, NATO, 2011, accessed at URL: https://www.nato.int/cps/ua/natohq/official_texts_75615.htm.

*** Charter of the United Nations, ONU, 1945, accessed at https://www.un.org/en/sections/un-charter/chapter-viii/index.html.

*** Angela Merkel: EU cannot completely rely on US and Britain any more, The Guardian, 2017, accessed on URL: https://www.theguardian.com/world/2017/may/28/merkel-says-eu-cannot-completely-rely-on-us-and-britain-any-more-g7-talks.

*** Consolidated Version of the Treaty on European Union, UE, 2007.

*** Defence cooperation: Council establishes Permanent Structured Cooperation (PESCO), with 25 member states participating, Council of the European Union, 2017, accessed at https://www.consilium.europa.eu/en/press/press-releases/2017/12/11/defence-cooperation-pesco-25-member-states-participating/.

*** Council conclusions on the revision of the European Union Maritime Security Strategy – Action Plan, EU, 26 June 2018, accessed at http://data.consilium.europa.eu/doc/document/ST-10494-2018-INIT/en/pdf.

*** EU defence cooperation: Council establishes a Military Planning and Conduct Capability (MPCC), Council of the European Union, 8 June 2017, accessed at https://www.consilium.europa.eu/ro/press/press-releases/2017/06/08/military-mpcc-planning-conduct-capability/.

*** European Union Maritime Security Strategy, EU, 2014, accessed at URL: https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT.

*** European Union Maritime Security Strategy – Action Plan (EUMSS AP), EU, 2014, accessed at https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf.

*** Joint declaration on EU-NATO cooperation by the president of the European Council, the president of the European Commission, and the secretary general of the North Atlantic treaty organization, EU, 2018, accessed at https://www.nato.int/cps/en/natohq/official_texts_156626.htm.

*** Lisbon Summit Declaration, NATO, 2010, accessed at https://www.nato.int/cps/en/natolive/official_texts_68828.htm.

*** Maritime Doctrine of the Russian Federation, Russian Maritime Studies Institute (US Naval War College translation), 2015, accessed at https://dnnlgwick.blob.core.windows.net/portals/0/NWCDepartments/Russia%20Maritime%20Studies%20Institute/Maritime%20Doctrine%20TransENGrus_FINAL.pdf?sr=b&si=DNNFileManagerPolicy&sig=fqZgUUVRVRrKmSFNMOj%2FNaRNawUoRdhdvpFJj7%2FpAkM%3D.

*** Maritime security: EU revises its action plan, EU, 26 June 2018 accessed at https://www.consilium.europa.eu/en/press/press-releases/2018/06/26/maritime-security-eu-revises-its-action-plan/

*** NATO Strategic Concept, NATO, 2010, accessed at https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.

*** The North Atlantic Treaty, NATO, Washington DC, 1949, accessed at http://www.mae.ro/sites/default/files/file/pdf/TRATATUL%2520NORD-ATLANTIC.pdf.

*** United Nations Convention on the Law of the Sea (UNCLOS), UN, 1982.

Adler E., Barnett M., *Security Communities*, Cambridge University Press, 1998.

Angela Merkel: EU cannot completely rely on US and Britain any more (2017), accessed at https://www.theguardian.com/world/2017/may/28/merkel-says-eu-cannot-completely-rely-on-us-and-britain-any-more-g7-talks

Buzan B., *People, States and Fear*, Harvester Wheatsheaf, 1991.

Cohen R., Mihalka M., *Cooperative Security: New Horizons for International Order*, The Marshall Center Papers, No. 3, 2001.

D'Aponte T., *A geopolitical overview on the Mediterranean Sea the approach of the euro-med policy towards the countries of the southern front (from Morocco to Egypt)*, Rivista Italiana di Economia Demografia e Statistica, Volume LXVIII n.2, Aprile-Giugno, 2014.

De Coning C., *The United Nations and the*

comprehensive approach, Danish Institute for International Studies, Report 2008:1.

Deutsch K.W., *et al*., *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience*, Princeton: Princeton University Press, 1957.

Donald Trump: Without the US, the French would be speaking German (2018, November, the 13th), accessed at https://www.politico.eu/article/donald-trump-without-the-us-the-french-would-be-speaking-german/

Drent M., *The EU's Comprehensive Approach to Security: A Culture of Co-ordination?*, Studia Diplomatica, 2011, LXIV-2.

Feldt L., Dr. Roell P., Thiele R. D., *Maritime Security – Perspectives for a Comprehensive Approach*, ISPSW Strategy Series: Focus on Defense and International Security, No. 222, 2013, accessed at URL: https://www.files.ethz.ch/isn/162756/222_Feldt_Roell_Thiele.pdf

Fransas A., Nieminen, E., Salokorpi, M., *Maritime Security and Security Measures – Mimic Study in the Baltic Sea Area*, Kymenlaakso University, Kotka, Finland, 2013.

German Chancellor Supports Creation of European Security Council (2018, October 7th), accessed at https://www.strategic-culture.org/news/2018/10/07/german-chancellor-supports-creation-of-european-security-council.html .

Glaser C., *The Security Dilemma Revisited*, World Politics, Vol. 50, No. 1, 1997.

Horrell S., Nordenman M., Slocombe W.B., *Updating NATO's Maritime Strategy*, Brent Scowcroft Center on International Security, July 2016.

Hoyt T.D., Winner A. C., *A Cooperative Strategy for 21st Century Seapower: Thinking About the New US Maritime Strategy*, Maritime Affairs, National Maritime Foundation, Vol. 3, No. 2, 2007.

Kaim M., Kempin R., *A European Security Council Added Value for EU Foreign and Security Policy?*, German Institute for International and Security Affairs – SWP, 2019.

Kegö W., Molcean A., *Russian Organized Crime: Recent Trends in the Baltic Sea Region*, Institute for Security and Development Policy, Stockholm-Nacka, 2012.

Krasner S., *International Regimes*, Ithaca: Cornell University Press, 1983.

Lachowski Z., *Confidence and Security Building Measures in the New Europe*, Oxford University Press, 2004.

Noua doctrină militar-maritimă: Rusia și-a definit inamicii în oceanul planetar (2017, July 22nd), accessed at https://sputnik.md/russia/20170722/13705010/doctrina-maritima-rusia-inamici.htm

Merkel joins Macron in calling for EU army to complement NATO (2018, November 13th), accessed at https://www.politico.eu/article/angela-merkel-emmanuel-macron-eu-army-to-complement-nato/

Pirozzi N., *The EU's Comprehensive Apprroach to Crisis Management*, DCAF Brussels, EU Crisis Management Papers Series, June 2013.

Proelss A., Müller T., *The Legal Regime of the Arctic Ocean*, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht, 2008.

Puchala D. J., *International Politics Today*, New York, 1971.

Puheloinen A., *Russia's geopolitical interests in the Baltic Area,* Finnish Defense Studies, 1999.

Rahman C., *Concepts of Maritime Security - A strategic perspective on alternative visions for good order and security at sea, with policy implications for New Zealand*, Centre for Strategic Studies: New Zealand Victoria University of Wellington, 2009.

Roberts P., *Will the Alliance discover navies again?,* NATO Review Magazine, NATO, 30 April, 2018.

Roucek J. S., *The Geopolitics of the Baltic States*, The American Journal of Economics and Sociology, Vol. 8, No. 2 (Jan., 1949).

Stohs J., Dr. Bruns S., *Maritime Security in the Eastern Mediterranean*, Kiel International Seapower Symposium, 2017, Kiel, 2017.

Taylor M., *Community, Anarchy, and Liberty,* New York, Cambridge University Press, 1982.

Trump demands NATO countries meet defense spending goals 'immediately' (2018, July 12th), taken over from https://www.cnbc.com/2018/07/11/trump-demands-nato-countries-meet-defense-spending-goals-immediately.html.

THE EURO-ATLANTIC MARITIME SECURITY COMPREHENSIVE APPROACH

Captain (N) Ioan CRĂCIUN, PhD*
Commander (N) Valentin-Cătălin VLAD, PhD Student **

The update or development of the Euro-Atlantic Maritime Strategies has largely resonated with the assertion of the intentions of the North Atlantic Treaty Organization (NATO) and the European Union (EU) to promote and defend their values and interests both at the level of the vital space, represented by the Euro-Atlantic Maritime Space, and beyond wherever the situation and the needs of international maritime security impose it.

To this end, streamlining the Euro-Atlantic maritime security process and maintaining it must be a defining element for the success of this process, for which the aim of a comprehensive approach to maritime security calibrated on security community theory may be a viable solution.

Keywords: Maritime security comprehensive approach; Euro-Atlantic maritime security strategies; regional cooperation.

Introduction

The end of the twentieth century and the beginning of the twenty first century found the Euro-Atlantic community connected to the challenges and threats to regional and international maritime security, and their diversity and dynamism prompted North Atlantic Treaty Organization (NATO) and European Union (EU) to reevaluate and calibrate their own doctrinal and action choices to the odds imposed by maintaining international credibility and legitimacy in a comprehensive – interinstitutional and multi-disciplinary approach.

We therefore find NATO and the EU mandated to lead or act in an integrated conjugated effort to ensure and maintain international maritime security in the Mediterranean Sea or the Gulf of Aden against threats to maritime security – piracy, illegal migration, terrorism, and on the other hand acting in support of riparian nations to the operational areas to overcome existing challenges and build their own maritime leadership and execution capabilities.

In this respect, Margriet Drent[1] signaled that the full success of military operations and actions undertaken to restore or maintain the climate of peace and stability as promoted by the United Nations Charter is dependent on the comprehensive approach of binomial determined by military and civilian institutions in support of initiating and developing their own capabilities that allow states in need to stabilize and sustain themselves socially, economically, militarily or politically.

We note, therefore, that the international security environment has compelled the international community to determine and adopt a comprehensive course of action to ensure the involvement, empowerment and cooperation of all relevant governmental or non-governmental actors across multiple converging directions.

The comprehensive strategic approach to Euro-Atlantic maritime security

NATO and the European Union have taken over the concept of a comprehensive or integrated approach to the individual and collective security process from its promoters and developers, the Organization for Security and Co-operation in Europe[2] (OSCE) and the United Nations (UN), in order to initiate and develop security cooperation at regional and international level according to regional particularities, international legal provisions and common security interests, needs and safeguards.

The importance of security cooperation for the successful approach to collective security

Romanian National Defence University
e-mail: *craciun64@gmail.com*
****ROU NAVY***
e-mail: *valentin.vlad@navy.ro*

process is well emphasized by the OSCE in its own security concept, where it is seen as *"beneficial to all participating States while the insecurity in and/ or of one State can affect the well-being of all"*[3].

As a consequence, ensuring and maintaining internal security, individually and collectively by each state, is seen as defining for regional or international common security, stability and prosperity, in compliance with the provisions of the international treaties and fundamentals laws (UN Charter), which will ensure the credibility and legitimacy of the entire security process in the end.

The adoption of a comprehensive approach to the process of securing Euro-Atlantic maritime security at NATO and EU level is determined on the one hand by the fact that all member states of the two organizations have assumed a comprehensive approach together with their member state of the UN and OSCE, and on the other hand that they have adopted, developed and implemented this approach in their own concepts and strategies by combining political, civilian and military instruments[4].

Thus, the dynamics and the diversity of challenges and threats to Euro-Atlantic and international security prompted NATO to reassess and adapt its predominantly politico-military response options[5], bringing on the NATO Summits' agendas in Bucharest (2008) and Lisbon (2010) the concept of comprehensive approach as a consequence of the idea that *"military means, although essential, are not enough on their own to meet the many complex challenges to our security"* [6], unless these are complemented by interinstitutional and multi-country measures to ensure the development, stability and self-sustaining of the security environment at regional and international level.

The success of the comprehensive approach to the Euro-Atlantic security process is closely linked to the opening of the Alliance to regional cooperation and consultation with relevant actors, international institutions and organizations for security and cooperation in order to promote democratic values and strengthen mutual trust, as is also stipulated in the Charter of the United Nations[7].

One year after the Lisbon Summit, the direction of the new Strategic Concept[8] was already mirroring itself in the new Allied Maritime Strategy[9] which placed the actions of allied maritime capabilities under the comprehensive Euro-Atlantic security approach to crisis management and maritime security through cooperation (dialogue, partnership, consultation).

In this respect, NATO's maritime component is recognized and valued as the traditional feature of engaging in a comprehensive and fully-fledged approach to the Euro-Atlantic and international maritime space with other maritime actors interested in promoting and maintaining regional maritime security, also globally.

As part of NATO's comprehensive approach, the Allied Maritime Strategy aims to maintain traditional partnerships with relevant maritime actors (UN, EU) and to contribute to conflict prevention, developing maritime capabilities in line with current threats, maintaining freedom of navigation and enforcing the legal regime international shipping.

Also, within this comprehensive approach, the Alliance proposes that the planning process for potential maritime actions and operations should consider the possible consequences or influences they would have on regional or international agencies and organizations, partners or non-partners, but above all to exploit the benefits of attracting and actively involving them into the maritime security process.

The adoption of the comprehensive approach has materialized as a doctrinaire once allied implementation of the Allied Joint Doctrine[10] (AJP-01) in 2017, thus managing *"to harmonize Alliance actions with the efforts of international organizations and NGOs"*[11] by assuming as objectives to develop cooperation with partners and therefore to increase NATO contribution beside them for regional and international stabilization and reconstruction.

Essentially, adopting the comprehensive NATO approach is clearly delineated by the unilateral positioning and firmly declares its readiness and openness to inter-institutional and multi-country cooperation on the line of Euro-Atlantic and international maritime security.

Having the same freedoms and democratic values as NATO, it was natural for the European Union to show the same interest for the comprehensive orientation of its own maritime security process.

As a result, through the security and defense policies such as the European Security and

Defense Policy (ESDP) and the Common Security and Defense Policy (CSDP), the EU manifests its desire to address disputes and security crises in an integrated approach between the phase of their emergence and the process of political, social, military and economic reconstruction as characteristic to the process of reaching the desired final state[12].

The active involvement of the European Union alongside the United Nations, the North Atlantic Treaty Organization or other actors relevant to regional and international maritime security (China, India, Japan, Russia, USA) in combating piracy in the Aden Gulf and supporting Somalia to eradicate the causes of the pirate-like phenomenon and furthermore to develop regional countries' decision-making and action capabilities need it to manage illegal actions are good examples of a comprehensive approach to international maritime security with direct benefits to European and, implicitly, Euro-Atlantic maritime security[13].

As a consequence, the comprehensive approach to European security aims to increase the level of cooperation between the EU and its partners and to empower[14] all members to formulate complementary concepts and strategies that support the effort unity at the level of all military and civilian, governmental organizations[15] with direct effects on conflict prevention and the elimination of threats (terrorism, illegal migration, cross-border crime, arms trafficking) to regional and international maritime security.

The European Union's Maritime Security Strategy (EUMSS), which emerged in 2014 under the slogan *"the sea matters"*[16], is the proof of the full understanding of the importance of the Euro-Atlantic maritime space for European security and its anchoring to the regional security community concepts as promoted by Wagenen[17], Deutsch[18], Adler[19], Taylor[20], Cohen[21] or Mihalka[22] prove realism, measure and opportunity.

The main lines of action of the European Maritime Strategy follow the course of action defined by the integrated approach to maritime security and consist of initiating and developing regional maritime cooperation tailored to the particularities of the main Euro-Atlantic maritime basins (Baltic Sea, North Sea, Mediterranean Sea, Black Sea, Atlantic and Arctic Ocean).

The interest in the European maritime security comprehensive approach is highlighted by the fact that the EUMSS aims to cover *"both the internal and external aspects of the Union's maritime security"*[23] such as being a *"comprehensive framework, contributing to a stable and secure global maritime domain"*[24].

The EUMSS defines the political and strategic framework for involving all actors (military, civilian, governmental, non-governmental) at national, European and international level in order to overcome the challenges and combat symmetric or asymmetric threats to European maritime security within an inter-institutional and multi-country cooperation[25].

The entire European comprehensive maritime security process will seek to respect international legal requirements by channeling joint maritime security planning, risk management, conflict prevention and crisis response.

Conclusions

In conclusion, the Comprehensive Approach to Euro-Atlantic Maritime Security circumscribes perfectly the provisions of the UN Charter and the comprehensive approaches of the UN and OSCE, which also gives the Alliance and the Union equally credibility and international legitimacy as necessary for attracting and empowering all states, institutions or international agencies in the process of initiating and developing regional maritime security communities.

The dimensioning of maritime security communities at the Euro-Atlantic maritime basins subscribes the theory of streamlining the security process promoted by Taylor[26] and is the key element of the comprehensive approach by transferring the responsibility of maritime security to the regional actors, considering the regional geopolitics, particularities, opportunities and limitations and therefore connecting regional security to international maritime security.

Considering the direct contribution of NATO and EU to the Euro-Atlantic and international maritime security and the purpose and objectives of their own maritime security strategies, it can be said without any doubt that the Alliance and the Union are fully connected to the evolution of the Euro-Atlantic and international maritime security but there is a need to find out the optimal way to complement each other. Their comprehensive,

inter-institutional and multi-disciplinary approach is identified as essential to the success of the process of ensuring Euro-Atlantic, regional and international security, stability and prosperity[27].

NOTES:

1 Margriet Drent, *The EU's Comprehensive Approach to Security: A Culture of Co-ordination?*, Studia Diplomatica, 2011, LXIV-2, p. 3, accessed at URL: https://www.clingendael.org/sites/default/files/ pdfs/20111000_sd_drent_approach.pdf, at 26 May, 2019.

2 Conference on Security and Cooperation in Europe Final, OSCE, accessed at URL: https://www.osce.org/helsinki-final-act?download=true at 27 May, 2019.

3 The OSCE Concept of Comprehensive and Cooperative Security, OSCE, 17 June, 2009, accessed at URL: https://www.osce.org/secretariat/37592?download=true, accessed at 28 May, 2019.

4 A "comprehensive approach" to crises, NATO, 2016, accessed at URL: https://www.nato.int/cps/su/natohq/topics_51633.htm, at 30 May, 2019.

5 NATO official webpage, accessed on https://www.nato.int/nato-welcome/index.html, accessed at 30 May, 2019.

6 Lisbon Summit Declaration, NATO, 2010, accessed at URL: https://www.nato.int/cps/en/natolive/official_texts_68828.htm?selectedLocale=en at 30 May, 2019.

7 Charter of the United Nations, UN, chapter VIII, accessed at URL: https://www.un.org/en/charter-united-nations/ at 31 May, 2019.

8 Strategic Concept for the DefenCe and Security of the Members of the North Atlantic Treaty Organization, NATO, 2010, accessed at https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf, at 31 May, 2019.

9 Alliance Maritime Strategy, NATO, 2011, accessed at https://www.nato.int/cps/ua/natohq/official_texts_75615.htm, at 01 June, 2019.

10 Allied Joint Doctrine (AJP-01), NATO, 2017, accessed at URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602225/doctrine_nato_allied_joint_doctrine_ajp_01.pdf, at 02 June, 2019.

11 *Ibidem*, p. 1.6.

12 European Security Strategy – A secure Europe in a better world, EU, 2009, accessed at URL: http://www.consilium.europa.eu/en/documents-publications/publications/european-security-strategy-secure-europe-better-world/, at 03 June, 2019.

13 Fight against piracy, EU, 03 May 2016, accessed at URL: https://eeas.europa.eu/topics/maritime-security/428/fight-against-piracy_en, at 03 June, 2019.

14 EU enhances its comprehensive approach to external conflicts and crises, EU, 2013, accessed at URL: http://europa.eu/rapid/press-release_IP-13-1236_en.htm, at 03 June, 2019.

15 Lutz Feldt, Dr. Peter Roell, Ralph D. Thiele, *Maritime Security – Perspectives for a Comprehensive Approach*, ISPSW Strategy Series: Focus on Defense and International Security, No. 222, 2013, accessed at URL: https://www.files.ethz.ch/isn/162756/222_Feldt_ Roell_Thiele.pdf, at 04 June 2019.

16 European Union Maritime Security Strategy (EUMSS), UE, 2014, p. 2, accessed at https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT, at 04 June, 2019.

17 Donald J. Puchala, *International Politics Today*, New York, 1971, p. 165.

18 Karl W. Deutsch, et al., *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience*, Princeton: Princeton University Press, 1957.

19 Emanuel Adler, Michael Barnett, *Security Communities*, Cambridge University Press,1998.

20 Michael Taylor, *Community, Anarchy, and Liberty,* New York, Cambridge University Press, 1982.

21 Cohen R., Mihalka M., *Cooperative Security: New Horizons for International Order*, The Marshall Center Papers, No. 3, 2001.

22 *Ibidem*.

23 European Union Maritime Security Strategy (EUMSS), *op.cit.*, p. 2.

24 *Ibidem*, p. 2.

25 *Ibidem*, p. 3.

26 Michael Taylor, *op.cit.*, pp. 167-168.

27 *** A Global Strategy for the European Union's Foreign and Security Policy, EU, 2016, p. 9, accessed at URL: https://europa.eu/globalstrategy/sites/globalstrategy/files/pages/files/ eugs_review_web_5.pdf on 05.06.2019.

BIBLIOGRAPHY

*** AAP 6, *NATO Glossary Of Terms And Definitions* (English And French) Edition 2013.

*** A "comprehensive approach" to crises, NATO, 2016, accessed at https://www.nato.int/cps/en/natolive/topics_51633.htm

*** A comprehensive approach, NATO, 2009, accessed at https://www.nato.int/summit2009/topics_en/19-comprehensive_approach.html

*** A framework for enhanced international maritime security cooperation and awareness, CJOS COE, 2011, accessed at http://cjoscoe.org/docs/MSA_Strategic_Framework_V1.0.pdf

*** A Global Strategy for the European Union's Foreign and Security Policy, EU, 2016, accessed at http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

*** Allied Joint Doctrine (AJP-01), NATO, 2017, accessed at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602225/doctrine_nato_allied_joint_doctrine_ajp_01.pdf

*** Allied Maritime Strategy – A theory for success?, Kiel International Seapower Symposium Conference Report, 2018, accessed on https://www.

kielseapowerseries.com/files/ispk/ content/KISS18/KISS2018_final_Web.pdf

*** Alliance Maritime Strategy, NATO, 2011, accessed at URL: https://www.nato.int/cps/ua/natohq/official_texts_75615.htm

*** Charter of the UN, ONU, accessed at URL: https://www.un.org/en/charter-united-nations/

*** Conference on Security and Cooperation in Europe Final, OSCE, accessed at URL: https://www.osce.org/helsinki-final-act?download=true

*** Consolidated Version of the Treaty on European Union, UE, 2007.

*** Defence cooperation: Council establishes Permanent Structured Cooperation (PESCO), with 25 member states participating, Council of the European Union, 2017, accessed at https://www.consilium.europa.eu/en/press/press-releases/2017/12/11/defence-cooperation-pesco-25-member-states-participating/

*** EU defense cooperation: Council establishes a Military Planning and Conduct Capability (MPCC), Council of the European Union, 8 June 2017, accessed on https://www.consilium.europa.eu/ro/press/press-releases/2017/06/08/military-mpcc-planning-conduct-capability/

*** Council conclusions on the revision of the European Union Maritime Security Strategy – Action Plan, EU, 26 June 2018, accessed at http://data.consilium.europa.eu/doc/document/ST-10494-2018-INIT/en/pdf

*** EUCAP Nestor renamed as EUCAP Somalia, EU, accessed at URL: https://www.eucap-som.eu/eucap-nestor-renamed-as-eucap-somalia-new-website/

*** EUCAP Sahel Niger, EU, accessed at URL: https://eeas.europa.eu/csdp-missions-operations/eucap-sahel-niger_en

*** EU enhances its comprehensive approach to external conflicts and crises, EU, 2013, accessed at URL: http://europa.eu/rapid/press-release_IP-13-1236_en.htms

*** European Union Maritime Security Strategy, EU, 2014, accessed at URL: https://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT

*** European Union Maritime Security Strategy – Action Plan (EUMSS AP), EU, 2014, accessed at https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf

*** European Security Strategy – A secure Europe in a better world, EU, 2009, accessed at URL: http://www.consilium.europa.eu/en/documents-publications/publications/european-security-strategy-secure-europe-better-world/

*** Fight against piracy, EU, 03 May 2016, accessed at URL: https://eeas.europa.eu/topics/maritime-security/428/fight-against-piracy_en

*** Joint declaration on EU-NATO cooperation by the president of the European Council, the president of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, EU, 2018, accessed at https://www.nato.int/cps/en/natohq/official_texts_156626.htm.

