MILITARY NATIONAL SECURITY SERVICE

NATIONAL SECURITY REVIEW

Issue 1/2024

BUDAPEST
2024

Scientific Periodical of the
Military National Security Service

Responsible Publisher:

Maj. Gen. Norbert Tajti, Director General
Chairman of the Scientific Board

Postal Address

Katonai Nemzetbiztonsági Szolgálat Tudományos Tanácsa
1021 Budapest, Budakeszi út 99-101.
1525 Budapest, Pf. 74.

Colonel István Talián
06(1) 386-9344/1504, HM 61-504
e-mail: natsecreview@knbsz.gov.hu

website:
https://www.knbsz.gov.hu/hu/publikaciok.html

HU ISSN 2063-2908

Publication Conditions

Dear Authors,

The e-mail address, publication conditions and reference system of the National Security Review magazine have been renewed. Due to the changes, please review the new set of conditions at the end of the scientific periodicals. (In addition to the previous ones, it can also be found in digital form at https://www.knbsz.gov.hu/hu/publikaciok.html)

Manuscripts intended for the National Security Review magazine starting with the 2nd issue of 2024 are requested to be submitted according to the new guidelines, given that the proofreading will also be done accordingly.

Thanks for your understanding and cooperation:

The Responsible Editor

TABLE OF CONTENTS

ALEXANDRU MALACENCO PhD

INTELLIGENCE STRUCTURES IN THE SOVIET MOLDAVIA, IN THE FIRST POST-WAR YEARS

Abstract

After more than three decades since the USSR collapsed, the subject regarding the contribution of the Soviet espionage to the process of reestablishing the Soviet power in Bessarabia has remained unstudied. Based on the documents from the Archive of the Security and Intelligence Service of the Republic of Moldova, the author aims to analyse the organizational structure, the duties and the staff of one of the most veiled units of the People's Commissariat for State Security (in Russian: NKGB) of the Moldavian SSR, in the period between 1944 and 1945 – the UNIT (Department) 1 of foreign intelligence, (in Russian: razvedka). Unit 1 of the NKGB of the Moldavian SSR was responsible for foreign intelligence, or, in other words, it was the espionage service of the Union Republic outside the Soviet Union.

Ethnical composition of the unit 1 of the NKGB' staff of and the peculiarities of its organization will point out who the soldiers from the first line of the 'invisible front' were and what was their role in the process of institutionalizing the Soviet power in the Moldavian SSR, in the first post-war years. The main question that arises is who were in the service of "Moldavian espionage", in the first post-war years? So, we will try to analyse and give answers to it.

Keywords: Unit 1 of the NKGB, espionage, organizational structure, staff, Moldavian SSR, the Soviet Union.

Introduction

Espionage[1] and history have one common trait – they are placed between crooked mirrors, so (often) you no longer know who is lying and who is telling the truth. In general, it is spoken about espionage openly very rarely and very little. Traditionally, official historiography somehow overshadows the score executed by espionage and its role in the course of historical events.

[1] Espionage – activity through which military, political, economic or other secret information is obtained through spies, secret agents or illegal means of surveillance. In some cases, it differs from the broader category of obtaining information through aggressive working and illegal methods. Counter-espionage aims to detect and prevent espionage by the opposite party. CAMPEANU, Ilies – MARINESCU, Cornelia (eds.): *Universal Encyclopedia Britannica*. Litera Publishing House, Bucharest, 2010/14, p. 310.

More than three decades after the breakup of the USSR, the contribution of Soviet espionage to the process of restoring Soviet power in Bessarabia has remained an unstudied topic. Although historian Pavel Moraru has written several extensive works on the topic of secret services in Bessarabia, during the XX century,[2] it is worth mentioning that expressly that to the NKGB Moldavian SSR Department 1 (the espionage service of the Union Republic) has not been dedicated any study. Another work that mentions tangentially the activity of Soviet espionage in Bessarabia is the volume with the memoirs of Gavriil Volkov, President of the KGB of the Moldavian SSR, between 1979 and 1989.[3] It should be noted that the author is limited to the case of Soviet spies – "Gheorghe Emanuel and the Zoti family" – operating in Bessarabia since 1931, but without making any specific mention about the topic of this study.

In this context, in order to complete the attested historiographical vacuum, based on unpublished documents from the Archive of the Security and Intelligence Service of the Republic of Moldova, the author aims to analyse the organizational structure, the functional attributions and the staff of one of the most secret departments of the People's Commissariat for State Security (in Russian: NKGB) of the Moldavian SSR, between 1944-1945 – Department 1 for foreign intelligence. Department 1 of the NKGB of the Moldavian SSR was responsible for foreign intelligence activity, or, in other words, it was the espionage service of the Union Republic outside the border of the Soviet Union.

In this scientific approach, we will focus, in particular, on the analysis of the ethnic composition of the staff of the NKGB Department 1 of the Moldavian SSR and the specifics of its structural organization. Elucidating these elements will allow us to understand who were the invisible soldiers on the front line of the "shadow front", as well as their role in the process of re-establishing and consolidating Soviet power in the Moldavian SSR since 1944?

---

[2] MORARU, Pavel: *Urmașii lui Felix Dzerjinski: organele Securității Statului în Republica Sovietică Socialistă Moldovenească 1940–1991*. [Descendants of Felix Dzerzhinski: State Security organs in the Moldavian Soviet Socialist Republic 1940-1991.] National Institute for the Study of Totalitarianism, Bucharest, 2008.; MORARU, Pavel: *SMERȘ in Bessarabia 1944–1954.* Editura Militară, Bucharest, 2013.; Pavel Moraru, *Serviciile Secrete și Basarabia, dicționar 1918–1991*. [The Secret Services and Bessarabia, dictionary 1918–1991.] Bucharest, Editura Militară, 2008.; MORARU, Pavel: Organizarea și activitatea structurilor securității statului din RSSM [The organization and activity of the state security structures in the SSSR] (1940-1991). In: COROBCA, Liliana (ed.): *Panorama Comunismului în Moldova Sovietică*. [Panorama of Communism in Soviet Moldova] Polirom, Bucharest, 2019, pp. 312-314.

[3] ВОЛКОВ, Гавриил: *Взгляд Через Десятилетия.* [VOLKOV, Gavriil: A look over decades.] SIS of the Republic of Moldova, Chisinau,2004, pp. 113-136.

By this study,[4] the author tries to bring to the attention of the reader an original and almost unresearched subject in the local historiography. The research is meant to fill in like a puzzle piece the knowledge void related to the history of the espionage structure in the Soviet Moldavia, starting with the first post-war years – who created it, who managed it and whose interests it served. Aside from the ordinary curiosity towards the espionage activity and spies in general, we consider this subject of high interest for those interested in studying the history of the Soviet security bodies in Bessarabia, as the new data made available expand the knowledge horizon in this field of research in the local historiography.

"Moldavian espionage", in the first post-war years

Between March and August 1944, Bessarabia was occupied and "absorbed" by the USSR for the second time, being territorially broken up and transformed into a Union Republic – the Moldavian SSR – arbitrarily constituted by Moscow on August 2, 1940[5]. The same Soviet security organs that operated in 1940-1941 were also involved in the process of territorial reoccupation of Bessarabia in 1944,[6] in order to re-establish and institutionalize Soviet power.

---

4 In a primary version the study was published by the author in 2021 in a collection of articles: MALACENCO, Alexandru: Cine activa în serviciul „spionajului moldovenesc" în anii 1944-1945? [Who worked in the service of Moldavian espionage" in 1944-1945?] *Latinitate, Romanitate, Românitate,* CEP USM, Chișinău, 2021/4, pp. 213-221.

5 Following the annexation of Bessarabia on June 28, 1940 by the Soviet Union, on August 2, 1940, the Supreme Soviet of the USSR adopted the *Law on the Formation of the Moldavian Soviet Socialist Republic*. The final territorial size of the Moldavian SSR was the result of transactions between the Soviet leadership in Moscow and that of the Ukrainian SSR. Therefore, the composition of the Moldavian SSR included the districts of Grigoriopol, Dubasari, Camenca, Ribnita, Slobozia, Tiraspol in the former Moldavian Autonomous Soviet Socialist Republic and six counties of Bessarabia (Balti, Bender, Cahul, Orhei, Soroca and Chisinau). And Northern Bucovina, Hotin, Ismail, Cetatea Alba counties were forcibly, arbitrarily included in the Ukrainian SSR. Thus, the Moldavian SSR remained with an area of 33, 7 thousand km² of Bessarabia, which had 44,422 km². "*The formation of the Moldavian SSR resulted in the amputation of the territory of Bessarabia, the territorial disintegration of the Bessarabian population, the dispossession and the inclusion of its territory in various administrative units of Soviet Ukraine*". For more details see: MORARU, Anton: *Istoria Romanilor: Basarabia și Transnistria 1812-1993*. [History of the Romanians: Bessarabia and Transnistria 1812-1993.] Aiva Publishing House, Chișinau,1995, pp. 324-330; PETRENCU, Anatol: *Basarabia în al Doilea Război Mondial 1939–1945*. [Bessarabia in the Second World War 1939–1945.] Prut Internațional, Chișinau, 2006, pp. 29-33; GRIBINCEA, Mihai: *Basarabia în primii ani de ocupație sovietică 1944–1950.* [Bessarabia in the first years of Soviet occupation 1944–1950.] Dacia, Cluj-Napoca, 1995, p. 17, 29.

6 MALACENCO, Alexandru: Serviciile de securitate în teritoriile „eliberate" de către URSS în primii ani postbelici. [State security services in the territories „liberated" by the USSR in the first postwar years.] In: PREUTU, Cristina – PETRENCU, Anatol: *Fațete ale Comunismului în România și în R(A)SS Moldovenească. Politică, Societate și Economie*. [Facets of Communism in Romania and in the Moldavian R(A)SS.] Publishing House Universității "Al. I. Cuza", Iaşi, 2020, p. 66.

Thus, *"the Soviet NKGB was re-established in the Moldavian SSR with the gradual occupation of the territory of Bessarabia, in the spring-summer of 1944, by the Red Army. From the point of view of the organizational structure, the NKGB-MGB of the Moldavian SSR represented a smaller replica or a miniature copy of the Soviet «secret police» of the USSR"*.[7] Therefore, the number, name and attributions of the NKGB subdivisions of the Moldavian SSR were largely similar to those of the NKGB of the USSR, but adjusted to the territorial area and the territorial-administrative division of the Union Republic, during 1944–1946.[8]

Therefore, the nomenclature of the NKGB subunits of the Moldavian SSR began with department (unit) 1 (first), responsible for foreign intelligence, or, in other words, the espionage subunit of the Union Republic. Consequently, the counterintelligence, according to the NKGB nomenclature of the Moldavian SSR, was assigned direction 2 (two).[9]

Based on the NKGB Order of the Soviet Union, No. 00391 of October 12, 1944, Iosif Mordoveţ – NKGB Commissioner of the Moldavian SSR, on October 30, 1944 issued the order with No. 158, establishing the structure of the staff states of the NKGB Moldavian SSR Department 1.[10] So, from the outset, we learn that the foundation of the structure of the staff states and the organizational chart of the espionage service of the Moldavian SSR in 1944 were based on the express ordinances of the Union NKGB in Moscow.

Analysing the content of Order No. 158 of October 30, 1944, we note that the order itself has an annex that represents a tabular document in which the states of functions assigned to each subdivision of the NKGB of the Moldavian SSR are listed.[11] Therefore, the spy department of the Moldavian SSR consisted of 3 sections and the secretariat, had 17 positions in total, of which 6 were leadership positions.[12]

According to the studied documentary source, NKGB Moldavian SSR Department 1 had the following organizational structure:

Management of department (2 functions);
secretariat (4 functions);
section 1 – intelligence activity in Romania (4 positions);
section 2 – intelligence work on emigration (4 positions);

---

7 MALACENCO, Alexandru: Comisariatul Poporului pentru Securitatea Statului al RSS Moldovenești: Structura Organizatorică între anii 1944-1946. [The People's Commissariat for state security of the Moldavian SSR-organizational structures in the period 1944–1946.], *Akademos, Magazine of Science, Innovation, Culture and Art*, 2019/4, p. 106.

8 Ibid. p. 106.

9 Ibid. p. 104.

10 Archive of the Security and Intelligence Service of the Republic of Moldova (ASISRM), Administrative Fund (f. a.), inventory (inv.) 8, d. 27, f. 327.

11 Ibid. f. 328.

12 Ibid. f. 328.

section 3 – operational registration section (in Russian: учётная информационное отделение; 3 functions).[13]

In addition, we mention that the deputy head of the 1st Department of the NKGB of the Moldavian SSR also held the position of head of section 1 - the informative activity in Romania.[14]

Given that no other archive documents have been identified that would explain the attributions and powers of the NKGB Department 1 sections listed above, we can only deduce them from the name of their area of activity.

It is not by chance that in the organizational structure of the 1st Department of the NKGB of the Moldavian SSR, the 1st section dealt with the specific intelligence activity in Romania. This is explained, on the one hand, by the political and geographical realities of that period, and on the other hand, by the historical and cultural affinity between the Moldavian SSR (Bessarabia) and Romania. Thus, the Moldavian SSR was on the western border of the USSR, bordering on Romania, a country that, in the years of the Second World War, between 1941 and 1944, fought with the Soviet Union. Another element that cannot be neglected and which, from Moscow's perspective, generated threats to the security of the Union Republic, and implicitly to the interests of the Soviet Union, was the fact that Bessarabia, in the interwar period, was part of the Kingdom of Romania. Moreover, linguistically, culturally and historically, Bessarabia was a geographical space inherent to Romania, which was (and is) obvious and well known to Moscow.[15] That being said, and given that the informative activity on Romania was structurally located in the foreground in the organizational chart of NKGB Moldavian SSR Department 1, the section being headed directly by the deputy head of Department 1, the great importance that the NKGB attached to the clandestine obtaining of information of interest from Romania in the first post-war years is outlined.

Although, as mentioned above, the author did not identify archival documents that would stipulate what the tasks are of Section 1 of the 1st Department of the NKGB of the Moldavian SSR, from the Order of Commissioner Iosif Mordoveţ no. 0012 of October 24, 1945, we deduce that one of its activity priorities was to uncover the nests of legionnaires.[16]

---

13 Ibid. f. 328.

14 Ibid. f. 328.

15 Фурман, Дмитрий: *Молдавские молдаване и молдавские румыны: влияние особенностей национального сознания молдаван на политическое развитие Республики Молдова.* [Furman, Dmitry: Moldovan Moldovans and Moldovan Romanians: the influence of the peculiarities of the national consciousness of Moldovans on the political development of the Republic of Moldova.] *Доклады Института Европы № 206, Publishing House: «Русский сувенир», Москва, 2007, pp.* 278-315.

16 ASISRM, f. a., inv. 8, d.7, f. 76.

In the mentioned document, in the context of an incident in the work of legionnaires, the NKGB Moldavian SSR Commissioner sent to the management of Department 1, and directly to the officers of Section 1 (responsible for the informative activity in Romania), indications of the need to ensure thorough preparation and rigorous control of the agents to be sent abroad.[17] Moreover, the content of the Order reveals that section 1, through agents, creates nests of ghost legionnaires to uncover and supervise the authentic ones outside the republic, in this case, Romania. Therefore, we find that the legionaries posed an external danger to the Soviet regime in the Moldavian SSR, and given that the subject was under the control of Commissioner Mordoveţ himself, we appreciate that combating this hostile element was treated with great attention and importance by the espionage structure of the NKGB of the Moldavian SSR.

We point out that the interest of "Moldavian espionage" into Romania was within the priorities of the Union NKGB, where, respecting a certain symmetry, the intelligence activity on Romania was part of Directorate 1 of the General Directorate for Foreign Intelligence of the NKGB of the Soviet Union.[18] Analysing the organizational structure of the NKGB-MGB of the USSR between 1943 and 1946, we deduce that Romania was among the top intelligence priorities of the NKGB of the USSR until 1946, in common with Germany, Poland, Czechoslovakia, Hungary, Bulgaria, Yugoslavia and Greece.[19] The situation changed in 1946, when, after the restructuring of the NKGB into the MGB,[20] directorates 1 and 2 of the Soviet MGB's General Directorate of Foreign Intelligence were dealing with the USA and Great Britain, in the context of the beginning of the "Cold War". At this stage, the intelligence activity in Romania (as well as in Poland, Czechoslovakia, Hungary, Greece, Yugoslavia, Albania, Bulgaria) was managed by the 5th Directorate of the MGB of the USSR,[21] which allows us to deduce that for the Soviet espionage at Union level, the countries in the immediate proximity of the USSR took a back seat in the list of intelligence priorities.

Returning to the analysis of the organizational structure of the NKGB Moldavian SSR Department 1, Section 2 was followed consecutively – the informative activity in emigration.

---

17 Ibid. f. 76.

18 Петров, Н.В.: *Кто руководил органами госбезопасности 1941-1954.* [Who led the States Security Organs 1941-1954.] Handbook, Звенья, Москва, 2010, p. 36.

19 Ibid.

20 NKGB (НКГБ – Народный Комиссариат Государственной Безопасности СССР) – People's Commissariat for State Security of the USSR. The acronym comes from the official name of the secret political police of the USSR between 1941 (February – July), 1943 – 1946. Subsequently, on March 22, 1946, the NKGB was transformed into the Ministry of State Security, known by the abbreviation MGB, which is translated into Russian as Министерство Государственной Безопасности СССР. See: Кокурин, А. И. – Петров, Никита В.: Лубянка*: ВЧК–ОГПУ–НКВД–НКГБ–МГБ–МВД–КГБ* 1917–1991. [Kokurin, A. I. – Petrov, Nikita V.: Lubyanka: Cheka–OGPU–NKVD–NKGB–MGB–MVD–KGB 1917-1991.] Справочник, Handbook, Москва, МФД, 2003/7, p. 634.

21 Петров 2007, p. 37.

From the name of section 2, we deduce that its task was to carry out the informative (espionage) activity among the Bessarabians who took refuge outside the borders of the USSR. In this context, we mention that after Bessarabia had been re-occupied by the Red Army in the spring – summer of 1944, as in 1940-1941, many Bessarabians took refuge with their families in Romania.[22] However, according to Article 5 of the Armistice Agreement signed on 12 September 1944, "Romania was obliged to hand over to the Soviet Union the Soviet citizens who were taken by force or evacuated".[23] In view of the above, we admit that the informative activity of Section 2 of Direction 1 of the NKGB Moldavian SSR was mainly focused on Bessarabian refugees in Romania.

Regarding section 3 of the NKGB Division 1 of the Moldavian SSR – operational registration section, we assume that it was responsible for storing and systematizing the information, according to certain specific criteria and algorithms.[24]

Therefore, we find that Order No. 158 of October 30, 1944 analysed above, includes only data on the names of the sections of Division 1 of the NKGB of the Moldavian SSR and the number of function states allocated to each. Instead, Order No. 108 issued a year later, on March 2, 1945, entitled "Announcement of the placement of the personnel of the 1st Unit of the NKGB of the Moldavian MSSR", presents the identity data of the staff occupying the respective positions.[25]

Based on the mentioned order, the author has developed a table that includes the organizational structure of the NKGB Moldavian SSR Department 1 in 1945, the functions, the staff of the subunit, as well as the rank held by them (for more details, see table no. 1 of the Annex). Analysis of the surnames of the 17 cadres of the Moldavian SSR's espionage structure allows us to deduce that the overwhelming majority of them were of foreign origin, that is brought from the USSR. We highlight the following nationalities: Russians - Brezhnev, Kolesnicova, Petrov, etc., Ukrainians – Mordovets, etc., Jew – Vainberg, Armenian – Madakian.[26] We note one possible exception, namely Muntean Andrei Efimovici, senior operational officer of section 3,[27] who, by name, could be a native. But given that all the other staff-members of Department 1 were of foreign origin, we assume with a high degree of probability, that Muntean A. was either from the left bank of the Dniester River in the former MASSR (Moldavian Autonomous Soviet Socialist Republic) or from the Ukrainian SSR.

---

22 GRIBINCEA 1995, p. 22.

23 Ibid; Armistice Convention of 12 September 1944 signed between the Romanian Government, on the one hand, and the Governments of the Soviet Union, the United Kingdom and the United States of America, on the other. For details see: N.a.: CONVENȚIE DE ARMISTITIU din 12 septembrie 1944. Uniunea Europeana.

24 MITROKHIN, Vasili (ed.): *KGB lexicon: The Soviet Intelligence Officer's Handbook*. Routledge, London, 2002, p. 88. ISBN 0-7146-8235-7

25 ASISRM, f. a., inv. 8, d. 1, p. 141, 140, 139.

26 Ibid. pp. 140, 139.

27 Ibid. f. 139.

Given that in the period 1944-1953, the tendency of the USSR's cadre policy was to supplement the NKGB-MGB of the Moldavian SSR with loyal personnel brought in from within the Soviet Union,[28] it is not surprising that the staff of one of the most secret sub-units - Department 1 of the NKGB of the Moldavian SSR, was also made up of non-natives.

In the same context, we attest that the staff of the Secretariat of Department 1 also includes the function of translator. Although it is not expressly stipulated, it is logical to admit that the translator's role in the direction was to mediate the communication between the other 16 "Moldavian spies" and the native population of the Moldavian SSR.

Also, in order to consolidate one of the obvious conclusions drawn from this study, we highlight the indication of Commissioner Iosif Mordoveţ no. 24 of November 21, 1944, which stipulated that all the operative staff of the NKGB of the Moldavian SSR, including that of Unit 1, was required to study the "Moldavian language"[29] according to the pre-established weekly schedule.[30] By extension, we can deduce that the operative staff of the NKGB of the Moldavian SSR was in corpore brought from inside the Soviet Union, at least for the years 1944-1945. On the other hand, in the archive documents studied by the author in the context of other research, *"for the first post-war years (1945-1947), several NKGB Moldavian SSR staff-members were identified with the name of the family of Bessarabian origin, but who occupied various lower hierarchical positions in the apparatus of the republic's security commissariat, such as: prison guards of the NKGB Moldavian SSR, translators, drivers, typists and gate guards and auxiliary staff"*.[31]

---

28 MALACENCO, Alexandru: Poliția Secretă a RSS Moldovenești – Efectiv și Sarcini în primii ani postbelici [The Secret Police of the Moldavian SSR – effective and tasks in the first post-war years]. *Studia Universitatis Moldaviae, Revistă științifică*, 2019/10, p. 180, 181.; Alexandru MALACENCO 2020, pp. 69-71.

29 Relevant to the subject of the aggressive propagation of the «Moldovan» language and artificial identity in the Soviet era in our space, the historian from the Republic of Moldova - Octavian Țîcu, explains very clearly in one of his books that *"Soviet «Moldovanism» was the state policy of the USSR in the MSSR and the MASSR, which had as its fixed idea the cultivation of a political, ethnic, historical, cultural and linguistic difference between the Romanian population of the MSSR and that of the rest of Romania, a policy constantly promoted in this area from 1924 to 1989"*. In the same work, the historian also highlights an important element that outlines the role of the Soviet security organs (NKVD, NKGB-MGB) in the construction of identity in the Moldavian SSR, revealing that *"the repressive nature of the identity shaping the Soviet Homo Moldovanus can be observed through researching of some NKVD files of the period, filed against people with views opposed to the Soviet regime"*. ȚÎCU, Octavian: *Homo Moldovanus Sovietic. Teorii și practici de construcție identitară în R(A)SSM 1924-1989.* [Homo Moldovanus Soviet. Theories and practices of identity construction.] Editura Arc, Chișinău, 2018, p. 374, 376.

30 ASISRM, f. a., inv. 8, d.7, f. 76.

31 MALACENCO 2020, p. 71.

Conclusion

The researched archival sources allow us to answer unequivocally the questions set by the author at the beginning of this study. Thus, taking into account the information presented in black and white in the Soviet documents about the identity data of the "Moldavian espionage" cadres it clearly proves that they were brought from the Soviet Union, but it also proves the necessity to organize courses of "Moldavian language", which otherwise proves that the staff of Department 1 did not know the language of the majority population of the republic. Therefore, the clear and irrefutable answer to the question; who were operating in the "Moldavian espionage" in the years 1944-1945 is: No Moldavians! Intuiting this answer, the author considered it necessary to question from the start the phrase "Moldavian espionage" by using quotation marks.

Therefore, the intelligence department of the Moldavian SSR, consisting of 3 sections and the secretariat, had 17 positions in total, of which 6 were leadership positions. Of the 17 cadres working in the direction, 16 had names of Russian, Ukrainian, Armenian, Jewish origin, so they were brought from the Soviet Union. At the order of the NKGB Commissioner of Moldavian SSR, the entire staff of Department 1, without exceptions, was obliged to study the "Moldavian language".

From the studied documents it is clear that the structure of the staff and the organizational structure of the spy service of the Moldavian SSR in 1944 were based on the express orders of the Union NKGB from Moscow. In essence, the 1st direction of the NKGB of the Moldavian SSR – both in terms of the ethnic composition of its staff, but also of the activity priorities, resulting from the name of the sections – was an extension or a miniature appendix of the Soviet espionage from Moscow. In other words, the espionage unit of the Soviet Moldavia in the first post-war years, was undoubtedly created and managed by the Soviets, and was exclusively pursuing the interests of Moscow, aimed at preserving and protecting the occupation-regime in the republic.

Therefore, the role of the NKGB Department 1 of the Moldavian SSR was to protect the Soviet regime from foreign threats. From the researched documents, we see that one of the external dangers for the Soviet regime in the Moldavian SSR was considered to be the legionaries. The fight against this hostile element was treated with great attention and importance by the espionage structure of the Moldavian NKGB, which, through the agents managed by Section 1, was forming nests of phantom legionaries to expose and monitor the genuine ones outside the republic, in this case in Romania. Furthermore, from the organizational structure of Department 1 of the NKGB of the Moldavian SSR, we note that within it, there was an entire section – Section 1, which was dedicated to intelligence work in Romania. From this, we deduce the special importance that the Soviet NKGB, through its extension – NKGB Moldavian SSR, gave to the clandestine obtaining of information of interest from Romania, in the first postwar years.