*** Lisbon Summit Declaration, NATO, 2010, accessed at https://www.nato.int/cps/en/natolive/official_texts_68828.htm

*** Maritime security: EU revises its action plan, EU, 26 June 2018, accessed at https://www.consilium.europa.eu/en/press/press-releases/2018/06/26/maritime-security-eu-revises-its-action-plan/

*** NATO Strategic Concept, NATO, 2010, accessed at https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

***, NATO official webpage, accessed on https://www.nato.int/nato-welcome/index.html.

*** Sahel Region, URL: accessed on https://www.britannica.com/place/Sahel

*** Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization, NATO, 2010, accessed at https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

*** The OSCE Concept of Comprehensive and Cooperative Security, OSCE, 17 June 2009, accessed at URL: https://www.osce.org/secretariat/37592?download=true

*** The North Atlantic Treaty, NATO, Washington DC, 1949, accessed at http://www.mae.ro/sites/default/files/file/pdf/TRATATUL%2520NORD-ATLANTIC.pdf

*** United Nations Convention on the Law of the Sea (UNCLOS), UN, 1982.

Adler E., Barnett M., *Security Communities*, Cambridge University Press, 1998.

Cohen R., Mihalka M., *Cooperative Security: New Horizons for International Order*, The Marshall Center Papers, No. 3, 2001.

D'Aponte T., *A geopolitical overview on the Mediterranean Sea the approach of the euro-med policy towards the countries of the southern front (from Morocco to Egypt)*, Rivista Italiana di Economia Demografia e Statistica, Volume LXVIII n.2, Aprile-Giugno *2014.*

De Coning C., *The United Nations and the comprehensive approach*, Danish Institute for International Studies, Report 2008:1, accessed at URL:https://www.diis.dk/files/media/publications/import_efter1114/report-200814_the_united_nations_and_the_comprehensive_ approach.pdf

Deutsch K.W., et al., *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience*, Princeton: Princeton University Press, 1957.

Drent M., *The EU's Comprehensive Approach to Security: A Culture of Co-ordination?*, Studia Diplomatica, 2011, LXIV-2, accessed at https://www.clingendael.org/sites/default/files/pdfs/20111000_sd_drent_approach.pdf

Feldt L., Dr. Roell P., Thiele R. D., *Maritime Security – Perspectives for a Comprehensive Approach*, ISPSW Strategy Series: Focus on Defense and International Security, No. 222, 2013, accessed at URL: https://www.files.ethz.ch/isn/162756/222_Feldt_Roell_Thiele.pdf

Fransas A., Nieminen E., Salokorpi M., *Maritime Security and Security Measures – Mimic Study in the Baltic Sea Area*, Kymenlaakso University, Kotka, Finland, 2013.

Glaser C., *The Security Dilemma Revisited*, World Politics, Vol. 50, No. 1, 1997.

Horrell S., Nordenman M., Slocombe W.B., *Updating NATO's Maritime Strategy*, Brent Scowcroft Center on International Security, July, 2016.

Hoyt T.D., Winner A. C., *A Cooperative Strategy for 21st CenturySeapower: Thinking About the New US Maritime Strategy*, Maritime Affairs, National Maritime Foundation, Vol. 3, No. 2, 2007.

Kaim M., Kempin R., *A European Security Council Added Value for EU Foreign and Security Policy?*, German Institute for International and Security Affairs – SWP, 2019.

Pirozzi N., *The EU's Comprehensive Apprroach to Crisis Management*, DCAF Brussels, EU Crisis Management Papers Series, June, 2013.

Proelss A., Müller T., *The Legal Regime of the Arctic Ocean*, Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht, 2008.

Puchala D., J., *International Politics Today*, New York, 1971.

Roberts P., *Will the Alliance discover navies again?,* NATO Review Magazine, NATO, 30 April, 2018.

Stohs J., Dr. Bruns S., *Maritime Security in the Eastern Mediterranean*, Kiel International Seapower Symposium 2017, Kiel, 2017.

Taylor M., *Community, Anarchy, and Liberty,* New York, Cambridge University Press, 1982.

RISKS AND THREATS IN THE CURRENT OPERATIONAL ENVIRONMENT

LtCol. Associate Professor Alexandru HERCIU, PhD*

The dynamic evolution of the phenomenon of warfare from its classical-conventional physiognomy to a predominantly unconventional one, manifested in extreme environments (cyberspace, electromagnetic environment, informational environment, CBRN environment, human psyche) today and in the predictable future, is the consequence of the continuous adaptation to the complexity of today's challenges to humanity. These challenges are expressed and established in the literature by the terms: hazards, risks, threats, vulnerabilities.

Keywords: hybrid threat; asymmetry; irregular component; unconventional component.

Introduction

Contemporary conflicts display the physiognomy of wars of attrition, in which superior conventional forces are attracted to areas that place them in unfavorable positions, ambushed and then harassed to complete wear. This tactic is applied by an inferior enemy, who has the advantage of knowing the terrain perfectly and is usually supported by the local population. Today, these operations take place in the urban jungle, characterized by continuity and at the same time by the different intensity of hiring the opposing forces by the hybrid adversary.

In the case of hybrid conflicts, the tendency regarding the share of the typology of actions in terms of the dangers, risks, and threats that define them, exhibits a shift from regular, traditional to unconventional and especially to asymmetric ones. They tend to become generalized and manifested throughout the conflict and throughout its spectrum.

They will also express themselves in the future by coordinated actions, especially in low visibility conditions, without a distinct fingerprint, which will lead to an intense and constant rhythm of struggle. In order to fulfill this imperative, the military force will be a carefully proportioned conglomerate of types of units that are capable of engaging the opponent who develops hybrid actions on each component in a distinct but coordinated manner to maintain continuity and a high rhythm of operations.

From this point of view, the armed forces must be prepared to execute a wide range of missions in a joint and multinational context in different regions and a complex operational and consequently uncertain environment. They will face a variety of hybrid threats and simultaneous combinations of actions that will change and adapt permanently.

This fact requires the anticipation, identification, and understanding the goals of a wide variety of actors, with a role in conflict resolution, from the planning phase of the operation to integrate, coordinate and synchronize their efforts.

We consider that hybrid threat is the highest operational risk in the near and medium-term and therefore are the focus on a possible engagement of a joint multinational force.

Aspects of the concept of "hybrid conflict"

Hybrid threats occur where conventional, irregular, and asymmetric threats overlap in time and space. The conflict may involve individual participants, groups, or states operating at the local, transnational, or global level. Such conflicts may include acts of violence within communities, acts of terrorism, cyber-attacks, insurgency, crime, or disorder.[1]

From the analysis of the above, we can synthesize the concept of "Hybrid Threat (HT)".[2] In the perception of American military theorists (analyzing the particular conditions of military experiments in Afghanistan and Iraq), it expresses

*"Carol I" National Defence University
Land Forces Department within Command and Staff College
e-mail: herciu_alexandru12@yahoo.ro

the combination of conventional military forces endowed with sophisticated weapons, complex command and control systems (C2) and combined tactics with irregular elements such as insurgents or criminal organizations.

This combination of both conventional and irregular forces, the ability of these forces to migrate and transform in both directions, resulting in unrestricted violence against weaknesses, makes the hybrid threat extremely effective. In order to attain the "hybrid" frame, these entities (military units, rebel factions, criminal groups, guerrillas, terrorists, insurgents, separatists, partisans) will cooperate in the context of their interests.

It is therefore considered that future conflicts cannot be viewed separately, by types of threats or separate challenges. Most likely, armies must be able to cope simultaneously with all types of threats, to be able to operate successfully against all types of opponents in complex conflicts in all possible environments. This is, according to the authors, the essence of the hybrid war.[3]

As for the theory and practice of hybrid warfare, the Russian approach differs from the American one. In the conflict in Ukraine (2014), Russia applied a range of actions that resulted in the achievement of its political goals, besides a declared classical war. In February 2013, Valeri Gherasimov, Chief of Staff of the Russian Army, wrote in an article published in the VPK Russian Defense Journal, that war and peace are becoming increasingly mixed. Conflict methods have changed and now involve extensive use of political, industrial, information, humanitarian, and non-military measures. All this, he said, can be supplemented by attracting the local population and using the disguised armed forces.[4]

In light of the events which occurred a year later, the statement by the Russian military official demonstrates the premeditation and the conscious application of hybrid actions. These resulted in the urgent annexation of Crimea and the proclamation of New Russia's independence. General Gherasimov continues in his speech: "The rules of employment have changed significantly. The use of non-military methods to achieve political or strategic goals has, in some cases, been far more effective than using force. [...] The widespread use of asymmetric means can help neutralize the enemy's military superiority. This includes the use of special forces and internal opposition to create a permanent front within an enemy state, and the impact of propaganda tools, forms, and methods that are continuously improved."[5]

From the study of these attempts to explain and define the "war or hybrid conflict", we consider that it is a strategy that includes both a multitude of different actors (state, non-state actors, sponsor states), but also multiple hazards, risks, and threats (non-conventional nuclear forces, Special Operations Force, Chemical, Biological, Radiological and Nuclear Weapons – ADMCBRN, and Toxic Industrial Materials-TIMs). All these occur:

- In the physical environment, of conventional nature (conventional military forces in the legitimate state service);
- Through unconventional forces and means (such as nuclear forces; special operations forces; chemical, biological, radiological and nuclear weapons of mass destruction – CBRN WMD; Toxic Industrial Materials-TIMs; and improvised explosive devices – IEDs);
- In asymmetric forces (guerrillas, insurgent groups and activated separatists, terrorist, and criminal organizations).
- In the virtual cybernetic (informational) environment that has become a favorite in recent incidents.

All of them are engaged in combat in a combined and coordinated manner, against a superior adversary in military forces and means.

Typology of risks and threats in hybrid conflicts

In general, the phrase "risks and threats" is used without necessarily differentiating the meanings of the two notions. Used together, at first glance, we could understand that the risk relates to the object that could generate a specific hazard at a given time and under certain conditions, the source of the danger – the first one to manifest itself. The threat involves the fulfillment of these conditions and the imminence of hostile event occurrence by an aggressor (the author), an explanation that is not far from the truth.

In our opinion, the risk is part of the threat, the first identified indication of the potential danger concerning the purpose in which it could be used. The "threat" state is generated to the extent to which the identified risks could be exploited as well as

the recognition of the target, in the conditions of gradual amplification of the state of danger or even the direct passage from a very low threat level to one very high. In other words, one or more risks of a specific type can generate a threat of the same nature.

When it comes to risks and threats in the context of the contemporary operational environment, frequently defined as "a system of systems in which each actor involved seeks to realize his interests", in a hybrid conflict, we should also approach issues from this perspective. The strategy adopted by a potential opponent is complicated, complete, and manifests itself in all the variables of the operational environment. It is a conglomerate of conditions, circumstances, and influences that influence the engagement of capabilities and limits the commander's decision.[6]

Concerning the issue of "hybrid threats", the Romanian Army Doctrine uses the construction in the sense of those threats that are generated by an opponent capable of performing both classical and asymmetric actions, in a simultaneous and coordinated manner. It targets the exploitation of the vulnerabilities outside the legal framework, making it difficult to anticipate. [7]

Once these vulnerabilities have been identified, the opponent will try to achieve its goals by any means, using available resources at the right time and place. Thus, this is intended to create effects on vulnerable elements that, once affected, produce the desired changes, and ultimately achieve the objectives.

Depending on their nature, hybrid risks and threats can be split into:

a) Conventional risks and threats;

b) Unconventional risks and threats;

c) Asymmetric risks and threats.

Depending on the environment, hybrid risks and threats may be a combination of:

a) Risks and threats encountered in the physical environment;

b) Risks and threats encountered in the virtual (information) environment.

The overlapping of the risks and threats manifested in these plans and dimensions generates a potpourri of unique complexity, expressed in the literature in the combination of "Hybrid Threats".

Asymmetric (irregular) risks and threats

The last decade of the 20th century and the first decade of the 21st century were stages marked by the two wars in Iraq (1991 and 2003), Afghanistan (2001), Georgia (2008) and Ukraine (2014). These confrontations involved regular forces and proved that, from now on, the wars waged by the direct engagement of conventional armed forces tended to become a matter of the past. We advance this statement because of the disproportionate, irrational nature of the result of the different military potential and the apparent outcome. Therefore, military intervention is not always the optimal or necessary solution for achieving the purpose of the war.

Our analysis of the social phenomenon that is war, from the perspective of its hybridity, leads us to two central judgments, namely:

- When conventional forces have been used to punish leaders or governments for unwarranted actions, policies or divergent orientations, we are dealing with a total physical asymmetry, a net superior advantage in forces and means from the aggressor;

- The percentage of the conventional ingredient in the economy of war tends to decline, becoming a deterrent and intimidating force to achieve goals by other means designed to replace military action.

From this perspective, we consider that currently and in the future, the tendency to express the conventional confrontations is to be replaced by conflicts carried out with unconventional means and methods, asymmetric by nature.

Simultaneously with the wars mentioned above, at this stage of transition to a new era of armed confrontations, a series of conflicts of armed groups of different values and origins took place. They aim to achieve their goals by means and ways of gaining the advantage over a conventional superior aggressor, and thus of an asymmetry other than that obtained through technological capabilities, potential or decision-making and action superiority.

The causes which may feed future conflicts are:

- The persistence of social inequalities;

- The adverse effects of the perpetual process of globalization;

- Inequitable distribution of resources and unequal economic development;

- The activation, revival and feeding of the traditionalist and ethnic movements as a form of resistance to assimilation in various forms.

Their asymmetric character results from the lack of visibility, the nature of objectives, and ideas that contradict the generally accepted values, beliefs, priorities, legal and moral constraints, as well as the unconventional methods it uses to overcome the superiority of opponent[8] or to influence and control the masses.

This type of threat refers to those actions that involve the use or threat of use of force by irregular forces, groups or individuals, usually ideologically or critically motivated, to cause change or preservation of a specific state of affairs, which is a challenge for government or state authority.[9] Their specificity is represented by the ambiguity, levels of operations, and the status of the actors involved.[10]

The most representative asymmetric risks and threats are insurgencies, guerrilla, separatism, terrorism, and organized crime. In the following lines, we will analyze the main peculiarities of the most representative of them.

Insurgency/insurrection. The term insurgency comes from the Latin word "insurgent" borrowed in French as "insurgence" used in the sense of insurrection, uprising and rebellion; [11] it is a form of armed struggle, organized by rebellious forces, to change the existing political situation, [12] using subversion and violence [13].

Unlike other forms of asymmetric struggle, the specificity of this type of uprising consists in the support and participation of popular masses or of a significant part of them, against a reactionary political regime, or for the expulsion of an occupying army from the national territory. The overthrow/ dissolution of the legally constituted government is achieved through subversive actions and armed conflict.

As a rule, broad popular consensus and support is obtained and mobilized around the idea of social injustice, considered legitimate and often ideological, but may also be based on criminal ambitions. In order to achieve the desired goal, insurgents seek to take full advantage of the operational environment, trying to determine political change through the conviction and coercion of the population, concentrating their efforts on highlighting and exaggerating perceived, real or fabricated injustices.

The insurgency can be considered an irregular activity, carried by a movement or an organized group. This can be included on a broader range of irregular actions, which, as a whole, signifies a threat to states or human society, especially in less stable regions of the world. Insurgency can be considered to be the fundamental irregular activity due to the character and nature of its causes. It can also turn to other types of irregular actions in order to reach the desired end.

Insurgent groups are armed groups belonging to rebel movements with social, ethnic, or religious claims that struggle to determine the political change in a particular geographical or administrative area and benefit from population support.[14]

We consider that uprisings, insurgency, insurrection are different stages of an ideological movement. The uprising is the first stage of expressing a feeling of dissatisfaction with the political situation or government authorities, which is spontaneously manifested and can turn into a violent insurgency movement.

As the popular masses support is gained, while weakening legitimate political power, the insurgency movement fulfills its political goals and acquires the characteristics of insurrection. Therefore, if the uprising is a spontaneous action, manifested at a particular moment and in a specific place, insurgency as a form of struggle gains local or regional character. It tends to grow in intensity and as an area of territory and population up to when it grows at the national level and meets the conditions for producing political changes.

Guerrilla. The term "guerrilla" comes from Spanish, and has been taken in French with the form of "guerilla" and defines those irregular forces operating in occupied or controlled territories by the enemy. These forces act according to the rules of attack by surprise, harassment, destruction and even terrorist means and pursue limited local goals (overthrowing a government, getting rights, state independence, territorial separatism or autonomy, conquering political power).

The name comes from the partisan war in Spain and the Latin American countries, where the "guerrilla" designates a band of partisans, adepts of an idea/doctrine, a fighter for a common cause, in a formally unstructured detachment. [15] Guerrilla war is defined as those militaries, or paramilitary operations carried out in hostile territory held by

the enemy by irregular, predominantly indigenous forces. [16]

Formations of partisans/resistance groups are those groups of fighters who come from civilian or former military personnel from occupied territories. They place the cause of the liberation movement before their interest and act violently on an independent invader or in co-operation with regular conventional forces, through tactics specific to the guerrilla [17].

Guerilla aims at striking a superior adversary in the identified vulnerabilities, without any logic and ethics, rhythmicity, or other rules. Guerilla acts permanently, day and night, everywhere and by any means against a regular army of occupation, with high fighting capacity, but not by the tactics of an army, but by actions specific to the harassment war (attacks, sabotage, ambush, incursions, raids).

The ultimate goal of the guerrilla is not to achieve victory in terms of decisive defeat of the occupation forces, but to attract and maintain them in a perpetual war, wear and weakness. Undertaking small-scale attacks, specific to the guerrilla, with the fulfillment of limited objectives, should be analyzed from a perspective of judicious planning and coordination so as to have an accurate perspective of the magnitude and effectiveness over time of this type of resistance movement.

Another defining characteristic of the guerrilla is the superiority of knowing the confrontational environment, being covered and supported by the population in the area, which allows it to strike and retreat. This aspect is considered to be operationally significant and distinguishes between this asymmetric threat and all the others. Therefore, the guerrilla is considered to be a phenomenon complicated to control and counteract.

Structured terrorism. Terrorism designates all actions committed by a group or organization by deliberately and systematically using violent means or threats of a kind to cause fear and mistrust, panic and insecurity, ignoring any humanitarian norms.[18]

The aim is to create a climate of insecurity through the practice of terror, directed against the objectives selected based on the representative symbol of a superior adversary, usually a state nation (dignitaries, military commanders, majority or minority population, national symbols, religious symbols, symbols and values of democracy). Fighting these targets facilitates the fulfillment of political, religious, or ideological goals by non-state actors by acting themselves or coordinated with other actions.

Depending on the motivation it generates, terrorism can be of an ethnic, nationalistic, and ideological nature. Depending on the nature of the exploited risk we identify chemical, biological, radiological and nuclear (CBRN) terrorism; environmental terrorism; cyber terrorism; those who practice the assassination; hijacking of planes; abduction of persons; under different motivations.

Terrorist cells are the elements of execution of terrorism. They are, in particular, those who ensure the achievement of the goals of the rebel, extremist, fundamentalist terrorist groups through actions that have a psychological impact on the masses. Their actions lead to political or military constraints in favor of them, by state or leaders.

The defining elements of terrorism are:

- The extreme violence carried out by surprise, directed against highly vulnerable civilian targets on or outside national territory; and

- The devastating psychological impact on human communities, non-discriminatory effects, and the media broadcasting of attacks.

If in the case of other forms of asymmetric manifestation of the hybrid conflict we are dealing with recognized facets of the war, we can say that terrorism has nothing to do with the war, because of its means of acting against civilian targets in a non-selective way.[19]

Organized cross-border crime. The term "organized crime" defines the existence of criminal groups at a given time in society, structured in "branches" on the principle of belonging to one of their illegal activities, in order to obtain significant illicit income.

Criminal organizations are generally built into pyramidal structures (gangs, drug cartels, mafia families, triads, thieves' associations, traffickers, clandestine laboratories and printers and more recently, "academies of criminals"). These organizations are based on strict internal discipline rules and a Code of Conduct, built around the defense of the secrecy and conspiracy at any cost. The roles of the members are clearly established within the hierarchy (strict specialization).

The leader of the criminal group usually exhibits a dictatorial leadership style based on the principle

of total and unconditional loyalty, suppression of freedom of thought, exemplary punishment of deviations from the group's rules and strict access to information on group organization, activity, training and recruitment of new members.

The main representation of organized crime is corruption, as a result of the use of financial means, in order to obtain economic or political advantages by using forms of coercion, blackmail, bribery, buying off, influence or intimidation.

False insurgency or guerrilla movements. Typical manifestations of armed criminal groups in the hybrid conflict often take the form of false insurgency or guerrilla movements. These criminal activities are carried out in failed or underdeveloped countries, in regions rich in natural resources and where the control of authorities is non-existent or inefficient. Violent actions are most often directed against the civilian population in order to terrorize and maintain control over the area and communities, to obtain the material and financial benefits of collecting products and taxes. Unlike the resistance movement, which has as its leading mobile a noble cause, which prevails over the personal interest of fighters, the fight against false guerrillas is based on the personal and group interest of its members. In these circumstances, guerrilla specific actions against security forces aim at surviving the organization and preserving the economic benefits and psychological superiority.

Criminal insurgency differs from the classical insurgency. The criminal insurgency can be defined as the activity of groups with economic interests that create their production facilities, transport, and markets for illegal products. This type of insurgency deals with illegal activities such as arms trafficking, narcotics, human beings trafficking, kidnapping, slavery, blackmail and any other profitable criminal activity. Transnational criminal groups, organized in cartels, create self-supporting and complementary networks with other criminal groups with which they cooperate to control illicit product markets. Aspects related to the work of false insurgency groups are linked to the illegal economic nature, clandestine, extremely violent criminal activities of punishing and intimidating the civilian population and government authorities. They have to demonstrate their determination, influence, corruption and undermining political power, the ability to control regions and law enforcement agencies.

Risks and threats in the virtual (information) environment

Information Operations (INFOOPS). This is a component of the spectrum of military operations and includes the military actions directed, planned, and conducted to influence the decision-making process of a potential adversary. They facilitate the achievement of political and military objectives by influencing the will of the leaders. [20]

This type of operation affects the quality of information and the information process of the enemy, while at the same time operating safely and protecting the own system. They involve the integrated engagement of a wide range of capabilities, tools and techniques to achieve specific effects in support of operations. This type of action will be integrated at all levels of operations and will be applied across the entire spectrum of missions. Effects in the information environment can be created through a variety of coordinated military actions that will contribute to the overall goal of the operation.[21]

INFOOPS are conducted in order to maintain the decision-making and acting superiority against the existing or potential external influences of the opponent and are accomplished by actions of:

- Influencing the perceptions and attitudes of the opponent or potential opponent (influencing activities);
- Information protection focused on maintaining freedom of maneuver in the information space by protecting data and information supporting decision-making (information protection activities);
- Attack the data and information delivery system that supports the enemy or potential enemy C2, information, surveillance and target acquisition systems (activities directed against command and control system).

The objectives of the information operations are achieved through the planned and coordinated synchronization of military capabilities, tools and techniques that influence, and protect information or information systems. These are psychological operations:

- presence, attitude and posture;
- information security operations (OPSEC);
- information security (INFOSEC);
- deception;
- electronic warfare;
- physical destruction;
- engaging key leaders;
- computer network operations (CNO).

Psychological Operations (PSYOPS). There are non-violent actions of psychological nature, planned and conducted to influence attitudes and behaviors in the sense of facilitating the achievement of political and military objectives. Psychological operations can be considered a real "war of mind against the mind".

Psychological operations (PSYOPS) seek to discredit or, on the contrary, improve the image of governments or leaders, sometimes creating confusing situations, easy to exploit, discouraging some initiatives and encouraging others. Psychological operations are based on a vast database of geographic, political, economic, cultural, religious, psychosocial, history, tradition, habits and infrastructure information regarding a theater of operations.

Psychological operations also involve the diffusion of tampering adverse documents in order to discredit opponents and produce conflicts and disagreements among them. Misinformation (the manipulation of information), an essential element of psychological warfare, begins in peacetime before the conflict itself and has very complex objectives, generally pursuing psychological destabilization and polarization of the population. Manipulation intensifies with the preparation and initiation of the first phases of the conflict.

PSYOPS retains direct control over content, dissemination and audience. The effectiveness of psychological operations requires the early preparation of resources such as linguistic support, graphic and print capabilities, radio and TV broadcasting capabilities and other dissemination mechanisms.

Propaganda is a frequent political practice of peace among nations, as a form of indirect aggression instead of military aggression. In the Doctrine of Psychological Operations of the US Armed Forces of 2003, one of the few official definitions of propaganda in a military doctrinal document can be found. It is defined as "any form of communication in support of national goals to influence the opinions, emotions, attitudes or behaviors of any group of people, for the direct or indirect benefit of the sponsor of this communication." [22]

Here, propaganda is classified into:

- *Black Propaganda*, in which it is understood that the information would emanate from a source other than the real one;

- *Gray Propaganda*, where the source is not identified;

- *White Propaganda*, where either the source or sponsor is known to the public.

The International Court of Justice cannot rule out the protection against psychological aggression because they cannot be legally incriminated. The only defense is the use of the same means of psychological warfare. Because the propaganda targets a foreign adversary, it is up to each government to defend its state against the aggression of propaganda. [23]

From the above, it follows that the opponent who develops hybrid actions uses the tactics of terror, aiming to identify and exploit those uncovered parts and vulnerabilities of the opponent, that is superior in military terms. The hybrid enemy aims to provoke a sense of insecurity and mistrust in the government's ability to secure the nation's protection and thus apply pressure on the political factor to achieve "victory", without engaging the military forces.

Achieving surprise. In the context of the hybrid conflict, the achievement of surprise becomes a critical condition. It is accomplished by performing some specific, precise actions on well-defined objectives with decisive effects on the morale of the forces and the leadership. Special forces, the elite structures (teams or detachments of special forces or commandos), prepared to execute actions with high power of destruction, will have an essential role in achieving success.

Terror tactics are the most effective combat methods used by the enemy who develops hybrid actions against opponents as part of the concept of "total war". Affiliated or independent terrorist groups can attack their opponent anywhere, anytime. Special Forces can also use the terror tactics for which they are well equipped, armed, trained and motivated.

The sensitive elements primarily targeted by the hybrid enemy are the civilian population and the environment. Therefore, the key to counteracting this type of threat is to adopt those education, supervision, monitoring, protection and active measures to reduce their vulnerability.

Peculiarities of asymmetric operations

The forces and actions specific to irregular warfare create favorable conditions for the emergence and development of asymmetries, which are often manifested in the context of conventional confrontation. These have the effect of defeating the opponent's forces. Some armed forces, especially those belonging to totalitarian regimes or states with defective governments, can cooperate with asymmetric, complementary actions in support of conventional military objectives. The effect of major combat operations can be exacerbated, perpetuated or exploited through asymmetric actions to keep instability through insurgency, terrorism, crime and social disorder.

Asymmetric operations comprise a broad range of military and paramilitary forces, which are usually supported by the indigenous population. Irregular forces can demonstrate the combined capabilities of separatist, insurgent, guerrilla, and criminal elements.

Irregular forces favor indirect [24] and asymmetric approaches. This form of war can engage the entire range of military actions and capabilities in order to erode the strength of their adversaries, their influence and their will. The typically irregular warfare is a wear and tear that erodes state and non-state regional opponents, and may have ramifications and connections with transnational actions as a result of political, economic and financial globalization.

Its purpose is to gain the legitimacy of actions and influence on the relevant population. Different types of irregular forces can use different levels of violent and non-violent actions to exert their influence. Access to technology will have an impact on irregular forces operations. In the context of the hybrid conflict, especially at the tactical level, they can apply standard techniques, tactics, and procedures to regular forces but will use asymmetric means and applications.

The conventional component of the hybrid threat, even under defeat conditions, can be reactivated or can be favored and sustained through irregular and asymmetric actions. Asymmetric operations aim at attacking the abstract components of the adversary's effort, against the hybrid threat, such as: the motivation to fight and trust the soldiers and commanders, political and diplomatic decisions, public opinion, the interests of private institutions, the nation's will to fight and support the war effort, will and collective involvement of alliances and coalitions.

One of the most dangerous aspects of the hybrid threat is the ability of its components to become "inside" and "outside" in extremely varied forms. For example, native military forces can strip their uniform, signs and other indicators of their state and belonging, and they can mix and hide among the local population. The insurgent forces can abandon the weapons and innocently protest in the opposite direction.

Criminals can wear the uniform and harness of local police forces to gain access to essential targets. Hybrid threats will benefit from the difficulties of a clear identification of the actors, threat as a threat, a situation that is to their advantage. The operational environment abounds in actors doing activities against the interests of member states of the supporting force, but without a visible, clear signature of their status as a threat. Often these actors will leave the imprint impression similar to the opposing or neutral forces.

In conclusion, we consider that opponents of hybrid threats will encounter severe difficulties in identifying and separating the "set of problems", specific to each type of threat. They will be forced to apply force-building measures to cover more lines of operation. The hybrid opponents will continue to move their effort and permanently point out that whatever option they choose as inappropriate.

Conclusions

From the conventional, unconventional and asymmetric risks and threats, a new concept called "Hybrid Risks and Threats" emerges, which manifests itself in the contemporary operational environment and involves complex approaches to information, decision and action.

From the analysis of the specific properties of the risks and threats that occur both in the physical space and those in the virtual environment, they can affect national, regional or global security, and can lead to planning, preparation and execution of hybrid military actions.

The great military powers of the world – such as the US, Russia or an international coalition of states – can now be easily challenged against a conventional opponent. The major challenge of today and the predictable future is not this, but

rather the way in which the potential opponent will organize assets, adapt and fight, developing unique capabilities such as weapons of mass destruction or asymmetric crime and environmental terrorism. They will be directed against people and their living environment to counterbalance and achieve their strategic goals.

NOTES:

1 *AJP-2(A), Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), Draft 2012, pp. 1-2.

2 Training Circular No. TC 7-100, *Hybrid Threat*, Headquarters Department of the Army, Washington DC, July 2010, p.v.

3 Valerică Cruceru, *Războiul hibrid în gândirea militară americană (Monografie)*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2015, p. 28.

4 Ana Stan, *Rusia a ridicat războiul la rang de artă* (articol), 02.09.2014 available at adev.ro/nb9y9f accessed at March 3, 2015.

5 Valery Gherasimov, *Tsennost nauki v predvidenii*, Voyenno-Promysblennz Karyer, 8(476), 27 februarie 2013, available at http://www.vpk-news.ru/articles/14632 accessed at April 2, 2014.

6 *AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012, p.2-O-3.

7 ***Doctrina Armatei României*, Bucureşti, 2012, p.173.

8 *AJP-01(D), Allied Joint Doctrine*, December 2010, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), pp.2-7.

9 ***Doctrina Armatei României*, Bucureşti, 2012, p.121.

10 Teodor Frunzeti, *Convenţional şi neconvenţional în acţiunile militare*, în revista CSSAS *Impact strategic* nr.4[45]/2012, p.8.

11 Available at dexonline.ro accessed at July 28th, 2019.

12 T.C.-7-100, Department of the Army Training Circular No. 7-100, *Hybrid Threat*, pp.2-1.

13 *AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012, pp.2-I-5.

14 Valerică Cruceru, *Theory and practice in modern guerilla warfare (Short review)*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2013, p. 20.

15 Available at dexonline.ro accessed on July 28th, 2019.

16 *AAP-6, NATO Glossary of Terms and Definitions*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012, p. 2-G-4.

17 Valerică Cruceru, *Theory and practice in modern guerilla warfare (Short review)*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2013, p. 20.

18 Available at dexonline.ro accessed at July 28th, 2019.

19 Valerică Cruceru, *Theory and practice in modern guerilla warfare (Short review)*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2013, p. 21.

20 ***Doctrina Armatei României*, Bucureşti, 2012, p.134.

21 *AJP- 3(B), Allied Doctrine for the Conduct of Operations*, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 16 March 2011, pp. 1-17.

22 Călin Hentea, *Operaţiile informaţionale sau noile haine ale propagandei*, available at www.lumeamilitara.ro/ accessed at April 25, 2015.

23 Mihaiu Mărgărit, *Ucraina şi războiul hibrid, în tentativele Rusiei expansioniste ale Moscovei de revenire a ei la masa marilor decizii ce privesc geopolitica mondială*, Pulsul Geostrategic, Nr.175, 20 Septembrie 2014, available at www.ingepo.ro accessed at July 28, 2019.

24 ***Conducere militară planificare operaţională* (Curs universitar), Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2009, p. 29.

BIBLIOGRAPHY

*** *Military management operational planning* (University course), Publishing House of the National Defence University "Carol I", Bucharest, 2009.

*** The Doctrine of the Romanian Army, Bucharest, 2012.

AAP-6, *NATO Glossary of Terms and Definitions, North Atlantic Treaty Organization,* NATO Standardization Agency (NSA), 2012.

AJP-01 (D), *Allied Joint Doctrine,* December 2010, North Atlantic Treaty Organization, NATO Standardization Agency (NSA).

AJP-2 (A), *Allied Joint Doctrine for Intelligence*, Counter-Intelligence and Security, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), 2012 Draft.

AJP-3 (B), Allied Doctrine for the Conduct of Operations, North Atlantic Treaty Organization, NATO Standardization Agency (NSA), March 16, 2011.

Training Circular No. TC 7-100, Hybrid Threat, Army Headquarters Department, Washington DC, July 2010.

Cruceru Valerică, *The Hybrid War in American Military Thought* (Monograph), "Carol I" National Defence University, Bucharest, 2015.

Cruceru Valerică, *Theory and practice in modern guerilla warfare* (Short review), Publishing House of the National Defence University "Carol I", Bucharest, 2013.

Frunzeti Teodor, *Conventional and unconventional in military actions,* in the journal CSSAS Strategic Impact no.4 [45] / 2012.

Gherasimov Valery, *Tsennost nauki v predvidenii,* Voyenno-Promysblennz Karyer, 8 (476), February 27, 2013.

Hentea Călin, *Information operations or new clothes of propaganda*, on www.lumeamilitara.ro/

Mihaiu Mărgărit, *Ukraine and the hybrid war, in Moscow's expansionist Russia's attempts to return it to the table of major decisions regarding world geopolitics*, Geostrategic Pulse, No.175, September 20, 2014 on www.ingepo.ro

Stan Ana, *Russia raised the war to the rank of art* (article), 02.09.2014 on truth.ro/

www.vpk-news.ru/www.dexonline

PLANNING AND TEACHING STYLES IN MILITARY PHYSICAL EDUCATION

LtCol. Lecturer Gabriel Constantin CIAPA, PhD*

The success of acquiring information, whether theoretical or practical, depends to a large extent on the information's organization and structuring over well-defined periods of time, on its quantity, on the material basis available, but also on the quality and training of the military physical education specialist and on the way in which information is transmitted. Therefore, this material is divided into two parts. The first part deals, in a synthetic way, with the main documents of planning, organization and management of the military physical education activity, in some cases providing examples, in order to facilitate their understanding and performance. The second part of this article is directed to teaching styles in physical education, to the way of transmitting the information provided in the documents specific to military physical education, orientation that has in sight the teacher/specialist/trainer in this military branch.

Keywords: military physical education; plan; style; lesson; specialist; anticipation.

Introduction

The purpose of precise and valuable collective or individual training, anchored in the reality of the battlefield, must be based on the concrete aspects of the combat actions, carried out in the theaters of operations. Or, even in the case of military physical education, the completion of the training is also conditioned by this reality and by the projection in time of the information to be transmitted. In order to achieve a positive end, it is necessary for the military physical education specialist to possess a high level of knowledge, not only in the direction of the execution of motor actions, but also in the conception, in the precise and real planning to understand the phenomenon, and also increased interest in this military specialty.

If for the planning of the knowledge to be transmitted, vision and projection in time are needed – in my view, projection means performing an anticipation of the motor actions (in the case of military physical education) that the military personnel has to go through and ensuring the information and didactic framework, for meeting the objectives set, for the way the information is transmitted. It is necessary to have a high pedagogical teaching background, experience, openness to the new and, why not, patience. Each human being is an individual entity, with a distinct personality, with possibilities of assimilating knowledge in different rhythms and moments.

Planning in military physical education

In approaching the main planning documents in military physical education, we start from the certainty of the existence of the specifications regarding the necessity of preparing the main documents for the organization, planning and management of the military physical education.

As it is known, planning is an activity of a man who seeks to achieve specific goals. It is one of the most important activities, performed by the specialist/trainer of military physical education, and has a *"high degree of complexity... determined by a multitude of variables"*[1]. Such variables are: "The time period for which the cybernetic conception is elaborated, the nature of components of the physical education and sports model, the place of activity, the composition of the subject groups/classes by sex criterion, the composition of the subject groups/classes by the level of physical and motor training criterion"[2]. The documents based on which the specialist scientifically enhances the instructional-educational process are the following: *the thematic plan, the calendar plan and the lesson plan/didactic project* (for education) or *the activity plan* (for training).

***Military Technical Academy**
e-mail: *ciapagabriel@yahoo.com*

The first planning document is the annual *thematic plan*[3]. In accordance with the Regulation of military physical education, this document is mandatory. It is elaborated for a period of one year and includes the components of the instructional-educational process (motor qualities, skills and motor abilities), the number of lessons in which they are dealt with, their positioning in the training year, the time allotted to each of the components. Some specialized works also admit the mention of tests.

The completion of an annual thematic plan can be done considering several aspects: the number of thematic lessons can be higher or lower, depending on the general objectives to be achieved; in one lesson, one, two (the time allotted to each topic is determined by the specialist, depending on the purpose and complexity of the lesson) or three themes (time is usually allotted equally, but here, also, it is the complexity that determines the distribution of time) can be addressed; the time mentioned is not the maximum for the lesson, 50 or 100 minutes, the thematic components being allotted 60-70% of the total minutes, the rest being found in the beginning (1, 2, 3) and ending segments (7, 8).

The second document, *the calendar plan*[4], is also the most argued by all the great specialists. It is prepared for a shorter period, which may vary depending on the structure of the training year (quarterly, half-yearly, etc.). The calendar plan is prepared on the basis of the annual thematic plan, the components of the thematic plan can also be found in it. The major difference between the two is given by the *Appendix to the calendar plan*[5], a document that includes all the systems and means of action (physical exercises) for each thematic subcomponent: speed, skill, strength, etc. and by the codified completion in the calendar plan of these means of action. Such means of action are taken and filled in the *Appendix,* having as sources of inspiration various specialized manuals, specialty magazines, observation of other specialists. Other means can be mentioned and used, but only after they have been experimentally validated, in relation to the teaching tasks.

The means of action listed in the Appendix to the calendar plan must be very clearly described, specifying: *"the name of the motor act or action; the initial, intermediate or final position of the performer's body; the distance, duration or load of physical effort; the execution tempo; the number of repetitions; the duration of the pause between repetitions and its nature; the working group and the actual method of practice"*[6].

The means of action can be *simple: force*, F1 (F1 is exercise number 1, specified in the Appendix to the calendar plan, in the group of motor qualities) – from the position facial supported recumbent, flexion of the forearms on the arms, 2 x 20 repetitions, passive pause for 40 seconds between the series, frontal practice or *complex*: *football*, Ft2 (Ft2 is exercise number 2, specified in the Appendix to the calendar plan, in the group of motor skills and abilities specific to sports tests and branches), 1-2x, passive pause for 1 minute and 30 seconds; a) dribbling in a straight line on a distance of 25 m and executing a shot at goal, tempo 60%, 3 x, active pause for 20 seconds; working group: two rows of four students each; b) dribbling among six cones placed in a straight line at 2 m from each other, passing to a colleague who is located obliquely 5 m ahead of the last cone, receiving the ball again and executing a shot at goal; tempo 60%, 3 x, active pause for 30 seconds; working group: two rows of four students each.

The calendar plan is presented in two forms: *descriptive* – each means of coding is clearly filled in next to the thematic components and *graphic* – there is a coding next to the thematic components (1/2x, 3/4x, etc.). Whether it is conceived one way or another, the calendar plan must contain the same elements as the thematic plan to which it is added, mandatory *means of action* coded or clearly stated and *tests*. It is very important that in elaborating it, the following must be taken into account when recording the means of action: the time allotted through the thematic plan must be spent with the means of action and not exceed it, the way of filling in the boxes is not standardized – various written mention formulas may be chosen, so many means of action, as dosage, must be planned, so as to cover the time allotted to the theme in the annual thematic plan.

The third document of military physical education is *lesson plan/didactic project/activity plan* of the instructional-educational process. This document is the one that allows the achievement of the operational objectives of the lesson, which allows the management of the current lessons.

It represents the materialization of the detailed thinking of the specialist for carrying out the immediate tasks of the lesson. It is an embodiment of the anticipatory capacity of the specialist to meet the training objectives during the time allotted to the military physical education lesson.

In its preparation, a series of essential elements are followed, logically structured, in the same sequence each time. *The first element* aims to set the objectives that must be realistic, respect the allotted time, observe the training plans – the objectives are not addressed to the specialist, but they concern the military personnel; they must be explicit and show potential motor changes in the military; pursue a single operation through short expression; fit into a logical structure of general training. In order to understand the goal setting we will exemplify some of the keywords used in military physical education: list, state, describe, identify, cooperate, grant, execute, perform, development, improvement, verification, acquisition, consolidation, perfection, etc.

The second important *element* is found in the analysis of the human component available to the specialist (number of military personnel, sex, level of training), of the conditions for the instructional-educational process (materials, geoclimatic). *The third element* seeks to *"elaborate methodological-organizational strategies: allocation of the time allotted to the lesson for each segment, establishing the order of thematic approach"*[7]; choose the three "M"s (methods, means, materials) necessary to achieve the lesson objectives; effort dosing; working groups; types of practice.

The last, extremely important aspect, also called *"assessment of the efficiency of the current activity"*, aims to develop a system for assessing the quality of fulfilling the teaching tasks both by the military and by the leader of the instructional process. However, all these aspects of planning would be useless if they did not materialize concretely, if their content were not put into practice and if the teaching activity no longer took place.

Teaching styles in military physical education

Teaching in military physical education is defined as the activity of transmitting learning content, theoretical and/or practical, specific to the educational or training activity. Specifically, it involves the content presentation, explaining the essential aspects of notions, developing practical and theoretical skills, all of these being based on the objectives and purposes of this activity and of the social order.

The efficiency of teaching is also conditioned by the style approached by the specialist in military physical education. The typology of teaching styles was first developed by Mosston M. and Ashworth Sara from the desire to conceive a guide for teachers in the field. According to them, the spectrum consists of 11 styles, of which five are centered on specialist and six on student/military. Teaching styles are absolutely necessary because students/military must be able to assimilate what the specialist teaches.

However, the choice of teaching styles may depend on the specificity of the motor actions, the homogeneity of the group and its level of preparation, the ability to understand the knowledge, the objectives of the lessons, the educational level and the experience of the specialist and, most importantly, from my point of view, on the interest and moral-social value of the group for this form of training. Understanding that people assimilate information differently, it is clear that there must be different teaching styles to adapt to learning styles.

"The teaching style represents a set of behaviors selected and used by the specialist in order to achieve the educational objectives"[8]. We can say about the teaching style that it is given by the individual-particular way of accomplishing the teaching process. The teaching style used in the lessons is purely the choice of the specialist. In listing these teaching styles in military physical education, we consider two directions of analysis: depending on the approach of the activity, we find *order, practical, reciprocal, "personal verification", "inclusion" styles*; depending on the orientation of the action we have the direct and indirect style. To these styles others can also be added, which I place into a group of rather pseudostyles, when this way of transmitting information in the physical education system appears. These styles are the democratic and the negligent ones.

Order style[9]. The transmission of knowledge is made unidirectionally, the decisions being made only by the specialist, without the existence of any dialogue between the military and trainers in an

authoritarian, distant and cold way. It may represent the approach of the unprepared, confident, with teaching tendencies. In this case, only the military are to blame for the lack of knowledge, but this style is required and necessary when the military has to respond quickly and promptly to orders, when the safety of the performers is paramount and when the accuracy is sought. For example, this style can be used when a perfectly synchronized warm-up is required, in sports where synchronization is a requirement in order to obtain a higher score (synchronous swimming, martial arts, dance, etc.), in opening or closing festivities of major sports competitions, in marches and military parades.

Practical style[10]. The specialist demonstrates the motor act or action and sets the opportunity for the military to practice and develop their skills at their own pace. As the military perform the teaching tasks, the specialist will walk among them, providing individual and group feedback. For example, the specialist demonstrates how to perform a martial arts arm technique. As the students learn the technique, the specialist will go and provide an answer regarding the acquisition of this technique. Defining for this style is individual practice, even in private.

Reciprocal style[11]. The defining features for this style are highlighted by social interaction, mutual help, offering and receiving immediate response to the motor actions carried out with the help of a partner. The role of the specialist is to indicate what needs to be executed, to provide answers and indications during the execution of the motor act or action by the work partners. The military will work together, in pairs, constantly providing feedback on what is being done and what is not. Suggestive for this style are the gymnastic exercises performed with the help of a partner and also the technical procedures of the different sports of wrestling.

"Personal verification" style[12]. It is very similar to the reciprocal style, except that the military will perform motor activities on their own. They are offered performance criteria, assessment standards and a summary of mistakes they can make in executing motor actions. This style allows the military to practice and self-correct at their own pace and to assess their own learning and to check their own performance. During classes, the specialist will work with the students to set goals and objectives. Defining for this style is self-assessment, based on specific criteria. This type is found in sports such as basketball, archery, golf, rock climbing, surfing and skateboarding in different exercises, performed in the gym.