Following the research of the archive materials, in conjunction with some literature, it was established that the interest of the "Moldavian espionage" for Romania was matching with the priorities of the Moscow NKGB for 1944-1946. The analysis of the organizational structure of the USSR NKGB-MGB, in the period 1943-1946, allows drawing the conclusion that Romania was among USSR NKGB's top intelligence interests up to 1946, jointly with Germany, Poland, Czechoslovakia, Hungary, Bulgaria, Yugoslavia and Greece. After the restructuring of the NKGB into the MGB in 1946, Romania became a secondary intelligence priority for the soviet espionage system at Union level, and since as the Cold War started, all the attention was turned towards the Anglo-Americans. Another conclusion drawn from the present research allows distinguishing an asymmetry of priorities established in the USSR espionage system, after 1946 for the Union level and peripheries – the Republics. Thus, on the one hand, Romania became a secondary espionage priority for Moscow at the Union level, after the institutional restructuring of the NKGB in 1946, but on the other hand, for the Moldavian SSR, continued to be a priority. The observed asymmetry points out that for the republics, in this particular case, for the Moldavian SSR, the intelligence priorities were determined by the local political and geographical realities of the region, namely the neighbourhood with Romania and most important – the undeniable historic, cultural, national and linguistic affinity with the Romanian state. These similarities had to be distorted, perverted and undermined, in order to preserve the Soviet totalitarian regime in the occupied territory. It is worth mentioning that in the researched archive materials, no directives or orders indicating a possible change in the main intelligence priorities of the Moldavian SSR after 1946 had been identified. Consequently, we can assess that for the espionage structure from the Soviet Moldavia, Romania continued to be a constant intelligence priority, during the first post-war years.

At the same time, among the archive sources studied so far by the author, no documents were identified that would describe the attributions and competences of the NKGB Moldavian SSR Department 1. Although the express knowledge from the archival documents of the functional attributions of each section or Department 1 of the NKGB of the Moldavian SSR would be of great scientific interest for the history, we admit that these documentary sources are still secret, either in the archives in Chişinău or in Moscow, which is why they cannot be consulted for research purposes.

Assuming that in an uncertain future, this type of documents will be declassified and accessible to researchers, this would undoubtedly make an important contribution to a more complete knowledge of the role of Soviet espionage, in the process of consolidation and institutionalization of the Soviet regime in Bessarabia. But given that espionage is a discrete activity, that is widely speculated only, but essentially little known about it, the declassification of documents that would explain the tasks, methods and means in the field is unlikely.

Name of subunits and functions	Number of functions	Surname, first name, patronymic	Rank
Management			
Head of Department	1	Breantsev Gheorghii Mihailovici	lieutenant colonel of state security
Deputy Head of Direction (by cumulation, Head of Section 1)	1	Ciuguevets Evghenii Efimovici	1st lieutenant of state security
Secretariat			
Department Secretary	1	Grineva Maria Nikolaevna	special service sergeant major
Operational officer	1	Tiscov Nicolai Ivanovici	junior lieutenant of state security
Typist	1	Kolesnikova Concordia Mihailovna	special service sergeant major
Translator	1	Ranov Alexei Vladimirovich	No Rank
Section 1 (intelligence activity in Romania)			
Head of Section (by cumulation, Deputy Head of Department 1)	-	-	-
Deputy Head of Section	1	Madakian Nicolai Iacovlevici	captain of state security
Senior operational officer	1	Petrov Sergey Petrovich	1st lieutenant of state security
Operational officer	2	Perev Vasilii Nikolaevici	junior lieutenant of state security
		Vainberg Grigorii Samuilovici	sergeant major of the special service
Section 2 (intelligence work on emigration)			
Head of Section	1	Logachiov Semyon Semyonovich	captain of state security
Senior operational officer	1	Dragunov Mihail Danilovici	junior lieutenant of state security
Operational officer	2	Kovkov Gheorghii Gherghievici	junior lieutenant of state security
		Mordovet Leonid Iosifovich	special service sergeant major
Section 3 (operational registration section)			
Head of Section	1	Salamatov Zosim Fedotovich	captain of state security
Senior operational officer	1	Muntean Andrei Efimovici	junior lieutenant of state security
Operational officer	1	Oleksici Nina Ivanovna	junior lieutenant of state security
Total functions	17		

Table 1: The personnel of Unit (Department) 1 of the NKGB of the Moldavian

SSR in 1945*The table was developed by the author based on documentary sources from ASISRM, inventory 8, d. 1, f. 141, 140, 139; d. 27, f. 328; For translating some terms we used. See: MITROKHIN 2002, p. 451

Bibliography:

CAMPEANU, Ilies – MARINESCU, Cornelia (eds.): *Universal Encyclopedia Britannica*, Litera Publishing House, Bucharest, 2010/14.

ФУРМАН, Дмитрий: *Молдавские молдаване и молдавские румыны: влияние особенностей национального сознания молдаван на политическое развите Республики Молдова.* Доклады Института Европы № 206, Publishing House: «Русский сувенир», Москва, 2007.

GRIBINCEA, Mihai: *Basarabia în primii ani de ocupație sovietică 1944–1950*, Dacia, Cluj-Napoca, 1995.

Кокурин, А. И. – Петров, Никита В.: Лубянка*: ВЧК–ОГПУ–НКВД–НКГБ–МГБ–МВД–КГБ*, 1917–1991: Справочник. Handbook, Москва, МФД, 2003/7.

MALACENCO, Alexandru: Cine activa în serviciul „spionajului moldovenesc" în anii 1944-1945? [Who worked in the service of „Moldavian espionage" in 1944-1945?] *Latinitate, Romanitate, Românitate,* CEP USM, Chișinău, 2021/4, pp. 213-221.

MALACENCO, Alexandru: Comisariatul Poporului pentru Securitatea Statului al RSS Moldovenești: Structura Organizatorică între anii 1944-1946. [The People's Commissariat for state security of the Moldavian SSR-organizational structures in the period 1944–1946.], *Akademos, Magazine of Science, Innovation, Culture and Art*, 2019/4.

MALACENCO, Alexandru: Poliția Secretă a RSS Moldovenești – Efectiv și Sarcini în primii ani postbelici [The Secret Police of the Moldavian SSR – effective and tasks in the first post-war years]. *Studia Universitatis Moldaviae, Revistă științifică*, 2019/10.

MALACENCO, Alexandru: Serviciile de securitate în teritoriile „eliberate" de către URSS în primii ani postbelici. [State security services in the territories „liberated" by the USSR in the first postwar years.] In: PREUTU, Cristina – PETRENCU, Anatol: *Fațete ale Comunismului în România și în R(A)SS Moldovenească. Politică, Societate și Economie*. Publishing House Universității „Al. I. Cuza", Iaşi, 2020.

MITROKHIN, Vasili (ed.): *KGB lexicon: The Soviet Intelligence Officer's Handbook*. Routledge, London, 2002. ISBN 0-7146-8235-7

MORARU, Anton: *Istoria Romanilor: Basarabia și Transnistria 1812-1993.* Aiva Publishing House, Chișinau,1995.

MORARU, Pavel: Organizarea și activitatea structurilor securității statului din RSSM (1940-1991). In: COROBCA, Liliana (ed.): *Panorama Comunismului în Moldova Sovietică*. Polirom, Bucharest, 2019.

MORARU, Pavel: *Serviciile Secrete și Basarabia, dicționar 1918–1991*. Editura Militară, Bucharest, 2008.

MORARU, Pavel: *SMERȘ in Bessarabia 1944–1954.* Editura Militară, Bucharest, 2013.

MORARU, Pavel: *Urmașii lui Felix Dzerjinski: organele Securității Statului în Republica Sovietică Socialistă Moldovenească 1940–1991*. National Institute for the Study of Totalitarianism, Bucharest, 2008.

N.a.: CONVENȚIE DE ARMISTITIU din 12 septembrie 1944. Uniunea Europeana, n.d. online: http://legislatie.just.ro/Public/DetaliiDocument/31 (Download time: 02/14/2024)

PETRENCU, Anatol: *Basarabia în al Doilea Război Mondial 1939–1945*. Prut Internațional, Chișinau, 2006.

Петров, Н.В.: *Кто руководил органами госбезопасности 1941-1954,* Handbook, Звенья, Москва, 2010.

ȚÎCU, Octavian: *Homo Moldovanus Sovietic. Teorii și practici de construcție identitară în R(A)SSM 1924-1989.* [Homo Moldovanus Soviet. Theories and practices of identity construction.] Editura Arc, Chișinău, 2018.

ВОЛКОВ, Гавриил: *Взгляд Через Десятилетия.* [A look over decades.] SIS of the Republic of Moldova, Chisinau,2004.

ISTVÁN BANDI

SOVIET INTELLIGENCE ACTIVITY FROM THE 1960s TO THE REGIME CHANGE IN THE SECURITATE'S COUNTERINTELLIGENCE FILES

Abstract

A number of works has already been published on the activities of the "contraspionaj tările socialiste", an organizational unit that performed a specific task in the Ceauşescu era's counterintelligence. Noteworthy works on organizational history have been published: in the Florian Banu, Securitatea 1948-1989, Monografia[1] edited by Liviu Țăranu. As its title indicates, it is a monographic work on the organizational history of the Securitate as a whole, in the framework of which, a short and concise summary of the organizational history of counterintelligence against socialist states can be read. Sorin Aparaschivei[2] prepared a more detailed study on organizational history, by analysing the unit's activities. In their monographic works, the researchers Remus Ioan Stefureac, Mircea Stan and Tudor Pacurariu examined the role of the Securitate in preventing the activities of the Soviet intelligence services against the socialist states.[3]

In the present study, we primarily examine the fate of Romanians, in the operation of the mentioned organizational unit, based on the documents of fond 0110 in CNSAS, a unit against socialist states. In the course of my previous research, it seemed that the aforementioned organizational unit did not distinguish between citizens coming from or not coming from the Soviet Union, during its prevention activities. Our research hypothesis are; whether the procedure against the mentioned persons changed in the period from the 1960s to the regime change in December. At the same time, we were also curious about the means and manners in which the Romanians were treated by the Securitate officers.

Keywords: Securitate, 1958-1989, Romanian counterintelligence, Soviet active operations, Bessarabian Romanians.

1 BANU, Florian – ȚĂRANU, Liviu: *Securitatea 1948-1989, Monografie* vol I., Editura Cetatea de Scaun, Târgoviște, 2016, p. 228.

2 APARASCHIVEI, Sorin: UM 0110 – Contraspionaj ţari socialiste (anti-KGB). Infiintarea si primi ani (1963-1973). [UM 0110 – Counterespionage of the socialist countries (anti-KGB). The establishment and the first years (1963-1973)] *Historia*, n.d.

3 STEFUREAC, Remus Ioan: *Conflictul secret din spatele scenei România versus Rusia. 50 de ani de realități, mituri și incertitudini.* [The secret conflict behind the scenes Romania versus Russia. 50 years of realities, myths and uncertainties.] Editura RAO, București, 2015, p. 185; STAN, Mircea: *Programul de masuri active al KGB-GRU impotriva Romaniei (1964-1989).* [The program of active measures of the KGB-GRU against Romania (1964-1989)]. Editura Militara, Bucuresti, 2021; PACURARIU, Tudor: Planul Nistru-1989, *Implicarea G.R.U. in Revolutia din Decembrie,* Editura Evenimnetul si Capital, Bucuresti, 2020.

The political framework of the Soviet-Romanian relationship from 1958 to 1989

Romania's situation in the period between 1948 and 1958 depended directly on the foreign and security policy of the Soviet Union, so in the early years of the Cold War, Moscow's relationship with the West was dominated by the communist ideological approach, which was faithfully copied by the Romanian party. The guarantee of the Soviet Union's own security in the first years after the Second World War was the sovietisation of the territories made into vassal states, which effectively transferred the right of decision in the political, social, economic and military fields to the Soviet Union. In the first decade after the Second World War, Bucharest was a loyal ally of Moscow, then it changed its direction almost visibly and started building its own line of communism. The wind of change began in 1955, as the Soviet Union concluded a peace treaty with Austria. Taking advantage of the spirit of the Geneva summit, which somewhat eased East-West relations, the first secretary of the Communist Party of Romania Mr. Gheorghe Gheorghiu-Dej began negotiations with Moscow in 1955 to withdraw the Soviet army, but the negotiations proved unsuccessful. However, in 1957, due to the new orientation of Khrushchev's foreign policy, which included the 1956 Suez Crisis, in order to strengthen his political strategy of "peaceful coexistence", and the Soviet leader's desire to restructure his military budget, the Soviet and Romanian leadership signed the Soviet agreement on the temporary stationing of troops in Romania. Finally, the withdrawal of the Soviet military formations took place in June-July 1958. Externally, the withdrawal of the Soviet army made it easier for Romania to move away from Moscow in the future, but at the same time, on a domestic political level, the party leadership, headed by Gheorghiu-Dej, ordered another wave of arrests and tightened ideological control, thus proving its ideological commitment to Moscow.[4]

The party leadership in Bucharest persistently opposed Moscow's aspiration to integrate Romania into the CSTO, to turn it into an agricultural hinterland, a supplier of raw materials to the Soviet Union and other socialist countries. Disagreements arose between the Soviet Union and Romania within the Warsaw Pact from the beginning of the 1960s, for example, in the early 1960s in Moscow, the issue related to the problems of agriculture, according to which Romania should have become an agricultural state, or the questioning of the decision to build the Berlin Wall are just some of those among topics that increased the tension between the Soviet Union and Romania. The events related to the Cuban crisis and the rejection of the Soviet monolithic management concept further accelerated Romania's independence policy within the Warsaw Pact.[5]

---

4 GIURESCU, Dinu C. – ŞTEFĂNESCU, Alexandru: Ilarion Ţiu, *România şi comunismul. O istorie ilustrată.* [Romania and communism. An illustrated history.] Editura Corint, Bucureşti, 2010, pp. 149-150; CONSTANTINIU, Florin: *O istorie sinceră a poporului român*. [An honest history of the Romanian people.] Editura Univers Enciclopedic, Bucureşt, 2011.

5 GARTHOFF, Raymond: *When and Why Romania Distanced Itself from the Warsaw Pact*. CWIHP Bulletin, 1995/5, p. 111.

In parallel with the mediating role in the Soviet-Chinese diplomatic dispute, the party leadership in Bucharest announced in April 1964, the reduction of Soviet influence.[6] Khrushchev's removal from power did not bring significant changes in Romanian-Soviet diplomatic relations.

With Ceauşescu's rise to power in 1965, Soviet-Romanian relations further sharpened, as the new Romanian party general secretary already then suggested that the Warsaw Pact should be reformed and the principle of cadre rotation should be applied.

Before the invasion of Prague in 1968, Brezhnev's intention to make peace also fell through, as historian Mihai Retegan notes from the consultative meeting of the communist parties held in Budapest in February 1968, the RKP leadership signalled to Moscow by leaving in protest that it would not accept it as the primary negotiating forum of the initiated international communist movement. It did not accepted the relevant proposals, because they violated the principle of national sovereignty and independence (according to the Romanian concept). Furthermore, this action pointed out, as the historian Mihai Retegan also stated, that Brezhnev, who started a new course with the aim of recovering/redoing Khrushchev's concessions, did not make it possible to transform the hard image of the Communist Party of the Soviet Union.[7] The Soviet Union manifested itself in this direction in August 1968, when, alongside the Soviets, the Bulgarian, Polish, Hungarian and GDR military units marched into Czechoslovakia. The entry was thoroughly exploited by Ceauşescu, so the event became a significant moment in the history of misunderstandings between the two states.

A serious “break of bread” (break in the relations) took place in 1971, when, after the Romanian Party General Secretary's visit to the People's Republic of China and other Asian countries, the Romanian Ministry of Foreign Affairs issued a firm statement, according to which the Soviet Union's attitude towards Romania was more negative than towards other member states, and although a Romanian Consulate General was opened in Kiev in January 1971, and in March 1972 a consular agreement was signed between Romania and the Soviet Union, relations between the two states still did not improve.

Finally, a sort of Soviet-Romanian diplomatic status quo emerged following the 1976 meeting between Brezhnev and Ceauşescu. However, Romania's real economic situation would not have required this.

---

6 A thorough analysis of the "April Declaration" can be found in the work of Mihai CROITOR: *In umbra Kremlinului. Gheorghe Gheorghiu-Dej si geneza declaratiei din aprilie 1964.* [In the shadow of the Kremlin. Gheorghe Gheorghiu-Dej and the genesis of the April 1964 declaration.] Editura Mega, Cluj-Napoca, 2012.

7 RETEGAN, Mihai: *1968. Din primavara pana in toamna.* [1968. From spring to autumn.] RAO, Bucuresti, 2015, pp. 95-96.

As a result of the previously launched mass industrialization and the fact that Romania faced successive economic and financial crises in the Western world in the '80s and the Ceauşescu regime, which was struggling to pay off its foreign debt, despite the less than friendly relationship, asked for Soviet help in the supply of energy resources. In order to ensure this practically also meant the fall of the above-proclaimed independence and sovereignty.

The momentum of Ceauşescu's special policy finally wears off in the second half of the 1980s, as the Helsinki agreements adopted in 1975, whose human rights clauses became primary diplomatic requirements in the 1980s, and this situation made Romanian diplomacy extremely vulnerable.[8] Thus, France, which previously ensured economic and political dominance, closed itself to Romania, especially after the "Afacearea Tănase".[9] Diplomatic relations with the USA developed in a similar way, since the diplomatic groping towards the United States of America that began in the 1960s finally ended with success in 1975, as Romania received the "biggest trade discount" and this right was regularly extended until 1988, however, at the time of signing, Romania also undertook to ensure political freedoms.[10] This political condition, that is, European and human rights, which the Romanian political elite demanded so much after August 1968, was not respected, and in the 1980s they significantly limited the foreign policy activities of the regime and ultimately contributed to the deterioration of its international reputation, and finally the led to the collapse of the dictatorship.

In the 1980s, the Soviet Union remained the last refuge for the Socialist Republic of Romania (SRR), as it was the owner of basic raw material resources,[11] the closest state within the Warsaw Pact and also a great power, to which it could turn based on a common ideological approach.

---

8 For details of the impact of the Helsinki Accords on the Ceauşescu regime, see: ALDEA, Patriciei González: *Helsinki 1975. Începutul sfârşitului. Degradarea regimului din România şi singularitatea lui în blocul de Est (1975-1990)*. [Helsinki 1975. The beginning of the end. The degradation of the regime in Romania and its singularity in the Eastern bloc (1975-1990)]. Curtea Veche, Bucureşti, 2008.

9 In 1982, Romanian intelligence was tasked with killing dissidents Virgil Tanase and Pauk Goma. Matei Haiducu, who was entrusted with the execution of the operation, did not carry out the order, and even reported to the DST for the French countermeasures, and thus caused a serious loss to the Romanian intelligence agencies of the time and later eroded the remaining credibility of the Ceauşescu regime in the West with his statements on public TV.

10 The renewal of the Romanian clause went through three stages: in the first, attention was directed to the emigration of the Jews, in the second, the emphasis was placed on both the persecution of the Hungarians and the emigration of the Jews. Thirdly, the case was about Bucharest's policy regarding Hungarians and religions not recognized as cults. For details see: HARRINGTON, Joseph F.: *Relaţii romano-americane: 1940-1990.* [Romanian-American relations: 1940-1990.] Editura Institutul European, 2002, p. 557.

11 XENOFONTOV, Ion Valer: *Romania in sistemul de sceuritatet europeana in secolul XX – inceputul secolului XXI.* [Romania in the European security system in the 20th century - the beginning of the 21st century.] USM, Chisinau, 2021, p. 125.

Ceauşescu, however, lost the mediating role he played in international diplomacy before 1985 when Gorbachev came to power and then with the announcement of perestroika and glasnost, Romania became completely isolated from the West, and in contrast to Gorbachev's soft power ideas, it manifested itself as a specific post-Stalinist dictatorship.[12] However, in practice, the compelling reality of Soviet-Romanian bilateral economic cooperation remained unavoidable for the Romanian dictator. The economic and diplomatic rigidity led to enormous social tension and finally, as is known, in December 1989 revolutionary events swept away the dictatorship marked by Ceauşescu.

The influence of Soviet-Romanian political relations on the state security organization

After the brief overview of neighbourhood policy, which was far from cloudless from the 1960s to the regime change, it is worthwhile to review the specialized body of the security structures of the Romanian state apparatus with the aim of to what extent the relationship between the two states is reflected in the state security structures.

On the basis of Decree No. 141 on the "Organization and Operation of the Ministry of the Interior" issued in 1963, the previous organizational structure of the Securitate changed, and with it a professional-methodological change took place, moving from mass prevention to a preventive procedure, in the framework of the Counter-Espionage Directorate. The department dealt with, among other things, Council of Mutual Economic Assistance (CMEA) objects and delegations sent to Western countries, as well as Western delegations arriving in the Socialist Republic of Romania.[13] It can already be clearly demonstrated here that the Securitate also dealt with socialist states behind the Iron Curtain.

As early as 1963, operative groups of 1-2 people worked in the "socialist counter-espionage sector" at the county inspectorates, except for a few counties where the current operational problems occurred in a greater proportion (Cluj, Constanta, Timișoara), where this number was increased to 5 officers. Starting in 1968, as a result of the Soviet military invasion of Czechoslovakia, the number of counterintelligence officers dealing with the "special problem" (anti-Soviet) increased significantly. In the summer of 1973, the newly reorganized Intelligence Unit against Socialist Countries, now designated UM 0920/A, had the priority task of the "special problem". This also meant development and the strengthening of this area. Within UM 0920/A, it had a total of 16,350 databases, that is, this number of persons attracted the attention of the organizational unit, of which 920 persons were under preliminary control at that time.

---

12 Ibid. 128.

13 BANU – ȚĂRANU 2016, p. 116.

In order to monitor persons subject to “Special Problem” (anti-Soviet) activities, the Counterintelligence Directorate organized its own network of agents for the counterintelligence unit of the socialist countries (UM 0920/A.), agents who were *"recruited under circumstances that required special care in order to prevent possible disclosures in relation to selection, control and maintenance*”. Thus, in July 1973, the UM 0920/A unit had 708 agents.[14]

From December 15, 1978, another reorganization took place, which could also be attributed to Mr. Pacepa's escape, so the materials addressed to the former 0920/A military unit were forwarded to the unit code UM 0110 within the State Secretariat for State Security (DSS), the said unit was a new to its leader, Colonel Constatin Iosif. According to the operating instructions of the DSS and the military unites in accordance with the provisions contained in its operating regulations, the 0110 departments, which operated within the county safety inspectorates, had the following scope of influence and responsibilities:

The Securitate's counter-espionage bodies had to prevent and eradicate the hostile activities of foreign intelligence agencies with the Romanian party and state policy, which in practice meant action against cases of espionage, treason, ideological diversion, and subversion. Preventive measures were applied primarily to diplomats and embassy officials, military attachés, press correspondents, and economic representatives of socialist states.[15] Counter-espionage was also tasked with revealing the information sources used by foreign embassies, the contact-building methods and procedures they used, and the incitement of Romanian citizens into hostile activities.[16] Based on these, all Romanian citizens who came into contact with diplomatic, commercial, or cultural representatives of any socialist state became suspect. The 0110 (county agencies) territorial units of the counter-espionage were responsible for the prevention of hostile activities carried out by the journalists of the "Făgăraș" (socialist) countries, as well as the collection of information about them, as well as the foreigner who was previously involved in the management of agents of the mentioned states and mixed-owned companies the control of persons and even their descendants, as well as the operative processing of persons visiting socialist countries, and finally the prevention of the introduction and distribution of defamatory printed materials and audio materials by the citizens of the “Făgăraș” countries into the territory of Romania. It was also necessary to collect data on the representatives and delegations of cultural, scientific and artistic institutions from socialist states. A register was kept of foreigners who sought to establish permanent private relations with Romanian citizens.

---

14 APARASCHIVEI n.d.

15 In dosarul cu cota FCX 0001132 socialist states were codified. The problem of socialist states bearing the code name “Făgăraș”, CAER was “Poiana Rusca”, USSR – “Rodna”, People's Republic of Hungary – “Lotru”, R.P. Poland – “Godeanu”, R.S. Czechoslovakia – “Bucegi”, R.P. Bulgaria – “Ciucas”, R.D. Germany – 'Tarcau', R.P. Cuba – 'Vladeasa', R.S.F. Yugoslavia – 'Semenic', R.P.: Albania – 'Zarand', R.P.D. Vietnam – 'Almaj', R.P.D. Korea – 'Gilau', R.P. China – 'Birgau', R.P. Mongolia – 'Caliman'. The use of these pseudonyms was introduced from January 1981. See the mentioned note on page 83.

16 ACNSAS FCX 0001132, p. 78.

The above-mentioned 0110 anti-espionage territorial units were tasked with identifying and preventing hostile actions by citizens, doctoral students and teachers from socialist countries studying at the universities of the Socialist Republic of Romania.

In accordance with the relevant regulations, quarterly summaries were prepared from the follow-up of foreign tourists, as well as statistical analyses of the data of Romanian tourists traveling to the mentioned countries.