"Inclusion" style[13]. The specialist plans and establishes a variety of tasks that have different levels of difficulty. Thus, the military decide which task is most appropriate for their abilities, aspirations and motivations. This style offers a customized and learning development approach. Important for this style is that the military can select the same didactic task, but with a higher level of difficulty, that can make them evolve faster. Difficulty levels are created by the specialist depending on the group to be trained. He/she also constantly adjusts the working level and verifies the performance achieved by the military in the training process, according to the criteria and standards established in the planning act. This style may be adopted within the lessons with martial arts themes, when the difficulty level of the technical procedures can be increased or decreased depending on the members of the training group.

The direct style[14] is action-oriented from the trainer's perspective. By approaching this style, the efficiency of the practice is increased, the chances of error during the execution of the motor acts and actions are reduced, the chances of better coordination and management of the group participating in the training increase. This procedure also has its shortcomings, consisting of: the lack of the possibility to differentially approach the military and *"focusing on learning outcomes and not on the ongoing process"*[15]. A logical example of action sequences for this teaching style may be: explaining and demonstrating the content to be learned, executing motor actions by the military, correcting any possible mistakes, presenting methodical indications, correcting mistakes again and then, resuming the execution of motor acts.

The indirect style[16] is action-oriented from the military personnel's perspective. With this style, they are considered to have the opportunity to choose the path for the fulfillment of the didactic tasks, resulting in their better involvement in the didactic act. The indirect style can be attributed two major disadvantages: a longer time for performing tasks and the lack of control over the group to be trained.

The negligent style belongs to whom is disinterested in the outcome of their work, lacking the motivation for the educational act. He/she will accept any proposal from the trainers, he/she is passive in military physical education lessons, not demanding, maintaining a low level of training, below the real potential of the military.

The democratic style is based on a very good cooperation between the military and the trainer, the stimulation of the initiative, a strong motivation and confidence given to those to be trained. Yet, in some cases, this style may lead to the trainer's instructions being neglected and even the attempt not to perform the motor action. It is considered a beneficial style for the act of socialization and motor evolution, but from my point of view, it and should not be used as a fundamental permanent style in this military branch.

From my point of view, the military physical education specialist should not adopt only one of the styles and only use it in the teaching act. He/she must combine the positive elements of them, adapt them to the group whom he/she addresses to and manage the whole activity according to the objectives and tasks to be fulfilled. Moreover, the quality of military physical education specialist/trainer is acquired through adequate training as a result of participating in forms of training in specialized institutions, and requires a summary of psycho-pedagogical, professional, didactic and communication skills, which aim to their orientation towards achieving the objectives of the learning act, for the benefit of the trained persons and the military institution.

Conclusions

Projection, planning and teaching are three concepts and, at the same time, defining activities for the purpose of the training act. Without a clear vision and without the anticipation of the actions, that the military can undergo in real combat situations, the military physical education training will lack the adaptation of the training content to the fundamental requirement of the army: accomplishment of combat missions. The embodiment of the projection of the training content in the planning documents represents an important step in achieving the objectives of the military physical education, a rational and normal direction, after all, for the specialists in this field.

The transposition of the training content in the lesson, the performance of the teaching act itself represents the essential stage through which the transfer of knowledge from the specialist to the military is made. How is this transfer made? The quantity and quality of the specialized and pedagogical knowledge acquired prior to the teaching act, the pedagogical and life experience, the quality of the superior cognitive processes of those managing the activity, the capacity for social interaction, the desire to reach the objectives set at any cost the perseverance are just a few reference points and reasons with which the physical education specialist builds his/her own modality, his/her own teaching style. Stating these few reasons makes us believe, at the same time, that a specialist in military physical education is not built from one day to another.

NOTES:

1 Ghe. Cârstea, *Theory and Methodology of Physical Education and Sports*, Ed. AN-DA, Bucharest, 2000, p. 137.
2 *Ibidem*.
3 Ghe. Cârstea, *Educaţia fizică: teoria şi bazele metodicii*, Ed. ANEFS, Bucharest, 1997, p. 197.
4 *Ibidem*, p. 201.
5 *Ibidem*, p. 207.
6 Ghe. Cârstea, *Teoria şi metodica educaţiei fizice şi Sportului*, Ed. AN-DA, Bucharest, 2000, p. 144.
7 A. Dragnea şi colab., *Educaţie fizică şi sport – teorie şi didactică*, Ed. FEST, Bucharest, 2006, p. 185.
8 *Ibidem*, p. 163.
9 M. Mosston, S. Ashworth, *Teaching Physical Education*, First Online Edition, Spectrum Teaching and Learning Institute, SUA, 2008, p. 76.
10 *Ibidem*, p. 94.
11 *Ibidem*, p. 116.
12 *Ibidem*, p. 141.
13 *Ibidem*, p. 156.
14 A. Dragnea şi colab., *Educaţie fizică şi sport – teorie şi didactică*, Ed. FEST, Bucharest, 2006, p. 163.
15 *Ibidem*.
16 *Ibidem*, p. 164.

BIBLIOGRAPHY

Cârstea Ghe., *Theory and methodology of physical education and Sport*, AN-DA Ed., Bucharest, 2000.

Ciapa G.C., *Physical training of the Romanian military in modern conflicts,* "Carol I" National Defence University, Bucharest, 2018.

Ciapa G., *Military physical education – a form of combat preparation. Research report no. 1*, Publishing House of the "Carol I" National Defence University, Bucharest, 2015.

Dragnea A., et al., *Physical education and sports – theory and teaching,* FEST Ed., Bucharest, 2006.

Epuran M., Horghidan, V., *Psychology of physical education,* ANEFS, Bucharest, 1994.

Mosston M., Ashworth S., Teaching Physical Education, First Online Edition, Spectrum Teaching and Learning Institute, USA, 2008

www.academia.eduwww.cognifit.comwww.education.cu-portland.eduwww.thepeproject.com

PRINCIPLES AND METHODS OF TRAINING IN MILITARY PHYSICAL EDUCATION

LtCol. Lecturer Gabriel Constantin CIAPA, PhD*

The connection between theory and the application of theoretical knowledge in the practice of military physical education, is realized in some situations with quite ambiguity and difficulty. The result of this syncope will be found immediately in the training level of the trained persons. A cause of this syncope can be represented by leaving aside certain fundamental theoretical specialized knowledge, absolutely necessary for the educational act. Therefore, in the first part of this material, I will approach the training principles specific to the sub-domain of military physical education, in order to achieve an interpretation, necessary both for their understanding and for their importance in the act of training in the specialized military system. The second part of this material is dedicated to the classical methods of training in physical education. This material aims at a reiteration of the two fundamentals of military physical education, providing a synthesis and, possibly, a supplement of the specialized military literature.

Keywords: military physical education; principles; methods; training; practice.

Introduction

The subsystem of military physical education must be under permanent change and adaptation to the new conditions required by the military system. This is why a deep inclination to all the real possibilities that can lead to finding solutions for improving both the activity itself and the finished product – meaning the military/fighter – is required. Whether we focus on the material basis or on the theoretical scientific resources, they must converge and be found in the quality of the trained person.

Applying the theoretical knowledge from military physical education to the practice of training will only facilitate the acquisition of motion actions or the development of motor skills and abilities, under the conditions of lucid, real, rigorous, constant preparation of military for combat, of a rhythmic conduct of specific activities, of permanent assessment and control.

Military physical education, as a subsystem of general education, requires functioning according to clear rules, having precise functions and objectives, its own methodology and terminology. Also, military physical education uses a series of fundamental knowledge that have the purpose of performing motor actions. Some of these training fundamentals in this military specialty are the principles of training and methods of training in physical education.

Military Technical Academy
e-mail: *ciapagabriel@yahoo.com*

Training principles in military physical education

The instructional-educational process of military physical education is an activity that is carried out under the norms, provisions, rules or different training requirements. The necessity of such rules or requirements starts from the training needs of the army, in order to achieve its training purposes. Some of them bear the name of training principles[1], principles that have been established as necessary and mandatory in the specific training in this field, being recognized and observed by all great specialists of military physical education. These principles are the following: active and conscious participation, intuition, accessibility, systematization and continuity and linking the training with the requirements of the practical activity, thorough learning.

The principle of active and conscious participation[2]. From the statement of this principle it can be understood that it follows two directions of analysis of the participants in the training process: the first direction is given by the requirement of the active involvement of the military in the training, and the second is aimed at their awareness regarding

the training. The observance of the two directions ,drawn by this principle, requires the fulfillment of several tasks by the training participants, trainers and military to be trained.

A first aspect is provided by the objectives of the instructional-educational process within the meaning of their understanding, why they must participate in such training programs. The role of the trainers is crucial in creating the correct and realistic motivational factor for the military to practice physical exercises.

The second point of interest follows the logical sequence of motor acts and actions that military must learn. This sequence must be understood, memorized and applied when appropriate. An extremely important role is given to the trainer who can, through the planning and structuring of the learning material, contribute to the facilitation or hindering of the learning or development of the motor structures, and he/she must also know the key elements of the methodological structure of the learning procedures.

The third aspect, that this principle pursues, is to create an appropriate attitude of military sensitization and accountability for learning the teaching material. They should be encouraged to work independently, they should be given the opportunity to choose from the solutions offered by the trainers and they should be stimulated and encouraged to adopt an objective attitude towards the training process towards the teaching methods.

The last side of this principle aims to train the military in the capacity of self-assessment and objective self-evaluation of executions of motor acts and actions, as well as of the results obtained after the training. There is almost always "somebody else" to blame for the lack of one's own performance, sometimes finding really embarrassing justifications for poor results and lack of participation in training.

The principle of intuition[3]. This principle highlights the importance of the first human signaling system: the sensory one. *"Intuition implies knowledge of reality through the senses, analyzers, receptors of the human body"*[4]. In the subsystem of military physical education, the principle of intuition aims to stimulate as many analyzers (visual, hearing, tactile).

Accessing them as a whole can be reflected in the speed and quality of learning the material. Obviously, the military with deficiencies of such analyzers, although they should not exist in training in the military system, have to suffer in receiving and learning the motor acts. In order to obtain results, we try to stimulate the analyzers through the three classic methods of training: the demonstration, the presentation of iconographic materials and the observation of other military personnel, training methods that I will approach in the second part of this material. The principle of intuition requires that the material to be transmitted can be seen and accessed by all those attending the training; also, the principle requires the stimulation of the second signaling system of the human body.

The principle of accessibility[5]. This principle highlights the importance of carrying out the instructional-educational process according to age, sex and training level. Accessibility should not be understood as a minimum effort and objectives that the military must meet in the instructional-educational process, but as a requirement that, in order to be fulfilled, must exert physical effort, they must work if they wish to evolve.

In order to comply with this principle, military trainers must seek: *"Careful selection of stimuli, especially physical exercises; establishment of an adequate dosage of physical effort; the use of methodical regulators to accelerate the process of acquiring motor acts or actions by the subjects; adapting the training and education methods and methodical procedures to the level of understanding and psycho-motor development of the subjects; differentiation of subjects' assessment"*[6] (according to the Regulation of military physical education, 2012, their assessment is carried out by age groups, education or training).

In order to apply this principle, it is necessary for the trainer to know the military attending the training to create a working rhythm related to the reaction of the military to the stimuli, and to apply the following teaching rules: from easy to difficult, from simple to complex and from known to unknown.

The principle of systematization and continuity[7]. This principle is relevant from the point of view of the activity planning and the correct preparation of documents for conducting military physical education lessons. Its central elements, systematization and continuity are essential conditions for achieving the objectives

of military physical education. In order for the principle of systematization and continuity to be found in the activity of military physical education, the following requirements must be observed: the ordering and logical programming of the contents to be transmitted within the same training cycle; the new contents to learn must be based on the old ones, already existing, which in turn become support for the following knowledge; the background of the instructional-educational process must be structured and programmed in such a way as to provide the possibility of logical links between the years of training or the years of education; the obligation of military participation in training constantly – absences can lead to the loss of knowledge acquired or create gaps in training.

The principle of linking training to the requirements of practical activity[8]. For many specialists in military physical education, this principle is not a priority, but rather something secondary. The principle emphasizes the importance of anchoring training in the reality of armed combat. In other words, what is learned must be useful in the potential situations of armed combat, truly gain practical value, and knowledge must be adaptable to the requirements of the combat. There are many situations in the instructional-educational process in which the content is transmitted only to cover some learning material and nothing more. This happens precisely because of the lack of specialized knowledge, unawareness of the requirements of the armed combat and the promotion of the same old content year after year, irrelevant for the practice of real-life situations. The specialized literature also names this principle that of modeling, whose purpose is to create possibilities for generalizing the teaching material itself, to apply the knowledge learned under totally new, unpredictable conditions, other than those in which the instructional-educational process took place.

The principle of thorough learning[9]. The principle of sustainability, as it is also called in the specialized literature, is conditioned by the other principles. The sustainability of the contents learned is conditioned by: the large number of repetitions provided to the motor acts and actions during the training process; planning, preferably, of a small volume of the content to be learned in a certain period – conditions are ensured, as a time budget, for a greater number of repetitions than if a large volume of learning had been planned for the same time unit; awareness of the stage of military preparation and of the level of knowledge acquired by them.

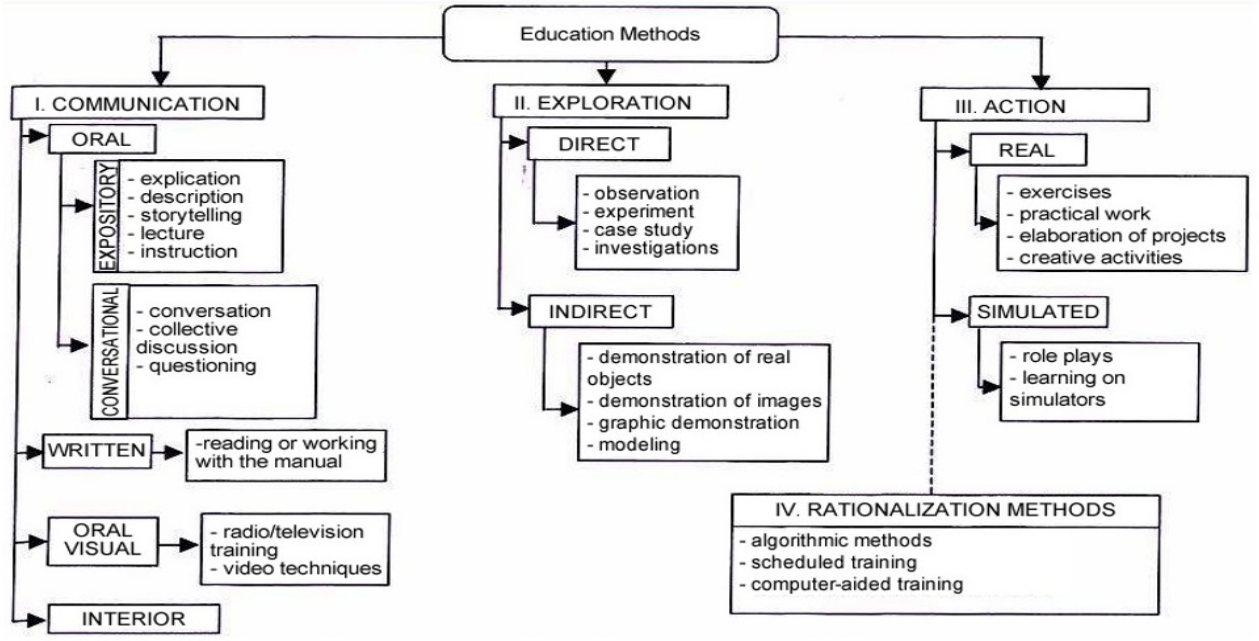


Figure 1. *Classification of educational methods*[10]

Methods of training in military physical education

Pedagogy calls the method the *way to* achieving the goals and a way of working. This notion will always arouse defining tendencies from all specialists. In my view, the method represents the totality of the didactic elements used to achieve the objectives of the military physical education or the operational objectives of the lesson through logical actions, designed in time. The choice of training methods and their use in military physical education lessons rests solely with the science of those conducting the activity. Such training methods are closely linked to the means of achieving the goals of the lessons and reaching the goals set. The method and the means are indissolubly linked and mutually interconditioned. A solid support of theoretical and practical knowledge will facilitate the choice of the training methods necessary for the instructional-educational act.

Over the years the specialists in the field have tried several taxonomies, according to various criteria. Eventually, in each of them the same methods are found. In figure 1 we illustrate such a taxonomy and will develop the one established in this field.

In the opinion of some of the specialists in physical education the methods of training are verbal (explanation, exposition, storytelling etc.) and nonverbal (practice, practical assessment, demonstration etc.). But most specialists in the field accept more easily the classical approach to training methods. These methods also apply to the subsystem of military physical education. According to the classical approach we have verbal, intuitive and practical training methods. The verbal methods are based on the ability to transmit the knowledge through language of the leaders of the educational act. These verbal methods are as follows: *lecture* – a method that applies to higher education, especially, and is based on scientific arguments and appropriate specialized terminology; *explanation* – this is the most used method and for some trainers, the only one, unfortunately. The explanation must be logical, precise, clear and intervene at the right time. In the instructional-educational process, the explanation may precede the demonstration, intervene after the demonstration or concurrently with it (the use of these two methods at the same time is harder to achieve and not recommended in case of learning difficult technical procedures).

Other methods are: *storytelling* – it addresses children, mainly, and the information transmitted and its assimilation are helped by the references related to the elements of everyday life and known by the little ones; *description* – is made through a content of the language suitable for the group to be trained; *conversation* – highlights the need for permanent dialogue between military and sports trainers; *individual study* – is carried out on the establishing of teaching tasks for military by trainers and their guidance towards studying specialized bibliography; *brainstorming* – it is not used often, but it stimulates the active involvement of the military in training. According to this method, motivated points of view are expressed which are also accepted, but not defined as solutions for the didactic tasks. In a relatively short time, for several days, the unresolved educational task is brought into discussion, motivated opinions are presented again, and the most efficient solutions are admitted under the guidance of the specialist.

The first intuitive method is *demonstration* – together with explanation and practice, it is the most used in military physical education. In order to be effective, it must be carried out at model level either by the specialist (it is also called a direct demonstration) or by another military from the training group, whose technical training allows it (it is also called intermediated demonstration). The second intuitive method is *observing the execution of other military personnel* – it is a choice of the trainer through which the negative or positive aspects of the executions of the colleagues are highlighted. The last intuitive method is the one using "*iconographic material*"[11] (sketches, drawings, kinograms[12], video materials, graphics, etc.). It is used when there is no possibility to perform the demonstration at the model level or as a supplement to it.

The third group of training methods, the practical ones, can actually be reduced to a single, generally accepted one: the *practice method*. The practice method involves the execution of the content to be learned in a conscious and systematic way. It follows in the logic of learning, in military physical education, after the verbal and intuitive methods. It is addressed entirely to the military who must be trained, under the guidance and supervision of the trainer.

Ghe. Cârstea names six types of practice: *"practice for developing motor skills and abilities; practice for development, education of motor skills; practice for the optimization of physical body development* (it is realized, in particular, within the third link of the lesson of military physical education – the selective influence of the locomotive apparatus, through exercises specific to the basic gymnastics)*; practice for developing organizational capacity* (it is realized in each lesson due to the use of the means specific to basic gymnastics, of the front and formation exercises, developing the capacity of self-organization and self-management of the military); *practice for developing the capacity to practice autonomous physical exercises* (understanding the structure of the military physical education lesson as well as the means used may determine the military to freely work certain sequences of the lesson, under the supervision of the trainer); *practice for developing the capacity to practice independent physical exercises* (in the military physical education lessons, theoretical and practical bases necessary for practicing physical exercises during the spare time are laid)*"*.

In the development of motor skills and abilities, the exercise method can take the following forms[13]: "*group practice* – repetitions follow only one motor skill before moving on to the next; *separate practice* – the military does not perform identical tasks in successive attempts; *variable practice* – the motor act or action is acquired regardless of its parameters (direction, speed, tempo, etc.). It can be illustrated by the fact that it will be very easy for the military to make the transfer of motion information in order to make a precision grenade throw at a distance of 25 m, if they had previously prepared at distances of 15 m, 20 m, 30 m; *constant practice* – only one parameter changes during executions (for example, movement direction or reaction speed); *mental practice* – aims at the mental achievement and repetition of the succession of exercises to be performed, imagining the motor act or action can be an advantage in learning motor tasks; *analytical practice* – follows the breakdown of difficult technical procedures into smaller learning units and the work to acquire them (it is not necessary to insist on the use of this form because the wrong dynamic stereotypes can be created and can be explained by the lack of fluency in the complete execution of the technical procedures, their speed of execution, etc.); *global practice* – it aims at the complete execution of the motor skills and can be used alone in the case of very simple skills, in which learning can be produced by imitating the actions of the trainer.

Analytical or global practice, in the development of motor skills, can have as effects "precision of movements, safety, speed in execution and low energy consumption provided there is a judicious control of the training program"[14]. Epuran[15] presents the benefits and effects of practice: "gradually shortening of the time for performing the tasks; gradual specialization (acquiring new motor skills and abilities over time); gradual removal of unnecessary movements and muscle strain (by forming automatisms, the coarse movements disappear and even a muscular relaxation is obtained in the execution of the technical procedures, these becoming very precise); fixation of new combinations of movements; decreased sensitivity towards the different external barriers; tendency to shift attention from process to outcome (during the execution of the movements, the military are no longer focused on the execution of the technique but on its outcome); fatigue reduction (by practice, the appearance of fatigue is delayed as a result of programming and directing the effort within the instructional-educational process); better selection and interpretation of external and internal indicators (appreciation of spatial-temporal parameters is a good example); gradual reduction of execution errors (as a result of the repetition in a sufficiently large number of a motor actions, any mistake in carrying out the process or technique itself can be eliminated); unification of partial actions (in case of technical procedures during the learning or development of the difficult motor skills, as a result of the analytical exercise and the summation of motor gestures, one can gradually arrive at manifesting motor action as a unitary whole)". All these effects of the practice are, eventually, in the quality of the trained military.

Conclusions

Starting from the need to understand the military specialty theory of military physical education, to apply such knowledge in practice, this material pleads for the acquisition and application

of the fundamental knowledge of this subsystem of general education, it pleads for building the skills to conduct training activities specific to this field, based simultaneously on theory and practice, it reinforces the idea that the training activities should be conducted by specialists in the conditions of a correct attitude towards the theoretical bases. Also, this material militates to raising awareness on the importance of specialized theoretical knowledge, respect for specialists and their quality, especially since this field may be considered a foundation for the development of other military specialties.

NOTES:

1 Ghe. Cârstea, *Teoria şi metodica educaţiei fizice şi Sportului*, Ed. AN-DA, Bucharest, 2000, p.77.

2 *Ibidem,* p.78.

3 *Ibidem,* p.79.

4 *Ibidem*, p.80.

5 *Ibidem.*

6 *Ibidem*, p.81.

7 *Ibidem*.

8 *Ibidem*, p.82.

9 *Ibidem,* p.83.

10 I. Cerghit, *Metode de învăţământ*, Ediţia a III-a, Ed. Didactică şi Pedagogică, R.A., Bucharest, 1998, p. 98.

11 *Ibidem*, p.88.

12 Successive and logical graphic representation of the basic movements that make up a process or a technical element.

13 A. Dragnea şi colab., *Educaţie fizică şi sport – teorie şi didactică*, Ed.FEST, Bucharest, 2006, p.152.

14 G. Ciapa, *Self-defense – physical and psychological support in military modern conflicts*, Strategic changes in security and international relations, Strategii XXI, Vol. 3, p. 299.

15 M. Epuran, V. Horghidan, *Psihologia educaţiei fizice*, ANEFS, Bucharest, 1994, p. 180.

BIBLIOGRAPHY

Cârstea Ghe., *Theory and methodology of physical education and Sport*, AN-DA Ed., Bucharest, 2000.

Cerghit I., *Methods of education,* Third Edition, Didactic and Pedagogical Edition, R.A., Bucharest, 1998.

Ciapa G.C., *Physical training of the Romanian military in modern conflicts,* "Carol I" National Defence University, Bucharest, 2018.

Ciapa G., *Self-defense – physical and psychological support in military modern conflicts*, Strategic changes in security and international relations, Strategies XXI, Vol. 3, Bucharest, 2015.

Dragnea A., et al., *Physical education and sport – theory and teaching*, FEST Ed., Bucharest, 2006.

Epuran M., Horghidan V., *Psychology of physical education*, ANEFS, Bucharest, 1994.

THE CYBER SECURITY OF CRITICAL INFRASTRUCTURES IN AN INCREASINGLY CONNECTED WORLD

LtCol. Eng. Vasile Florin POPESCU, PhD*

In an increasingly connected world, critical infrastructures have become more vulnerable than ever to cyber security threats, whether they come from national states, criminal organizations or individuals. This new vulnerability stems from fundamental changes in the technological systems of organizations (government and private). In this regard, the Virtual Critical Infrastructure of any organization / nation represents an arena where security is absolutely imperative. Cyber protection has become crucial in every sector of activity, and the absence of measures to protect critical infrastructures threatens to cause huge damage to the functioning of the company.

Keywords: critical infrastructures; cyber space; cyber threats; vulnerabilities; information and operational technology systems.

Aircraft hijacked from the normal course. Underground trains stuck in tunnels below cities. Broken dams flooding cities. Power cuts. Blocked telecommunications. Unusable 112 emergency calls. These moments of chaos and panic and other potential consequences of attacks on critical infrastructure can at best only cause these drawbacks, and in the worst case, they can lead to loss of human life or widespread destruction.

Nowadays, about half of the world's population lives in urban areas and it is assumed that the urbanization process will accelerate, so that only one third of the planet's inhabitants will live outside urban areas by 2050[1]. This development raises a number of challenges that also influence infrastructures, whose reliable and efficient functioning will determine how cities are able to meet the demands of quality of life[2]. Some of these infrastructures are called "critical" because the welfare of the society is fundamentally based on their reliability. They can be understood as the fundamental elements of the sustainability of society, the security and security of supply. Critical infrastructures offer people access to a wide range of goods, the availability of which is essential for the resilience of communities[3,4].

Etymologically, according to Oxford English Dictionary, the term infrastructure is a combination of the Latin prefix "infra" with the meaning of "under" and the suffix "structure", which shows how a mechanism is constructed. The association of the term "critical" with that of "infrastructure" defines that type of infrastructure that disrupted can lead to major damage.

The critical character of the infrastructures is given by:

- Their uniqueness;
- The vital character in the functioning of the economic, social, political, military, information systems, etc ...);
- Sensitivity to changes;
- High vulnerability to threats from the external environment.

Depending on their importance for the functionality of the systems and processes, the infrastructures are divided into three categories[5]:

- Common infrastructures;
- Special infrastructures;
- Critical infrastructures.

Critical infrastructures are divided into two important categories[5]:

- Physical:
  - International;
  - of the economy of the states;
  - of the different industrial sectors;
  - of companies / companies;

***Ministry of National Defence**
e-mail: *popescuveve@gmail.com*

- of projects;
- of air and rail and naval transport;
- of the financial system;
- of the house, of the town/village, of the country and of the continent;
- military;
- of the public order system;
- of the intelligence and security system of the state;
- of the health and protection system of the citizen, family and community.

- Virtual:
  - of the communication systems;
  - of networks and databases;
  - of cyber space.

In an increasingly connected world, critical infrastructures have become more vulnerable than ever to cyber security threats, whether they come from national states and criminal organizations or individuals. This new vulnerability stems from fundamental changes in the technological systems of organizations (government and private). Such organizations - army, police, firefighters, providers of medical services and utilities, banking systems, transport systems, etc ... act with two types of technological systems: information technology systems and operational technology systems.

Information technology systems provide basic functions of the office, such as: email communication, payroll, human resources, etc., while operational technology systems control the physical equipment and personnel essential to fulfill their mission. In the past, operational technology systems consisted of stand-alone systems that made them secure. Now, systems operating technology systems run on the same software and hardware platforms commonly, known as IT systems. These systems are well known to hackers and are therefore significantly less secure.

What led to this convergence of information technology systems with operational technology systems? Here are some examples:

A homeowner remotely adjusts the thermostat to his home to lower the temperature while on vacation. A doctor visualizes the insulin use of patients on a desktop computer. Companies remotely monitor the condition and location of trains, buses and trucks; oil and gas flow through pipelines; or the use of water or electricity to manage these services effectively. While the technologies in these examples improve our lives, they can make us vulnerable at the same time.

I am saying this because as the number of interconnected devices continues to grow, the number of potential access points for hackers to disrupt critical infrastructure also increases. In this regard, the Virtual Critical Infrastructure of any organization/nation represents an arena where security is absolutely imperative. Cyber protection has become crucial in every sector of activity, and the absence of measures to protect critical infrastructures threatens to cause huge damage to the functioning of the society as a whole.

Virtual or cybernetic space is a set of means and procedures, based on information and communication technology (ICT), and consist of hardware, software, internet and information services, and control systems becoming critical infrastructure for the socio-economic activity of any nation, a transnational organization or project. Different dictionaries and encyclopedias define cyber space as follows:

- Cyber-space: a computer network made up of a global network of computer networks, that use TCP/IP network protocols to facilitate data sharing (Source: Online Romanian Dictionary);
- Cyber space is the electronic computer network environment where online communication takes place. Wikipedia, http://en.wikipedia.org/wiki/Cyberspace[6].
- A metaphor to describe the non-physical terrain, created by computer systems: Online systems create a cyber space where people can communicate with each other, perform research, or simply buy things. http://www.webopedia.com/TERM/C/cyberspace.html[7].
- Cyber space is a field characterized by the use of electronic devices and electromagnetic spectrum to store, modify and exchange data through network systems and associated physical infrastructures. In fact, cyberspace can be considered as the interconnection of human beings through computers and telecommunication, regardless of geographic position.http://searchsoa.techtarget.com/definition/cyberspace[8].

The US Government defines the slightly wider cyber space. The Presidential National Security Directive no. 23 and 54 define cyberspace as the interdependent network of information

technology infrastructures, including the Internet, telecommunication networks, computer systems, users and those who control critical industries. The common use of the term also refers to the virtual information environment and interactions between people.

The definitions offered by Webster, Wikipedia, or the Oxford Dictionary are not absolute and comprehensive enough. The concept of virtual space has expanded in the meantime, including trade, finance, energy, stock exchanges and so on. The objectives of the attacks in the virtual environment can be classified into three major groups:

- the public sector and government agencies;
- the private sector, mainly critical infrastructure operators;
- citizens.

Cyber attacks can be classified, depending on their source and impact, as follows:

- *Attacks sponsored by states*

The real world and physical conflicts have expanded into the virtual world of cyberspace. In recent years, cyber attacks have been detected against critical country infrastructures and specific targets. Some examples that are widely known by the public are: Estonia's cyber attack in 2007, which led to the temporary deactivation of a large part of the critical infrastructure of the Baltic countries, the cyber attack launched by Russia against Georgia in 2008 as a prelude to earthquake-like invasion, the Stuxnet case with cyber attacks against SCADA systems, the Duqu's case of cyber attacks against industrial organizations, the cyber attacks suffered by the US Government's classified networks by hackers in Chinese territory. In recent years, some states have invested considerable economic, technical and human resources in developing persistent advanced threats (AAP), aggressively attacking and choosing very specific goals, in order to maintain a steady presence within networks of possible victims. AAP attacks are very difficult to detect because they use techniques and components that are specifically designed to infiltrate and remain in the network without being detected.

Attacks sponsored by private organizations

The objective of many private organizations is to obtain industrial and economic secrets from other competing organizations, and this type of attack is often executed with government support;

- *Attacks of organized crime groups*

Organized crime gangs, also known as computer gangs, began to work in cyberspace, exploiting the possibility of anonymity that this domain offers. The objective of these types of gangs is to obtain sensitive information for their subsequent use for fraud and for significant economic gains.

- *Hackers*

With the advent of the Internet, but especially in recent years, hacker activities have become one of the greatest threats to governments and organizations of all kinds. The principles of this aggression are the anonymity and the free distribution of information through cyber space, essentially via the Internet. Their mission is to "attack" the cyber space of people, companies, projects or other organizations that violate any of their principles or interests. This implies that the cyberspace of governments in most countries around the world, banks, telecommunications companies and critical infrastructure providers, Internet service providers and ultimately all cyberspace are likely to be hacked with the goal to steal sensitive information.

• *Attacks of privileged (in-house)*

These groups are one of the greatest threats to the cyberspace security of nations, companies /projects because they are often an integral part of all the attacks outlined above ... from a spy infiltrated by a state or an employee who work for gangs of terrorists or cyber criminals, dissatisfied employees, etc.

Conclusions and recommendations

The need to stimulate cyber defense for critical infrastructures is clear. However, the question now turns into: How do we get there? In this regard, we have developed some recommendations to contribute to effective collective actions.

- Developing a national strategy for cyber education: to truly protect critical infrastructure, we must have qualified people. Therefore, it is necessary for cyber education to become a higher priority in the educational process. Romania does not have a strategy of education in the field of cybersecurity, that will feed and finance national centers of excellence in the field of cybersecurity.
- Another recommendation is trans-organizational mentoring and knowledge transfer.

Organizations with less cyber security experience or smaller cybersecurity teams can learn from the experience of their more experienced colleagues. Larger organizations should also encourage their experts to participate in industry associations, public-private partnerships and regional organizations, which provide all opportunities for formalizing inter-organizational guidance and knowledge transfer.

- Creating better strategies for sharing information between the government / state and the private sector: cyber security experts seem to agree that for an optimal level of security in all sectors, cooperation is essential.
- Performing scenarios exercises for potential crises: when it comes to critical infrastructure, a real disaster is not the time to learn from mistakes. Such preparation must take place in advance, in crisis scenarios exercises that simulate how a response team would deal with an unexpected incident.

NOTES:

1 Rizea M. et al. UN (United Nations), *World Urbanization Prospects: The 2018 Revision*, Key Facts, 2018. Available online: https://population.un.org/wup/Publications/Files/WUP2018-KeyFacts.pdf (accessed at 10 November, 2018).

2 Riffat S., Powell R., Aydin D., *Future cities and environmental sustainability. Future Cities Environ*, 2016, 1–23 [CrossRef].

3 Hay A.H., Willibald S., *Making Resilience Accessible. Access: An Enabler of Community Resilience Southern Harbour,* 2017, available online: https://www.southernharbour.net/assets/docs/SH_Access20WhitePaper_2017_0307%C6%92.pdf (accessed at 14 January, 2019).

4 Hay A., *Surviving catastrophic events: Stimulating community resilience*. In Infrastructure Risk and Resilience:Transportation; IET: Stevenage, UK, 2013, pp. 41–46.

5 Alexandrescu G., Văduva Gh., *Infrastructuri critice. pericole, ameninţări la adresa acestora. sisteme de protecţie*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2006.

6 http://en.wikipedia.org/wiki/Cyberspace

7 http://www.webopedia.com/TERM/C/cyberspace.html

8 http://searchsoa.techtarget.com/definition/cyber space

BIBLIOGRAPHY

Rizea M. et al. UN (United Nations), *World Urbanization Prospects: The 2018 Revision*, Key Facts, 2018. Available online: https://population.un.org/wup/Publications/Files/WUP2018-KeyFacts.pdf (accessed at 10 November, 2018).

Riffat S., Powell R., Aydin D., *Future cities and environmental sustainability. Future Cities Environ*, 2016, 1–23. [CrossRef].

Hay A.H., Willibald S., *Making Resilience Accessible. Access: An Enabler of Community Resilience Southern Harbour,* 2017, available online: https://www.southernharbour.net/assets/docs/SH_Access20WhitePaper_2017_0307%C6%92.pdf (accessed at 14 January, 2019).

Hay A., *Surviving catastrophic events: Stimulating community resilience*. In Infrastructure Risk and Resilience: Transportation, IET: Stevenage, UK, 2013.

Alexandrescu G., Văduva Gh., *Infrastructuri critice. pericole, ameninţări la adresa acestora. sisteme de protecţie*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2006.

WAYS OF CYBERTERRORISM

Commander Professor Sorin TOPOR, PhD*

Cyberattacks are now becoming more and more complex, more frequent and with increasingly destructive effects. Regardless of the type or value of an organization, it affects information of public and private infrastructures. Moreover, the target may be the private information of those who hold, even temporarily, various public or official positions in a state. In other words, cyberattacks can be directed towards the information profile of a target by affecting data about identity, about finance, by changing information from personal conversations and other private life activities etc.

In this context, terrorism aims to perform actions with clear goals, only once or in series, having as motivation the resistance to political, economic or social changes and producing global information effects. It is well known that the development of terrorism is favored by the development of information technology. Through these, terrorist organizations seek to enhance the perception of terror, by capturing the attention of the global media and by transmitting apocalyptic messages. On the other hand, the anti-terrorist structures are trying to stop or at least hold under certain control these directions of evolution.

The purpose of this article is to determine the content of the concept of cyber terrorism, starting from the analysis of the main factors of public insecurity and social disorder that facilitate the development of modern forms of terrorism. In order to do so, we will try to underline the essential aspects that are relevant for understanding the forms it takes and the ways it works.

Keywords: terrorism; cyber terrorism; cyber spying; cyber frauds; e-propaganda; e-training; radicalization.

At present, within human society, information flows very rapidly through the modern IT&C capabilities. Thus, the mass-media strengthens its function as a basic tool for analyzing, transmitting, shaping opinions, setting or correcting working agendas etc., all of which have as their primary objective the "trade of information". Therefore, the information sold must be beautifully presented in suggestive images, if it is a material situation and/or with charismatic attributes if they stem from socio-human life situations. For this, real science has emerged, such as: neuromarketing, image counseling, clothing consultancy etc.

We could say that all of these have the main purpose of capturing the attention of a target audience, whether trained or not, educated or not. Thus, we notice that the traditional methods of communication can no longer be the only ones used in order to capture the attention of a target population segment. For a media action to be successful, the audience needs to be seduced with information. Moreover, in order to reach the feelings of the people in the respective audience, modern information techniques and technologies are needed to optimize the abilities to communicate at global level. We also refer to the easy access to Internet services, news services provided by various TV and radio channels and print media, other services and communication technologies such satellite communication, mobile phones etc.

As terrorist organizations promote extreme violence, they also have their audience. This audience is seduced by stimulating the perception of having a high level of „psychological power" over other persons. Only thus could we explain why this type of audience listens to and supports the message sent by the leaders of the terrorist organizations. The most eloquent examples come from the current conflict areas from Afghanistan, Middle East, Africa etc., areas where the armed reaction is encouraged by stimulating people's perception that the US led the warfare against Islam; or in the Palestinian-Israeli area where the idea promoted is that of discretionary application

*"Carol I" National Defence University
e-mail: *sorin.topor@yahoo.com*

of citizenship or visa-granting policies on the highly complex migration situation from the ISIS/ Daesh-controlled areas; or in other areas of "social resistance" where there are anarchist groups and vigilantes who militate for so-called "defence of human rights through violence" as a form of social reaction to abuses of intelligence services and other governmental institutions (ex: yellow jackets movement, in France, in 2018).

Under these circumstances, we may say that the main target of contemporary terrorism is to obtain or maintain public insecurity and social disorder within the state. If within this information society – attribute increasingly used for characterizing the current stage of social evolution – information has become more significant than the other social dimensions, terrorist organizations also undergo changes being compelled to adjust communication methods to the demands of information consumers. Thus, keeping in mind these traditional terrorism patterns, we may state that cyber terrorism becomes the most attractive means, well-adapted to the contemporary information environment, allowing the exploitation of the facilities provided by cyberspace to the benefit of terrorist organizations. Thus, the Internet becomes a place for providing the information controlled by terrorist organizations, the effects of which are perceived by people are as an amplification of the traditional terrorist threats. Moreover, the Internet becomes a tool of control and manipulation, the emotionally controlled person being encouraged to kill, to maim, to self-destruct or to cause other material damage.

We consider that this form of terrorism is much more complex than hacking itself and any cybercrime, being exploited by terrorist structures for propaganda, for obtaining financial support, for obtaining information and for ensuring private communication among the members of their organizations[1].

Gabriel Weiman[2] identified at least six different ways of using cyber space for terrorist purposes as follows:

1. *As a psychological warfare tool.* Different images are broadcast for the purpose of spreading terror among the target population (pictures or clips of hostages being beheaded – belonging to a certain nationality or to employees of a corporation, etc.).

2. *As a propaganda tool.* Terrorist organizations can advertise their actions through live shows, online and anywhere in the world. Dissemination of information facilitates the popularization of their achievements and the abatement of errors.

3. *As a financial tool*. It is known that Al-Qaeda received financial aid thanks to Bin Laden's wealth and the contribution of several non-governmental organizations through various sponsorship methods. Experts such as Jimmy Gurule are pointing to Bitcoin as an appropriate means of providing financial support to a terrorist organization[3]. The specific activities of organized crime managed by Daesh, and we are talking about gasoline smuggling, can be part of this type of sponsorship if payments are made with crypto-currency.

4. *As a recruitment tool.* Using the Internet, Daesh has multiplied the number of foreign fighters in comparison with what Al Qaeda held. The massive distribution of images and videos showing the "correct" mujahedin's life and the success of Daesh's actions against non-Muslim enemies (including human executions) among the population helped opening information and recruitment offices around the world. The success of these methods, as expected, has proved to be of real interest among young Muslims.

5. *As a tool to hide the organizational system and their leadership*. Practically, the hierarchy and manner of organization of the terrorist groups could be concealed by building up real networks of communication. Thus, at present, the importance of leadership through a vertical hierarchy was blurred by horizontal network leadership. Members or terrorist groups have been able to support each other, have been able to coordinate and plan attacks etc., in a cheaper and safer way. In Al Qaeda, all the "jihad brothers" were called to use the PalTalk service in order for leaders not to be detected.

6. *As a documents storage place*. On the Internet, on the web pages, we can find numerous manuals and guides on how to build explosives, about urban fight, guerrilla and survival tactics etc. The aspects that we consider essential for the activity of cyber terrorism, which we identified by analyzing the most frequent contemporary terrorist events, were grouped in the next four categories. Given that most of the information comes from open sources, where information does not always have a great level of credibility, we need to say that this ranking is based on information identified in various reference sources and the personal

interpretation of hypothetical possibilities of attack from cyber terrorists.

Cyber espionage

Cyber espionage is one of the most important and intriguing international issues of contemporary society. Current reality confirms that an information system should no longer be protected only against those identified or self-named as "bad boys," but against anyone who deliberately or accidentally enters in the comfort zone of the target. That is why one of the biggest problems of the government is the definition of cyber espionage. Many organizations have created their own definition that usually refer to factors that can cause data and information destruction during an attack on a computer network, or that hide the identity of the attacker or the way the stolen information was used etc.

In our analysis we start from the definition to be found in Tallinn Manual 2.0, which is also accepted in NATO. Starting with 2013, the provisions under Rule 32 specify that cyber espionage is "any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party." In the manual, this definition is only valid at peacetime and regulate legal relationships among state actors. Moreover, cyber espionage must be distinguished from computer network exploitation (CNE) activities. Apparently, we should not approach this definition when we talk about cyber terrorism as a sample of asymmetric warfare. Yet, the Tallinn Manual outlines some of the expert groups' conclusions that the Al-Qaeda attack on the US on September 11, 2001, is assimilated from the international legal point of view to the self-defence right to an armed attack[4], a situation that allows us to continue to use it.

Our analysis becomes more complicated when we overlap the definition with the conclusions of "Snowden" case, in which Edward Snowden has shown that anyone can spy, the Internet offering a high level of anonymity. A lot of data and information can be purchased from mobile devices connected to various Internet services, such as: iPads, tablets, mobile phones, smartphones and more. All these devices can be simultaneously in multiple relations, in various cyber and communications networks. Although there are legal provisions for sanctions an interception of cellular phone calls, it has been proven that organized crime structures and even some governmental structures can intercept and monitor calls of mobile phones. When the phone is used, a digital network allows tracking the geographic location of that device, identified under a cellular phone number; allows the activity to be determined while moving between cell sites and on the Internet etc.

Under these circumstances, nothing prevents terrorists from using the same techniques. Cyber-espionage can therefore also be used to support terrorist acts. It provides: facilitating unauthorized access; intercepting data packets; infecting computer systems with viruses; blocking the data communication process; software piracy; cloning of electronic payment devices; social engineering activities; identifying work schedules and behavioral patterns of the target etc.

From a security perspective, the risks and implications of a major cyberattack with terrorist origins can be comparable to those of the Cold War. By extrapolating these risks to a much higher degree of national or multinational interest, we will notice that procedurally nothing changes. For example, electricity network infrastructures, water treatment facilities, rail and road management nodes, air-port facilities etc., are all vulnerable to cyber espionage and other information threats. Cyber espionage can prepare for directly hitting the targets, it can provide information in support of malicious actions which are not aimed at initiating a direct attack and it may extract information to blackmail the target and obtain funds.

It is obvious that for this approach there is a need for a real force in these field, a specialized capability that, as far as we know, does not exist in the organization of any contemporary terrorist structure. However, this reality does not have to "encourage" us too much. The lessons learned let us know that when a powerful terrorist leader has enough funds and wants to buy something on the black market, he may get anything. Having money gives one the possibility to buy the services of individuals recognized as having real performances in on-line criminal activity or supporters of terrorist ideologies, good specialists in using cyber espionage instruments. By stimulating their pride, they might „solve" all the information objectives set.

Cyber frauds committed in support of terrorist activity

According to the Romanian Criminal Code, computer fraud is "the introduction, modification or deletion of computer data, the restriction of access to such data or the denial of any kind of computer system functioning in order to obtain a material benefit for oneself or for a third party, if damage was caused to a person"[5]. As we can see, this definition does not involve any link with terrorism. The definition refers to a crime specific area.

Nowadays, more and more criminals, in order to commit criminal activities outside physical or geographic boundaries, exploit the speed, the comfort and anonymity offered by the computer environment, seriously harming the victim, sometimes exerting threats on people anywhere in the world.

Although there is no universally recognized definition for cybercrime, criminal law enforcement practices distinguish between the two types of Internet crimes, namely:

• Advanced cybercrime (or high technology crimes) – they include sophisticated attacks against components and software programs;

• Base cybercrime – this includes those "traditional" crimes that have become "upgraded" due to the advent of the Internet. Among these, we include crimes against children, financial crimes and even some crimes related to terrorism.