The reports from the 0110 area agencies included: completed cases in each work area/line – which were detailed with reference to what the activity consisted of, the operational measures taken by Counterintelligence on the case, the manner in which the case was closed and the result achieved.[17] The information needs defined in the 1960s and 1970s did not change significantly even in the 1980s. The scope of those to be observed and processed are still lecturers from foreign higher education institutions, doctoral students who in some form came into contact with diplomatic missions, that is, a preliminary inspection file (dosar de urmarire informativa – DUI) was opened for all university citizens who were suspected of gathering information, the others they just watched. For the purpose of neutralization and prevention, the obtained information materials were analysed quarterly, or as needed, and appropriate measures were taken depending on the obtained information. Based on the aforementioned regulations, the heads of the central and county divisions of the Securitate (separate organization 0110), as well as the heads of the central and county units of the Anti-Espionage Directorate, were responsible for its implementation.

The officers of the 0110 organizational units had to strive to identify and document in time the persons suspected of assassination, terrorist-subversive activities, as well as the identification and documentation of agents from foreign reactionary organizations and their activities, as well as the documentation of the aforementioned activities with photographic technology/film cameras in the early stages and through the records made during the control procedure. All cases in which completion was expected were submitted to the central unit for approval.[18] That is why it is easy to track anti-system cases in archival sources, since every case that was successfully investigated had to be reported to and authorized by the central bodies several times.

The socialist member states of "Poiana Rusca", that is CMEA, were subjected to similar procedures, so that, for example, commercial and economic representatives arriving in Romania, as well as heads of navigation and transport agencies, as well as representatives of commercial companies and heads of branches, were put through an informative preliminary inspection dossier, for processing as soon as they occupied their station.[19] Other persons with diplomatic status were subject to mandatory information surveillance.

---

17 ACNSAS FCX 0001132, pp. 79-81.

18 ACNSAS FCX 0001132, pp. 74-76.

19 ACNSAS FCX 0001132, p. 65.

Actions against state security were neutralized, and the emphasis was placed on the use of appropriate legends to carry out the secret investigation and, in the course of exploiting the situation, to obtain data on the commission of acts falling under the jurisdiction of the militia, on behaviour violating the status of the person operating in the foreign representation in Romania. The counter-espionage carried out all operational administrative measures, such as the warning, using a suitable legend, and in all cases, the approval of the central unit was unavoidable for any kind of action against the person operating in the foreign representation, closing the case. During the prevention activity against foreign citizens, there was close and thorough coordination between the concerned counties and the centre in Bucharest. The use of special devices at the headquarters and residences of foreigners was based on thorough study and only with the approval of the Minister/Secretary of State.[20]

The management of the professional organization held briefings at the national level, at which the officers were given a detailed briefing on the latest tasks, their solvability, the news and the requirements, etc. Each county 0110 department was obliged to compile an subject matter file on the diplomatic institutions (consular offices, shipping agencies, commercial offices, etc.) operating in its area and located in the territory of the county Securitate inspectorate.[21] In the 1980s, the 0110 prevention agencies were required to finalize cases in cases of foreign nationals who were suspected or proven of active participation in espionage, as well as in cases in which the act was not classified as a crime from operational considerations, only with the agreement and support of the central unit was feasible.

Used by the Romanian counterintelligence agencies against foreign diplomats/citizens, the so-called preventive measures were: positive influence; drawing attention (on the target person); desinformation; expiry; declaration as persona non grata and interruption of travel/stay in the Socialist Republic of Romania; informing the diplomatic representation – through the liaison office of the National Inspectorate of the Militia (Inspectoratul General al Miliţiei – IGM) about what kind of crime is being investigated against the person concerned, notifying the Ministry of Foreign Affairs, in most cases using a “cover” or “legend”, about those that offend the Romanian state and about actions incompatible with the status of a diplomatic representation, and the last form of action was the operative prosecution and the initiation of the investigation.[22]

The counterintelligence unit with the military unit code 0110, as a result of intensive reconnaissance work in the mid-1980s, found out that the Soviet intelligence agencies intensively used economic and commercial facilities to cover diplomatic cadres and agents delegated to the Socialist republic of Romania in order to fulfil their information needs.

---

20 ACNSAS FCX 0001132, p. 62v. (verso)

21 ACNSAS FCX 0001132, p. 53.

22 ACNSAS FCX 0001132, p. 49.

During this period, the independent counterintelligence unit of the socialist countries was organized into four divisions, two of which dealt exclusively with the operations of the KGB and the GRU.[23] In 1989, the number of employees of this independent directorate-sized unit was 304.

Bessarabian Romanians in the focus of Romanian counterintelligence (sub lupa Securitatii)

In the 1960s, under problem 200 (problem 200 is the operational name), an operation took place that retrospectively checked all those persons who settled in the old country for various reasons during the Second World War. Thus, for example, the Securitate's county-level bodies checked all over the country those who stayed in Romania between 1945 and 1960 and obtained their citizenship documents in the Socialist Republic of Romania.

According to archival sources, during the inspection, a previous committee[24] operating at the county level in August 1945 (its members were the representatives of the Allied Inspection Committee, the delegates of the Romanian Armistice Committee and the prefect or sub-prefect of the given county), which investigated the situation of those exempted from repatriation and those who applied for it was a committee, its minutes were retrieved and used by Securitate officers in the mid-sixties. In the majority of cases, in 1945, all those who held public office positions, engaged in commercial activities or had a registered company in Romania, teachers, and in cases where the person could prove that he would marry in the near future, were exempted from repatriation.

The number of persons checked per county was several thousand or thousands, as nearly 200 persons were checked only in the city of Găești in Dâmbovița County based on the materials of the previous repatriation committee.[25] In the county seat of Târgoviște, 459 persons were investigated on a similar scale, who were also previously in the register of the repatriation investigation committee and in 1969 these all belonged to the A200 problem area of the Securitate,[26] that is, persons who were considered risky persons according to the Securitate's counterintelligence body. In justified cases, the Securitate was not satisfied with checking the records of its own operative and partner bodies (miliţia), but instead ordered the persons concerned to be interviewed in person and, by definition, had a résumé written by the person concerned in the form of a statement. With the information gathered in this way, they were able to continue the secret inspection even more thoroughly.

---

23 BANU – ȚĂRANU 2016, p. 228.

24 For more details on the repatriation of Romanians from Bessarabia and Bukovina, see: Marius Oprea's article: ISTORIA FARA PERDEA In 1945, rusii au negociat cu pistolul pe masa, iar romanii cu inteligenta: un avocat roman a salvat sute de mii de Basarabeni si bucovineni de la deportare. URSS, n.d.

25 ACNSAS Fond FCX 0000968 pp. 41-49.

26 ACNSAS Fond FCX 0000968 pp. 78-109.

This was also the case of Romanian citizen Nicolae Vornicescu, a resident of Valea Mare (Gaest district), who was born in the Soviet Union (more precisely in Russia) in the village of Lozova in 1913. During the inspection, it was established that the named person first arrived at the forest farm in Gaiesti in 1940, even before the Ribbentrop-Molotov Pact. His return to his native village and then his call-up to the Romanian Royal Army took place after the 1941 invasion of Bessarabia.[27] In 1944, he resettled in Gaieste and also worked as a forester until the time of the Securitate investigation in 1965. It is important to note that the repatriation committee set up on the basis of the Soviet-Romanian armistice agreement of September 12, 1944 did not send Vornicescu (born Ciocan) back to Lozova in Bessarabia, and it is certain that the forester working in Gaiesti was informed of the terrible starvation and the violent measures of the Soviet authorities which killed 100 000 residents of Bessarabia.[28] The professional officer of the population registrar, despite having named himself, indicated in his resume that he could prove his identity with his military record, where he was listed as Vornicescu, and he admitted that he used to live in Lozova with the surname Ciocan and that all his family members who stayed there also use the surname Ciocan, the officer states that *"Vornicescu's name is a distorted name, because even at the present time he cannot prove the origin of this name with any documents, his real name is Ciocan."*[29] These unclear cases made the related persons suspicious in the eyes of the Securitate.

The acquisition of personal identity,[30] or more precisely, its arrangement, can be linked to the year 1950, as it was then that the process of personal identification was centralized and placed under the authority of the Ministry of the Interior. Therefore, it is not surprising that the starting point of the Securitate's operational checks conducted in the 1960s and 1970s, in relation to establishing identity, is in every case related to a 1950 measure.

---

27 On June 22, 1941, the German and Romanian armies in the north and the Romanian army in the centre and south crossed the river Prut and entered the territory of the SSR of Moldova. On July 26, 1941, the border was restored until June 28, 1940 through the conquest of White Fortress.

28 CAȘU, Igor: *Dușmanul de clăsă: represiuni politice, violență și resistance în R(A)SS Moldovenească*, *1924–1956*. [The enemy of the social classes: political repression, violence and resistance in the Moldavian R(A)SS, 1924-1956.] Cartier, Chișinău, 2014, pp. 189-210.

29 ACNSAS Fond FCX 0000968 p. 51.

30 After the establishment of the communist system, the order of personal documents, regulated by Decree 2072/1950, changed. According to § 40 of the aforementioned decree, the people's councils were authorized to maintain and amend the civil registry records through the General Directorate of the Militia, under the guidance and control of the Ministry of the Interior. The procedure for the issuance, handling and registration of documents will not change even after the introduction of Decree 278/1960. For more details see: N.a.: Evidenţa persoanelor în România (istoric), LegeAZ.

Gheorghe Niculina, who was born in 1922 in the village of Divizia (Cetatea Alba, formerly Basarabia, part of the Kingdom of Romania, after the Second World War, the Moldavian SSR-Soviet Union) has a similar inspection history, who was inspected as one of the citizens from the "Apolodor" states[31] in the 1960s. in the second half. Her case begins with an anonymous report, when the anti-espionage units of Targoviste UM 01303 (Targoviste 1st Tank Regiment) (the local anti-espionage unit of the Directorate of Military Intelligence of the Security Service) received an anonymous letter in which the woman raising three children was called a Russian, who only subleases part of his property to Romanian officers, and often visits the USSR. The anonymous whistle-blower practically accused Gheorghe Niculina of espionage.[32] From the autumn of 1967, agent reports ("agent Adriana") were received for the counter-espionage of the military unit (Targoviste 1st Tank Regiment) that Ms. Niculina *"…knows a lot of information about the unit, Capt. Radut Florian tells her, who is 1st Tank Regiment platoon commander. ..."*[33]. In addition to the involvement of additional agents, the reconnaissance activity also involved the installation of technical devices (mail checking, wiretapping).

In addition to the military counterintelligence (Directia Contrainformatii in Armata – DIA), the Securitate's III Counterintelligence Directorate (Directia Informatii Interne – Directia a IIIa) became involved in the roll-up of Niculina's activities. By all means, they were trying to *"identify the suspicious connections of those mentioned above during trips to Bucharest",*[34] which in reality were completely natural trips, since a passport and visa were needed to travel to the Moldovan SSR. Niculina was followed and watched by the Romanian communist secret service until 1977 (archival records show the proceedings against him). Niculina, who was demonstrably in the focus of the Securitate in 1967, produced numerous secret service materials, but their probative value, as a commander supervising the operation stated in his instructions to his subordinates (majors Toma and Gheorghiu) working on the case in April 1969: *"From all the data collected ...() it seems that you opened the file of (named – addition of the author) without checking and confirming the initial data, no operational aspects have arisen at the moment. He was born abroad, visits his parents, talks, writes with them, brings things, does business and loves the men – officers, around whom he revolves (...)."*[35] At the end of the evaluation, the regional commander of the military counterintelligence stops the procedure in a firm order, with the stipulation, so that the military counterintelligence officers dealing with Niculina coordinate with the Dâmbovița Provincial Securitate command.

---

31 Operational code name for socialist member states, which was periodically assigned this code name by a designated organizational unit of the Securitate.

32 ACNSAS Fond FCX 0000968 p. 152.

33 ACNSAS Fond FCX 0000968 p. 147.

34 ACNSAS Fond FCX 0000968 p. 150.

35 ACNSAS Fond FCX 0000968 p. 147 v.

Thus, the military counterintelligence line of the case was closed, however, the III Counterintelligence Directorate continued the case, since a person like Niculina, who after returning from the Soviet Union (sic) reported that *"...the citizens there talk about when comrade Ion Gheorghe Maurer[36] was in the Soviet Union, he would have asked the Soviet leadership for Bessarabia, and they replied that it would not be given. After that, the leadership of the Soviet Union took the measure of telling the people the «truth» at party and citizen meetings, where they openly told them what the Romanians wanted, and the speakers at the meetings said suggested that they should want to go to Romania, if must, they would fight to the last drop of blood. He also participated in such gatherings, because he realized that they were telling the truth there, not like us."*[37]

Two facts can be ascertained from the report of the agent with the pseudonym "Romeo": that Prime Minister Ion Gheorghe Maurer discussed the issue of Bessarabia with the Soviet leadership, and that the Soviet authorities started extensive propaganda in this regard. Historical analyses of the former event have shown that during 1964, at the leadership level of the two states (Chivu Stoica, member of the RKP PB and Prime Minister Ion Gheorghe Maurer), the former negotiated with A. Mikoyan with the Chairman of the Presidium of the Supreme Council of the Soviet Union between May 26 and June 9, 1964, and on July 7-14 between Alexey Maurer. Among other things, he discussed the issue of Bessarabia with Kosygin. According to the Soviet side, Romania ignores the liberating role of the Soviet army, and as a result, they create an anti-Soviet atmosphere and even support nationalist manifestations.[38]

Finally, by 1977, the officers of the III Counterintelligence Directorate produced more than 60 reports on the case, the last one in November 1977, from which we learn that an undercover officer contacted Niculina under the pretext of talking about the officer who was staying at her apartment. During the disguised data collection operation, no information of secret service value was obtained, and nothing proves this better than the fact that the secret service work lasting almost a decade – even though there was a sober professional warning at an early stage that there was no suspicion of espionage in the case – was completely unnecessary for years was conducted against him, so that it was finally brought up on his personnel file that the procedure was initiated because he *"maintains relations with soldiers from Tirgoviste, knowing certain military activities. From time to time, he visits the Soviet Embassy in Bucharest. He and his daughters often travel to the Soviet Union (sic! Moldova SSR -*

---

[36] Ion Gheorghe Maurer (1902-2000) communist politician, lawyer. In 1957-1958, as a member of the close entourage of the Romanian Party General Secretary Gheorghe Gheorghiu-Dej, he was the Minister of Foreign Affairs of Romania, in 1958-1961, as the President of the Great National Assembly, he was the Head of State of Romania, and in 1961-1974, he was Prime Minister.

[37] ACNSAS Fond FCX 0000968 p. 148.

[38] CEBOTARI, Svetlana: Relațiile moldo-române în perioada anilor 1945-1990. [Moldovan-Romanian relations during the years 1945-1990.] In: COROBCA, Liliana (ed.): *Panorma comunismului în Moldova sovietică, Context, surse și interpretări*. [Panorama of communism in Soviet Moldova, Context, sources and interpretations.] Editura Polirom, Iaşi, 2019, pp. 724-737.

author's comment). He can be suspected of gathering information for the purpose of transmission."[39] The secret service tools and procedures that have been used for years in relation to Niculina have failed, as the operational technical section of the mentioned personnel card reads: *"He suspects that listening devices have been placed in his phone(...)"*, and in the case of surveillance, *"he believes that they are being followed, sometimes they check (...)*" and under the rubric of checking mail, it was noted that *"(...) suspects that their correspondence is being checked". "The results of the ten years of secret service work were summarized on the mentioned document, that is (...) the original suspicion was not substantiated"*, which ultimately led to *"the material being filed as inconclusive"*.[40] In the meantime, the case was transferred to the UM 920/A unit, which also confirms the custom that once someone is registered by the secret service, they remain in the register for a surprisingly long time.

There are hundreds of cases in the records of the specialized counterintelligence unit of the Dâmbovița County Securitate from the 1970s and 1980s alone, and in the majority of cases, either Romanians from the former Romanian territories (Bessarabia, Northern Bukovina, Southern Dobrudja) or their descendants were involved in the secret service under procedures. This is evidenced by the filing volume, in which the cases/dossiers of the Dâmbovița County Counter-Espionage Unit 920/A against socialist states and the legally continuous counter-espionage county unit 0110 were entered from the mid-seventies to the mid-80s. Based on the data in this file, it can be clearly outlined in what directions the mentioned county counterintelligence worked, how many agents it had, which officers and what cases and lines they worked on during the mentioned period.[41]

Comparing the above cases with the reminiscences of Colonel Ion Burdulea, who was assigned to the organizational unit against socialist states in 1973, and was appointed to the Dâmbovița County (UM 920/A) unit from 1975, and who in his reminiscences presents cases from his professional career that are recognizable, can be identified in the files of the previously mentioned organizational unit kept in the CNSAS, since 90 pages[42] of material handled by him were found from these and based on which the reader gets the impression that the main characteristic of the officer's work was that he, the state security officer of the field, was such worked in the cases of citizens who were not born in the territory of Romania at the time and had family and friendly relations with citizens of the neighbouring Soviet Union (Moldovan SSR, Ukrainian SSR (Bukovina), and also acted against persons who contacted the At the Soviet embassy, at their workplace, they contacted – since they knew Russian – the specialists delegated from the Soviet Union to factories in Romania. Retired colonel Burdulea repeatedly mentions that starting in 1973, more than a hundred "professionals" from the Soviet Union stayed in Dâmbovița County for a long time to provide technical assistance for the assembly and commissioning of equipment imported from the Soviet Union.

---

39 ACNSAS Fond FCX 0000968 p. 161.

40 ACNSAS Fond FCX 0000968 pp.161-161v.

41 ACNSAS Fond FCX 0000969 pp. 1-144.

42 ACNSAS Fond FCX 0000969 pp. 163-253.

There are indications from some of them that they have done study work on some Romanian citizens in order to recruit them as "agents".[43] Colonel Burdulea also states that after the Soviet advisers were withdrawn from Romania at the request of Gheorghiu-Dej, the "persons who fled the Soviet regime" who requested the restoration of their documents (citizenship - author's note) as former citizens, came under the crosshairs of state security and were even checked, as they were suspected of, that Soviet state security would have infiltrated Romania in this way. According to Burdulea, no person belonging to this category was identified in Dimbovita county who would have been in the service of the Soviet intelligence services.[44]

The archival sources only show that in the executed cases there were suspicions rather than realized, exposed espionage cases. In no case was the handing over of secret document(s) documented, no arrest(s) or successful house search(s) during which spy equipment was seized. Before and during the revolutionary events of 1989, there were no materials that could be supported by archival sources that would indicate a Soviet threat or a well-founded intelligence intervention.

On the other hand, Burdulea dedicated a separate chapter to the beginning of the end in his retrospective volume, and places this period between 1985 and 1989,[45] a chapter in which he suggests that the Romanian state security officers had guessed the end of the end of the communist political system. This is also thought-provoking, since in the light of the archival sources, the question arises as to what the anti-espionage agents of the Securitate could and did uncover, since on June 11, 1986, an order was received from the command of the Securitate's independent anti-espionage organization (UM 0110), what exactly needs to be done is "*the identification and control of the descendants of all enemy categories from the professional jurisdiction, primarily residents, former agents, and those who were previously for study or service purposes (stayed in the territory of Romania) and suspects, each case according to importance (must be documented), education, workplace, access to state secrets, according to the frequency of travel in the area of interest, must be subject to an operative procedure."*[46] This instruction also reflects the most important feature of the Romanian state security at the time, the strong central control, that is the instruction system that basically determines the daily routine, against whom and what kind of secret procedure should be initiated. This also means that individualization in the Securitate organization is unlikely to have been possible.

On February 16, 1989, an annual national evaluation meeting was held in Bucharest with the participation of the Securitate's central and county level 0110 organisations' (defence against socialist states) leaders.

---

43 BURDULEA, Ioan: *"Vânătoarea de spioni." Amintirile unui ofițer de informații din celebra UM110 – Unitatea anti-KGB. "*Spy Hunt." [Memoirs of an intelligence officer from the famous UM110 – Anti-KGB Unit.] Eveniment si Capital, Bucuresti, 2022, p. 143.

44 Ibid. pp. 134-135.

45 Ibid. pp. 261-268.

46 ACNSAS fond FCX 0001132 p. 39.

The head of the Securitate, colonel-general Iulian Vlad and his political deputy, major-general Ioan Marcu, were present at the leadership meeting. According to the situation assessment report, in the framework of a short overview, the most important problems with the characteristic of the neighbouring states was presented, and the case of agents operating undercover in Romania who carried out provocative or subversive acts was discussed.

At this meeting, it was deemed that the secret service activities of the "Făgăraș" states (Warsaw Treaty states) were coordinated by "Rodna" (Soviet Union). In support of this statement, an example was given that an unidentified radio transmission, not characteristic of personal contact, was detected in the representative office of such a state (embassy representation – author's note). the Romanian bodies. At the meeting, it was raised anonymously that the activities of the diplomats of some socialist states to distribute materials with hostile content were documented.

The report on the meeting describes in detail the methods by which counterintelligence against socialist states works and their shortcomings and discusses, among other things, that 20% of the diplomats subject to vetting cannot actually be controlled by counterintelligence agencies. According to the evaluation, evaluating the practical results of the preventive activities of the bodies, it was established that the specialized units did not meet the expectations. General Niculicioiu Victor, the commander of the anti-espionage unit against socialist states, assessed the situation as saying that in 1989 the county's territorial divisions performed below their capabilities. In the summary report, department 0110 in Brăila County was named as the weakest performing unit.

The issue of tourists, visiting relatives and small border traffic was discussed separately, as well as the operational processing of these areas, and the meeting came to the conclusion that the problems that have arisen can only be solved effectively in cooperation with other departments.[47] The report does not mention a single word about the increase in the number of Soviet tourists, the increase in the activity of Soviet officers present under cover, nor about the expected occurrence of any extraordinary secret service phenomena or other extraordinary events.

Examining other counties as well (Brăila,[48] Prahova,[49] Vaslui[50]), it can be established that even in December 1989, the increase in the activity of the Soviet spy services was not documented in the concerned counties.

47 ACNSAS Fond 0110 0002444 pp. 78-79.

48 FCX 0002444 on the activities of unit 0110 of Brăila county

49 FCX 0002742/3 Fond 0110 Dosar problema "Contraspinaj sovietic, fosti rezidenti, descendenti" (judetul Prahova).

50 FCX 0002633 Fond 0110 Vaslui county about the activities of unit 0110

The archival sources rather show that in the mentioned counties even during the days of the revolution, on December 16-17-18-19, the meetings with the agents and the reports were made of the incoming and outgoing Soviet ”nationals” (sic!) (Bessarabian – author's note) about Romanian citizens and agent briefings were held regarding their future activities.[51]

For example, the annual activity report of the Olt County Securitate unit 0110 dated December 19, 1989 (!) was submitted to the central bodies in Bucharest with the usual wording and content/structural structure in previous years. *“The 1989 report of Department 0110 was realized in an atmosphere of patriotic strengthening, deep satisfaction, and high esteem shown by the communists. It is still a political event of the recent past for our entire people – the party's XIV. Its congress, which is an event of extraordinary importance from the point of view of the country's economic and social development, is under its overwhelming influence(...)”*.[52]

The tumultuous introduction continued with the praise of Nicolae Ceauşescu, and then, according to the customs, an accurate picture of the number of agents was given, as well as evaluations of the various counterintelligence areas with detailed data. So also, about the fact that “Rodna” (the code name of the Soviet Union within counterintelligence), in 1989, covered the entire county of Olt with 25 agents in such a way as to secure the spy centres operating in the territory of the county. These centres were actually companies to which Soviet specialists arrived to carry out and supervise certain projects (installations, constructions, commissioning). The organizers of the exhibition and the employees of the commercial representation were also considered spies. All in all, representatives of the Soviet Union visited Olt County 77 times throughout the year.

The annual report concluded with the assignment of tasks for the first quarter of the following year, in which only “chewing gum” texts on general efficiency improvement were formulated.[53]

All in all, it can be said that since the 1960s, the Securitate's counter-espionage bodies have had the constant task of detecting and preventing the activities of the Soviets in Romania. Within that, serious efforts were made to systematically register, search for, check on, and recruit Romanian-speaking Soviet citizens from outside the 1947 national borders (Bessarabia, Bukovina) or those who had relocated in the meantime. All this happened in order to create cases, depending on the political relationship between Romania and the Soviet Union, and to prepare summarizing materials that satisfy and support the political (pre)conception of the Romanian party leadership.

---

51 FCX 0002742/3 Fond 0110 Dosar problema ”Contraspinaj sovietic, fosti rezidenti, descendenti” pp. 436-436 v.

52 ACNSAS Fond 0110 0001252 p. 152.

53 ACNSAS Fond 0110 0001252 pp. 152-155.

Conclusion

This processing work sheds light on the fact that the Securitate had been systematically documenting the subversive activities of the enemy's spy services, ordered from above, since 1986, and had regularly collected data, indicating the Soviet intervention.

Based on the materials of the 0110 territorial units of the mentioned counties (Dâmbovița, Prahova, Brăila, Vaslui), it can be stated that the demand for news, in the 1960s and 1970s, remained unchanged until 1989; that is Romanians with roots in Bessarabia remained in the registers, and even those who relocated, and also their refuged descendants were included in the Romanian state security databases, as persons to be checked. The control of people leaving and entering the Soviet-Romanian border section, the close monitoring and control of the "(spy)" activities of Soviet citizens working in Romania fell under the same secret service approach, as the control of Romanians of Bessarabian origin and their descendants.

Such a fixation of the Securitate's activity means a kind of stagnation of the organization, since it seems from the sources that it did not react to the geopolitical changes of the 80s, due to the inertia of the organizational culture, or to the fact that the organizational structure dealing with the socialist states within the Securitate had not attributed a greater importance to information, indicating geopolitical changes, and also interpreted and distorted the obtained information, according to the usual analysis pattern; thus, meeting the expectations of the highest political leadership. This is confirmed by the instruction of Iulian Vlad, the commander of the Securitate, dated November 20, 1989, which still stated that the primary and most important task was to ensure "thorough knowledge of enemy plans and effective action to neutralize hostile activities against the country".[54] This is the task of the Securitate's counterintelligence and the entire organization.

Bibliography:

ALDEA, Patriciei González: *Helsinki 1975. Începutul sfârşitului. Degradarea regimului din România şi singularitatea lui în blocul de Est (1975-1990)*. Curtea Veche, Bucureşti, 2008.

APARASCHIVEI, Sorin: *UM 0110 – Contraspionaj tari socialiste (anti-KGB). Infiintarea si primi ani (1963-1973)*, Historia, n.d. Online: https://historia.ro/sectiune/general/um-0110-contraspionaj-tari-socialiste-567294.html (Download time: 10/09/2022)

BANU, Florian – ȚĂRANU, Liviu: *Securitatea 1948-1989, Monografie* vol I., Editura Cetatea de Scaun, Târgoviște, 2016.

BANU, Florian – ȚĂRANU, Liviu*: Securitatea 1948-1989, Monografie vol I*, Editura Cetatea de Scaun, Târgoviște, 2016.

[54] ACNSAS Fond FCX 0001132 mapa cu ordine orinetari ale unitatii centrale 4.

BURDULEA, Ioan: *„Vânătoarea de spioni." Amintirile unui ofițer de informații din celebra UM110 – Unitatea anti-KGB.* Eveniment si Capital, Bucuresti, 2022.

CAȘU, Igor: *Dușmanul de clăsă comes in detail about the phenomenon of RSSM starvation after the Second World War. Represiuni politice, violență și resistance în R(A)SS Moldovenească*, *1924–1956*, Cartier, Chișinău, 2014.

CEBOTARI, Svetlana: Relațiile moldo-române în perioada anilor 1945-1990. In: COROBCA, Liliana (ed.): *Panorma comunismului în Moldova sovietică, Context, surse și interpretări*. Editura Polirom, Iaşi, 2019, pp. 724-737.

CONSTANTINIU, Florin: *O istorie sinceră a poporului român*. Editura Univers Enciclopedic, Bucureşt, 2011.

CROITOR, Mihai: *In umbra Kremlinului Gheorghe Gheorghiu-Dej si geneza declaratiei din aprilie 1964.* Editura Mega, Cluj-Napoca, 2012, Online: https://www.academia.edu/3327808/In_umbra_Kremlinului_Gheorghe_Gheorghiu_Dej_si_geneza_Declaratiei_din_Aprilie_1964_In_the_Shadow_of_Kremlin_Gheorghe_Gheorghiu_Dej_and_the_genesis_of_the_Declaration_issued_in_April_1964%20%20 (Download time: 28/09/2023)

GARTHOFF, Raymond: *When and Why Romania Distanced Itself from the Warsaw Pact*. CWIHP Bulletin, 1995/5.

GIURESCU, Dinu C. – ŞTEFĂNESCU, Alexandru: Ilarion Ţiu, *România şi comunismul. O istorie ilustrată,* Editura Corint, Bucureşti, 2010.

HARRINGTON, Joseph F.: *Relaţii romano-americane: 1940-1990*, Editura Institutul European, 2002.

N.a.: Evidenţa persoanelor în România (istoric), LegeAZ, n.d. Online: https://legeaz.net/dictionar-juridic/evidenta-persoanelor-romania-istoric (Download time: 10/09/2022)

OPREA, Marius: ISTORIA FARA PERDEA In 1945, rusii au negociat cu pistolul pe masa, iar romanii cu inteligenta: un avocat roman a salvat sute de mii de Basarabeni si bucovineni de la deportare. URSS, n.d. Online: https://monitoruljustitiei.ro/profesii-juridice-si-retele-judiciare/avocati/istoria-fara-perdea-in-1945-rusii-au-negociat-cu-pistolul-pe-masa-iar-romanii-cu- intel-20475874/ (Download time: 10/09/2022)

PACURARIU, Tudor: Planul Nistru-1989, *Implicarea G.R.U. in Revolutia din Decembrie,* Editura Evenimnetul si Capital, Bucuresti, 2020.

RETEGAN, Mihai: *1968. Din primavara pana in toamna*, RAO, Bucuresti, 2015.

STAN, Mircea: *Programul de masuri active al KGB-GRU impotriva Romaniei (1964-1989).* Editura Militara, Bucuresti, 2021.

STEFUREAC, Remus Ioan: *Conflictul secret din spatele scenei România versus Rusia. 50 de ani de realități, mituri și incertitudini.* Editura RAO, București, 2015.

XENOFONTOV, Ion Valer: Romania in sistemul de sceuritatet europeana in secolul XX – inceputul secolului XXI. USM, Chisinau, 2021.

ISTVÁN SOLTI PhD – IMRE DOBÁK PhD

THE BOUNDARIES OF OSINT

Abstract

OSINT (Open Source Intelligence), as a field of information gathering from open sources, is unintentionally pervasive in our lives. Its various methods make an indispensable contribution, not only to the work of individuals, but also to that of economic actors and even public organisations, including government bodies, responsible for security. However, their application also presents a number of advantages, but also a number of disadvantages. It has evolved beyond the use of traditional open sources and is closely linked to cyberspace and the various ICT solutions based on it. At the same time, their spread and their dynamic changes have a direct impact on OSINT methods. Taking into account the changes, caused by the effects of continuous development, the paper aims at reflecting on the boundaries of open source information gathering as a category.

Keywords: OSINT, intelligence gathering, development of OSINT, ICT, boundaries of OSINT, OSINT techniques, cyberspace, security, national security

Introduction

Nowadays, there is a significant literature on open source information gathering. It mainly describes the advantages of OSINT and its techniques. The reason is that this area of information gathering can be made available to anyone (be it a private individual, a company, an NGO or a public authority). However, its effective use can be based on a number of professional skills and knowledge that influence its effectiveness. In the security sector, its importance has increased, although there is traditionally disagreement in the existing literature on the real value of open information and its importance in supporting decision making.[1]

Where is the boundary of OSINT activity? We only need to look at the openly available resources, or even at the wide range of methods that, although widely available, requires specific knowledge. In many cases; some of these methods may be considered open as a solution available on the Internet, but they may still raise also legal or even ethical issues.

In the security sector, OSINT's approach is dual. On the one hand, in maximising the potential for information gathering, on the other hand, the issue of protecting data and information that may become openly available becomes important.

[1] BEST, Jr. R.A. – CUMMING, A.: Open Source Intelligence (OSINT): Issues for Congress, CRS Report for Congress, 2007, p. 2.

Thus, in addition to the professional aspects of gathering open information, there may also be aspects of protection and awareness of the information that is openly available, as well as the conscious use of information (influence, disinformation). Social media platforms are among the most important sources of today's main security threats. The information presented there has in itself a direct impact on security in many cases. Examples include the war between Russia and Ukraine, the recruitment activities of terrorist networks, or even the influencing of the masses.

Methods

This paper does not aim to define the boundaries between the open and secret collection of information. It is not intended to do justice to the views of different trends. It does, however, aim to draw attention to the grey area between the two phenomena. The reason is that, in our experience, the importance of economic actors and scientific research based on data has increased in recent years. This has brought to the fore the question of where the boundaries of OSINT might be drawn. Business actors have an interest in bringing as many information sources and information-gathering tools as possible under OSINT, so that they can use them legally. In contrast, the role of science is to debate these claims. It is also worth broadening the scope of the studies, because the effectiveness of business and public actors engaged in OSINT activities is directly influenced not only by the open availability of data, but also by the professional ability to process the sources and even the availability of the necessary financial resources. As a methodology, we intend to draw conclusions from the international literature on the subject and to highlight the extreme complexity of the issue in parallel with the emergence of artificial intelligence

Possible boundaries of the category

Over the past decades, OSINT has essentially evolved from its former narrow conceptual framework. With a little goodwill, almost anything that is open source and of relevance to its collector can be categorised here. In the background, however, the development of cyberspace and the protection of privacy rights have led to serious professional debates and research. The most important issues are the legality of data collection solutions, the problem of easily accessible and open data (is all data that is available on a public platform really public data?) and the question of mass data collection and processing. In fact, OSINT cannot only cover the collection of information through ICT solutions, but in our online world, open information gathering based on electronic sources has become almost unique.

It is clear from the literature that professional debates related to the legality and limits of OSINT methods have already come to the fore.[2]

[2] TEN HULSEN, Leonore: Open Sourcing Evidence from the internet – the protection of privacy in civilian criminal investigations using OSINT (OPEN-SOURCE INTELLIGENCE). *Amsterdam Law Forum*, 2020/2, p. 44.

A specific question is whether, in conducting OSINT in cyberspace, we should primarily look at openly available “sources” or at “methods” that only deeper technical (even hacker) knowledge can provide access to OSINT information and complex analysis. The question arises whether all solutions found on the Internet can be considered ethical and legal for the OSINT activity, since their open availability does not clearly mean that their use becomes “legal”. As explained by Eijkman and Weggemans in their study, this mode of intelligence gathering has side effects that need to be addressed. For the argument that social networking sites are public property and can be accessed by anyone does not override the fact that OSINT conducted in this way directly or indirectly affects someone's privacy and future opportunities.[3] As a consequence, the use of OSINT needs to be balanced, which requires developing accountability of organisations.[4] Open 'access' also needs to be considered in terms of what makes a solution to help interpret information open, in a cyberspace where hacking techniques are often freely available.

OSINT, according to its literature, has a number of traditional sources, usually highlighted as the media, public government data, professional and scientific publications, commercial data, grey literature and, with the advance of the information society, the Internet.[5] However, the traditional division of resources is very general, despite the fact that all types can be examined both horizontally and vertically. For example, consider the field of scientific publications. The history of the development of OSINT shows that its sources are scientific periodicals, which used to be published on paper and nowadays are published on digital media. In the past, subscribers to a periodical were sent it by post or anyone could buy it freely in a shop or borrow it from a library. Today, digital copies are available free of charge or by subscription from the publisher's website. However, there are also academic works that are commissioned, put out to tender or produced for the information of a limited interest group. Before the digital age, these publications remained unknown or difficult to access for the unauthorised. If an unauthorised person wanted to know about them, he or she could only obtain them by using some combination or lie. Of course, even in the online world, access to a publication can be restricted. However, some of them may eventually be leaked into the public domain by individual authorised users, even against the will of the authors, and it is considered an accepted OSINT practice to include those who are authorised to know by using a “fake” online identity.[6]

The same is true for personal data. In the past, if someone introduced themselves to people they knew, they knew their name, address, details and characteristics. It was therefore only possible to get to know him or her from the workplace, home, family, etc., and from the records of public bodies.

---

3 EIJKMAN, Q. – WEGGEMANS, D.: Open source intelligence and privacy dilemmas: Is it time to reassess state accountability? *Security and Human Rights*, 2013/4, p. 293.

4 Ibid. p. 296.

5 UNGUREANU, Gabriel-Traian: Open Source Intelligence (OSINT). The Way Ahead, Journal of Defense Resources Management, 2021.

6 See e.g. BIALKSA, Aleksandra: Open Source Intelligence tools and resourcees handbook. 2020. p. 499.

Nowadays, the individual registers with a username on a social networking site. On the social networking site, the username and the real name become public data, the person and the username are linked on the site. Everyone likes to use easy to remember data, so we don't change our usernames. We use the same usernames on different sites, for different registrations. Even where the username does not appear on the public interface. We also don't want to make it public which online clothing store we shop at, which online services we use, which telephone service we use, or even which mail service we use. Yet, registrations can be collected by cloud username, because the online world treats this as public data. So, each account can be linked to a specific person. But this is not the nature of personal data.[7] The vast majority of the literature on OSINT is based on the assumption that what is available from the public domain is free to collect and free to manage.[8] However, in the case of personal data, public availability does not usually constitute a legal basis for processing.[9] In other words, the fact that a piece of data has been published in grey literature or can be found in some part of the online space does not in itself imply that it can be obtained through open-source information gathering. Consequently, we can agree with those analysts who rightly point out that legality does not necessarily derive from the information available.[10]

OSINT operators are not above all. They live and work under the jurisdiction of a state and therefore need to know and apply the legal framework.[11] In the view of the Berkeley protocol authors, OSINT activities must be in compliance with the law. Investigators need to be familiar with data protection laws and the details of the right to privacy, which is protected under international law. They emphasise that just because information is publicly available does not mean that its collection and use does not affect privacy. Data collectors should also be aware of the mosaic effect, which means that even anonymous public data can become vulnerable to re-identification if a sufficient dataset containing similar or additional information is processed.[12]

A similar finding was made for some areas of OSINT in a study by Hribar, Podbregar and Ivanusa in 2014. They found that, while OSINT is not considered a potentially harmful data collection method, an analysis of the use of OSINT quickly reveals that it is not as harmless as it appears.

---

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR) paragraphs 6 and 7

8 See e.g. BAZZELL, M.: *Open Source Intelligence Techniquues: Resources for searching and analyzing online information – Eighth Edition.* Independently published*,* 2021. p. 5.

9 GDPR, (41)-(51)

10 N.a.: Berkeley Protocol on Digital Open Source Investigations. Human Rights Center, University of California, Berkeley/UN Office of the High Commissioner for Human Rights, New York and Geneva, 2022, p. 20.

11 Ibid. p. 19.

12 Ibid. p. 12.

Government agencies, organisations, groups and individuals sometimes use OSINT in ways that are not clearly legal.[13] In their study, they categorised information sources into four groups: white, grey, black and non-existent information. Of these, white information is fully accessible to the public. Grey information is that which is not widely published or disseminated but is legally accessible. Information that can only be obtained through specific channels includes preliminary forms, technical reports and standards documents, yearbooks, dissertations, working papers, data repositories, registers, private company reports, searchable photographic records, and personal records produced by non-profit organisations, educational organisations.

In the case of the grey zone, it was argued that the rules of normal logic could be followed, and the importance of the "fuzzy logic" of Loftifali Askar Zadeh was emphasised.[14] Fuzzy logic is different from classical logic. It deals with the formal principles of approximate reasoning, and considers exact reasoning as a constraint on decision making. The authors argued that using fuzzy logic, the grey zone of OSINT can have other values, such as legal-legal, or ethical-unethical, etc. Since OSINT can be on the boundary of legal and illegal, it is not always possible to determine exactly whether it is completely legal or completely illegal. Classical logic therefore makes OSINT always grey, unable to clearly define its boundaries and characteristics and consequently the threats to security. Fuzzy logic describes precisely those boundaries that classical logic cannot.[15]

Open vs. secret information gathering

The categorization of information gathering methods, the "INTs"[16], is a theoretical classification of data collection by source, that is we categorize data according to the source from which they are obtained and the way in which they are obtained. An important conclusion can also be clearly drawn, namely that intelligence methods do not select according to whether or not the information is attributable to a person.

We also know from the descriptions of the different intelligence methods, which have been explored with a high level of sophistication and scientific rigour, that a significant part of the information of interest to intelligence services (80-95%[17], as commonly mentioned in the literature) may be open source, and that a significant part

---

13 HRIBAR, Gašper – PODBREGAR, Iztok - IVANUŠA, Teodora: OSINT: A "Grey Zone"? *International Journal of Intelligence and CounterIntelligence*, 2014/3, p. 533.

14 Ibid. p. 535.

15 Ibid. pp. 535-537.

16 JENSEN, Carl J. – MCELREATH, David H. – GRAVES, Melissa (ford.: Tamás Gábor): *Bevezetés a hírszerzésbe.* [Introduction to Intelligence.] Antall József Tudásközpont, Budapest, 2017. 4. fejezet

17 GIBSON, Stevyn D.: Exploring the Role and Value of Open Source Intelligence. In: HOBBS, C. – MORAN, M. – SALISBURY, D. (ed.): *Open Source Intelligence in the Twenty-First Century*: *New Approaches and Opportunities (New Security Challenges Series).* Palgrave Macmillan, New York, 2014, p. 10.

of the data obtained is personal data. Moreover, the different intelligence methods do not even distinguish from the data processing side which actor in the information chain the personal data relates to. It could be the identity of the source of the information providing the basic data, the agent acquiring the data, the images of soldiers in photographs, the metadata of intercepted phone calls, or even personal data extracted from processed social profiles. This in itself implies that a significant part of the use of intelligence gathering methods is already covered by the issue of secret information gathering.[18] In fact, there is an intelligence mode, HUMINT, which can be almost entirely linked to this. The only exception to the previous statement is Open Source Intelligence (OSINT). In the case of Open Source Intelligence, the use of any means of secret information gathering is conceptually unintelligible, as there is no question of covert behaviour or the use of covert methods.

Unlike intelligence gathering, secret information gathering is a legal institution, that is it is created by law, it cannot exist without law, its framework can only be defined by law and its limits can only be set by law. We also know from the jurisprudential development of secret information gathering that its existence arises from the protection of fundamental human rights and is closely linked to them. It is primarily a legal institution designed to protect the rights of the individual and is derived from them, and is intended to represent a limitation on the power of the state.[19] It follows, however, that the collection of secret information cannot be regarded as one of the branches of intelligence gathering. It has legal relevance only if the collection of information in the intelligence branches involves the processing of data on individuals.[20]

If we examine the issue from the perspective of the intelligence services of the states, we can start from the assumption that there are two possible ways of gathering information by the services: open source information gathering and secret information gathering. In reality, however, there are complex manifestations. For example, if a European national security agency acquires commercial satellite imagery from open source, it is using IMINT as an intelligence methodology through open source acquisition. If the same content image was captured by a state national security agency's drone for its own use, it is conducting IMINT using a classified intelligence gathering tool. It is also conducting classified information collection if it purchases the commercial satellite imagery through its covert company. The example shows that it is the methodology, not the data, that determines the distinction between the two forms of information collection.

---

18 Identifying covertly applicable instruments, e.g. Spain, ORGANIC LAW 2/2002 of 6th May regulating a priori judicial control of the Centro Nacional de Inteligencia (National Intelligence Centre); Italy, Law No. 124 of 3 August 2007; Croatia, Decision Promulgating the Act on the Security Intelligence System of the Republic of Croatia by the Croatian Parliament at its session on 30 June 2006; Netherlands, Wet op de inlichtingen- en veiligheidsdiensten 2017.

19 N.a.: The Johannesburg principles on national security, freedom of expression and access to information. Article 19, Global Campaign for Free Expression, London, 1996.

20 GDPR (50) pont

As a result of the previous considerations, it can therefore be said that the task of the law is not to regulate each intelligence gathering method in isolation, but to define the secret information gathering within each intelligence gathering method. At the same time, however, it can also be stated that it is still true that the legal regulation of open-source intelligence gathering by intelligence agencies is typically superficial in the various legal systems.[21] States are primarily concerned with the issue of secret information gathering, issuing regulations at national level.

Conclusion

Thanks to the cyberspace that pervades our days, OSINT solutions are now part of our lives. But beyond the benefit of rapid access to open information, their deeper, targeted application raises a number of questions. These essentially concern the issues of data usability and personal data, indicating that OSINT activities and data usability have a number of moral and legal limitations beyond the technical possibilities. OSINT as an intelligence branch or method, despite the often mentioned “grey zone” at its borders, can be distinguished from the areas of secret information gathering, regulated by law, despite the fact that the information gathering possibilities and uses offered by cyberspace can make it extremely complex.

A common perception of OSINT is that it is a cost-effective activity, but this is only partially true. In the era of mass information access, the real value may no longer be the quantity of information, but the extraction of meaningful information from it. However, this requires professional skills, resources and the development of an expert and analytical base. Just think of the professional businesses that act as information brokers, helping both business and government. They may be involved in analysing and interpreting information, or even in providing the credibility that is essential for rapid decision-making. In addition to its often-mentioned advantages (e.g. cost-effectiveness, timeliness, secure application - the possibility of risk-free "research") and to disadvantages (e.g. information dumping, language skills, time factor), the issue of information reliability has become a major concern.

On OSINT information platforms, we may also be confronted with the phenomenon of pseudo-news/misinformation/disinformation, which is becoming more and more prevalent in our digital information environment. However, the filtering of this open information has also become an important task, due to its security implications. Open data that can be massively collected increase the phenomenon of profiling, in particular the possibilities for data collection (e.g. trend analysis) by global business actors. This is where the further development of the information technology environment, the increasing use of artificial intelligence and data, the text mining technologies come to the fore. At the same time, the unclear boundaries of OSINT also create opportunities, as the ever-expanding free resources available in open, digital form create significant market demand for OSINT capabilities.

[21] EIJKMAN – WEGGEMANS 2013, p. 296.

Understandably, business actors are inevitably moving towards OSINT opportunities that can increase their efficiency and even give them a competitive advantage in the grey area.

Bibliography:

BAZZELL, M.: *Open Source Intelligence Techniquues: Resources for searching and analyzing online information – Eighth Edition.* Independently published, 2021.

BEST, Jr. R.A. – CUMMING, A.: Open Source Intelligence (OSINT): Issues for Congress, CRS Report for Congress, 2007. Online: https://sgp.fas.org/crs/intel/RL34270.pdf (Download time: 10/02/2024)

BIALKSA, Aleksandra: Open Source Intelligence tools and resourcees handbook. 2020. Online: https://i-intelligence.eu/resources/osint-toolkit (Download time: 10/02/2024)

EIJKMAN, Q. – WEGGEMANS, D.: Open source intelligence and privacy dilemmas: Is it time to reassess state accountability? *Security and Human Rights*, 2013/4, pp. 285-296. https://doi.org/10.1163/18750230-99900033

GIBSON, Stevyn D.: Exploring the Role and Value of Open Source Intelligence. In: HOBBS, C. – MORAN, M. – SALISBURY, D. (ed.): *Open Source Intelligence in the Twenty-First Century*: *New Approaches and Opportunities (New Security Challenges Series).* Palgrave Macmillan, New York, 2014, ISBN 978–0–230–00216–6, https://doi.org/10.1057/9781137353320,

HRIBAR, Gašper – PODBREGAR, Iztok - IVANUŠA, Teodora: OSINT: A "Grey Zone"? *International Journal of Intelligence and CounterIntelligence*, 2014/3, pp. 529-549. DOI: 10.1080/08850607.2014.900295

JENSEN, Carl J. – MCELREATH, David H. – GRAVES, Melissa (ford.: Tamás Gábor): *Bevezetés a hírszerzésbe.* Antall József Tudásközpont, Budapest, 2017. ISBN: 9786155559198

N.a.: Berkeley Protocol on Digital Open Source Investigations. Human Rights Center, University of California, Berkeley/UN Office of the High Commissioner for Human Rights, New York and Geneva, 2022.

N.a.: The Johannesburg principles on national security, freedom of expression and access to information. Article 19, Global Campaign for Free Expression, London, 1996. ISBN 1 870798 89 9
https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf (Download time: 10/02/2024)

TEN HULSEN, Leonore: Open Sourcing Evidence from the internet – the protection of privacy in civilian criminal investigations using OSINT (OPEN-SOURCE INTELLIGENCE). *Amsterdam Law Forum*, 2020/2, pp. 3-48. DOI: 10.37974/ALF.353

UNGUREANU, Gabriel-Traian: Open Source Intelligence (OSINT). The Way Ahead, Journal of Defense Resources Management, 2021. Online: https://www.academia.edu/74627992/OPEN_SOURCE_INTELLIGENCE_OSINT_THE_WAY_AHEAD (Download time: 10/02/2024)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR)

TAMÁS DRUSZA

A NEW APPROACH TO DEFINING SOCIAL PURPOSES OF SECRET INTELLIGENCE SERVICES

Abstract

An important part of intelligence studies is the examination of the question of what role the secret services play in the functioning of society. The researchers so far are indebted to a general approach that can integrate the areas and the tasks that characterize these organizations. The article formulates the basic social purpose and the unique functions of intelligence services, starting from a sociological point of view and from the concepts of interest and the public benefit. This sufficiently general approach offers the possibility for further scientific analysis of the issues of social interests related to services.

Keywords: Definition of intelligence, intelligence studies, theories of intelligence, social tasks of intelligence, social functions of intelligence

Introduction

It is believed that intelligence is the second most ancient craft, yet it became a science only a few decades ago, in the 20th century, to begin investigating the subject. Presumably, this is not independent of the fact that the institutionalization of intelligence services[1] – similar to current ones – was a process that began in the second half of the 19th century, and was completed in the first half of the twentieth century. This was when the activity, which had previously only been carried out on an ad hoc basis, began to become a professional one and take on a stable organizational form. The Second World War and the years that followed certainly showed that these organizations are indispensable for modern states, so the discipline that we now identify as "intelligence studies" sprang up.

One of the central issues in the literature – primarily among Anglo-Saxon researchers – is the definition of the concept of intelligence. The latest writings also emphasize that scientists are still indebted to the widely accepted scientific definition of this concept.[2] Of course, this does not mean that different researchers would not have ideas about it at all.

1 In the study, the names intelligence service and secret service refer to the same organizations. This term refers to organizations that deal with intelligence, espionage and counter-terrorism.

2 SCHEFFLER, Alessandro – DIETRICH, Jan-Hendrik: Military Intelligence: Ill-Defined and Understudied. *International Journal of Intelligence and CounterIntelligence*, 24 May 2023, pp. 1-20.

Rather, it refers to two other things: On the one hand, to the fact that the scientific research of the secret services is still in its infancy, let's face it, 70 years is not very long, when measured on a scientific scale, especially in a subject where it is difficult to get data that can be analysed. On the other hand, it may be also a consequence of the fact that the research of secret services is typically based on national foundations. This means that the researchers of a given country typically start from the perception and/or the organizational solutions of "intelligence" of their own country, during the research. Of course, this is understandable, as studying these organizations is not easy for domestic researchers either. The result of all this is that there are many different theoretical definitions for the same concept, and no consensus has yet been formed around any of them.[3] Although the idea is tempting, in the following article we do not want to deal with the general concept of intelligence. Instead, we want to examine why states maintain such organizations, what could be the reason that similar organizations exist in most countries of the world. We will examine what specific social functions this role entails and why these are essential from the point of view of the society. We also want to give an answer to the question; why the specific function is best performed by the secret services. Our research is still far from finished, so in this study we will not yet provide answers to all questions that satisfy the need for completeness, but we also do not consider it useless to introduce the conceptual framework of the theory to the scientific public and to those who are interested in this profession.