Therefore, we need to underline once more that no matter how changing the nature of cybercrime due to these new trends in computer systems and networks, not all Internet crime activities are cyber-terrorism. Generally, those activities recognized as being organized by crime structures are geared towards maximizing profits in the shortest possible time. These include theft, fraud, illegal games, the sale of counterfeit medicine, etc.[6] We considered it necessary to make these assertions in order to understand that police structures are committed to neutralizing all cybercrime. To counter terrorists, they are also supported by other structures specialized in combating logistic or financial activities that support terrorism. In fact, the G7 Ministers of Internal Affairs requested, at the meeting in Ischia, Italy, in October 2017, the sharing of information from the global platform, about so-called "foreign terrorist fighters" (FTFs), data sharing and the analysis of predominantly extremist activity. At the end of this summit, the Ministers stated, through a joint statement, that they would "support the role of INTERPOL as a global platform for the exchange of information on lost and stolen travel documents, as well as for the systematic examination of international travelers, including the exchange of biometrical information and data collected on the battle space. Last but not least, they said they were committed to encouraging all states to increase the use of its databases."[7] Besides, INTERPOL has been the pioneer of information exchange for the legal support of military actions since 2005 through the Vennlig Project, in Iraq, and later through the Hamah Project in Afghanistan. The information provided by INTERPOL allows undermining the activities of terrorist groups, banning the movement of terrorist fighters to return to conflict zones, assessing risk profiles and supporting investigations necessary for the execution of related arrests.

Why all these signals of alert? Because, starting in 2018, due to worrying developments of geopolitics, ideological and technological threats that make the prevention of cyber frauds mainly an issue of protecting affairs against the new and emerging forms of financial crime, there is a series of effects affecting the national security state of a state. Thus, between 20-24 November 2017, an EMMA (European Money Mule Action) initiative directed against transnational money laundering identified nearly $ 31 million in illicit transfers connected to cybercrime funds[8]. According to EMMA, 90% of this money can be used to support the terrorist activity of groups such as Boko Haram, the Islamic State and Hezbollah. These funds come from so-called money transports and crypto-funds, the transports that the authorities say are essential for operations that make the activity move from criminal to terrorist purposes. Moreover, at the G7 meeting from April 4-5, 2019, the Interior ministers decided to improve the requirements for online social networks and platforms, so that they can withdraw content that contributes to the radicalization and the organization of terrorist attacks. Facebook, Twitter, Google, and Microsoft representatives have also been invited to this meeting. One of the conclusions of the G7 summit was that social service software should be updated and allow automatic blocking of all the terrorist content already identified, along with the establishment of emergency protocols to

immediately withdraw the terrorist content that might become viral[9].

In the case of military operations to destabilize the power of militants in Iraq, Syria, Somalia, etc., extremist groups appear to be targeting online financial crime, through radicalization financing efforts[10], for recruitment inside Western nations and, last but not least, for the acquisition of firearms required to perform individual and local attacks with limited objectives. It is estimated that in the future, Western extremists could develop various methods of obtaining funds through cybercrime to test new technologies, whose targets are explosive-loaded drones[11]. As a matter of fact, the most frequent targets of cybercrime on which terrorist activity is based are those aimed at online purchase of various materials, rental of cars and apartments and the purchase of explosive, chemical and/or biological components.

Terrorist organizations and their sponsors can use the Internet to fund these activities. The way in which terrorists use the Internet to raise funds and acquire resources can be classified into four general categories:

- Direct request – refers to the use of websites, chat groups, e-mail and targeted communications to request donations from supporters.
- E-commerce – as it is known, e-commerce can take place only on Internet, with websites that can be organized as online stores with various products and where books, audio and video recordings or other articles can be provided to supporters.
- The use of online payment devices – online payment service devices provide specialized service through dedicated sites. Also communications platforms facilitate the transfer of funds electronically between customers.
- Sponsorship from charitable organizations - fund transfers are often made by electronic bank transfer, credit card or alternative payment facilities available through services such as PayPal or Skype.

"Money laundering" is another important organized crime activity to support terrorist organizations. An example of this is the case of a hacker, Younis Tsouli, who, in the UK, washed away illicit gains from bank card theft in order to finance terrorist acts[12]. In order to do so, he turned to several methods, including transferring through electronic payment accounts online, funds being routed through several countries before reaching the desired destination. The money thus washed was used both to pay Tsouli's registration of 180 sites where al-Qaida propaganda videos were being broadcast and to acquire the equipment needed for terrorist activities to use in several countries. It seems that around 1,400 credit cards have been used to generate approximately £ 1,6 million in illicit funds for terrorist financing.

E-propaganda, education and radicalization

By exploiting the Internet, terrorist groups can "benefit" from promoting their own ideologies to incite hatred and violence, or to prepare terrorist acts, to attract supporters, to assist training etc. The information networks of home users, of businesses and institutions that allow the connection of various information technologies can be programmed to simultaneously run an attack on cyberspace in different sites of the world on a service or network connected to the Internet.

One of the most popular methods of attack is the promotion of propaganda material. Generally, Internet propaganda takes the form of multimedia communications that provide the reader with a lot of information that includes ideological or practical instructions, explanations, justifications or that promotes life-aspects in a terrorist organization. These can include virtual messages, presentations, magazines, treaties, audio or video-files and video-games etc., developed by terrorist organizations or their supporters. However, unlike the legitimate approach of a point of view, what constitutes terrorist propaganda is often a subjective assessment of all the issues presented.

Promoting propaganda is not a forbidden activity. One of the basic principles of international law on the protection of human rights includes the right to the freedom of expression. It guarantees the right to share an opinion or to distribute content that may or may not be acceptable to others (subject to limited exceptions). One of the generally accepted exceptions to this right is the ban on the distribution of certain sexually explicit material, a ban considered to be in the public interest to protect the vulnerable groups. Other exclusions required by law and proven to be necessary refer

to communications that are clearly harmful to the protection of national security and international communications and are likely to incite violence against individuals or specific groups.

As it is well known, promoting violence is a common topic in terrorism-related propaganda. This is one of the main ways that explains why the content distributed on the Internet and related to terrorism exponentially increases the audience, the audience being emotionally affected. Propaganda on the Internet may include content such as clips depicting violent acts of terrorism or their simulations, encouraging the user to engage in virtual play to act as a terrorist.

Promoting extremist rhetoric that encourages violent acts is another common trend identified on IT platforms that host extremist content on the Internet. It is obvious that this content can be distributed to the public, either personally or through physical media such as CDs and DVDs. Still, the basic one remains the Internet, a space that offers a wide range of tools consisting of dedicated websites, video, chat rooms and discussion forums, online magazines, social networking platforms such as Twitter and Facebook, popular video and media sharing sites such as YouTube, Rapidshare, etc.

Terrorist propaganda has as its main targets the recruitment of supporters, radicalization and incitement to violence. The broadcast messages will seek to convey exciting factors of pride, achievement and dedication for extremist purposes. They can be used to demonstrate the effectiveness of terrorist attacks and to demonstrate commitment and fairness to those who have provided financial support.

Other objectives of terrorist propaganda may include the use of psychological manipulation to undermine the belief of a particular individual in its social values, or to promote feelings of anxiety, fear or panic in a particular population or segment. This can be achieved through the dissemination of misinformation through rumors, threats of violence or images of acts of violence. The target audience may include direct and/or public viewers affected by the potential advertising generated by such material.

The Internet is the ideal place to establish connections and relationships with those who are interested, young people representing ideal victims, often lured by the bravado of the age, the acute reaction to whatever they perceive as obsolete and haterism. Moreover, on the basis of their Internet use abilities, young people can develop implied advertising by redistributing online content through discussions and messages in which they communicate their opinions to site administrators and/or other members. Terrorist groups have recognized the "power" of this instrument and have begun to skillfully use it. Thus, they broadcast on the same platforms messages and programs of youthful indoctrination with radical messages.

Although the extent of success of their action cannot be measured, it is clear that the Internet risks are becoming a powerful tool for recruitment and radicalization. For this, Daesh shows various aspects related to professional opportunities, family life or community membership. This method does not only target young people or people already in the recruitment process, but anyone who comes in contact with their propaganda products, either through a redirected link or pop-up notifications. The messages used are not simple narratives, but they are carefully manufactured to achieve a psychological influence with gradual effects. The way in which they will be received is influenced by several factors including: education, age, occupation, relational environment, way of approach etc.

The radicalization of a person depends on the family, emotional, political, financial context of the individual at that time and other. Nizar Trabelsi, accused of planting a bomb in a military unit in Belgium, on behalf of Al Qaeda, during the interrogation within the criminal investigation, said that the initial element that led him to join the terrorist cause was the presentation of a photos of a girl killed in the Gaza Strip, by recruiters, in 2001[13].

Assisted training through IT learning systems

We noted that terrorist organizations use the Internet also for disseminating information. Among their products, there are a series of practical guides as online manuals, audio and video clips, information and other online platforms, all providing an assisted IT-learning system. Moreover, these cyber platforms provide detailed instructions, in an extremely easy way, which is more intuitive (often in multimedia format, mainly local and

international languages), on various themes such as: the particularities of building an improvised explosive device; ways of using firearms or white weapons, or other improvised weapons; methods of combining some currently non-hazardous substances and transforming them into poisons or other dangerous elements; details of the planning and organization of terrorist attacks, etc.

Therefore, the cyber-training platforms thus created can be considered virtual training camps, where physical training is executed individually with or without specialized assistance. These platforms can also be used to discuss or distribute the observations identified in the experiments, to communicate lessons learned about specific methods, techniques or operational knowledge, all for terrorist action training.

For example, the online magazine called Inspire, allegedly published by Al Qaeda, has as its primary objective the Muslims' training for jihad. This publication contains a large amount of ideological material designed to encourage terrorism, including statements attributed to Osama Bin Laden, Sheikh Ayman al-Zawahiri and other Al-Qaidae leaders or representatives.

Online training features include, among other things, tools necessary for counter-information activities, hacking and protection activities, tools to improve the security of communications links and other online connection activity, selection tools for the proposal of encryption methods and anonymization techniques. It seems that the interactive nature of digital platforms in the cyberspace, helps to consolidate those feelings of communion between individuals in different locations and geographic locations, thus encouraging the creation of networks of instructional and tactical materials exchange. Moreover, the Internet can be used not only as a means of publishing extremist rhetoric and videos, but also as a way of developing relationships, a way to seek the support of those responsible for targeted propaganda, etc.

Regarding the danger of Internet radicalization, it is worth mentioning that cyber space can be an effective environment for recruiting and educating minors, knowing that this category is significant for a large proportion of users. Propaganda distributed in order to recruit minors can take the form of cartoons, popular music and videos, or computer games. As a rule, propaganda products run on websites under the control of terrorists or their affiliates and are aimed at being viewed by minors. That is why they include a mixture of cartoons and stories with certain messages that promote and glorify various acts of terrorism, such as martyrdom and suicide attacks.

Other terrorist structures create and promote digital games. Their online nature turns them into real recruitment and training tools. Such games can promote any kind of violence against a state or a certain individual for a political party; they can set scales of value and other rewards for the "success" of going through the virtual stages, and they can be offered to a wider audience often being translated in several languages for the geographical area of interest.

On the basis of the above, we can see that Brenton Tarrant's attack could be part of an online training step. The video images simultaneously broadcast on the Facebook network, *pay attention* – the images were produced and posted live by the attacker through a video camera permanently on, showed how, on March, 8, 2019, he was driving a car to a mosque, he entered the building and open fire on those inside, in a non-discriminatory manner. Later, he was shown executing the wounded fallen in the street, changing his guns, shooting people in the street from behind the windshield, and the fact that he did not open the windows while driving.

It is clear that the event was a terrorist attack, supported by the "manifesto" published on the Internet denouncing immigrants as invaders. The Internet, Facebook, Twitter, and Google have enabled many talks and the broadcast of extraneous content materials on their platforms as a result of distributing video and video products from this event. Daily Mail, quoting Clement Thibault, an analyst on the global financial markets platform Investing.com, noted that". The live-streaming of New Zealand's shooting will certainly bring on more questions of regulation and scrutiny over Facebook. It helped provide a platform for today's horrific attack and will undoubtedly be called into question for facilitating the spreading of this event"[14].

Conclusions

As we can notice, cyber terrorism must be seen as a stage in the evolution of cybercrime adapted to terrorist purposes. It is clear that the resources

provided by the cyber space and the mechanisms of cybercrime are intermingled, being exploited to the fullest by the people from both the cybercrime and the terrorist area.

From the point of view of the development of cyber terrorism, we consider that three basic scenarios can occur, the differences between them deriving from different causal relationships. We do not rule out the possibility of others, but we consider them derivatives or solutions adopted according to the resources available and the training in this field.

The three scenarios for the development of cyber terrorism are the following:

Scenario 1 – Training traditional terrorists in hacking;

Scenario 2 – Enrolling hackers for organizing and executing terrorist attacks with IT devices aid and information support from the Internet, attacks similar to "cyber mercenaries";

Scenario 3 – Attracting hackers who share the ideologies of the terrorist organization and then become active members of it.

The main methods used in the sphere of cybercrime and which could be exploited for the purposes of terrorist attack are the following: password attacks; network access attacks and data packet interception; trusted access attacks; IP spoofing; attacks through social engineering; sequence number prediction attacks; attacks with hijacking of the session; attacks exploiting the weaknesses of technology; attacks exploiting shared libraries etc. All these methods can set up a criminal purpose serving and disclosing the exact motivation for which they were launched.

We conclude that there is no difference between the necessary knowledge and the set of tools used by hackers and cyber terrorists, the effects of completing the attack and its motivation being the only elements that differentiate them. The synergy of conventional terrorism means and the information warfare is very dangerous and, at the same time, an asset for terrorists because it combines lethal goals with the main purpose of fear generation. For cyber terrorists, the adoption of these information measures allows for free action in various geographic areas, in violation of the conventional physical boundaries of contemporary states. At the same time, traditional terrorists can use the information warfare to limit the cost of such an attack, as compared to a conventional attack. Thus, using information warfare, the "low cost/increased effects" ratio is far more attractive to terrorists that use it than to those who oppose it.

Cyber terrorism is neither information warfare nor an accumulation of cybercrime. It is something new, extremely versatile, which may overlap other socio-cybernetics shapes and has great potential for development. The way terrorists will adapt their methods and techniques to the information environment requirements will remain just an option for the management of the respective terrorist organization.

NOTES:

1 Manuel R. Torres Soriano, *Guerras por delegación en el ciberespacio -Proxy wars in cyberspace*, at http://revista.ieee.es/index.php/ieee/article/download/309/473, accessed at 15.10.2018.

2 Gabriel Weimann, *How modern terrorism uses the Internet*, United States Institute of Peace, at https://www.usip.org/sites/default/files/sr116.pdf, accessed at 14.09.2018 and 16.10.2018.

3 Apud Jimmy Gurule, în Dru Stevenson, *Effect of the national security paradigm on criminal law*, at https://law.stanford.edu/wp-content/uploads/2018/03/stevenson.pdf, accessed at 16.10.2018.

4 *Ibidem.*

5 *** https://legeaz.net/noul-cod-penal/art-249, accessed at 15.02.2019.

6 Uptin Saiidi, *Inside Interpol's Singapore cybercrime-fighting complex*, at https://www.cnbc.com/2017/05/17/inside-interpols-singapore-cybercrime-fighting-complex.html, accessed at 16.02.2019.

7 *** *G7 Ministers call for sharing of battlefield data on terrorists via INTERPOL*, at https://www.interpol.int/News-and-media/News/2017/N2017-144,accessed at 16.02.2019.

8 Liam Tung, *Australia helps EU in latest crack down on money mules*, at https://www.cso.com.au/article/630544/australia-helps-eu-latest-crack-down-money-mules/, accessed at 12.01.2019.

9 *** *G7 Interior Ministers Meeting: What are the outcomes?*, at https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes, accessed at 12.07.2019.

10 Timothy L. Quintero, *The Connected Black Mark.et: How the Dark Web Has Empowered LatAm Organized Crime*, at https://www.insightcrime.org/news/analysis/connected-black-market-how-dark-web-empowered-latam-organized-crime/, accessed at 12.01.2019.

11 *** *Threat Lens 2018 Annual Forecast*, at https://

worldview.stratfor.com/article/threat-lens-2018-annual-forecast-excerpt, accessed at 12.01.2019.

12 Michael Jacobson, *Terrorist Financing and the Internet*, în Studies in Conflict & Terrorism, at https://www.tandfonline.com/doi/pdf/10.1080/10576101003587184, accessed at 10.11.2018.

13 Melodie Bouchaud, *Belgium Condemned Over Unlawful Extradition of Terrorist to the US,* at https://news.vice.com/en_us/article/3kegx3/belgium-condemned-over-unlawful-extradition-of-terrorist-to-the-us, accessed at 3.11.2018.

14 *** https://www.dailymail.co.uk/news/article-6814269/Facebook-shares-drop-execs-quit-Christchurch-live-stream-shooting-stirs-outrage.html, accessed at 15.04.2019.

BIBLIOGRAPHY

*** *Anders Breivik, autorul atacurilor din Norvegia, ar putea primi „impresionanta" pedeapsă de 30 de ani de închisoare!,* at http://www.ghimpele.ro

*** *Cyber-attack: US and UK blame North Korea for WannaCry*, at https://www.bbc.com

*** *Decret nr. 212 din 31 octombrie 1974 pentru ratificarea Pactului internațional cu privire la drepturile economice, sociale și culturale* și Pactului internațional cu privire la drepturile civile și politice, in B.Of. nr. 146/20 noi. 1974, at http://www.cdep.ro

*** *Efectul Breivik: Circa o sută de norvegieni vor să devină „terorişti solitari"*, at http://www.financiarul.ro

*** *Facebook shares drop execs quit Christchurch live stream shooting stirs outrage*, at https://www.dailymail.co.uk

*** *G7 Ministers call for sharing of battlefield data on terrorists via INTERPOL*, at https://www.interpol.int

*** *Hacked: The Bangladesh Bank Heist*, at https://www.aljazeera.com

*** *Noul cod penal*, at https://legeaz.net

*** *Threat Lens 2018 Annual Forecast*, at https://worldview.stratfor.com

Bălan George, *Noua concepţie internaţională de acţiune doctrinară şi practică în combaterea terorismului*, at http://fs.legaladviser.ro

Bouchaud Melodie, *Belgium Condemned Over Unlawful Extradition of Terrorist to the US*, at https://news.vice.com

Bumiller Elisabeth, Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, at https://www.nytimes.com

Fedotov,Yury, *Taking action where we can to stop cybercrime*, at https://www.unodc.org

Flynn Matthew J., *Is There a Cyber War?*, Excelsior College, National Cybersecurity Institute Journal, Vol. 1 Issue 2, 2014, pp. 5-7.

Jacobson Michael, *Terrorist Financing and the Internet*, in Conflict & Terrorism Studies, at https://www.tandfonline.com

Jurj-Tudoran Remus, *Instigarea publică la săvârșirea unei infracțiuni de terorism și libertatea de exprimare în practica Curții Europene a Drepturilor Omului*, at http://revistaprolege.ro

Quintero Timothy L., *The Connected Black Market: How the Dark Web Has Empowered LatAm Organized Crime*, at https://www.insightcrime.org

Saiidi Uptin, *Inside Interpol's Singapore cybercrime-fighting complex*, at https://www.cnbc.com

Schmitt Michael N. (general editor), Liis Vihul (managing editor), *Tallinn Manual 2.0,* On the International Law Applicable to Cyber Operations, Cambridge, University Press, 2017.

Soriano Manuel R. Torres, *Guerras por delegación en el ciberespacio – Proxy wars in cyberspace*, at http://revista.ieee.es

Stevenson Dru, *Effect of the national security paradigm on criminal law*, at https://law.stanford.edu

Tanasă Remus, *Benedict Anderson şi destinul „Comunităţilor imaginate"*, at https://www.lapunkt.ro

Tung Liam, *Australia helps EU in latest crack down on money mules*, at https://www.cso.com.au

Weimann Gabriel, *How modern terrorism uses the Internet*, United States Institute of Peace, at https://www.usip.org

FILES FROM THE HISTORY OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

Laura-Rodica HÎMPĂ, PhD*

Unique institution through seniority, structure and organization, "Carol I" National Defence University has remarkably stood out, over time, among the military organizations of higher education in Romania, through the scope of its activities of training the officers in theory and practice. The article presents aspects of the constituting elements of the Superior War School (the initial name from 1889), with brief mentions of the years 1919, 1937 and 1939, illustrated with archival documents.

The research is based on the documents studied at the National Military Archives, the Service of the Central National Historical Archives, the Library of the Romanian Academy and the Library of the "Carol I" National Defence University.

Keywords: Superior War School; "Carol I" National Defence University; Bulletin of "Carol I" National Defence University.

The present research aims to capture some important moments from the evolution of over a century of "Carol I" National Defence University from the perspective of the archival documents. The stages captured here illustrate the baselines of the ideas around which the directions that have influenced over time the military higher education and implicitly the leadership levels of the Romanian Army were designed.

The limitations imposed by the reasonable dimensions of a scientific article led to the retrospective outlining of several decisive events: 1889, the year of its establishment; then the year 1919, which brought about the establishment of the Superior School of Intendance; 1937, the year in which the Bulletin of the National Defence University "Carol I" was created; 1939, the year in which the current headquarters were inaugurated and in which the first 50 years of activity were celebrated.

The time of the establishment of the Superior War School came in a context in which the need for training senior military personnel was seen as a national priority. Until 1889, high-ranking officers were sent to study in major European capitals, to prestigious military universities (Turin, Brussels, Paris, Berlin, Vienna). This kind of education ensureed elitist training through direct contact with European civilization and culture.

The establishment of the Superior War School, as a disseminator and training factor for the doctrine of the Romanian army, was a necessity following the founding of the General Staff on November 12th, 1859, through the High Order no. 83, signed by Alexandru Ioan Cuza. The officers who made up this body were recruited from those who had attended war schools abroad and who "possessed special military knowledge acquired through systematic studies"[1], but without having a particular Romanian military way of thinking.

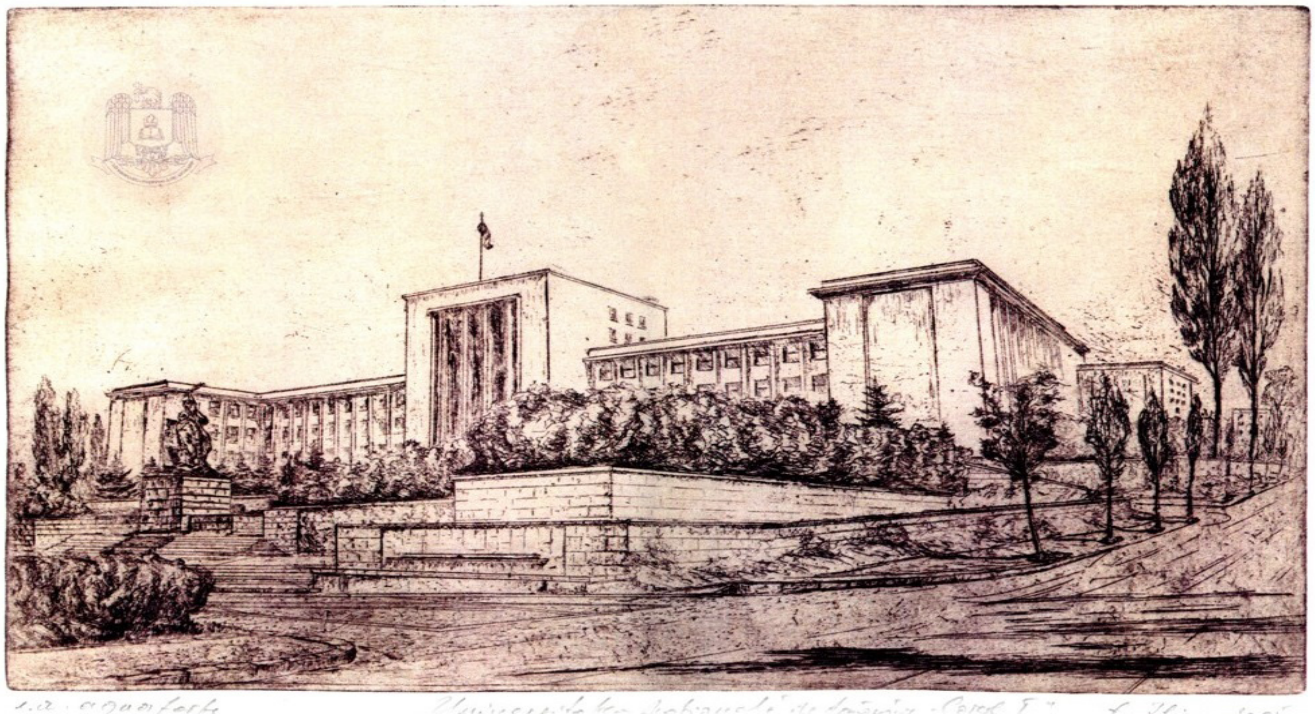
Founder of modern Romania, King Carol I envisaged the building, in Bucharest and almost all the cities county residence, administrative buildings, courts, churches, cinemas, "Carol I" Central University Library, certain high schools: "Matei Basarab", "Mihai Viteazul", "Gheorghe Şincai", "Spiru Haret", "Sfântul Sava", "Titu Maiorescu", "Iulia Haşdeu", Library of the Romanian Academy, State Monopolies House, "Carol I" National Defence University, The Council of Ministers, The Palace of the Ministry of Transport, the Ministry of Justice, the Agronomic Institute, the Royal Palace, the Patriarchate Palace, etc. "[2].

***"Carol I" National Defence University**
e-mail: *l.himpa@yahoo.com*

Thus, among the achievements of King Carol I a much honored one was also the Superior War School, established by the High Royal Decree, no. 2073, issued on August 8th, in 1889. In the first article of the law, the purpose of the institution was established as: the training of the General Staff officers and the dissemination in the army of superior military knowledge. The courses lasted two years, and the conditions that the candidates had to fulfill, listed in article five, were the following: to have held the rank of lieutenant, to have worked "at least two years in effective military service, to have had good conduct from all points of view, and be of a good physical build and completely healthy". A military physician had to give an endorsement certifying "the physical constitution of the candidate, especially the sight and hearing". (Appendix no. 1)

After 1919, given the situation created by the new alliances, concluded after the First World War, Romania's collaboration was limited to the Superior War Schools in Turin and Paris. Also, it is officially recognized that after the War for Integration (1914-1916) Romania took over the doctrine of the French Army[3].

Starting with the opening speech of the Superior War School, delivered by its founder, General Ştefan Fălcoianu[4], in November 1889, according to which "The need for the establishment of a Higher War School was felt and demanded by the Grand Army General Staff. (...) We will put all our efforts in fulfilling this duty to the best of our knowledge; we will claim and we are sure that we will gain the help of our most enlightened comrades, and thus, we hope that, together, we will make this important institution bear the fruits that the Army is waiting for from it "[5], we can now conclude, at this anniversary hour, after 130 years of effervescent activity, after name changes[6] and transformations, that the aforementioned words have reached their true meaning, year after year.



Engraving by Eugen Ilina, Union of Plastic Artists of Romania

Portrait of Stefan Fălcoianu.
Engraving by Nicolae Grigorescu,
Library of the Romanian Academy

Within the evolution of the General Staff, from the initial forms to the complex structure of today,

of conception and doctrinal preparation, all of them dominated by a specific national character, a decisive step was the appearance, in 1889, of the Superior War School, which put an essential mark on the education of high-ranking officers, at the same time encouraging cooperation with the other armies, research and innovation, all leading to the maximization of the operational capacity and thus to the efficiency of the whole army.

Thus, the noble purpose of the prestigious Romanian military higher education institution was kept alive and it achieved its goals, served with devotion and high feelings of patriotism, both by the senior officers of the Romanian Army that it trained, as well as by important names of the Romanian culture, starting with Nicolae Iorga, Grigore Alexandrescu, Simion Mehedinti, Dimitrie Gusti, Henri H. Stahl, Dimitrie Caracostea etc.

The need for modernization, improvement and alignment with the demands of the time led to a permanent extension of the fields of training of student officers.

Thus, in 1919, King Ferdinand issued the High Royal Decree no. 4729/1919 by which the "Intendance Section within the Superior War School"[7] was established, with a duration of two years.

"(...) In addition to the other factors that contribute to winning the battles, there is also the exponent of the economic body which, through its specialized training, organizes and directs the economy of the war on which the fate of the battles depends largely. The Superior War School, giving due importance to this sovereign principle in the preparation of the great Army, by setting up and operating the Intendance Section under the same roof and under the same management, completed the much-felt gap in the army's leadership and structure."[8]

Different areas were studied such as: financial mathematics, commercial law, political and national economy, finance, statistics, industrial and food chemistry, military law and administration, etc. (Appendix no. 2) By 1939, 19 years of alumni (348 graduates) had graduated from the Superior Intendance School.

Active participant in the most important events in the history of Romania since 1889 and up to now, the Superior War School trained entire series of General Staff officers and imposed, thanks to its teachers and commanders, the military knowledge needed for completing the mission; it knew how to keep up with the times and passed, sometimes even with human sacrifices, over the two World Wars and the Revolution of 1989. A burning candle for the fallen heroes is present in the Hall of Honor, and their names are engraved in white marble for eternal remembrance.

The year 1937 remains in the history of Superior War School, both by the appearance of the "Bulletin of the Superior War School", the first title of the publication, (Appendix no. 5), as well as by the start of the works for the construction of the new headquarters on Panduri Road.

Detached from the plethora of military periodic publications of the inter-war period, the Bulletin of the "Carol I" National Defence University remained the journal with the longest existence, completing, in April 2019, 82 years of tradition and value.[9]

The first issue of the Bulletin of "Carol I" National Defence University appeared in April-May 1937, with the approval and at the initiative of the General Staff, no. 2872/23 January 1937, a fact of special importance, also mentioned in the Regulations of the Superior War School of that year.

Not only the resistance in time is noteworthy in this case, but also the maintenance of the role of grandstand of the space of the highest ideas, in the service of the most important institution of military higher education in Romania.

In the Regulations of the "Superior War School" of 1937, both the purpose and the means of achieving the objectives of the institution were exposed. Two central ideas were emphasized: the higher education of the military officers and the provision of a training base, among the most modern ones, "for the command and management of the Major Units and for the election selecting General Staff officers"[10].

Among the methods of accomplishing the objectives set initially, the first one mentioned was the activity of the graduate officers "on the occasion of their service in the units or in headquarters (...) which proceeded so slowly compared to today's rapidity of the progress of military science", that it risked that the doctrine just received in the army might become obsolete. The inefficiency also came

from the lack of experience and authority of those who could not impose the knowledge acquired.

Secondly, emphasize was played on the role of "the publication through which the dissemination of new ideas was obtained, much faster, at the same time as teaching courses in the School and keeping the headquarters informed with official intellectual material, verified through numerous debates, very much. necessary for their documentation, for the application of the doctrine in the army"[11]. Another very important advantage underlined in the Regulation was the establishment of a community of views between the headquarters and the General Staff, which contributed from the beginning to building mutual trust and a more fruitful cooperation.

Following the line of thinking presented above, the Superior War School, as the official high-culture military body of the General Staff and with its approval, took the initiative of printing a "Bulletin", meant not only to remove the shortcomings of the first procedure, but at the same time to complete it.

Seen as a means of propaganda of the most advanced knowledge in the academic military community and of creating a unity of doctrine in the army, in each Bulletin different subjects were exposed so as to be better followed and applied: defense, attack, cavalry, infantry, artillery, engineer, mechanized means, etc.

The issuance of the Bulletin was considered one of the most important objectives of the Superior War School in its role of spreading the higher military knowledge in the army, about which the manager at the time, the adjutant general Paul Teodorescu, said: We confidently start off on this difficult mission which, for the love of serving the institution, we are ready to assume"[12].

The continuous changes at the level of military higher education in Romania and especially those produced in the dissemination of information have affected the means of communication and employment of human knowledge. The political, economic and social changes that have taken place over time have had a strong influence on the manner in which military specialists involved in the education process found information.

The new information technologies and social phenomena generated by the media, at the level of information and communication of all generations, have led to new communication practices, to a revolution in the practice of intellectual work, invariably leading to the preference of using a shorter text at the expense of traditional reading. In this context, Bulletin of "Carol I" National Defence University is currently a forum for debate and analysis for the academic and professional environments, the journal being opened equally to teachers, researchers, doctoral and post-doctoral students, students, military and civilian personnel from institutions belonging to the field of defense, public order and national security.

The importance and role of the bulletin in the development of the learning and research approach has been permanently analyzed and solutions have been applied which include, besides the publication in the online environment and the publication of a number in English, with quarterly periodicity, under the title: "Bulletin of Carol I National Defence University", both publications being available at http://buletinul.unap.ro/.

Starting with 2011, the Bulletin of "Carol I" National Defense University has become a prestigious publication in the field of "Military sciences, intelligence and public order" of the National Council for the Certification of Titles, Diplomas and Certificates of the University, indexed in international databases.

The spectacular evolution of technologies has triggered a wave of changes also in terms of the level of communications and the role they play in contemporary society. The subjects covered by the Bulletin have extended to areas until then reserved for specialists from other fields and the content of articles has been constantly reconsidered.

The manner of institutional learning, as well as the individual learning within the army are essential at the moment, ensuring the skills needed to access the world of digital information-research structures. The most visible are those concerning the typology of documents in the digital age, challenges to which people must be willing and able to adapt permanently. For example, e-learning is considered a learning opportunity that leads to the evolution of the capacity to perform independent work, but also to the capacity to be part of a team in which the Bulletin of "Carol I" National Defence University responds through its online version.

The attributes required to operate at high standards meant to quickly cope with organizational

changes can be found in the current way of putting together the Bulletin: flexibility, creativity, teamwork, cooperation, synthesis ability, intellectual curiosity and the significant cultural experience of the 82 years that passed.

The quarterly issue began in 1956 and continues to this day. The name was changed over time, in close connection with the official title of the institution, so that, in 1991, the name was changed in the "Bulletin of the Academy of High Military Studies"[13], then in 2003, in the "Bulletin of the National Defense University"[14], and since 2005 it has the current name: "Bulletin of Carol I National Defence University"[15].

Starting with 2011, the Bulletin of "Carol I" National Defence University is a prestigious publication in the field "Military sciences, intelligence and public order" of the National Council for the Certification of Titles, Diplomas and Certificates of the University, indexed and in international databases. From the documents kept in the archives and from the testimonies of the contemporaries regarding the evolution and transformation of the institution from the Superior War School to "Carol I" National Defence University, we also selected the year 1939, which was dedicated to the 50th anniversary of its existence, on which occasion the current headquarters of the institution was inaugurated with a lot of pomp, on December 6th, although World War II had already begun in Europe.

The moment had been prepared starting two years before, in 1937, with the call, repeated for two years in the newspapers, on the radio, in the Army Monitor (no. 1 - 12/1938), made to the former students and teachers to gather the historic materials necessary to compose an album of alumni, a book of memories, a statistics of the activity of the school, for the creation of a museum with objects, documents and photographs, etc. (Appendices 3, 4) Following the steps taken, a unique work was published: "The book of Memories of the Graduates 1889 - 1939", unfortunately in a single copy, which can be found at the Military Museum in Bucharest. Undeniably a source of particularly valuable information for the accomplishments and avatars of the first 50 years of the institution's life, of interest for the academic environment, but also for the general public, "The Book of Memories of the Graduates 1889 - 1939" is a work for which an enlargement of the degree of accessibility would be highly appreciated, and, why not, an anastatic issue might be made as a tribute to those who served here, then, and as a good example for the descendants.

1939 remains as a moment of balance of the first 50 years of activity of the Superior War School, years in which 3,270 specialized works were written, of which 309 military history works, 258 infantry tactics, 196 artillery tactics, etc.[16]

The years 1919, 1937 and 1939, on which we tried to cast these few retrospective looks, are stages of development along a series of events that marked the 130 existence of "Carol I" National Defence University. I have illustrated with some archive images this small painting, in order to somehow feel the perfume of the past epoch and to show these puzzle pieces, which now form the picture of our daily life, the life of those who proudly carry on the motto established by King Carol I: LABOR IMPROBUS OMNIA VINCIT!

Ad multos annos, „Carol I" National Defence University!

APPENDICES

Appendix 1. 1

DECREE OF ESTABLISHING THE SUPERIOR WAR SCHOOL

Înalt Decret 2073/8 august 1889

CAROL I,

Ptin graţia lui Dumnezeu şi voinţa naţională, rege al României, la toţi de faţă şi viitori, sănătate.

Având în vedere articolul 4 al legii din martie 1883, asupra serviciului de stat major, asupra raportului ministrului nostru secretar de stat la Departamentul de Război nr. 14.498, am decretat şi decretăm:

Art. 1. Se înfiinţează pe lângă Marele Stat Major o Şcoală Superioară de Război, destinată a forma ofiţeri de stat major.

Art. 2. Recrutarea ofiţerilor elevi pentru această şcoală se va face conform legii, prin concurs între locotenenţi şi căpitani de toate armele, care vor avea cel puţin doi ani de serviciu efectiv la o trupă, cu o bună conduită şi o constituţie fizică sănătoasă.

Art. 3. Numărul elevilor ce se vor admite va fi acum, la început, de zece. Ofiţerii elevi vor fi detaşaţi de la corpurile lor şi vor purta uniforma armei lor.

Art. 4. Examenul de admitere va fi scris, oral şi practic. El va consta din patru probe: proba scrisă, compusă din două compoziţii, din care una în limba franceză sau germană, proba orală asupra materiilor din program, proba practică constând într-o ridicare cu planşeta de recunoaştere pe teren şi proba de echitaţie.

Art. 5. Materiile concursului vor fi următoarele: legislaţia şi administraţia militară, arta şi istoria militară, artileria, fortificaţia, geografia, topografia, regulamnetele de infanterie, cavalerie şi artilerie.

Art. 6. Cursurile şcolii vor fi de doi ani. Vor începe în fiecare an la 1 noiembrie şi se vor termina la 1 iunie anul viitor, la de la 1 iunie la 1 octombrie, elevii vor fi exercitaţi pe teren la lucrări topografice, călătorii de stat major, călătorii pe graniţă şi participare la manevrele anuale.

Art. 7. Examenele vor avea loc în fiecare an, pe cursuri, îndată ce unul este terminat, iar examenul general va avea loc în luna octombrie a anului al 2-lea de studiu, asupra tuturor materiilor predate în şcoală şi înaintea juriului compus cum se va prescrie mai jos.

Afară de examene elevii vor fi supuşi la interogaţiuni asupra cursurilor şi vor executa în fiecare lună cel puţin o compoziţie scrisă la materiile hotărâte de direcţia studiilor.

Elevii vor fi exercitaţi la exerciţiul tactic al celor trei arme.

Exerciţiul pe teren se va face cu unităţi de garnizoană.

Art. 8. Toate cursurile vor fi obligatorii şi următoarele:

Anul I

Istoria militară	*30 lecţii*
Tactica infanteriei	*24 lecţii*
Tactica cavaleriei	*12 lecţii*
Mobilizarea	*14 lecţii*
Geografia militară generală	*20 lecţii*
Artileria şi tactica sa	*25 lecţii*
Fortificaţia	*20 lecţii*
Limba franceză	*20 lecţii*
Limba germană	*20 lecţii*

Anul al II-lea

Istoria militară	*30 lecţii*
Tactica şi strategia generală	*15 lecţii*
Geografia militară a României	*10 lecţii*
Telegrafia militară	*10 lecţii*
Căi ferate	*10 lecţii*
Serviciul de stat major	*25 lecţii*
Fortificaţia	*15 lecţii*
Administraţia	*20 lecţii*
Dreptul internaţional	*15 lecţii*
Limba germană	*20 lecţii*
Limba franceză	*20 lecţii*

Programele analitice se vor face de profesorii respectivi şi se vor aproba în prealabil de Comitetul Consultativ de Stat Major.

Art. 9. Profesorii acestei şcoli se vor numi de ministrul de Război, după propunerea Comitetul Consultativ de Stat Major.

Art. 10. Juriul de examinare, atât pentru admitere în şcoală, cât şi pentru absolvire, se va compune din trei ofiţeri superiori, brevetaţi din cele trei arme, şi doi membri din Comitetul Consultativ de Stat Major, din care unul preşedinte.

Juriul de examinare pentru admitere în şcoală va consta, după memoriile şi recomandările ofiţerilor candidaţi, conduita şi aptitudinea lor militară, şi un medic superior militar va da avizul său asupra constituţiei fizice a candidaţilor. Cei recunoscuţi improprii vor fi eliminaţi de la concurs.

Şeful Statului Major General va avea supravegherea atât asupra mersului, cât şi asupra examenelor în general.

Art. 11. La finele anului întâi, ofiţerii elevi, care se vor dovedi prin examenele parţiale că nu pot urma mai departe, se vor aduce înaintea juriului examinator, care se va pronunţa în mod definitiv şi, după raportul şefului Statului Major General, se vor trimite la corpurile lor.

De asemenea, la finele anului al II-lea, ofiţerii elevi care nu vor lua examenul de absolvire vor fi trimişi la corpurile lor.

Repetări de clase nu se vor admite sub niciun motiv.

Art. 12. Ofiţerii absolvenţi ai Şcolii Superioare de Război vor fi clasaţi pe rând de merit[17], se vor primi brevetul de stat major şi vor fi trimişi a face un stagiu de instrucţie de câte un an în corpuri de trupă, la o altă armă decât aceea de unde au venit, şi acolo vor comanda cel puţin timp de 6 luni o

companie, baterie sau escadron.

Art. 13. După stagiul de instrucţie la trupă, ofiţerii brevetaţi vor fi chemaţi, în rândul clasării lor de merit, a face stagiul de stat major 2 ani la Marele Stat Major şi 1 an în statele majore de corp de armată şi divizie.

Dacă în timpul stagiului la trupă şi în serviciile succesive de stat major se va constata că unii din ofiţerii brevetaţi nu corespund condiţiilor de aptitudine cerute, acei ofiţeri, după propunearea şefului de Stat Major General şi avizul Comitetului Consultativ de Stat Major, vor fi înapoiaţi la armele lor.

Art. 14. Un regulament interior al şcolii se va elabora de ministrul nostru secretar de stat la Departamentul de Război, care este însărcinat cu executarea decretului de faţă.

Dat în Castelul Peleş, la 8 august 1889.

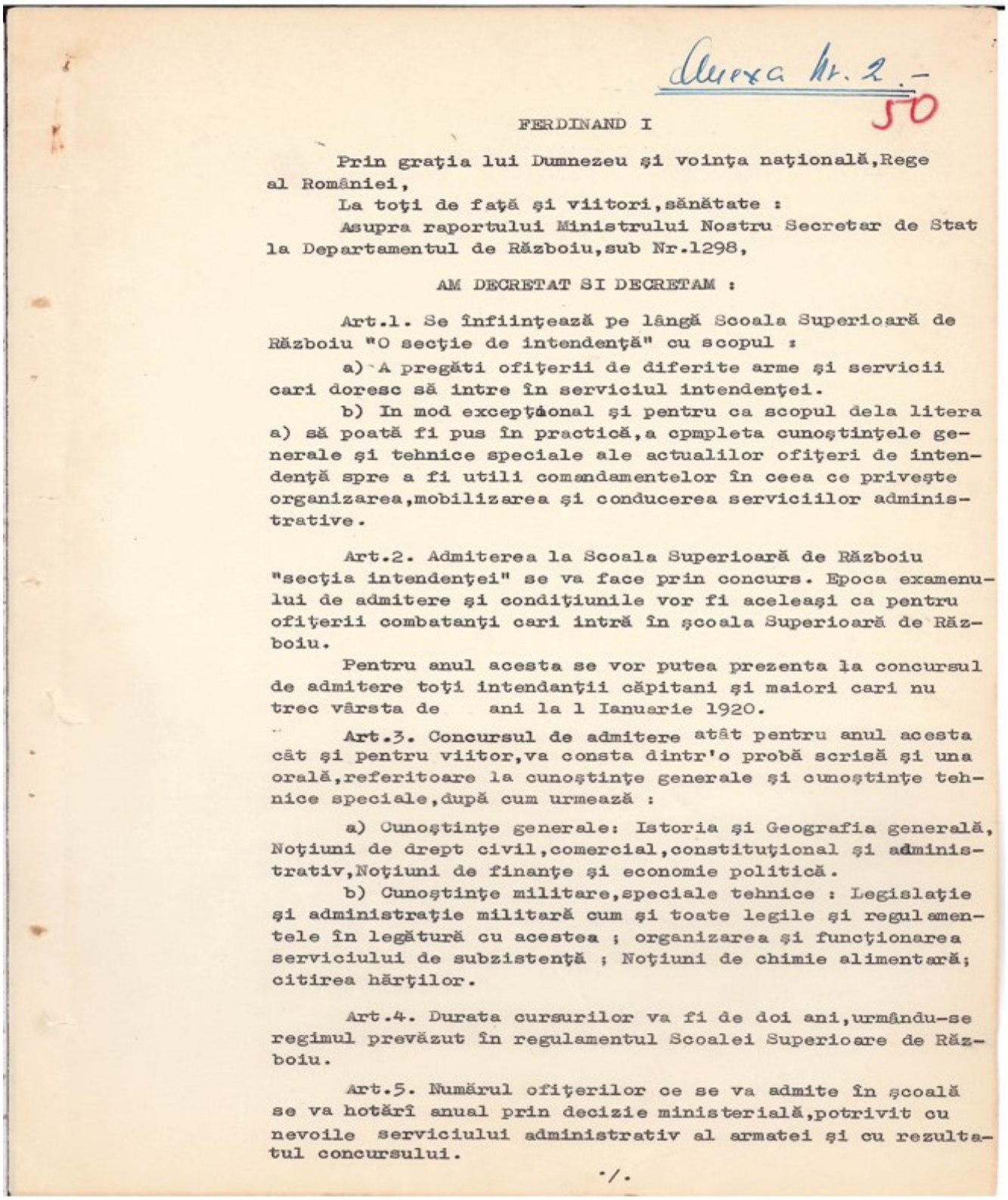
CAROL

Ministru de Război
General Gheorghe Manu

Monitorul Oastei, nr. 55/ 19 august 1889, pp. 891-894.

APPENDIX 2

DECREE OF ESTABLISHING "INTENDANCE SECTION" WITHIN SUPERIOR WAR SCHOOL, November 6th, 1919



Anexa Nr. 2.-
50

FERDINAND I

Prin graţia lui Dumnezeu şi voinţa naţională, Rege al României,

La toţi de faţă şi viitori, sănătate :

Asupra raportului Ministrului Nostru Secretar de Stat la Departamentul de Război, sub Nr.1298,

AM DECRETAT SI DECRETAM :

Art.1. Se înfiinţează pe lângă Scoala Superioară de Război "O secţie de intendenţă" cu scopul :

a) A pregăti ofiţerii de diferite arme şi servicii cari doresc să intre în serviciul intendenţei.

b) In mod excepţional şi pentru ca scopul dela litera a) să poată fi pus în practică, a cpmpleta cunoştinţele generale şi tehnice speciale ale actualilor ofiţeri de intendenţă spre a fi utili comandamentelor în ceea ce priveşte organizarea, mobilizarea şi conducerea serviciilor administrative.