The scientific problem

The question rightly arises as to why there is a need for a social investigation of secret services at all. We ourselves see several reasons. On the one hand, it is an activity with a controversial social role. We find that both lay people and scientists are often ambivalent about the question of whether secret services are necessary. Most of the time, their operation does not fit into the traditional state and government activities, so their legal regulations and institutions are not exactly conventional either. This is especially true for clandestine activities and their social control. If we still vote in favour of the secret services, then the question arises as to exactly what tasks these organizations should perform and what powers and tools should be provided to them, and perhaps in what direction and to what extent the current situation should be changed. In every country, sooner or later, a situation emerges that would justify a change, but it is often surrounded by heated debate or delay, due to uncertainty. All professionally based thoughts are needed to soften them. Even if these issues are settled, the debate will flare up again and again as to when the services can be called effective, or when they have failed, when they have used and when they have abused their undoubtedly powerful social authority. So, we see that there is a social demand and interest in investigating the issue.

[3] DOKMAN, Tomislav: Defining the Term "intelligence" – Insight into Existing Intelligence Knowledge. *Informatologia,* 2019/3-4, pp. 194–205.

However, all these questions[4] can be examined thoroughly, if we answer the basic question of why the services exist and what role their activities play in social functioning. We see that the research until now started typically from the process of the organizations' activities, they tried to understand and describe what these organizations do. We do not consider this to be an optimal approach, because the description of the activity alone does not directly shed light on its social role. And just to give an example, without it, its usefulness is difficult to examine. It is important to clarify that we do not wish to state what the services do, but rather what they should do in an ideal situation. In our opinion, a theory with great explanatory power is needed, which makes every aspect of the operation of the services explainable on a theoretical level, regardless of space and time and organizational structures. It must be clarified who the subjects of the activity are, what the object is and who the final beneficiaries are. In our opinion, it is advisable to do all of this in a conceptual framework, the task of which is to describe the social functioning. On the one hand, this makes the definition more objective, because we do not describe the activity by using our own terminology. On the other hand, it facilitates comparison and thus separation from other activities. Finally, it renders the wording neutral, which can remain functional regardless of the social order.

The method

Our research approach is basically based on two pillars. On the one hand, on the processing of the literature, the main purpose of which is to examine what the researchers think the intelligence services do and why. In this context, we will examine the most important researcher-positions, in terms of why the activities of secret or intelligence services are necessary, and we will examine the definitions given to the concept of intelligence, in terms of whether we can draw this conclusion regarding the final social function of the activity. Secondly, we will examine whether there is a concept through which we can put it in a new perspective and define the activity in question in general, by using the theoretical framework of other disciplines, primarily sociology. The examination of the specific activities of the services and their relationship with each other – which can be called intelligence studies – can already be carried out and completed on this basis.

Intelligence studies must necessarily be multidisciplinary, because it cannot create a new conceptual system that describes the behaviour of its participants. Its own conceptual system can only be valid within the scope of its own system. In other words, social science concepts are necessarily justified to describe the relations between services and the outside world.

---

4 GILL, Peter: Theories of Intelligence: Where Are We, Where Should We Go and How Might We Proceed? In: GILL, Peter – MARRIN, Stephen – PHYTHIAN, Mark (eds.): *Intelligence Theory*. Routledge, 2008.
GILL, Peter: Theories of Intelligence. In: JOHNSON, Loch K. (ed.): *The Oxford Handbook of National Security Intelligence.* 1st ed., Oxford University Press, 2010, pp. 43-58.

As for the approach, we ourselves have experienced that thinking about secret service activity typically starts from how the organization functions, that is it looks for the answers to what the services do. We ourselves chose the approach of sociology rather than basic science. The essence of this is that our starting point is the examination of the individual and the social actions of individuals and how the services as organizations fit into this. What purpose(s) do secret services work to achieve and what distinguishes their activities from the other governmental functions?

Literature review

In the last few decades, researchers have already dealt with many aspects of intelligence activity. The biggest polemic undoubtedly arose around the definition of the term itself. It is interesting to observe how conflicting definitions have emerged from the same terms and datasets. There were researchers who defined or understood the concept of intelligence as an ability, some as a process, and some as a result of this process. There were those who believed that secrecy should definitely be part of the definition, and there were those who believed that it should not be part of the definition. We think this polemic is a little self-serving, since the function should be clarified first, that is what exactly we are talking about. In our opinion, the discussion of the interpretation of a term that has many meanings and is used is rather a dialogue of the deaf: naturally, it cannot lead to a generally accepted definition. First of all, it is necessary to clarify what we want to define and then start researching for the correct definition. This is especially true when it comes to the definition of a complex activity.

However, perhaps this type of polemic cannot be said to be completely useless, since each definition contains references to the assumed social purpose. As a result, we will first review the ideas that specifically deal with social purpose, and then we will examine – for reasons of scope only a few – definitions that we think are more important and that seem usable.

The first author in whom this problem can be clearly identified is the ancient Chinese military theologian Sun Tzu, who defines the purpose of using spies as that in order to win, we need to know everything in advance, noting that the army can only achieve this and act correctly with the help of spies. In an indirect way, it also highlights the knowledge of the enemy's condition as a function. Finally, the idea appears that if we can use all the spies he suggests, no one will be able to spy on this secret system.[5] The logical built-up structure of Sun Tzu's system is clearly visible: he sees the victory of the prince as the ultimate goal, which he achieves with the help of the army, which is assisted by a well-structured secret and protected system of spies. It is also obvious, however, that this perception prioritizes winning open armed conflicts and battles, which, however, are not nearly permanent conditions for covert activities.

[5] N.a.: Chapter 13: The Use of Spies. Sun Tzu’s Art of War.

According to Michael Herman, intelligence is something that is produced, in order to – albeit from a distance – influence government actions. As such, this activity is an inseparable part of government decision-making, thus part of state operation.[6] According to him, intelligence power is a part of state power and it derives this power from the operation of intelligence services, which produce intelligence. This power then enables you to defeat your adversaries by making better decisions and disrupting enemy intelligence. Ultimately, the definition suggests that the main function of intelligence is to gain an advantage over enemies. According to Howard, the mission of intelligence is to provide information about other entities so that governments can assess the strength and intentions of allies and potential enemies.[7] It is clear that the above idea indicates government information as the ultimate goal, which, however, is probably characteristic of all state functions, so it is difficult to make distinction between them.

Bruce Berkowitz defined in a short article – the purpose of which was to separate investigative work (evidence) and intelligence – that the purpose of the latter is to inform officials and military commanders.[8] This definition considers the activity in question as an aid to state decision-making. For us, this separation may be important because both activities carry out secret information gathering activities.

Ferris sees intelligence as a kind of force multiplier, which, on the other hand, shows state leaders who and how to use the increased force.[9] In our opinion, the value of the definition is that it can be generalized to various areas of social functioning, but its weakness is that it does not explain the nature of power and the multiplier effect. According to Marc Lowenthal, these services are needed to support decision-makers in countless ways. It distinguishes three functions of the activity itself:

- Monitor the factors that threaten the existence of a nation;
- Ensuring long-term expertise. This is important in democracies so that after the mandate of the elected officials expires, and the new officials do not have to rebuild the information of the state from scratch;
- Supporting the policy making process.[10]

From this point of view, the first one is actually the only one that somewhat expresses the social purpose of the activity, the second one seems more like a function of the state bureaucracy, and the third one is true to some extent for all state functions. These are therefore not distinguishing factors in this form per se.

---

6 HERMAN, Michael: *Intelligence Power in Peace and War.* 1st ed. Cambridge University Press, 1996.

7 HOWARD, Michael: *The Invention of Peace: Reflections on War and International Order.* Yale University Press, New Haven, 2000.

8 BERKOWITZ, Bruce: The Big Difference Between Intelligence and Evidence. 2 February 2003

9 FERRIS, John: Diplomacy and diplomatists. In: BOYCE, Robert – MAIOLO, Joseph A. (eds.): *The Origins of World War Two: The debate continues.* Palgrave Macmillan, New York, 2003.

10 LOWENTHAL, Mark M.: *Intelligence: From Secrets to Policy.* 2nd ed. CQ Press, Washington, D.C, 2003

But even the first one is a very restrictive definition, because based on this, for example, US intelligence should only deal with countries that theoretically have enough nuclear weapons to destroy the US, which is certainly not the case.

In his 2008 article, Kahn approaches the role of intelligence primarily from the point of view of military conflicts. His way of thinking boils down to the fact that intelligence is a form of knowledge, and its main function is the optimization of resources. In peace, by increasing information, it reduces uncertainty and thus resolves conflicts, thereby contributing to the stability of the international order. In war, it reduces the sums to be spent on the purchase of weapons, shortens the duration of battles and thus saves on resources.[11] Kahn sees intelligence first and foremost as a means of defence, not of attack.

Michael Werner, on the other hand, describes intelligence as an activity that helps leaders cope with the dangers that arise from the struggle with rival powers. It manages risks and uncertainties in such a way as to reduce the likelihood and/or possible effects of the impediments. In practice, intelligence informs and executes. Werner gave the definition of intelligence as follows: *"Intelligence is secret, state activity to understand or influence foreign entities."*[12] The shortcoming of the latter formulation is that it only applies to foreign entities, and leaves the purpose of this activity in the dark.

According to Jennifer Sims, the function of intelligence is to be better than the enemy and ensure victory.[13] Jensen and his co-authors think similarly, according to whom the purpose of an intelligence product is to provide an advantage to the decision-maker by providing knowledge about our world. Alfred Rolington defines it as an action that involves gathering and evaluating knowledge, which also aims to provide an advantage.[14] The common point of these definitions is to ensure an advantage. There is no doubt that individual societies are in competition with each other, but these definitions are also indebted to answering for what reason and what advantage each country needs, and what distinguishes them from other state functions, which may also have the function of providing an advantage.

According to Peter Gill's definition, this activity is "*mainly secret activities — targeting, collection, analysis, dissemination and action—intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities*."[15] He sees the ultimate goal of the activity in terms of security and relative power over competitors.

---

11 KAHN, David: A Historical Theory of Intelligence. *Intelligence and National Security*, 2001/3, pp.

12 WARNER, Michael: Wanted: A Definition of 'Intelligence.' *Studies in Intelligence*, 2002/3.

13 SIMS, Jennifer: Defending Adaptive Realism: Intelligence Theory Comes of Age. In: GILL, Peter – MARRIN, Stephen – PHYTHIAN, Mark (eds.): *Intelligence Theory*. Routledge, 2008.

14 ROLINGTON, Alfred: *Strategic Intelligence for the 21st Century: The Mosaic Method*. Oxford University Press, Oxford, 2013.

15 GILL 2008, p. 214.

It is clear that a significant part of the authors apostrophizes the social function as a means of maintaining security, gaining an advantage, or even as a means of asserting power, perhaps they see them as some kind of optimizing, efficiency-improving function. The maintenance of security in itself is narrow thinking, because intelligence organizations operate in many situations that are not linked to any specific threat, just think of the gathering of intelligence information prior to economic decisions. We believe that all of these aspects may be true, and that there may be additional aspects in addition to these. Thus, we are looking for a definition that does not contradict the above, but rather includes and integrates them, and also allows the integration of additional aspects. The other aspect is that most authors consider the decision-maker and the decision to be the user of the intelligence work, although the information can also be used during the implementation of decisions, and it may even happen that the intelligence services themselves will be the executors of a decision. Overall, we see that the above definitions contain some elements of true social function, but do not fully explain it by themselves.

A new approach - the interest

Based on the above, we believe that research into the social function of secret state organizations is by no means complete. Since it seems to us that the research so far has moved around in a relatively narrow circle, we are now trying to outline the foundations of a new system of thought that is outside the above circle, but in such a way that it does not reject, but rather explains and incorporates the previous thoughts. As we mentioned above, since sociology is the basic science of the functioning of human societies, our system must be based on elements that can be interpreted within a sociological framework.

If we want to examine the social purpose of intelligence, then it seems obvious to examine the legal regulations. On the one hand, the legal regulations are the frameworks created outside the organizational system of the secret service, and on the other hand, these rules regulate the connection of the services to social systems. When we reviewed the regulatory environment of different countries, we looked for elements that are common and can be grasped from a sociological point of view. At the beginning of the research, we assumed that since the social organization is also significantly different, there may be differences in the social function between democratic and non-democratic systems, so in the first round we only reviewed the legal rules related to the former one.

In the framework of this work, we examined the legislative environment for secret services and secret information in a total of 30 democratic countries.[16]

[16] Author's remark: 27 member states of the European Union and the United States, United Kingdom, Norway.

One of the important common points of the legislation was the use of the expression "interest" – in 29 out of 30 related legislations we found the reference to interests in some form. The term is used in the indicative structure, for example: security interest, national security interest, public interest, important interest, political interest, economic interest, but it also appears in the form of activity that violates interest, the protection and enforcement of interests, and related activities. The challenge is that most of the time, legislation does not contain a definition of interest or the concepts created from it, or if they do, they typically use a list of examples or try to explain the interest by itself: e.g. national security interest = detection of activities that harm the important interests of the country.[17]

Based on the above, we thought that by properly adapting and applying interest as a sociological concept, we can get closer to creating a general explanation. Interest is a relatively little-researched phenomenon in sociology and other social sciences, especially if we take into account how often it appears in everyday language and security studies.

According to Zoltán Farkas, *"interest is the network of action opportunities created by institutions, which are the means or positive conditions for the satisfaction of needs for a given individual (or group); which can create social goods for the direct satisfaction of needs, and whose expected return is positive."*[18]

The definition is important and well-applicable to us from two points of view. On the one hand, it perceives interests as possibilities for action (possible action), which is essential, because ultimately the functioning of society and the state within it is realized through human actions. According to this, interests thus become objective entities independent of the individual, that is they can be counted and evaluated.

On the other hand, one of the important tasks of society and its institutions is to support the satisfaction of individual or group needs, primarily in areas where individuals cannot create the conditions and means for themselves. This activity primarily means the production of public goods. According to Farkas, *"social public goods are goods that are undivided for a given circle of individuals and that are accessible and usable for all individuals and form the social prerequisites for the satisfaction of needs"*.[19]

Most often, as an actor "created" for this purpose, the implementation of this task falls on the state. For members of a society, such public goods can be military security (national defence), public safety, administration of justice, macroeconomic stability, energy independence, economic growth, healing, education, etc.

---

17 Law No. 125 of 1995 on the national intelligence and security services of Hungary. https://net.jogtar.hu/jogszabaly?docid=99500125.tv (Download time: 10/5/2024.)

18 FARKAS, Zoltán: *Társadalomelmélet -- Az Intézményes Szociológia Elmélete*, *Harmadik Kötet*. [Social Theory -- The Theory of Institutional Sociology, Third Volume.] Bíbor Kiadó, Miskolc, 2011. p. 44.

19 FARKAS, Zoltán: A közjavak, a társadalmi egyesülés és az együttes cselekvés. [Public goods, social integration and collective action.] *Kultúra És Közösség,* 2022/1, p. 6.

It is clear that these are all goods (quasi state services) that contribute to the satisfaction of individual needs. Of course, the range of public goods is much wider than the above list. In our opinion, it is worth considering only those public goods that affect the entire circle of society, excluding the public goods of specific groups (for example, a local community). Public goods taken into account can be called general social public goods.

At the same time, it is reasonable to see that the social and state action aimed at creating public goods is not unlimited, but an important limitation is, for example, the available resources, the political power situation, the willingness of other societies and actors to cooperate, and possibly resistance. That is why, in this set of conditions, the number of implemented actions will always be significantly less than the number of possible actions. Those authorized to act must decide which of the available actions they will attempt to implement.

In the case of rational actors, the possible action can be realized if:

- The possible action is known;
- The action is worth implementing based on benefit and expenditure. This cost-benefit ratio can be direct, that is, it can be interpreted in terms of costs and benefits that can be expressed in money or other resources, or it can be indirect, that is, it can be interpreted, forgone benefit or that cannot be measured in money, for example, trust capital, in the creation of other possible actions.

The conclusion is that the implemented actions will be more valuable for society, the better the cost-benefit ratio. Thus, the state actually has four tasks:

1. To determine (recognize) the possible actions, possibly to create the possibility of action;
2. To analyse in detail the cost-benefit aspect of the action (ranking);
3. To select the best action alternatives;
4. Effectively and efficiently carry out the above, which can be called enforcement of interests.

Based on the above, counter-interest means that the possible actions of a given actor can reduce the number of possible actions of another actor, increase its costs, and reduce its benefit. The identity of interests means that the possible actions of the given actor do not reduce the number of possible actions of the other actor, or have a positive effect in terms of expenditure and benefits.

Interests and covert action

The purpose of the secret organizations is to support the above system of tasks through covert activity in cases where this support can only be carried out through this covertly performed activity. The latter can occur in the following cases:

- One needs data that cannot be obtained through open activity, but only through covert activity;
- Possible action exists only in the form of covert action;

- One can rightfully assume similar covert action by the opposing parties, which can only be detected and prevented by covert action.

Covert activity can be aimed at obtaining data, analysing it, and taking covert action. The latter can be aimed at supporting the identification of interests, but in some cases, it can also be the action itself. This explains how secret services can be organizations that collect, analyse and act on information at the same time, that is organizations involved in the production of the public good itself. These conditions also determine which public goods require secret information collection. In order to produce a significant range of public goods, there is no need for secret information gathering, secret action (in fact, open action may be more beneficial), and no secret action of an opposing party can be assumed.

The theory fits into the system of international relations in such a way that the creation of certain public goods is related to the situation and behaviour of foreign actors. In addition, societies generally have a more precise knowledge of and greater influence on themselves than on other societies. As a result, he has to resort to covert action much less often with regard to his own society, but we cannot completely rule out the possibility of this. Last but not least, societies are in a competitive situation for resources and power, so this competitive situation can lead them to take counter-interested actions.

The advantage of the above definition is that it can be clearly justified why something falls under the purview of secret organizations. On the other hand, it is also possible to clearly define what goal the secret activity should be aimed at achieving. Thirdly, the role of secret services can be clearly distinguished in the case of democratic and non-democratic political systems. In the latter case, the task system of the services is expanded with items that cannot be included in the above framework, because they are not public goods or society, but only aimed at achieving the production of public goods but they are aimed at achieving “social” good that are useful to a narrow circle (e.g. the power elite) only.

The application of the concept of the overall social public good expresses the importance of the fact that secret actions are necessary because they represent something important from the point of view of society, that is they satisfy the important needs of large masses. On the other hand, they also express that societies can express their choice of values by making choices about public goods (ranking them according to importance). In addition, it is important to clarify the legal framework of the secret activity so that it can only be used in connection with its above purpose.

The social sub-functions of the activities of secret services

Based on the above, the secret service activity fulfils the following roles in social functioning:

1. The intelligence (gathering) function: In this function, the secret services are necessary to make certain data available in the given society. This mainly means the data that some people (outside the given society) want to hide, for their own interests. Without this secret intelligence gathering organizations, obtaining this data would not be possible. With the data, the scope and ranking of possible actions can be determined, and these actions can be carried out effectively and efficiently.
2. The analytical function: In this function, the services look for logical connections between open and secret information known to them. Recognizing these relationships is first and foremost linked to the recognition and prioritization of interests, that is action alternatives (evaluation of costs and benefits). It can be implemented at the operational level, that is in connection with the interests of the services, and at the strategic level, that is in connection with the social interests themselves. The social importance of this function lies in the fact that others cannot access the secret information, so the process described above can only be carried out by the services. It is no coincidence that with the increase in the amount and variety of data, organizations specialized only in analysis (without intelligence capabilities) were created (fusion centres, strategic coordination organizations), and analysis activities were increasingly emphasized within the organizations as well.
3. Interest enforcement function: In this function, the services take concrete steps to enforce the strategic interests of the country, that is they contribute to the implementation of action options. Among the developed and available social action alternatives, the decision-makers will determine which ones will be implemented. A good example of this is the range of active measures that directly contribute to the conduct of elections free from foreign manipulation, thereby promoting the "production" of sovereignty and democracy as public goods.
4. Predictive function: In this function, the services try to use secret information to predict the possible or planned actions of their own or other relevant actors before they occur, as well as their consequences. The predictive function enables the identification of future factors affecting the range of interests, which expand or narrow the range of action alternatives, and influence their benefits and costs. In addition, within the framework of this function, the services predict the expected occurrence of rival advocacy activities. The importance of this function is given by the fact that, in the case of events involving potential harm to interests, prior knowledge can make it possible to avoid harm to interests or to reduce the degree of harm. A good example of the range of problems related to prediction is the question of the Russian attack in 2022.

The predictability of the Russian attack was a fundamental element of the Ukrainian society's need for security. Satisfying this need lay in preparing for different contingencies. However, for this, it was necessary to know what steps the Russians would take, and it was necessary to take preparatory steps. For this, the Ukrainian leadership faced countless alternatives of action, the choice largely depended on what the secret services had predicted regarding the place, time, and means of the Russian attack, as well as the expected reaction of the Ukrainian society and military. Several state institutions could make such predictions, but among them that of the secret services differed in that it could also contain data related to planned but secret Russian actions.

5. Preventive function: The preventive function is closely related to the predictive function, because activities that could be predicted to some extent can be prevented. Within the framework of this function, the services prevent the activities of rival parties related to the recognition and enforcement of their interests. A good example of this is counter-espionage activity.
6. Advisory function: In this function, the services can outline strategic action alternatives supported by secret data for decision-makers, and present the possible actions of rivals. In fact, this type of activity means articulating the country's interests and proposing which possible actions should be implemented and why.
7. Preparatory function: In this function, the services prepare the persons dealing with the enforcement of relevant interests, as well as the relevant members of society (sometimes all members). This preparation applies to those situations in which secret actions can result in advantageous situations for the prepared person and to those in which the secret actions of the opposing parties may cause them harm. First, a good example is the preparation for a negotiation with an adverse party related to the operation of the secret information collection system. A good example of the latter is either individualized or society-wide awareness activities.
8. Innovation function: This function results from the secret nature of the activity. Organizations are in a constant competition of creativity in order to maintain secrecy and reduce the secrecy of other actors. This competition for creativity forces the services to continuously innovate, which can then gradually seep into other areas of society as well. As an example, let's think about how employees who leave organizations take their knowledge with them and how they put it to the service of social actors.

Conclusion

From the above thought process, there are some conclusions that are worth recording:

1. Based on the above thought process, it is clear that the social purpose of the activity in question is positive, because it indirectly contributes to the satisfaction of social needs. It also follows from this that it is possible to argue in favour of its social usefulness.
2. It can also be stated that secret service activity is a consequence of the natural competitive situation between human societies, rather than its cause.
3. Through the above definition, the functions and the tools can be separated; thus, the purposes of law enforcement – as opposed to secret service covert activities – can be separated from each other.
4. Parties with the same interests and opposing interests can be identified and coincident interests can also be recognized. This can explain, for example, cases of espionage between allied countries.
5. The operation of the intelligence services of democratic and non-democratic countries becomes clearly distinguishable. In the case of the latter countries, it is usually possible to identify activities and organizational elements that are not necessary for the production of public goods for society as a whole.
6. Understanding and adequately introducing the concept of interest into the discourse, related to intelligence services, is important because it explains a special feature of secret services: these organizations can deal with many areas of social functioning, be it security, economy, science or health. The task of the state is to assert the interests of the given society in these areas, ensuring the highest and most efficient satisfaction of the needs.
7. It seems that an individual need, the lower it is in Maslow's pyramid, the greater the chance that the interests related to it are enforced with the help of secret activity. Issues related to personal security (see e.g. terrorist acts) are at the forefront of intelligence service activities and even international intelligence cooperation.

Summary

The purpose of our paper was to present a new approach regarding the social purpose and sub-functions of the activities of intelligence organizations. In our view, the literature definitions used so far focused primarily on sub-functions, possibly intelligence methods, and were less able to grasp their general function. In almost every country in the world, the interest as a term is part of the legislation, defining the tasks of secret services and at the same time of the public discourse about the operation of secret services. Despite this, interests did not appear in any definitional endeavours, which is presumably due to the fact that the scientific formulation of the concept of interest is not easy either.

Based on the line of thought outlined above, we see that the purpose of secret service action is to support the process of producing public goods for society as a whole, through secret action. Supporting this process means defining possible actions (within and outside society), prioritizing them and, in cases requiring covert action, their implementation.

By applying this system of thought, we get solid points of reference, through which we can give easier and, we believe, better quality answers to questions affecting the society. We can contribute to the members of society's better understanding, why these organizations are needed and what kind of needs they can satisfy. Many people think that the ultimate consumers of the "products of secret service" are government decision makers. We ourselves believe that on the one hand, not only government decision-makers, but also other actors are consumers of this service, and on the other hand, that the ultimate beneficiaries are citizens, we just need to find the mechanism that can describe that relationship. The results of such research can be well utilized in the preparation of political actors and in the training of employees of intelligence organizations, both separately and in connection with each other.

We do not consider this to be the end of our research. Many questions need to be examined more thoroughly, many elements of the theory need to be defined more precisely, and many connections need to be explained in more detail. At the same time, we think it is a theoretical framework, the publication of which is suitable for revitalizing the thinking about the social role of the secret services.