Art.2. Admiterea la Scoala Superioară de Război "secţia intendenţei" se va face prin concurs. Epoca examenului de admitere şi condiţiunile vor fi aceleaşi ca pentru ofiţerii combatanţi cari intră în şcoala Superioară de Război.

Pentru anul acesta se vor putea prezenta la concursul de admitere toţi intendanţii căpitani şi maiori cari nu trec vârsta de ani la 1 Ianuarie 1920.

Art.3. Concursul de admitere atât pentru anul acesta cât şi pentru viitor, va consta dintr'o probă scrisă şi una orală, referitoare la cunoştinţe generale şi cunoştinţe tehnice speciale, după cum urmează :

a) Cunoştinţe generale: Istoria şi Geografia generală, Noţiuni de drept civil, comercial, constituţional şi administrativ, Noţiuni de finanţe şi economie politică.

b) Cunoştinţe militare, speciale tehnice : Legislaţie şi administraţie militară cum şi toate legile şi regulamentele în legătură cu acestea ; organizarea şi funcţionarea serviciului de subzistenţă ; Noţiuni de chimie alimentară; citirea hărţilor.

Art.4. Durata cursurilor va fi de doi ani, urmându-se regimul prevăzut în regulamentul Scoalei Superioare de Război.

Art.5. Numărul ofiţerilor ce se va admite în şcoală se va hotărî anual prin decizie ministerială, potrivit cu nevoile serviciului administrativ al armatei şi cu rezultatul concursului.

·/·

57

Art.6. Anul acesta concursul de admitere va avea loc la M.St.M. (Scoala Superioară de Războiu) în prima jumătate a lunei Decemvrie.

Cererile de admitere la concurs, înaintate prin corpurile de trupă, comandamentele şi serviciile respective însoţite de aprecierile tuturor şefilor erarhici, vor trebui să sosească la M.St.M. (Scoala Superioară de Războiu), cel mai târziu la 1 Decemvrie 1919.

Pentru viitor admiterea la concurs se va face potrivit dispozitiunilor ce se vor prevedea în regulamentul Scoalei Superioare de Războiu (pentru secţia Intendenţei).

Art.7. Toate dispoziţiunile de detaliu relative la : funcţionarea secţiei de intendenţă, profesori, personalul de cadre al şcoalei, cursuri, programe, sisteme de cotare, examene, etc. se vor ştabili într'un regulament special, ce va forma o anexă a regulamentului Scoalei Superioare de Războiu.

Art.8. Ministru Nostru Secretar de Stat la Departamentul de Războiu este însărcinat cu executarea decretului de faţă.

Dat la Castelul Peleş, la 6 Noemvrie 1919.

FERDINAND.

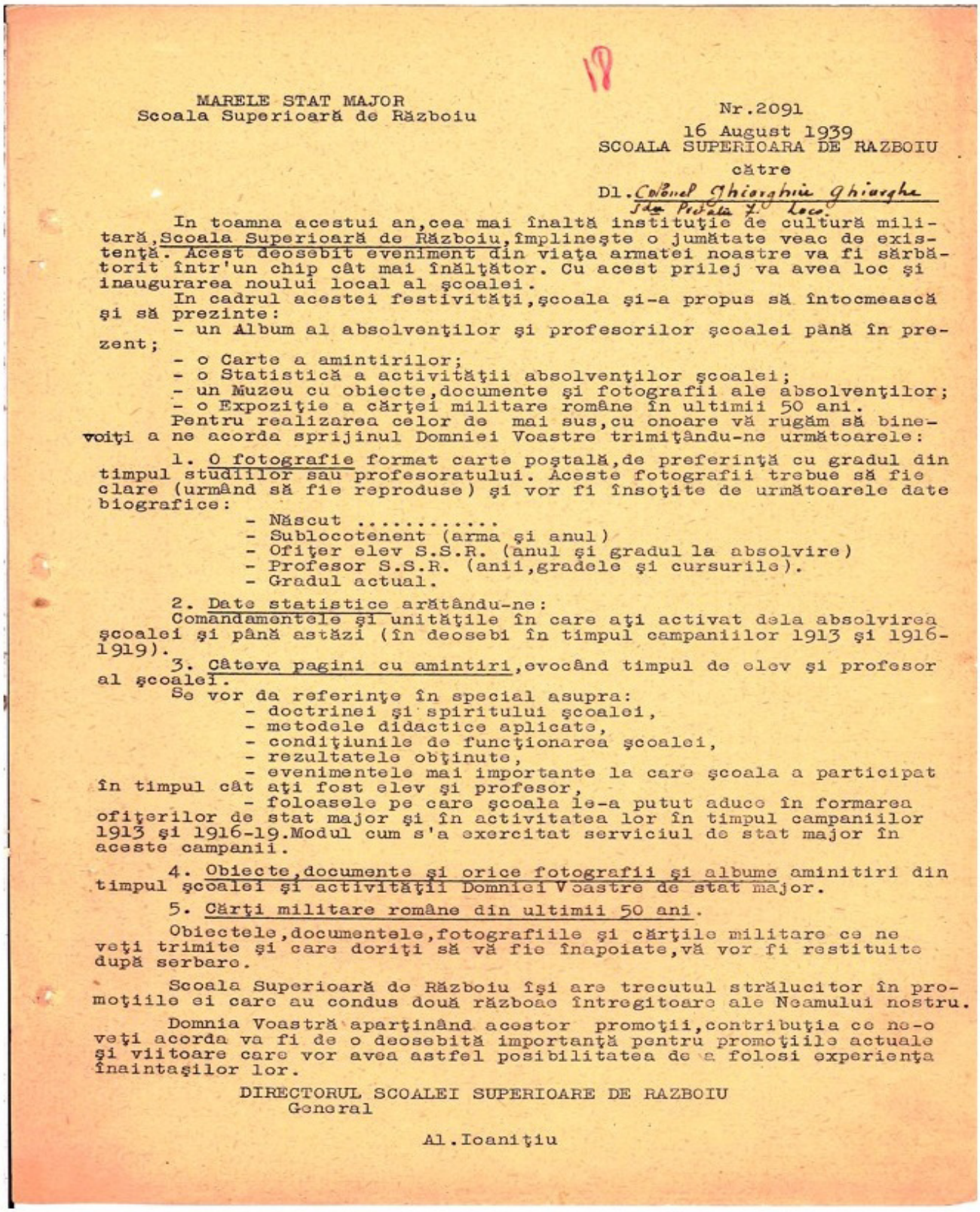
MINISTRU DE RAZBOIU
GENERAL DE BRIGADA
Ion Răşcanu

Nr. 4729

National Military Archives, The Superior School of War Fund, file no. 417, tab. 50-51.

APPENDIX 3

CALL FOR GATHERING MATERIALS UPON 50TH ANNIVERSARY OF SUPERIOR WAR SCHOOL, 1937



MARELE STAT MAJOR
Scoala Superioară de Războiu

Nr.2091
16 August 1939
SCOALA SUPERIOARA DE RAZBOIU

către

Dl. Colonel Ghiorghiu Ghiorghe
Str. Postăi 7. Loco.

In toamna acestui an, cea mai înaltă instituţie de cultură militară, Scoala Superioară de Războiu, împlineşte o jumătate veac de existenţă. Acest deosebit eveniment din viaţa armatei noastre va fi sărbătorit într'un chip cât mai înălţător. Cu acest prilej va avea loc şi inaugurarea noului local al şcoalei.

In cadrul acestei festivităţi, şcoala şi-a propus să întocmească şi să prezinte:

- un Album al absolvenţilor şi profesorilor şcoalei până în prezent;
- o Carte a amintirilor;
- o Statistică a activităţii absolvenţilor şcoalei;
- un Muzeu cu obiecte, documente şi fotografii ale absolvenţilor;
- o Expoziţie a cărţei militare române în ultimii 50 ani.

Pentru realizarea celor de mai sus, cu onoare vă rugăm să binevoiţi a ne acorda sprijinul Domniei Voastre trimiţându-ne următoarele:

1. O fotografie format carte poştală, de preferinţă cu gradul din timpul studiilor sau profesoratului. Aceste fotografii trebue să fie clare (urmând să fie reproduse) şi vor fi însoţite de următoarele date biografice:
   - Născut .....
   - Sublocotenent (arma şi anul)
   - Ofiţer elev S.S.R. (anul şi gradul la absolvire)
   - Profesor S.S.R. (anii, gradele şi cursurile).
   - Gradul actual.

2. Date statistice arătându-ne:
Comandamentele şi unităţile în care aţi activat dela absolvirea şcoalei şi până astăzi (în deosebi în timpul campaniilor 1913 şi 1916-1919).

3. Câteva pagini cu amintiri, evocând timpul de elev şi profesor al şcoalei.
Se vor da referinţe în special asupra:
   - doctrinei şi spiritului şcoalei,
   - metodele didactice aplicate,
   - condiţiunile de funcţionarea şcoalei,
   - rezultatele obţinute,
   - evenimentele mai importante la care şcoala a participat în timpul cât aţi fost elev şi profesor,
   - foloasele pe care şcoala le-a putut aduce în formarea ofiţerilor de stat major şi în activitatea lor în timpul campaniilor 1913 şi 1916-19. Modul cum s'a exercitat serviciul de stat major în aceste campanii.

4. Obiecte, documente şi orice fotografii şi albume aminitiri din timpul şcoalei şi activităţii Domniei Voastre de stat major.

5. Cărţi militare române din ultimii 50 ani.

Obiectele, documentele, fotografiile şi cărţile militare ce ne veţi trimite şi care doriţi să vă fie înapoiate, vă vor fi restituite după serbare.

Scoala Superioară de Războiu îşi are trecutul strălucitor în promoţiile ei care au condus două războae întregitoare ale Neamului nostru.

Domnia Voastră aparţinând acestor promoţii, contribuţia ce ne-o veţi acorda va fi de o deosebită importanţă pentru promoţiile actuale şi viitoare care vor avea astfel posibilitatea de a folosi experienţa înaintaşilor lor.

DIRECTORUL SCOALEI SUPERIOARE DE RAZBOIU
General

Al. Ioanitiu

National Military Archives, The Superior School of War Fund, file no. 413, tab. 18.

APPENDIX 4

RENEWED CALL (TO THE ONE IN 1937) FOR PAYING TRIBUTE TO THE SUPERIOR WAR SCHOOL, 1939

32

MARELE STAT MAJOR
Scoala Superioară de Războiu.

SEMICENTENARUL SCOALEI
SUPERIOARE DE RAZBOIU.
1889 - 1939

A P E L
către
Absolvenţii şi Profesorii Scoalei Superioare de Războiu şi Scoalei Superioare de Intendenţă.

In toamna acestui an, cea mai înaltă instituţie de cultură militară, Scoala Superioară de Războiu, împlineşte o jumătate veac de existenţă. Acest deosebit eveniment din viaţa armatei noastre va fi sărbătorit într'un chip cât mai înălţător. Cu acest prilej va avea loc şi inaugurarea noului local al şcoalei.

In cadrul acestei festivităţi, Scoala şi-a propus să întocmească şi să prezinte :

- un Album al absolvenţilor şi profesorilor şcoalei până în prezent;
- o Carte a amintirilor;
- o Statistică a activităţei absolvenţilor şcoalei;
- un Muzeu cu obiecte, documente şi fotografii ale absolvenţilor;
- o Expoziţie a cărţei militare române în ultimii 50 ani.

Pentru realizarea celor de mai sus, sunteţi rugaţi a ne acorda sprijinul trimiţându-ne imediat următoarele :

1. O fotografie format carte postală, de preferinţă cu gradul din timpul studiilor sau profesoratului. Aceste fotografii să fie clare urmând să fie reproduse, vor fi însoţite de următoarele date biografice:
   - Născut .....
   - Sublocot.(arma şi anul)
   - Ofiţer elev S.S.R.(anul şi gradul la absolvire)
   - Profesor S.S.R.(anii , gradele şi cursurile),
   - Gradul actual.

2. Date statistice arătându-ne :
Comandamentele şi unităţile în care aţi activat dela absolvirea şcoalei şi până astăzi (în deosebi în timpul campaniilor 1913 şi 1916-1919).

3. Câteva pagini cu amintiri, evocând timpul de elev şi profesor al şcoalei.
Se vor da referinţe în special asupra :
- doctrinei şi spiritului şcoalei,
- metodele didactice aplicate,
- condiţiunile de funcţionarea şcoalei,
- rezultatele obţinute,
- evenimentele mai importante la care şcoala a participat în timpul cât aţi fost elev şi profesor,
- foloasele pe care şcoala le-a putut aduce în formarea ofiţerilor de stat major şi în activitatea lor în timpul campaniilor 1913 şi 1916-19. Modul cum s'a exercitat serviciul de stat major în aceste campanii.

4. Obiecte, documente şi orice fotografii şi albume amintiri din timpul şcoalei şi activităţei Dvs.de stat major.

5. Cărţi militare române din ultimii 50 ani.

./.

- 2 - 33

Reuşita organizării lucrărilor de mai sus depinde numai de bunăvoinţa cu care Dvs.veţi răspunde - complect şi imediat - apelului şcoalei al cărei elev aţi fost.

Stăruim a vă atrage atenţiunea asupra numărului mare al acelora care încă nu au răspuns primului apel şi asupra timpului extrem de scurt care a mai rămas până la sărbătorirea semicentenarului.

DIRECTORUL SCOALEI SUPERIOARE DE RAZBOIU
GENERAL
Al.Ioanitiu

N o t ă:

Acest apel -începând din 1937- a fost repetat timp de 2 ani prin ziare, Monitorul Oastei (Nr.1,2,3,4,10,11 şi 12/1938) şi radio.

Acei care nu au trimis nici o dată sau au trimis date necomplecte, vor înainta imediat şcoalei, cele cerute prin prezentul apel.

Acei care au trimis toate cele cerute mai sus, ne vor comunica imediat data când ni le-au trimis.

---o---

National Military Archives, The Superior School of War Fund, file no. 413, tab. 32-33.

APPENDIX 5

FIRST ISSUE OF THE BULLETIN OF SUPERIOR WAR SCHOOL, APRIL-MAY 1937

ANUL I No. 1 APRILIE şi MAI 1937.

BULETINUL No. 1

Aprobat de Marele Stat Major

cu No. 2872 din 23. I. 1937.

SUMARUL:

DIRECŢIA, REDACŢIA ŞI ADMINISTRAŢIA.
ŞCOALA SUPERIOARĂ DE RĂZBOIU.
B-DUL I. C. BRĂTIANU No. 19 BUCUREŞTI.

Cuvânt înainte.

Regulamentul Şcoalei Superioare de Războiu, la art. 1, defineşte scopul Şcoalei astfel:

a) a răspândi în armată cunoştinţele militare superioare;

b) a procura ofiţerilor de toate armele o bază de pregătire în vederea comandei şi conducerii Marilor Unităţi, şi în vederea alegerii ofiţerilor de Stat-major.

Primul postulat regulamentar poate fi adus la îndeplinire prin două procedee, şi anume:

Unul, *cel deja practicat, prin ofiţerii absolvenţi ai Şcoalei, cu ocazia serviciului lor la trupă sau la comandamente.*

Procedeul acesta este aşa de lent faţă de rapiditatea de astăzi a progresului ştiinţei militare, încât se riscă ca doctrina de abia răspândită în armată să devină perimată.

Ineficacitatea lui mai provine şi din faptul că ofiţerii tineri de Stat-major, neavând nici autoritatea necesară, nici experienţă suficientă, nu pot să impună cunoştinţele primite în Şcoală; deci răspândirea lor, şi din această cauză, lasă de dorit.

Trebue însă recunoscut că acest sistem are un avantaj incontestabil, acela de a se servi de elemente vii, care pot să acţioneze direct, să aplice noile idei, să convingă şi să însufleţească, pe cel cu care vin în contact.

Un alt *procedeu este publicaţiunea. Prin aceasta se obţine:*

— difuzarea noilor idei, mult mai rapid, ea având loc în acelaş timp cu predarea cursurilor în Şcoală;

— ţinerea la curent a comandamentelor cu un material intelectual oficial, verificat prin numeroase dezbateri, foarte

ISTORICUL

ŞCOALEI SUPERIOARE DE RAZBOIU

1889–1939.

BUCUREŞTI

1939

NOTES:

1 History of the General Staff Documents 1859 - 1947, p. 5.

2 Ioan Scurtu, *The Inter-war Romanian Civilization* (1918-1940), Bucharest, Publishing House Romania Foundation, 2008, p. 24.

3 The Superior War School, *History of the Superior War School* 1889–1939, Bucharest, 1939, p. 376. From 1919 to 1939, 49 Romanian officers and 8 Romanian officers were sent to study the great art of war in Paris. The same account of scientific activity also highlighted the vast Romanian military literature "materialized in deep studies and material improvements of all kinds".

4 Central National Historical Archives Service (hereinafter SANIC), Fălcoianu Family Fund, file no. 4, tab 1 - 4. Ştefan Fălcoianu (06.06.1835 - 22.01.1905) graduated from the General Staff School in Paris in 1862, attached to the French Army until 1864; between 1870 and 1877 he was general manager of the Telegraphs and Posts; in 1876 he was appointed a member of the Romanian Academy, then held the position of vice-president; froms 20.10.1877 he was appointed Chief of Staff and took part in the actions of the Romanian Army in Plevna and Vidin; from 20.10.1883 he was director of the Romanian Railways; on 10.03.1883 he was promoted to brigadier general; between 23.06.1883 and 13.01.1886 he was war minister and general inspector of military schools in Ion Brătianu's office; on 10.05.1892 he was promoted to the rank of division general; on 08.06.1894 he was appointed commander of the 1st Corps of the Romanian Army; on 12.06.1894 he resigned from the army.

5 «Army Magazine», no. 21-22 / 1889, pp. 764-765.

6 Military Academy, General Military Academy, Academy of High Military Studies, National Defense University, «Carol I» National Defense University, the name received by Government Decision no. 969/25 August 2005.

7 Superior War School, *History of Superior War School 1889–1939*, Bucharest, 1939, p. 299.

8 *Ibidem*, p. 304.

9 See the article «80 years in the service of the military academic community: Bulletin of «Carol I» National Defense University between tradition and modernity», Laura-Rodica Hîmpă, "Bulletin of «Carol I», National Defense University, vol. IV, no. 2/2017, pp. 9-16. Also available at www.buletinul.unap.ro

10 The Regulations of the Superior War School, in*: Bulletin of the High School of War*, 1937, no. 1, April-May, p. 5. The issuance of the Bulletin was approved by the General Staff, order no. 2872/23 January 1937.

11 *Ibidem*, p. 6.

12 *Ibidem*.

13 Decision of the Government of Romania, no. 305/23 April 1991.

14 Decision of the Government of Romania, no. 1027/28 August 2003

15 Decision of the Government of Romania, no. 969/25 August 2005.

16 Mircea Mureşan, *National Defence University, Short History*, Bucharest, Publishing House of the National Defence University, 2004, p. 11.

17 În ordinea mediilor obţinute.

BIBLIOGRAPHY

The Romanian National Military Archives, the Higher War College Fund.

Romanian National Archives, Ştefan Fălcoianu Fund.

Bulletin of the Romanian Military Archives 1998–2019.

Bulletin of the Superior War School 1937–1948.

Bulletin of "Carol I" National Defence University.

Official Monitor 1872–2019.

Monitor of the Army 1872–1948.

Army Magazine 1877–1948.

Journal of Military History 2010–2019.

Journal of Royal Foundations 1934–1948.

Caracostea Dumitru, *The psychological aspect of the war,* Bucharest, "Cartea Românească" Publishing House, 1922.

Iorga Nicolae, *The History of Romanian Education*, Bucharest, Didactic and Pedagogical Publishing House, 1971.

Iorga Nicolae, *History of the Romanian army*, Bucharest, War Ministry Publishing House, vol. I, II, 1931.

Iorga Nicolae, *Soul states and wars. Lessons at the Superior War School in 1938*, Bucharest, Typography of the Superior War School, 1939.

History of the Romanian General Staff. Documents 1859-1947, Bucharest, Military Publishing House, 1994.

History of the Superior War School, Bucharest 1889–1939, Bucharest, Typography of the Superior War School, 1939.

Muresan Mircea, *National Defence University, short history,* Bucharest, National Defence University Publishing House, 2004.

Short John, *The inter-war Romanian civilization (1918-1940)*, Bucharest, Publishing House Romania Foundation, 2008.

Editor-in-Chief
Laura MÎNDRICAN
Editor
Irina TUDORACHE
Proof-Readers
Mariana ROŞCA

Sub-editor
Liliana ILIE
Cover
Andreea GÎRTONEA

ISSN (online) 2284-9378

The publication consists of 108 pages.

"Carol I" National Defence University Publishing House
Bucharest, no. 68-72 Panduri Street, 5 sector
e-mail: *buletinul@unap.ro*
Phone: 319.48.80/0215; 0453

1672/2019 C. 215/2019

AGENȚIA ROMÂNĂ DE ASIGURARE A CALITĂȚII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR
ROMANIAN AGENCY FOR QUALITY ASSURANCE IN HIGHER EDUCATION
Membră ENQA – Full member of ENQA
Înregistrată în EQAR – Registered in EQAR

ARACIS

CERTIFICAT
CERTIFICATE

Universitatea Națională de Apărare „Carol I" din București

a obținut, în urma evaluării instituționale, calificativul
GRAD DE ÎNCREDERE RIDICAT
pentru perioada 2015-2020
following institutional evaluation, attained the HIGH DEGREE OF CONFIDENCE rating for the period 2015-2020

BIROUL EXECUTIV AL CONSILIULUI ARACIS
EXECUTIVE BUREAU OF ARACIS

Președinte
President
Prof. univ. dr. Petrescu Iordan

Vicepreședinte
Vice President
Prof. univ. dr. Ghițulică Cristina

Director Departament de Evaluare Externă a Calității
Director of the Evaluation Department
Prof. univ. dr. Popa Ion

Director Departament de Acreditare
Director of the Accreditation Department
Prof. univ. dr. ing. Lache Simona

Secretar General
General Secretary
Prof. univ. dr. Stan Vasilica

Data eliberării/Release date:
29.10.2015

Nr. 129/2015

IEP
EUA Institutional Evaluation Programme

Institutional Evaluation Programme
Performance in Research, Performance in Teaching – Quality, Diversity and Innovation in Romanian Universities Project

"CAROL I - NATIONAL DEFENCE UNIVERSITY"
BUCHAREST-ROMANIA

Scientific peer-review publication indexed in international databases EBSCO, CEEOL & GOOGLE Scholar .

"Carol I" National Defence University Publishing House
Bucharest/Romania, sector 5, 68-72 Panduri Street
e-mail: buletinul@unap.ro
Phone: 319.48.80/0215; 0453

"CAROL I" NATIONAL DEFENCE UNIVERSITY
(Highly appreciated publishing house within "Military science, intelligence and public order"
of Titles, Diploma and University Certificates Awards National Council)

ISSN 2284-936X
L 2284-936X