Bibliography:

BERKOWITZ, Bruce: The Big Difference Between Intelligence and Evidence. 2 February 2003, Online: https://www.rand.org/pubs/commentary/2003/02/the-big-difference-between-intelligence-and-evidence.html. (Download time: 28/04/2024)

DOKMAN, Tomislav: Defining the Term "intelligence" - Insight into Existing Intelligence Knowledge. *Informatologia,* 2019/3-4. pp. 194–205. https://doi.org/10.32914/i.52.3-4.7.

FARKAS, Zoltán: A közjavak, a társadalmi egyesülés és az együttes cselekvés. [Public goods, social integration and collective action.] *Kultúra És Közösség,* 2022/1, pp. 5-21. https://doi.org/10.35402/kek.2022.1.1.

FARKAS, Zoltán: *Társadalomelmélet – Az Intézményes Szociológia Elmélete*, *Harmadik Kötet*. [Social Theory – The Theory of Institutional Sociology, Third Volume.] Bíbor Kiadó, Miskolc, 2011.

FERRIS, John: Diplomacy and diplomatists. In: BOYCE, Robert – MAIOLO, Joseph A. (eds.): *The Origins of World War Two: The debate continues.* Palgrave Macmillan, New York, 2003.

GILL, Peter: Theories of Intelligence. In: JOHNSON, Loch K. (ed.): *The Oxford Handbook of National Security Intelligence.* 1st ed., Oxford University Press, 2010, pp. 43-58. https://doi.org/10.1093/oxfordhb/9780195375886.003.0003.

GILL, Peter: Theories of Intelligence: Where Are We, Where Should We Go and How Might We Proceed? In: GILL, Peter – MARRIN, Stephen – PHYTHIAN, Mark (eds.): *Intelligence Theory*. Routledge, 2008.

HERMAN, Michael: *Intelligence Power in Peace and War.* 1st ed. Cambridge University Press, 1996. https://doi.org/10.1017/CBO9780511521737.

HOWARD, Michael: *The Invention of Peace: Reflections on War and International Order.* Yale University Press, New Haven, 2000. Online: https://www.jstor.org/stable/4547227 (Download time: 13/04/2024)

KAHN, David: A Historical Theory of Intelligence. *Intelligence and National Security*, 2001/3, pp. 79-92. https://doi.org/10.1080/02684520412331306220.

LOWENTHAL, Mark M.: *Intelligence: From Secrets to Policy.* 2nd ed. CQ Press, Washington, D.C, 2003.

ROLINGTON, Alfred: *Strategic Intelligence for the 21st Century: The Mosaic Method*. Oxford University Press, Oxford, 2013.

SCHEFFLER, Alessandro – DIETRICH, Jan-Hendrik: Military Intelligence: Ill-Defined and Understudied. *International Journal of Intelligence and CounterIntelligence*, 24 May 2023, pp. 1-20. https://doi.org/10.1080/08850607.2023.2187190.

SIMS, Jennifer: Defending Adaptive Realism: Intelligence Theory Comes of Age. In: GILL, Peter – MARRIN, Stephen – PHYTHIAN, Mark (eds.): *Intelligence Theory*. Routledge, 2008. Online: https://www.taylorfrancis.com/chapters/edit/10.4324/9780203892992-15/defending-adaptive-realism-intelligence-theory-comes-age-jennifer-sims (Download date: 03/05/2024)

N.a.: Chapter 13: The Use of Spies. Sun Tzu's Art of War, n.d. Online: https://suntzusaid.com/book/13. (Download time: 01/06/2024)

WARNER, Michael: Wanted: A Definition of 'Intelligence.' *Studies in Intelligence*, 2002/3. Online: https://www.cia.gov/resources/csi/static/Wanted-Definition-of-Intel.pdf (Download time: 01/06/2024)

DORKA HORVÁTH

THE BACKGROUND OF THE RUSSIAN–UKRAINIAN WAR IN TERMS OF NEW TOOLS AND METHODS OF WARFARE

Abstract

The twenty-first century has seen a huge evolution in warfare, with military operations improving. The Russian-Ukrainian armed conflict is a clear illustration of the impact of new technologies on traditional warfare, and the war is therefore being referred to by many as the first cyber world war of the 21st century. The war of revolutionary technologies covers a range of areas from cyber-attacks and disinformation to the economic impact on the global IT landscape, despite the fact that much of the conflict is taking place on the actual battlefield. In the following, it will be discussed in more details how old (traditional) and new forms of warfare co-exist in the Russian-Ukrainian war. Classical, traditional warfare has appeared in urban and information warfare. In the field of modern warfare, hybrid and asymmetric warfare in terms of the combination of non-traditional means of warfare, as well as closely intertwined cyber warfare, which usually targets critical infrastructures, government systems and communication networks, should be highlighted. In the context of modern warfare, the article discusses the impact of unmanned systems, electronic warfare and social media, which, in addition to the conduct of psychological operations, also increases the impact on the international community. Artificial intelligence plays a major role in conflict; the winning side in the technology race will have the greatest influence on the outcome of the war. The background to this competition is explored in this article, briefly touching on the influencing power of several international actors (Microsoft, Elon Musk, European Union, etc.).

Keywords: Russian-Ukrainian war, armed conflict, cyber warfare, hybrid warfare, asymmetric warfare, modern warfare, artificial intelligence

Introduction

For those who have never witnessed (not even the Cold) war, it would have been unimaginable to think of a reality of a new one coming, so soon and so close to the European Union's (EU) border. But as Carl von Clausewitz, military historian and theorist stated, "*War is […] an act of force to compel our enemy to do our will*",[1] which is just the case of the centre of this current paper, the Russian-Ukrainian war.

[1] VON CLAUSEWITZ, C.: *On War.* (J. J. Graham, Trans.) Wordsworth Editions, 1997, p. 75.

Warfare has seen important new advancements in the twenty-first century. Military operations and tactics have improved as a result of technological advancement, both accidentally and on purpose. A clear illustration of how new technology have changed traditional warfare is the Russian invasion of Ukraine.

According to several scientists, the war began in 2014 with the annexation of Crimea and the Donbass War,[2] and has escalated ever since as an ongoing international conflict between the two parties. By the time, the world has witnessed the utilization of various new tools and methods of warfare within its scope. These developments have significantly influenced the nature and dynamics of the conflict.

Key aspects

A few revolutionary weapons and technologies have been put to the test in the conflict between Russia and Ukraine. With Western assistance, Ukrainian forces have been able to acquire the most advanced defensive weapons gradually.[3] There has been a war of technologies, from cyberattacks and disinformation to the economic effects on the global IT scene, notwithstanding the fact that much of the conflict has taken place on the actual battlefield.[4] As will be examined in the followings, the old (traditional) and new forms of warfare is present together in the war of question and it is likely that asymmetric and hybrid forms of operations will be more and more often.[5]

Classical Warfare

Classical warfare generally refers to earlier periods in history, particularly the 19th and early 20th centuries. This period is about traditional warfare between great states, in which forceful and violent armies fight mainly in land battles with artillery support and firearms.[6]

The conflict has witnessed the use of long-range precision strikes for example, primarily by Russia. Cruise missiles, ballistic missiles, and artillery systems have been employed to target key military infrastructure and strategic locations.

---

2 FILIU, Jean-Pierre: For Ukraine, the war started in 2014, not in 2022. LeMonde, 20 February 2023.

3 TSERETELI, Aleksandre: War in Europe: Use of Technologies in the Russia-Ukraine War. Friedrich Naumann Foundation, 13 January 2023.

4 MCGEE-ABE, Jason: One year on: 10 technologies used in the war in Ukraine. TechInformed, 24 February 2023.

5 SZTERNÁK, György: A fegyveres küzdelem megvívása (Az új módszerek, formák háttere; a jellemzők vizsgálata). [Fighting the armed struggle (Background of the new methods and forms; examination of the characteristics)]. *Hadtudományi Szemle*, 2017/1, pp. 113-125.

6 GUTIÉRREZ, Fernando Casado – LÓPEZ, Fernando Oliván – GONZÁLEZ, Arturo Luque: Lawfare or the War Behind the Curtains: An Analysis of the Russian-Ukrainian Conflict. In: ÖZSUNGUR, Fahri (ed.): *Handbook of Research on War Policies, Strategies, and Cyber Wars.* IGI Global, 2023, pp. 239-255.

These strikes have allowed for significant destruction and disruption with minimal risk to Russian forces.[7]

The classical warfare has been present regarding the Russo-Ukrainian war in the following, main matters:

Urban Warfare

The classical face-to-face fighting in Ukraine has involved urban warfare scenarios, particularly in cities like Donetsk and Luhansk. Both sides have adapted their tactics to operate in built-up areas, utilizing tactics such as sniper fire, booby traps, and tunnel systems. Urban warfare poses unique challenges due to the dense civilian population and complex urban environments.

All levels of modern warfare—tactical, strategic, operational —come together in the urban environment, where crucial military, political and economic infrastructure is present. The political and military leaders of both Russia and Ukraine have recognized it, and as a result, the primary goals of both sides have been to control the urban centers of Ukraine. It is also undeniable that urban combat has been the key to military and political tactical, operational, and strategic planning and decision-making since the beginning of the war. The conflict between Russia and Ukraine has demonstrated that urban warfare is central to modern warfare and will probebly remain so.

Information Warfare

The war has been marked by intense information warfare, involving the dissemination of propaganda, manipulation of narratives, and the spread of disinformation through social media platforms. Both sides have used these tactics to shape public opinion, control the narrative, and delegitimize their adversaries.[8] In the followings, the paper will highlight how traditional information warfare has been evolved in today's Russo-Ukrainian war.

Modern warfare

In the two previous decades, there has been a changed form, nature, and "mixing" of "new" wars and military conflicts. New security risks and threats surfaced in the new millennium, and has partially led to the crisis in Ukraine in 2014, and the literature clearly labeled Russian intervention as a hybrid war.[9]

---

7 DICKINSON, Peter: Britain becomes first country to supply Ukraine with long-range missiles. Alantic Council, 11. 05. 2023.

8 N.a.: Ukraine: A year of information warfare in numbers [EN/RU/UK]. Reporters sans Frontieres, 21. 02. 2023.

9 BODA, József – BOLDIZSÁR, Gábor – KOVÁCS, László – OROSZ, Zoltán – PADÁNYI, József – RESPERGER, István – SZENES, Zoltán: *A hadtudományi kutatási irányok, prioritások és*

Tech plays had an essential role in supporting Ukrainians hoping to communicate with the rest of the world or to regain areas. Many have dubbed the conflict the "first cyber world war" of the 21st century due to the unprecedented speed and scope of the Internet and cyberattacks. The followings are key technologies that were utilized in the most technologically advanced war that humanity has ever witnessed.[10]

Hybrid Warfare

The conflict in Ukraine has been characterized by the use of hybrid warfare tactics, which involve a combination of conventional military operations, irregular warfare, cyber-attacks, disinformation campaigns, and economic pressure, that is, non-traditional means. Russia has employed these tactics to destabilize Ukraine and exert control over certain regions.

Another front of hybrid warfare is information war, as alluded before. As for an example of Ukrainian operations in that regard, during the Surkov Leaks, released in October 2016 and containing more than two thousand emails about Russian plans to seize Crimea from Ukraine and foment separatist unrest in Donbas.[11]

Cyber Attacks

Hybrid warfare and cyber warfare are interconnected concepts that intertwined in modern conflicts. While they are distinct in their nature, they frequently overlap and complement each other in the context of hybrid warfare strategies. As for cyber warfare, it involves the use of digital technology and computer networks to disrupt, sabotage, or gain unauthorized access to an opponent's information systems, infrastructure, or communications networks. It encompasses various activities such as hacking, denial of service attacks, data theft, and spreading misinformation or propaganda.[12]

The internet and the devices working in connection with it assume a critical part in military leadership, in the form of different military function and activities (operations support, control, leadership, strategies, planning, and so on.). These processes and functions can be severely impacted by cyberspace malfunctions which then can affect the nation's security, including critical infrastructure for instance, but in fact, all components of the nation's security.[13]

---

témakörök. [Research directions in military science, priorities and topics.] Államtudományi Műhelytanulmányok, Nemzeti Közszolgálati Egyetem, 2016/16, p. 7.

10 McGee-Abe 2023

11 Shandra, Alya – Seely, Robert: The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine. Royal United Services Institute, 16 June 2019.

12 Djenna, Amir –Harous, Saad – Saidouni, Djamel Eddina: Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. MDPI, 2021/10.

13 Boda et. al. 2016.

Thus it is enough to disable or limit the operation of a selected infrastructure that is important from the point of view of society's economic life or transportation through an information attack. As a result, an information attack on any central element of the system has an indirect or direct impact on the success of the armed struggle.
The essence is the full expansion of information processing, the access of military forces to information, and full political control over the execution of the military task.[14]

In the case of the present conflict, both sides have engaged in cyber warfare, targeting critical infrastructure, governmental systems, and communication networks. Cyber-attacks have been used for intelligence gathering, disruption of operations, and propaganda purposes. These attacks have demonstrated the vulnerability of modern societies to cyber threats and have become an integral part of the conflict. As for examples, with repeated distributed denial of service (DDoS) attacks and a cyberweapon made up of a trojan horse wiper malware that Microsoft identified as “FoxBlade”, Russia attempted to disrupt internet connectivity and paralyze Ukraine's command and control centres hours before the physical invasion began. On the other hand, in an effort to improve the resilience of its encryptions and systems, Ukraine has formed partnerships with numerous international technology firms, including Microsoft and Cloudflare.[15] All in all, according to Yuriy Schygol (Head of the State Service for Special Communications) in 2022, there were 2,194 cyberattacks and seven new kinds of viruses identified.[16]

Unmanned Systems

Within the scope of the modern warfare, both Russia and Ukraine have made use of unmanned systems, including drones, for reconnaissance, surveillance, and targeting purposes. Drones have provided valuable real-time intelligence, facilitated precision strikes, and enabled both sides to monitor and disrupt enemy activities.[17]

Elon Musk for instance promised to provide assistance to Starlink Internet in Ukraine. Musk maintained his word and Starlink is currently being utilized by Ukrainian drones to target forward Russian positions.[18]

Electronic Warfare

The conflict has seen an increased emphasis on electronic warfare capabilities, again in connection with the subsections mentioned before.

---

14 Szternák 2017.

15 McGee-Abe 2023

16 N.a.: Ukraine blames Russia for most of over 2,000 cyberattacks in 2022. Euronews, 17 January 2023.

17 Ciolponea, Constantin-Adrian: The Integration of Unmanned Aircraft System (USA) in Current Combat Operations. *Land Forces Academy Review*, 2022/4.

18 Tsereteli 2022.

Russia has deployed sophisticated electronic warfare systems to disrupt Ukrainian communications, radar systems, and command-and-control networks. These capabilities have significantly affected Ukraine's military operations and highlighted the importance of countering electronic warfare threats.

Electronic warfare (EW) systems have been utilized extensively throughout the conflict. In late February, not long before Russia attacked, Hawkeye 360 experts recognized GPS interference signals close to the Ukrainian-Belarus border, north of Chernobyl, after already getting signs across Eastern Europe with commercial satellites that were disturbing unmanned aerial vehicles working in the Luhansk and Donetsk districts.[19] As for the other party, the Ukrainian military, has used EW systems to jam GPS and communications signals from Russia, ensuring that the communications infrastructure is still protected.[20]

The Ukrainian military also has utilized virtual reality (VR) preparing frameworks to reproduce battle situations and train troopers in strategies and techniques. Before going to the front lines, soldiers can practice in a controlled and safe environment with this kind of training. In June 2022, Ukraine's Head of the state Volodymyr Zelensky made a 3D holographic transmission appearance, by holographic technology, to 200,000 top tech business people, investors and corporate pioneers at seven significant European tech occasions to raise awareness to offer financial and technological resources to start rebuilding Ukraine.[21]

Social Media

The Russian–Ukrainian war has witnessed significant advancements in the use of social media as a tool for warfare. It has turned into the most internet-accessible conflict in history with live updates and recordings distributed through different online entertainment media. Both sides have leveraged social media platforms to disseminate propaganda, shape narratives, and influence public opinion.

Social media has become a vital tool for conducting psychological operations (PSYOPS) in the Russian-Ukrainian war. These operations aim to influence the emotions, beliefs, and behaviours of target audiences. By targeting specific demographics, exploiting psychological vulnerabilities, and leveraging personalized content, both sides seek to shape public opinion and gain support for their respective causes.

---

19 N.a.: HawkEye 360 Signal Detection Reveals GPS Interference in Ukraine. HawkEye 360, 04 March 2022.

20 N.a.: Analysing the limitations of Russian EW capabilities in Ukraine. Army Technology, 10 May 2022.

21 MUSTOE, Howard: Video games and virtual reality prepare soldiers for a new type of warfare The Telegraph, 10 April 2022.

For instance, Putin's systems incorporate painting Ukraine and Western countries as immoral and evil and outlining messages with regards to power elements. Russia has grounds for retaliation since it is merely a victim that other world powers are exploiting.[22]

Other than that, utilizing location-based social media platforms, Ukraine has been able to target specific groups of Russian soldiers but vice versa, users' data might be observed by the Russian government surveillance system (SORM), while their capacity to uninhibitedly peruse the web may likewise be confined, making Russian publicity accessible.[23] For that matter, Ukrainian software that utilizes facial recognition to find the social media profiles of perished fighters, which specialists then use to advise family members and move bodies to the families. Exact strikes, successful observation and surveillance can to some degree to a limited extent be credited to the information which Ukraine is getting from the western partners.[24] Due to the absence of AI technologies, Russian forces have been at a "massive disadvantage." Experts in the military think that AI could be a big part of future conflicts because it can predict enemy movements and analyze a lot of data to find potential threats.

Apart from the parties of the war, friends and family members post updates and communicate with loved ones to inform them of their safety and whereabouts, which has also contributed to a significant increase in social media activity. (I would actually highlight a personal experience as an example; I started following *https://www.instagram.com/rick_the_hedgehog/* 3 years ago. Back at the time, it was a page about the pictures of adventures of a pet hedgehog. Since the war begin, the page has turned into a hedgehog-style first-hand information supplier as the users are living in Lviv. Their posts and stories contain pure data and footages of the current situation).

It is important to note that these new tools and methods of warfare regarding social media are not unique to the Russian-Ukrainian conflict. They have also been observed in other geopolitical conflicts and have raised concerns about the manipulation of information, erosion of trust, and the potential for escalating tensions in the digital domain.

Closure

It is undeniable that the conflict between Russia and Ukraine is the most technologically advanced conflict humanity has ever seen. Over the course of the past few centuries, it is evident that war and everything intertwined in it has changed and developed.

---

22 ABRAMS, Zara: The role of psychological warfare in the battle for Ukraine. American Psychological Association, 01 June 2022.

23 MCGEE-ABE 2023.

24 DANGWAL, Ashish: Ukraine Uses 'Controversial' Artificial Intelligence Tech In Its War Against Russia As Kiev Looks To Win The 'Digital War'. The EurAsian Times, 07 April 2022.

The ultimate objective remains the same despite the development of new warfare techniques and technologies, which is to be superior to others and safeguard sovereignty.

The military is expected to undergo significant reforms worldwide after the war is over. Each country put resources into its national security, and gathers information utilizing different methods including computer based intelligence/Artificial Intelligence. The state of warfare has shifted to one that is more technologically advanced, with the creation of new interdependencies that extend beyond just weapons systems. With the right tools and creative strategies, it will be necessary to adjust to this shift.[25]

It's important to note that the developments are not exclusive, but have been quite characteristic to the Russian-Ukrainian conflict and have wider implications for modern warfare, as they reflect evolving trends in the nature of armed conflicts around the world.

Bibliography:

ABRAMS, Zara: The role of psychological warfare in the battle for Ukraine. American Psychological Association, 01 June 2022, Online: https://www.apa.org/monitor/2022/06/news-psychological-warfare (Download time: 19/05/2023)

BODA, József – BOLDIZSÁR, Gábor – KOVÁCS, László – OROSZ, Zoltán – PADÁNYI, József – RESPERGER, István – SZENES, Zoltán: *A hadtudományi kutatási irányok, prioritások és témakörök.* Államtudományi Műhelytanulmányok, Nemzeti Közszolgálati Egyetem, 2016/16, p. 7.

CIOLPONEA, Constantin-Adrian: The Integration of Unmanned Aircraft System (USA) in Current Combat Operations. *Land Forces Academy Review*, 2022/4. DOI: 10.2478/raft-2022-0042

DANGWAL, Ashish: Ukraine Uses 'Controversial' Artificial Intelligence Tech In Its War Against Russia As Kiev Looks To Win The 'Digital War'. The EurAsian Times, 07 April 2022, Online: https://www.eurasiantimes.com/ukraine-uses-artificial-intelligence-tech-in-its-war-against-russia/ (Download time: 22/05/2023)

DICKINSON, Peter: Britain becomes first country to supply Ukraine with long-range missiles. Alantic Council, 11 May 2023, Online: https://www.atlanticcouncil.org/blogs/ukrainealert/britain-becomes-first-country-to-supply-ukraine-with-long-range-missiles/ (Download time: 12/05/2023)

[25] MCGEE-ABE 2023.

DJENNA, Amir –HAROUS, Saad – SAIDOUNI, Djamel Eddina: Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. MDPI, 2021/10, Online: https://www.mdpi.com/2076-3417/11/10/4580 (Download time: 18/05/2023)

FILIU, Jean-Pierre: For Ukraine, the war started in 2014, not in 2022. LeMonde, 20 February 2023, Online: https://www.lemonde.fr/en/international/article/2023/02/19/for-ukraine-the-war-started-in-2014-not-in-2022_6016441_4.html# (Download time: 08/05/2023)

GUTIÉRREZ, Fernando Casado – LÓPEZ, Fernando Oliván – GONZÁLEZ, Arturo Luque: Lawfare or the War Behind the Curtains: An Analysis of the Russian-Ukrainian Conflict. In: ÖZSUNGUR, Fahri (ed.): *Handbook of Research on War Policies, Strategies, and Cyber Wars.* IGI Global, 2023, pp. 239-255. DOI: 10.4018/978-1-6684-6741-1

MCGEE-ABE, Jason: One year on: 10 technologies used in the war in Ukraine. TechInformed, 24 February 2023, Online: https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/ (Download time: 10/05/2023)

MUSTOE, Howard: Video games and virtual reality prepare soldiers for a new type of warfare The Telegraph, 10 April 2022, Online: https://www.telegraph.co.uk/business/2022/04/10/video-games-virtual-reality-prepare-soldiers-new-type-warfare/ (Download time: 18/05/2023)

N.a.: Analysing the limitations of Russian EW capabilities in Ukraine. Army Technology, 10 May 2022, Online: https://www.army-technology.com/analyst-comment/limitations-russian-ew-capabilities/ (Download time: 21/05/2023)

N.a.: HawkEye 360 Signal Detection Reveals GPS Interference in Ukraine. HawkEye 360, 4 March 2022, (Online: https://www.prnewswire.com/news-releases/hawkeye-360-signal-detection-reveals-gps-interference-in-ukraine-301495696.html (Dowload time: 20/05/2023)

N.a.: Ukraine blames Russia for most of over 2,000 cyberattacks in 2022. Euronews, 17 January 2023, Online: https://www.euronews.com/next/2023/01/17/ukraine-crisis-russia-cyber (Download time: 18/05/2023)

N.a.: Ukraine: A year of information warfare in numbers [EN/RU/UK]. Reporters sans Frontieres, 21 February 2023, Online: https://reliefweb.int/report/ukraine/ukraine-year-information-warfare-numbers-enruuk (Download time: 16/05/2023)

SHANDRA, Alya – SEELY, Robert: The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine. Royal United Services Institute, 16 June 2019, Online: https://rusi.org/explore-our-research/publications/occasional-papers/surkov-leaks-inner-workings-russias-hybrid-war-ukraine (Download time: 16/05/2023)

SZTERNÁK, György: A fegyveres küzdelem megvívása (Az új módszerek, formák háttere; a jellemzők vizsgálata). [Fighting the armed struggle (Background of the new methods and forms; examination of the characteristics).] *Hadtudományi Szemle*, 2017/1, pp. 113-125.

TSERETELI, Aleksandre: War in Europe: Use of Technologies in the Russia-Ukraine War. Friedrich Naumann Foundation, 13. 01. 2023, Online: https://www.freiheit.org/south-caucasus/use-technologies-russia-ukraine-war (Download time: 10/05/2023)

VON CLAUSEWITZ, C.: *On War.* (J. J. Graham, Trans.) Wordsworth Editions, 1997. p. 75.

PÉTER POMOGÁCS

SECURITY IMPLICATIONS OF CHINA'S NAVAL PRESENCE IN THE INDIAN OCEAN REGION

Abstract

The geopolitical significance of the Indian Ocean region lies in its role of connecting the Pacific and Atlantic oceans with a network of vital sea lanes and maritime choke points such as the Malacca Strait, the Bab-el-Mandeb and the Suez Canal. Beijing's motives for expanding its influence in the Indian Ocean stems from the perceived vulnerability of Chinese energy supply routes, embodied in the "Malacca Dilemma". In order to secure shipping lanes vital for its economy, China established its first overseas naval base in Djibouti. Beside its Indian Ocean naval base, China continues to strengthen its blue-water navy. The prospect of a Chinese Indian Ocean fleet aligns with Beijing's active defence strategy. However, challenges such as the lack of effective air support and the difficulty of deploying its aircraft carriers in the Indian Ocean raise questions about the operational capabilities of the Chinese navy. The complex relationship between the United States, China and India adds another layer of uncertainty to the security environment of the region.

Keywords: China, Indian Ocean, choke points, Malacca-dilemma, blue-water navy

Introduction

The great powers involved in the strategic competition of the 21st century place great emphasis on securing access to sea trade routes in the Indian Ocean. Beside the regional contenders aiming for dominance in this maritime theatre, the People's Republic of China (PRC) has emerged as a central player, actively and assertively working on expanding its naval presence across the ocean. The transformative nature of China's entry into the Indian Ocean is highlighted by the Chinese affiliation with a number of ports and even a Chinese naval base in the region – a strategic repositioning that marks a shift in its former maritime posture. The background behind the change lies in the PRC's remarkable economic growth and its increasing reliance on maritime trade. At the heart of this shift is the famous "Malacca Dilemma", a concept that sums up China's concerns about the vulnerability of its energy and trade routes coursing through the narrow Malacca Strait. This has led the PRC to develop a more ambitious naval presence in the Indian Ocean, reflecting its commitment to securing vital shipping lanes.

As China assumes a more prominent role in the maritime security framework of the Indian Ocean, the region is witnessing a convergence of factors that are contributing to a complex security environment.

Abundant natural resources, confrontation of regional powers, non-conventional threats such as piracy, and strategically significant geographic choke points along global trade routes collectively create a series of challenges and opportunities that require new approaches from the interacting powers that are active in the region. In response to its internal and regional challenges, China took a historic step in 2017 by establishing its first overseas People's Liberation Army Navy (PLAN) base in Djibouti, East Africa.[1] This move, a symbol of China's rising economic and military prowess, underlines its commitment to securing maritime interests far beyond its immediate shores. Djibouti, strategically positioned at the high-traffic Bab-el-Mandeb Strait, the crossroads of Africa and the Middle East, provides China with a vantage point to monitor and safeguard critical sea lanes in the region. The base represents not only a physical extension of China's naval capabilities, but also a symbolic assertion of its global maritime influence. The central question of the future is not whether China will further expand its military presence in the Indian Ocean, but rather where and how this formidable power, now a major rival of the United States in the Indo-Pacific, will assert its influence.

China's financial entanglements in Pakistan, Sri Lanka, Myanmar, Tanzania, Mozambique, and other countries outside the Indian Ocean region, established through the construction and maintenance of maritime facilities, are viewed as long-term investments for Beijing. The scale of these investments could serve as a powerful diplomatic tool to increase Beijing's leverage in negotiations on future concessions, economic or even political favours. By embedding itself in the construction and operation of ports, China creates lasting ties that might influence the geopolitical landscape through economic means.

The PRC's maritime expansion in the Indian Ocean could also have serious implications for the balance of power between China and India. As the two countries compete for regional hegemonic influence, their diverging national interests in the Indian Ocean cause serious tension, and the possible future confrontation between them presents new security challenges. The regional presence of the United States, which owns the most capable navy in the world, further complicates the aspirations of the PRC. The United States is an active player in the Indian Ocean and has an intent to protect its own and its allies' economic and security interests in the region. The triangular dynamics between China, India, and the United States greatly influences the evolving security environment of the Indian Ocean, raising questions about cooperation, competition, and potential conflict.

The geopolitical significance of the Indian Ocean region

The vast maritime theatre of the Indian Ocean stretches from the eastern coast of Africa in the West to the western coast of Southeast Asia and Australia in the East.

[1] N.a.: China formally opens first overseas military base in Djibouti. Reuters, 1 August 2017.

Bordering the landmass of the Arabian Peninsula and South Asia, it encompasses the Red Sea, the Persian Gulf, and the Arabian Sea in the Northwest, the Bay of Bengal and the Andaman Sea in the Northeast, while it borders the Antarctic Ocean in the Southwest and the Pacific Ocean in the Southeast. The Indian Ocean is the third largest body of water, covering 19.5% of the total water surface of Earth,[2] surrounded by 33 states that are home to 2.9 billion people,[3] more than 1/3 of the global population (~8.1 billion).[4] The coastal states possess vast resources, including mineral oil and natural gas, with some being among the fastest-growing consumer markets globally. Positioned strategically between the robust economies of the Indian subcontinent and East Asia, and within the oil-rich Gulf region, the Indian Ocean has played a central role throughout history, as it has hosted crucial sea routes for global trade, gaining significance as one of the busiest maritime pathways for the exchange of manufactured goods, capital and services. The Indian Ocean is also indispensable for the global transportation of hydrocarbons. Ten coastal states in the region account for approximately 65% of the world's oil reserves.[5] The shipping lanes account for almost 50% of the global container traffic and approximately 70% of global crude oil traffic.[6]

Along these trade routes lie eight strategically important choke points:

- The Malacca Strait between Malaysia, Singapore and the Indonesian island of Sumatra, which connects Southeast Asia and the western Pacific region to the Indian Ocean. It is also the shortest sea route between China and Europe, the Middle East, India and Africa. More than 70% of China's crude oil and LNG exports is shipped through Malacca.[7]
- The Straits of Sunda and Lombok are busy waterways in the Indonesian archipelago that provide deepwater alternatives to the Malacca Strait. However, these alternative routes mean longer distances for ships travelling between China and Europe or the Middle East.
- The Strait of Hormuz, located between Oman and Iran is one of the world's most relevant choke points in terms of oil transit, connects the Persian Gulf and the Middle East to Asia, Europe, and Africa via the Indian Ocean.
- The Bab-el-Mandeb ("Gate of Grief") is situated between the Horn of Africa (Djibouti, Eritrea) and the Arabian Peninsula (Yemen), and it connects the Red Sea to the Gulf of Aden. It acts as a strategic link between the Indian Ocean and the Mediterranean Sea via the Red Sea and the Suez Canal, a narrow artificial passage in Egypt connecting the Red Sea and the Mediterranean Sea.

---

2 EAKINS, B.W. – SHARMAN, G.F.: World Ocean Volumes - Ocean, oceanic region and sea volumes calculated using the Ice Surface version of ETOPO1. 2010.

3 BARUAH, Darshana M. – LABH, Nitya – GREELY, Jessica: Mapping the Indian Ocean Region. Carnegie Endowment for International Peace, 15 June 2023

4 N.a.: Current World Population. Worldometers.

5 BARUAH – LABH – GREELY 2023

6 KURIAN, Anju Lis – VINODAN, C.: India and China in the Indian Ocean: Changing Dimensions of Maritime Strategy. Journal of Economic and Social Studies, January 2021, p. 3.

7 PASZAK, Paweł: China and the "Malacca Dilemma". Warsaw Institute, 28 February 2021

Along the Bab-el-Mandeb and the Suez Canal lies a key transit route for goods and energy transport between Europe, the Middle East, Asia and East Africa.

- The Mozambique Channel between Madagascar and Mozambique is the shortest sea trade route for goods transiting the Cape of Good Hope to East Africa and the Middle East.
- The Cape of Good Hope, situated at the southern tip of Africa and marking the meeting point of the Indian and Atlantic Oceans, is technically not considered a choke point as it is open on the southern side. Nevertheless, it is considered to be a crucial maritime passage. In 2016, approximately 9% of the global maritime oil trade, equivalent to 5.8 million barrels of crude oil per day, passed through the route around the Cape of Good Hope.[8] The Cape of Good Hope also serves as an alternative route in case the primary choke points, the Suez Canal or the Bab-el-Mandeb, are inaccessible. However, rerouting goods and resources around the Cape would increase costs considerably, as it would add thousands of kilometres of transit for ships travelling around Africa.

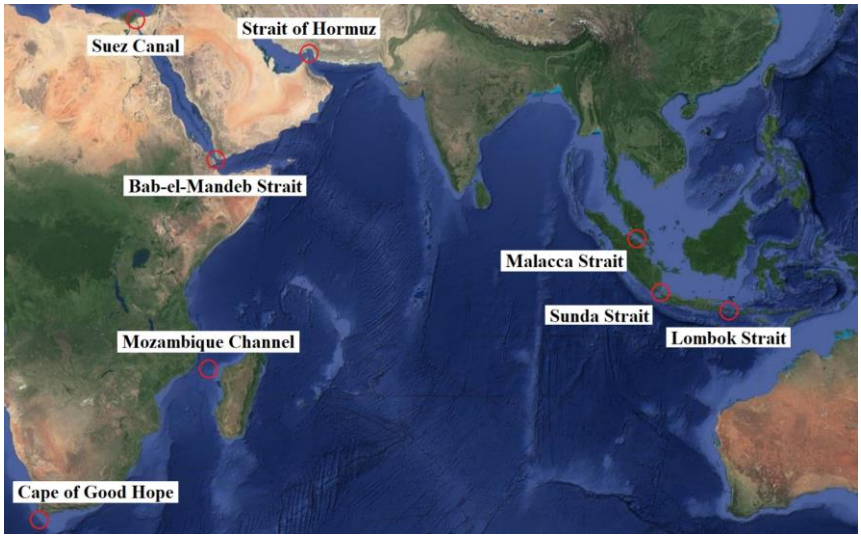

Figure 1: Major choke points of the Indian Ocean[9]

These bottlenecks connect relevant waterways, creating a shipping congestion. If they are either blocked or somehow unavailable, the alternative route is usually long, expensive, or in some cases impossible for large cargo ships and oil tankers to navigate due to shallow waters. From a military perspective, maritime choke points gain particular importance due to their potential to control access and deny passage to adversaries.

---

8 BURKHARDT, Paul: Africa's Hidden Oil Hub Grows After Traders Make Millions. Bloomberg, 29 May 2018.

9 Source: Google Maps

States possessing control over these narrow waterways can wield significant geopolitical leverage, limiting the mobility of opposing naval forces and impacting their ability to project power across the respective regions. The strategic positioning of naval assets at these locations enables securing national interests by ensuring uninterrupted flow of trade. Additionally, being stationed in proximity to vital choke points enhances a nation's capabilities in antisubmarine warfare and surveillance missions, thereby increasing maritime domain awareness. Surveillance and reconnaissance activities around choke points play a crucial role in detecting an opponent's marital movements, as identifying subsurface vessels in the open sea is significantly more challenging. In essence, maritime choke points represent geopolitical nodes where commercial and military interests intersect. Therefore, a country with a robust naval presence in the Indian Ocean also becomes a dangerous adversary or a valuable strategic partner for both the numerous active major players, and the coastal minor powers and island nations of the region.[10]

China's motives for expanding its influence in the Indian Ocean

The PRC's focus on continuous economic growth is a central element of its grand strategy,[11] compelling the nation to proactively engage with energy-producing and distributing countries, as China's rapid economic development over the past decades has relied heavily on foreign energy sources, and the relevance of such energy sources is expected to increase in the future. Crude oil products have been playing a central role in satisfying the substantial Chinese energy requirements. By 2003, The PRC became the second-largest consumer of oil after the United States.[12] In 2022, China consumed 14.3 million barrels of oil per day.[13] Consequently, Beijing is actively working on establishing strong connections across the Indian Ocean, particularly with states in the Middle East and the oil-producing countries of Africa.[14] The sea trade routes connecting the Chinese mainland with ports in the Middle East and along the coasts of Africa gained crucial importance in terms of China's energy security. China relies on oil trade from the Gulf States and Africa that provide more than 60% of its total oil imports.[15] The Indian Ocean serves as the primary channel for the transfer of fossil fuel from eight out of China's top ten suppliers.[16] Additionally, the region plays a central role as a transit zone for Chinese interactions with other African countries and Indian Ocean island nations as well. The Indian Ocean also serves as the primary trading route between China and Europe, one of the PRC's major markets, too.

---

10 BARUAH, Darshana M.: What Is Happening in the Indian Ocean? Carnegie Endowment for International Peace, 3 March 2021

11 BLACKWILL, Robert D. – TELLIS, Ashley J.: *China's Evolving Grand Strategy*. Council on Foreign Relations, 2015, p. 10

12 MALIK, Hasan Yaser: Beginning of an end in Indian Ocean. *IOSR Journal Of Humanities And Social Science*, 2013/3, p. 102.

13 N.a.: Leading oil-consuming countries worldwide in 2022. statista.com.

14 KURIAN – VINODAN 2021/1, p. 6.

15 WORKMAN, Daniel: Top 15 Crude Oil Suppliers to China. World's Top Exports, 2023.

16 Crude oil from Saudi Arabia, Iraq, the United Arab Emirates, Oman, Kuwait, Angola and Qatar crosses the Indian Ocean. Russia and Malaysia are the two exceptions. Source: WORKMAN 2023.

In 2003, Chinese President Hu Jintao expressed concerns regarding the security of China's energy imports, highlighting that approximately 80% of the country's oil imports traversed the Strait of Malacca.[17] The Strait of Malacca has been consistently viewed as a strategic vulnerability to Chinese national security, and President Hu raised attention that certain powers had persistently sought to assert control over navigation through this waterway. It is evident that under the term "certain powers" he meant the United States and the U.S. Navy's ability to dominate trade routes and maritime choke points. The problem of the lack of economically viable alternative routes and the vulnerability of the Chinese economy to a naval blockade was coined as the "Malacca Dilemma".[18] China heavily relies on a freely navigable Malacca Strait and a safe, secure, and stable Indian Ocean for trade, with a particular focus on undisrupted energy transportation. It is truly a dilemma that Beijing has still not managed to overcome.

Naval assets deployed in the Indian Ocean are necessary to safeguarding shipping lanes critical to China. The strategic location of the Chinese naval base in Djibouti enables China to expand its role in combating maritime threats and challenges. Naval assets could play a significant role in surveillance and reconnaissance activities. Monitoring regional developments, tracking naval and commercial movement, and gathering intelligence are potential functions that support both military and diplomatic decision-making. This surveillance capability can significantly enhance China's situational awareness of the region.[19]

The versatility of the locally deployed naval assets extends to humanitarian and disaster relief (HADR) missions as well. In the event of natural disasters or humanitarian crises in the region, China can use its regional naval capabilities to rapidly deploy resources and personnel, providing assistance and relief. This dual-use capability reinforces China's image as a nation that is able to contribute not only to security but also to the well-being of other states in times of crisis.[20]

Currently piracy and terrorism are among the most relevant security risks that threaten safe and undisrupted maritime transport in the Indian Ocean. The Houthi Militia in Yemen has frequently attacked and hijacked ships transiting the Red Sea since the onset of the Gaza war in October 2023. Positioned in close proximity to the Gulf of Aden and the Horn of Africa, China could rapidly deploy naval assets to effectively address maritime security threats in the Red Sea.[21] However, Beijing has chosen a cautious approach, refraining from taking decisive action or adopting a clear stance on the Red Sea crisis.

---

17 PASZAK 2021.

18 PASZAK 2021

19 COOPER, Zack: Security Implications of China's Military Presence in the Indian Ocean. Center for Strategic and International Studies, March 2018, p. 2

20 FEI, John: China's Overseas Military Base in Djibouti: Features, Motivations, and Policy Implications. China Brief, The Jamestown Foundation, 17/17, 22 December 2017

21 BISEN, Anurag: Delegitimising China's Naval Presence in the Indian Ocean Region. Manohar Parrikar Institute for Defence Studies and Analyses, 30 August 2022.

Despite China's efforts to promote the narrative of the United States' withdrawal from the Middle East and to undermine Washington's alliances and role as a reliable global and regional security guarantor, the limitations of China's regional advocacy capabilities are evident. The Houthi attacks against not only Israel, but also China's Arab partner states, highlight Beijing's lack of interest and limited ability to influence the situation in the Middle East. Throughout the ongoing conflict, there is no indication that China has sought to moderate Iran's actions or make any substantial efforts to influence the situation. As of January 2024, China has failed to contribute to maritime security in the Red Sea region, and its forces have been inactive in rescue operations. Even when Chinese interests such as freedom of navigation and shipping security are at stake, China continues to rely on the efforts of other countries, primarily the United States, which is consistently portrayed as the main instigator of the conflict by Beijing.[22]

Chinese inaction in the Red Sea seems illogical from a purely economic standpoint, as shipping costs and insurance premiums have sharply risen since 15 December 2023. The Shanghai Containerized Freight Index (SCFI), a benchmark for rates transporting goods from China, has surged by 161%, climbing from 1029 USD to 2694 USD. This increase is attributed to ships opting for the longer route around the Cape of Good Hope to avoid Houthi attacks near the Bab-el-Mandeb. Despite the sharp spike, the rates still remain below those experienced during the COVID-19 pandemic. While the Houthi attacks impact global shipping lanes, it is anticipated that Chinese trade will be mostly unaffected by this challenge.[23] So far, the Houthis have refrained from targeting oil tankers, and it is likely that they will avoid confronting Chinese vessels[24] to prevent a significant shift in Beijing's neutral stance. As major Arab states have refrained from joining a coalition against the Houthis, coupled with the absence of a UN mandate (unlike the mandate of the anti-piracy military task force in the Horn of Africa, which includes China), reinforces Beijing's perception that participating in a security operation against the Houthi Militia does not provide notable benefits.[25]

Chinese maritime presence in the Indian Ocean region

In 2004, the US-based government and military contractor and consulting firm Booz Allen Hamilton introduced the disputed "String of Pearls" hypothesis. The theory suggested that China aimed to enhance its naval presence on the Indian Ocean rim by constructing maritime infrastructure, as Beijing had been deeply concerned about its security in the Indian Ocean, primarily due to the possibility of a U.S. Navy blockade of the Malacca Strait, and to counterbalance the expanding maritime influence of

---

22 SELA, Ori – ORION, Assaf: China and the Houthis: Sounds of Silence. The Institute for National Security Studies, INSS Insight, No. 1810, 10 January 2024.

23 ABOUDOUH, Ahmed: Houthi attacks in the Red Sea help China criticize the US – but threaten long-term policy. Chatham House, 9 January 2024.

24 N.a.: Houthis Won't Target Chinese, Russian Ships in Red Sea. Voice of America, voanews.com, 19 January 2024

25 ABOUDOUH 2024.

India.[26] In the last 20 years there has been no clear indicator that the "String of Pearls" hypothesis would become a reality. Although the hypothesis is based on early exaggerated assumptions about encircling India, the PRC did begin to strengthen its naval presence in the Indian Ocean region.

There is one naval base that currently serve Chinese naval interests, and one port that has dual-use potential to provide logistical support for the PLAN in the foreseeable future:

– Port of Doraleh, Djibouti: The support base in the Port of Doraleh is the PRC's first overseas military base operated by PLAN,[27] located in Djibouti in the Horn of Africa, just a few kilometres away from Camp Lemonnier, a United States Naval Expeditionary Base.[28] The PLAN base was established in 2017, and it holds a strategic position at the southern gateway to the Red Sea, in the immediate vicinity of the Bab-el-Mandeb Strait. The base is expected to significantly enhance China's power projection capability in the western Indian Ocean region.[29] The PLAN has already used the port to conduct anti-piracy operations around the Horn of Africa. The facility is also expected to be involved in gathering intelligence, evacuation operations, supporting peacekeeping operations, and counterterrorism.[30]

– Gwadar, Pakistan: Located on the southwestern coast of Pakistan, near the entrance to the Persian Gulf, Gwadar lies close to crucial shipping lanes, including the Strait of Hormuz. While not functioning as a Chinese maritime base, Gwadar has significant potential. In April 2015, Pakistan and China announced their intention to develop the 45 billion USD China–Pakistan Economic Corridor (CPEC) within the Belt and Road Initiative.

  Gwadar plays a major role in CPEC and is also planned to be the maritime link between China and Pakistan.[31] The ties between Beijing and Islamabad are strong, with Pakistan being the most prominent recipient of Chinese arms export since 1991, including naval assets.[32] Increasing animosity toward India could also enhance the cooperation between the two countries, which might result in the dual-use of Gwadar Port as another service base for the PLAN in the Indian Ocean.

---

26 DRUN, Jessica: China's Maritime Ambitions: a Sinister String of Pearls or a Benevolent Silk Road (or Both)? Center for Advanced China Research, 5 December 2017.

27 ZHOU, Laura: How a Chinese investment boom is changing the face of Djibouti. South China Morning Post, 17 April 2017.

28 GERING, Tuvia – SLOANE, Heath: Beijing's Overseas Military Base In Djibouti. memri.org, 16 July 2021.

29 HUNEKE, Douglas: The Ghost of Zheng He: China's Naval Base in Djibouti. Berkeley Political Review, 19 April 2017.

30 SUCIU, Peter: China's Naval Base in Africa Is Getting Bigger. Is a Network of Bases Next? The National Interest, 11 May 2020.

31 ASHRAF, Sajjad: Gwadar – the "Economic Funnel for the Region". chinausfocus.com, 18 May 2017.

32 XUE, Maryann: China's arms trade: which countries does it buy from and sell to? South China Morning Post, 4 July 2021.

There has been concerns about maritime infrastructural investment and construction works conducted within the framework of the Belt and Road Initiative around the Indian Ocean rim that might serve Chinese military interests beside economic ones. The assumption that China is financing and building ports and related infrastructure to serve the PLAN both in times of peace and war is based on the dual purpose mandated by Chinese domestic laws, which require Chinese civilian ports to provide logistical support to the PLAN when needed.[33] According to critical voices, with the use of "debt-trap diplomacy", China is handing out unsustainable loans to low-GDP countries in order to gain influence; to get economic privileges like access to natural resources; to lease ports; and to gain favours, which might include the use of civilian ports of these financially dependent states as bases for PLAN activities.[34] "Debt-trap diplomacy" is increasingly viewed as a myth[35] and is even called a conspiracy theory,[36] so the security implications of Belt and Road Initiative investments need to be assessed carefully. Taking this into account, the following Chinese-affiliated ports emerge in the international press time to time that are suspected to serve Chinese naval interests in the future:

– Hambantota, Sri Lanka: According to the agreement made in 2016, the port has been leased to China for 99 years. The PRC has invested over 2 billion USD in the Hambantota port. Hambantota would be useful for the PRC to observe and expand influence over maritime routes stretching from the eastern coast of Africa to Southeast Asia, including those passing through the Bay of Bengal. Given its strategic positioning, Hambantota was said to be a likely candidate for a potential Chinese naval base in the future,[37] but after the failure of the previous China-friendly government, the unsustainable Chinese loan and the deep corruption surrounding the Hambantota deal,[38] the current Sri Lankan government does not seem to be a likely ally of Beijing.

– Kyaukpyu Port, Myanmar: In 2015, the Chinese CITIC Group won the contract for the construction of a deep-sea port and associated infrastructure in the town of Kyaukpyu. The cost of the project was 7.3 billion USD,[39] more than 10% of Myanmar's GDP (62.7 billion USD),[40] which would have meant serious financial debt burden for the country.

---

33 KARDON, Isaac: China's Military Diplomacy and Overseas Security Activities. Carnegie Endowment for International Peace, 26 January 2023.

34 WHITE, Joshua T.: China's Indian Ocean Ambitions: Investment, Influence, and Military Advantage. Brookings, June 2020, p. 3.

35 BRAUTIGAM, Deborah – RITHMIRE, Meg: The Chinese 'Debt Trap' Is a Myth. The Atlantic, 6 February 2021.

36 STONE, Rupert: China is losing ground in Sri Lanka. The Interpreter, 19 August 2022.

37 WOOLEY, Alexander – ZHANG, Sheng: Beijing Is Going Places—and Building Naval Bases. Foreign Policy, 27 July, 2023.

38 STONE 2022.

39 FILLINGHAM, Zachary: Backgrounder: Myanmar's Kyaukpyu Port. Geopolitical Monitor, 27 October 2023

40 N.a.: Myanmar: Gross domestic product (GDP) in current prices from 2008 to 2028. statista.com.

The deal was renegotiated after the Myanmar elections of 2015 with more favourable terms, but the effects of COVID-19 and the coup of 2021 have halted the project ever since.[41] The isolation of the State Administration Council, the military junta currently governing Myanmar, might mean an opportunity for Beijing to pressure the country to proceed on the megaproject.[42]

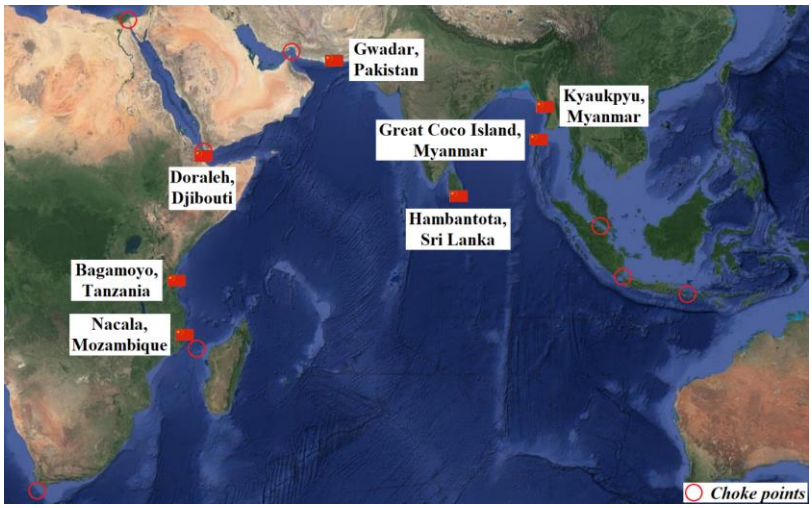

Figure 2: The naval base of Doraleh and major ports with Chinese affiliation in the Indian Ocean region[43]

– Great Coco Island, Myanmar: A persistent rumour has emerged periodically since the early 1990s that Myanmar allowed a Chinese signals intelligence facility on the Coco Islands. The archipelago has been undergoing noticeable transformation, displaying signs of military modernisation and the establishment of facilities to support aircraft. Recent images suggest that Myanmar might be preparing to conduct maritime surveillance operations from Great Coco Island.[44] This island is the largest in the archipelago located 60 km north of India's strategic Andaman and Nicobar Command.[45] Photos from January 2023, taken by Maxar Technologies, reveal increased construction activity on Great Coco. The images show two new hangars, a new causeway, and what appears to be an accommodation bloc, all situated near a recently lengthened 2300-metre runway and a radar station.

41 FILLINGHAM 2023.

42 N.a.: China pressures Myanmar to proceed on port project amid community concerns. Radio Free Asia, 1 June 2023.

43 Source: Google Maps

44 SYMON, Damien – POLLOCK, John: Is Myanmar building a spy base on Great Coco Island? Chatham House, 31 March 2023

45 N.a.: Chinese base or wild rumour? The Coco Islands mystery. Frontier Myanmar, 5 June 2023.

By late March 2023, visible evidence of land clearing efforts at the southern tip of Great Coco, just beyond the connecting causeway, suggests upcoming construction work. With Myanmar's armed forces struggling to maintain control over large areas, and with the economy in decline, China appears to be supporting the regime and safeguarding its investments. Chinese companies are reportedly operating on the ground, undertaking major infrastructure projects such as deepwater ports.[46]

– Bagamoyo Port, Tanzania: In 2013, a large deepwater port was proposed by the Tanzanian government. It is planned to be constructed near Bagamoyo, not far from Dar es Salaam, the most populous city of Tanzania. China's intention was to invest 10 billion USD to make Bagamoyo the most important port in Africa by 2017 in exchange for its lease for 99 years. The port would be part of the Maritime Silk Road. In 2018, the project began and construction started in the summer. However, Tanzanian President John Magufuli announced the temporary suspension of the construction in 2019.[47] In 2023, Beijing negotiated with the Tanzanian government to continue the project.[48] So far China has denied any plans to utilize the port for military objectives.[49] The strategic significance of Bagamoyo Port stems from its proximity to the Mozambique Channel.

– Nacala, Mozambique: Although the 230 million USD Chinese investment in the Mozambique port of Nacala[50] has not reached the same levels as in other states, it would be a mistake to consider it irrelevant. Unlike certain African countries like Tanzania or Kenya, Mozambique has not displayed a comparable reluctance towards Chinese loans and investments. Moreover, China enjoys popularity among the general population, as Chinese companies provide substantial sponsorship to a significant portion of the country's media.[51] Located in the middle of the Mozambique Channel, theoretically, Nacala port could prove to be a valuable asset for Chinese naval ambitions.

It has to be strongly emphasised that these projects are currently more about business in nature, contrary to critical voices that see military security implications associated with the Belt and Road Initiative projects in the Indian Ocean. It is true that the strategic importance of these ports cannot be overlooked, as they all have the potential to offer foothold in key geopolitical locations.

---

46 SYMON – POLLOCK 2023.

47 OIRERE, Shem: Tanzania Suspends $10B Bagamoyo Port Project. enr.com, 25 June 2019.

48 N.a.: China-Tanzania talks over Bagamoyo port project in progress: envoy. cgtn.com, 15 June 2023

49 JOCHHEIM, Ulrich – LOBO, Rita Barbosa: *Geopolitics in the Indo-Pacific: Major players' strategic perspectives.* European Parliament, July 2023.

50 WOOLEY, Alexander – ZHANG, Sheng – FEDOROCHKO, Rory – PATTERSON, Sarina: Harboring Global Ambitions: China's Ports Footprint and Implications for Future Overseas Naval Bases. aiddata.org, July 2023.

51 YOUNG, Ellie – TSANDZANA, Dércio: Beijing's global media influence 2022 – Mozambique. 2022.

As these ports become integral nodes in China's maritime economic network, there is a possibility that the distinction between economic and military objectives may blur over time, altering the balance of power in the Indian Ocean. However, the current outlook is that neither the PRC, nor any of the aforementioned countries are planning the military use of these ports.

Prospects for a Chinese Indian Ocean fleet

Naval bases and ports could only be useful if an oceangoing navy took advantage of them. The Chinese navy – currently the largest navy in terms of the number of naval assets[52] – and the ongoing efforts taken by the PRC to enhance its blue-water capabilities could result in enhanced Chinese naval presence in the Indian Ocean in the future.

	China[53]	USA[54]	India[55]
Submarines	59	67	16
Aircraft carriers	2	11	2
Cruisers	7	19	-
Destroyers	42	70	10
Frigates	41	22	16
Patrol and coastal combatants	142	89	164
Mine warfare, mine countermeasure	57	8	-
Command ships	-	2	-
Amphibious	141	176	21
Logistics and support	153	194	41
Total	644	594	270

Figure 3: Naval forces of major powers active in the Indian Ocean (without coast guard)[56]

[52] N.a.: Military and Security Developments Involving the People's Republic of China – A Report to Congress. U.S. Department of Defense, 19 October 2023, p. 52.

[53] N.a.: Chapter Six: Asia. The Military Balance, 2023/1. 14 February 2023, pp. 239-241, pp. 249-250.

[54] N.a.: Chapter Three: North America. The Military Balance 2023/1, 14 February 2023, pp. 38-40.

[55] Chapter Six: Asia, The Military Balance 2023, pp. 249–250.

[56] PLAN assets are predominantly located in the South China Sea and East China Sea, while U.S. Navy forces are dispersed across the Pacific, Atlantic and Indian Oceans.

According to the Center for Maritime Strategy Studies at Beijing University, the primary focus areas for the PLAN in the future will be the western Pacific and the northern Indian Ocean, the latter theatre extending from the Middle East and East Africa to the Malacca Strait.[57] It could be in the PRC's national interest to deploy two fleets of ocean-going vessels in the Pacific and the Indian Oceans, possibly centred around carrier battle groups to establish an effective naval presence in both oceans. The hypothetical Chinese Indian Ocean fleet would be based on strategic islands in the South China Sea and naval bases provided by friendly states like Pakistan in the Indian Ocean region. The concept of a two-ocean navy is in line with the Chinese active defence strategy, which means the establishment of a proactive forward defence line extending beyond its immediate waters of the South China Sea and East China Sea.

The PLAN is steadily increasing its naval presence in the Indian Ocean. According to the former Indian Navy chief, there are typically six to eight PLAN warships in the northern Indian Ocean at any given time,[58] but the PRC possesses over a hundred naval assets capable of operating in the Indian Ocean.[59] The lack of effective air support, however, is a major constraint that prevents any PLAN fleet in the region from engaging in meaningful combat with a state that has naval aviation or land-based fighter jets in range. The lack of air support is a considerable obstacle and severely hampers the PLAN's ability to project power in the region.

The deployment of aircraft carriers could be a solution to compensate for the lack of air capabilities. China aims to possess up to six aircraft carriers by 2035 to enhance its capabilities for blue-water operations,[60] which includes the possibility of deploying some of these carriers to the Indian Ocean. The PRC's first two carriers, primarily the Liaoning and to a certain extent the Shandong, serve as experimental carriers for carrier-construction and training purposes.[61] The PRC's third carrier, the Fujian was launched in 2022. Currently it is fitting out, while sea trials are expected in early 2024.[62] China's fourth aircraft carrier, which is rumoured to be nuclear-powered, is still on the drawing board,[63] or at least there has been no clear report of it being constructed.

---

57 COLLEY, Christopher: A Future Chinese Indian Ocean Fleet? War on the Rocks, 2 April 2021.

58 SONWALKAR, Prasun: 'Keeping a close eye on Chinese presence in Indian Ocean,' says Admiral Lanba. Hindustan Times, 13 March 2019.

59 BECKER, Jeffrey: China Maritime Report No. 11: Securing China's Lifelines across the Indian Ocean. U.S. Naval War College, CMSI China Maritime Reports. 11 December 2020, p. 6.

60 CHAN, Millie – RUI, Guo: China will build 4 nuclear aircraft carriers in drive to catch US Navy, experts say. South China Morning Post, 6 February 2019.

61 POMOGÁCS, Péter: A Kínai Népköztársaság repülőgép-hordozó programja. [The aircraft carrier program of the People's Republic of China.] *Felderítő Szemle*, 2021/2, p. 99.

62 LAU, Jack: China's Fujian aircraft carrier spotted in new position, bringing it a step closer to sea trial, analysts say. South China Morning Post, 27 November 2023.

63 HUANG, Christine: China's next aircraft carrier: nuclear-power speculation continues. South China Morning Post, 9 October 2022.

The vast expanse of the Indian Ocean might raise questions about the practicality of deploying a carrier in the region. In the event of hostilities, a carrier could find itself thousands of kilometres away from the conflict zone, taking days or even weeks to reach the scene. Smaller and stealthier vessels like frigates may offer a broader protective range for Chinese interests.[64] Moreover, currently all of the PRC's carriers are outfitted with conventional propulsion, which gives them limited range[65] – although well-positioned naval bases in the Indian Ocean would partly solve this problem, based on the strongly hypothetical assumption that sovereign states allow China to use their ports for logistic support. Until the PLAN achieves mastery in carrier-based aviation, its ability to participate in combat operations beyond counter-piracy or relatively low-risk missions (such as supporting humanitarian and disaster relief operations) remain limited.[66]

While the role of a future Chinese Indian Ocean fleet could involve cooperation with the United States and Indian navies to safeguard shipping lanes, the fact that the United States and China have identified each other as their primary strategic competitors[67] may culminate in a political and military alliance between the US and India directed against China. For this reason, it is rather unlikely that the PRC would publicly announce its Indian Ocean fleet until it becomes fully operational. Due to political considerations, Beijing may refrain from labelling it as a fleet even then, so as not to escalate tensions with the United States and India.

Based on the consistent efforts to deploy warships with blue-water capabilities, it can be concluded that the PLAN is currently just acquiring the necessary components to support an Indian Ocean fleet.[68]

Conclusion

The Indian Ocean holds increasing economic, political, and security significance on the global stage, with its maritime choke points, trade routes and coasts spanning Africa, the Middle East, South Asia, Southeast Asia and Australia. Established regional players like India, alongside emerging powers such as China, are expanding their presence in the Indian Ocean, investing economically, politically, and militarily in the region. Given its economic potential, vital shipping lanes, and abundant resources, the Indian Ocean is set to play a crucial role in geopolitical competition in the coming decades.

---

64 COLLEY 2021.

65 HÁDA, Béla: *A Kínai Népköztársaság és az Amerikai Egyesült Államok haditengerészeti erőviszonyai – tények és nézőpontok*. [Naval Power Relations between the People's Republic of China and the United States of America – Facts and Perspectives.] Stratégiai Védelmi Kutatóintézet, Elemzések, 2020/24, 4 December 2020, p. 4.

66 COLLEY 2021.

67 N.a.: The White House: National Security Strategy. 12 October 2022, p. 23.

68 COLLEY 2021.

The Chinese maritime strategy reflects Beijing's concerted efforts to secure energy trade routes and establish a formidable naval presence, primarily to counterbalance India and the naval superiority of the United States, and to safeguard its economic interests. China's presence in key locations around the Indian Ocean, coupled with its quickly improving naval capabilities, signify a strategic shift to enhance its influence and protect its national interests, particularly in energy transit. The prospect of a Chinese Indian Ocean fleet, while not yet fully realised, remains a plausible development in the context of Beijing's long-term strategic objectives. Maritime choke points and critical sea routes further highlight the geopolitical importance of naval presence and control over maritime pathways.

The competition for dominance over the Indian Ocean is not only about military power, but also includes economic and diplomatic influence. China's investments, often facilitated through the Belt and Road Initiative, are not only aimed at securing maritime commercial interests, but also strengthening economic cooperation and diplomatic relations with host nations.

As China, India, and the United States interact within the vast theatre of the Indian Ocean, the need for collaboration and recognition of mutual interests becomes increasingly relevant. Traditional and non-traditional security challenges, including piracy, terrorism, and natural disasters could provide opportunities for stakeholders to engage in cooperative efforts. In the 21st century, the changing security environment of the region will significantly affect global security as well.

Bibliography:

ABOUDOUH, Ahmed: Houthi attacks in the Red Sea help China criticize the US – but threaten long-term policy. Chatham House, 9 January 2024 Online: https://www.chathamhouse.org/2024/01/houthi-attacks-red-sea-help-china-criticize-us-threaten-long-term-policy (Download time: 25/01/2024)

ASHRAF, Sajjad: Gwadar – the "Economic Funnel for the Region". chinausfocus.com, 18 May 2017, Online: https://www.chinausfocus.com/finance-economy/gwadar--the-economic-funnel-for-the-region (Download time: 27/11/2023)

BARUAH, Darshana M. – LABH, Nitya – GREELY, Jessica: Mapping the Indian Ocean Region. Carnegie Endowment for International Peace, 15 June 2023, Online: https://carnegieendowment.org/2023/06/15/mapping-indian-ocean-region-pub-89971 (Download time: 2/12/2023)

BARUAH, Darshana M.: What Is Happening in the Indian Ocean? Carnegie Endowment for International Peace, 3 March 2021, Online: https://carnegieendowment.org/2021/03/03/what-is-happening-in-indian-ocean-pub-83948 (Download time: 30/11/2023)

BECKER, Jeffrey: China Maritime Report No. 11: Securing China's Lifelines across the Indian Ocean. U.S. Naval War College, CMSI China Maritime Reports. 11 December 2020, Online: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1010&context=cmsi-maritime-reports (Download time: 04/12/2023)

BISEN, Anurag: Delegitimising China's Naval Presence in the Indian Ocean Region. Manohar Parrikar Institute for Defence Studies and Analyses, 30 August 2022, Online: https://www.idsa.in/issuebrief/Delegitimising-China-Naval-Presence-in-the-Indian-Ocean-Region-abisen-300822 (Download time: 2/12/2023)

BLACKWILL, Robert D. – TELLIS, Ashley J.: *China's Evolving Grand Strategy*. Council on Foreign Relations, 2015, Online: https://www.jstor.org/stable/pdf/resrep21418.8.pdf (Download time: 1/12/2023)

BRAUTIGAM, Deborah – RITHMIRE, Meg: The Chinese 'Debt Trap' Is a Myth. The Atlantic, 6 February 2021, Online: https://www.theatlantic.com/international/archive/2021/02/china-debt-trap-diplomacy/617953/ (Download time: 15/01/2023)

BURKHARDT, Paul: Africa's Hidden Oil Hub Grows After Traders Make Millions. Bloomberg, 29 May 2018, Online: https://www.bloomberg.com/news/articles/2018-05-29/africa-s-hidden-oil-hub-grows-after-making-millions-for-traders (Download time: 28/11/2023)

CHAN, Millie – RUI, Guo: China will build 4 nuclear aircraft carriers in drive to catch US Navy, experts say. South China Morning Post, 6 February 2019, Online: https://www.scmp.com/news/china/military/article/2185081/china-will-build-4-nuclear-aircraft-carriers-drive-catch-us-navy (Download time: 04/12/2023)

COLLEY, Christopher: A Future Chinese Indian Ocean Fleet? War on the Rocks, 2 April 2021, Online: https://warontherocks.com/2021/04/a-future-chinese-indian-ocean-fleet/ (Download time: 28/11/2023)

COOPER, Zack: Security Implications of China's Military Presence in the Indian Ocean. Center for Strategic and International Studies, March 2018, Online: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180627_Cooper_SecurityImplications.pdf (Download time: 28/11/2023)

DRUN, Jessica: China's Maritime Ambitions: a Sinister String of Pearls or a Benevolent Silk Road (or Both)? Center for Advanced China Research, 5 December 2017, Online: https://www.ccpwatch.org/single-post/2017/12/05/china-s-maritime-ambitions-a-sinister-string-of-pearls-or-a-benevolent-silk-road-or-both (Download time: 25/11/2023)

EAKINS, B.W. – SHARMAN, G.F.: World Ocean Volumes – Ocean, oceanic region and sea volumes calculated using the Ice Surface version of ETOPO1. 2010, Online: https://www.ncei.noaa.gov/sites/g/files/anmtlf171/files/2023-01/World%20Ocean%20Volumes.pdf (Download time: 5/12/2023)

FEI, John: China's Overseas Military Base in Djibouti: Features, Motivations, and Policy Implications. China Brief, The Jamestown Foundation, 17/17, 22 December 2017, Online: https://jamestown.org/program/chinas-overseas-military-base-djibouti-features-motivations-policy-implications/ (Download time: 2/12/2023)

FILLINGHAM, Zachary: Backgrounder: Myanmar's Kyaukpyu Port. Geopolitical Monitor, 27 October 2023, Online: https://www.geopoliticalmonitor.com/backgrounder-myanmars-kyaukpyu-port/ (Download time: 27/11/2023)

GERING, Tuvia – SLOANE, Heath: Beijing's Overseas Military Base In Djibouti. memri.org, 16 July 2021, Online: https://www.memri.org/reports/beijings-overseas-military-base-djibouti (Download time: 27/11/2023)

Google Maps: https://www.google.com/maps/@-2.3869315,74.524863,9392833m/data=!3m1!1e3!5m1!1e4?entry=ttu&g_ep=EgoyMDI0MDkyOS4wIKXMDSoASAFQAw%3D%3D (Download time: 27/11/2023)

HÁDA, Béla: *A Kínai Népköztársaság és az Amerikai Egyesült Államok haditengerészeti erőviszonyai – tények és nézőpontok*. [Naval Power Relations between the People's Republic of China and the United States of America – Facts and Perspectives.] Stratégiai Védelmi Kutatóintézet, Elemzések, 2020/24, 4 December 2020, Online: http://real.mtak.hu/120691/1/SVKI_Elemzesek_2020_24_AKinaiNepkoztarsasagesazAmerikaiEgyesultAllamokhaditengereszetieroviszonyaiHadaB..pdf (Download time: 9/12/2020)

HUANG, Christine: China's next aircraft carrier: nuclear-power speculation continues. South China Morning Post, 9 October 2022, Online: https://www.scmp.com/news/china/military/article/3195306/chinas-next-aircraft-carrier-nuclear-power-speculation (Download time: 04/12/2023)

HUNEKE, Douglas: The Ghost of Zheng He: China's Naval Base in Djibouti. Berkeley Political Review, 19 April 2017, Online: https://bpr.berkeley.edu/2017/04/19/the-ghost-of-zheng-he-chinas-naval-base-in-djibouti/ (Download time: 27/11/2023)

JOCHHEIM, Ulrich – LOBO, Rita Barbosa: *Geopolitics in the Indo-Pacific: Major players' strategic perspectives*. European Parliament, July 2023, Online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751398/EPRS_BRI(2023)751398_EN.pdf (Download time: 22/11/2023)

KARDON, Isaac: China's Military Diplomacy and Overseas Security Activities. Carnegie Endowment for International Peace, 26 January 2023, Online: https://carnegieendowment.org/2023/01/26/china-s-military-diplomacy-and-overseas-security-activities-pub-89687 (Download time: 22/11/2023)

KURIAN, Anju Lis – VINODAN, C.: India and China in the Indian Ocean: Changing Dimensions of Maritime Strategy. *Journal of Economic and Social Studies*, 2021/1, Online: https://discovery.researcher.life/download/article/d98376bb31d23c408b1692272f35b56b/full-text (Download time: 13/11/2023)

LAU, Jack: China's Fujian aircraft carrier spotted in new position, bringing it a step closer to sea trial, analysts say. South China Morning Post, 27 November 2023, Online: https://www.scmp.com/news/china/military/article/3242991/chinas-fujian-aircraft-carrier-spotted-new-position-bringing-it-step-closer-sea-trial-analysts-say (Download time: 04/12/2023)

MALIK, Hasan Yaser: Beginning of an end in Indian Ocean. *IOSR Journal Of Humanities And Social Science*, 2013/3, pp. 100-111, Online: https://www.iosrjournals.org/iosr-jhss/papers/Vol14-issue3/R0143100111.pdf (Download time: 01/12/2023)

N.a.: China formally opens first overseas military base in Djibouti. Reuters, 1 August 2017, Online: https://www.reuters.com/article/us-china-djibouti/china-formally-opens-first-overseas-military-base-in-djibouti-idUSKBN1AH3E3/ (Download time: 5/12/2023)

N.a.: Chapter Three: North America. The Military Balance 2023/1, 14 February 2023, Online: https://www.tandfonline.com/doi/full/10.1080/04597222.2023.2162715 (Download time: 11/01/2024)

N.a.: China pressures Myanmar to proceed on port project amid community concerns. Radio Free Asia, 1 June 2023, Online: https://www.rfa.org/english/news/myanmar/project-06012023165833.html (Download time: 28/12/2023)

N.a.: China-Tanzania talks over Bagamoyo port project in progress: envoy. cgtn.com, 15 June 2023, Online: https://africa.cgtn.com/china-tanzania-talks-over-bagamoyo-port-project-in-progress-envoy/ (Download time: 28/11/2023)

N.a.: Chinese base or wild rumour? The Coco Islands mystery. Frontier Myanmar, 5 June 2023, Online: https://www.frontiermyanmar.net/en/chinese-base-or-wild-rumour-the-coco-islands-mystery/ (Download time: 28/11/2023)

N.a.: Current World Population. Worldometers, Online: https://www.worldometers.info/world-population/ (Download time: 27/11/2023)

N.a.: Houthis Won't Target Chinese, Russian Ships in Red Sea. Voice of America, voanews.com, 19 January 2024, Online: https://www.voanews.com/a/houthis-won-t-target-chinese-russian-ships-in-red-sea/7446893.html (Download time: 25/01/2024)

N.a.: Leading oil-consuming countries worldwide in 2022. statista.com, n.d. Online: https://www.statista.com/statistics/271622/countries-with-the-highest-oil-consumption-in-2012/ (Download time: 1/12/2023)

N.a.: Military and Security Developments Involving the People's Republic of China – A Report to Congress. U.S. Department of Defense, 19 October 2023, Online: https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF (Download time: 05/11/2023)

N.a.: Myanmar: Gross domestic product (GDP) in current prices from 2008 to 2028. statista.com, n.d. Online: https://www.statista.com/statistics/525760/gross-domestic-product-gdp-in-myanmar/ (Download time: 27/11/2023)

N.a.: The White House: National Security Strategy. 12 October 2022, p. 23. Online: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (Download time: 22/07/2023)

N.a.: Chapter Six: Asia. The Military Balance, 2023/1. 14 February 2023, Online: https://www.tandfonline.com/doi/full/10.1080/04597222.2023.2162718 (Download time: 11 January 2024)

OIRERE, Shem: Tanzania Suspends $10B Bagamoyo Port Project. enr.com, 25 June 2019, Online: https://www.enr.com/articles/47134-tanzania-suspends-bagamoyo-port-project (Download time: 28/11/2023)

PASZAK, Paweł: China and the "Malacca Dilemma". Warsaw Institute, 28 February 2021, Online: https://warsawinstitute.org/china-malacca-dilemma/ (Download time: 28/11/2023)

POMOGÁCS, Péter: A Kínai Népköztársaság repülőgép-hordozó programja. *Felderítő Szemle*, 2021/2, pp. 93-105. Online: https://www.knbsz.gov.hu/hu/letoltes/fsz/2021-2.pdf (Download time: 20/01/2022)

SELA, Ori – ORION, Assaf: China and the Houthis: Sounds of Silence. The Institute for National Security Studies, INSS Insight, No. 1810, 10 January 2024, Online: https://www.inss.org.il/publication/china-houthi/ (Download time: 25/01/2024)

SONWALKAR, Prasun: 'Keeping a close eye on Chinese presence in Indian Ocean,' says Admiral Lanba. Hindustan Times, 13 March 2019, Online: https://www.hindustantimes.com/india-news/keeping-a-close-eye-on-chinese-presence-in-indian-ocean-says-admiral-lanba/story-pr7dzln0KC1wPxLrzV182M.html (Download time: 04/12/2023)

STONE, Rupert: China is losing ground in Sri Lanka. The Interpreter, 19 August 2022, Online: https://www.lowyinstitute.org/the-interpreter/china-losing-ground-sri-lanka (Download time: 15/01/2023)

SUCIU, Peter: China's Naval Base in Africa Is Getting Bigger. Is a Network of Bases Next? The National Interest, 11 May 2020, Online: https://nationalinterest.org/blog/buzz/chinas-naval-base-africa-getting-bigger-network-bases-next-153146 (Download time: 27/11/2023)

SYMON, Damien – POLLOCK, John: Is Myanmar building a spy base on Great Coco Island? Chatham House, 31 March 2023, Online: https://www.chathamhouse.org/publications/the-world-today/2023-04/myanmar-building-spy-base-great-coco-island (Download time: 28/11/2023)

WHITE, Joshua T.: China's Indian Ocean Ambitions: Investment, Influence, and Military Advantage. Brookings, June 2020, Online: https://www.brookings.edu/wp-content/uploads/2020/06/FP_20200615_chinas_indian_ocean_ambitions_white-1.pdf (Download time: 25/11/2023)

WOOLEY, Alexander – ZHANG, Sheng – FEDOROCHKO, Rory – PATTERSON, Sarina: Harboring Global Ambitions: China's Ports Footprint and Implications for Future Overseas Naval Bases. aiddata.org, July 2023, Online: https://docs.aiddata.org/reports/harboring-global-ambitions/Harboring_Global_Ambitions.html (Download time: 28/11/2023)

WOOLEY, Alexander – ZHANG, Sheng: Beijing Is Going Places—and Building Naval Bases. Foreign Policy, 27 July, 2023, Online: https://foreignpolicy.com/2023/07/27/china-military-naval-bases-plan-infrastructure/ (Download time: 27/11/2023)

WORKMAN, Daniel: Top 15 Crude Oil Suppliers to China. World's Top Exports, 2023, Online: https://www.worldstopexports.com/top-15-crude-oil-suppliers-to-china/?expand_article=1 (Download time: 2/12/2023)

XUE, Maryann: China's arms trade: which countries does it buy from and sell to? South China Morning Post, 4 July 2021, Online: https://www.scmp.com/news/china/military/article/3139603/how-china-grew-buyer-major-arms-trade-player (Download time: 27/11/2023)

YOUNG, Ellie – TSANDZANA, Dércio: Beijing's global media influence 2022 – Mozambique. 2022, Online: https://freedomhouse.org/country/mozambique/beijings-global-media-influence/2022 (Download time: 28/11/2023)

ZHOU, Laura: How a Chinese investment boom is changing the face of Djibouti. South China Morning Post, 17 April 2017, Online: https://www.scmp.com/news/china/diplomacy-defence/article/2087374/how-chinese-investment-boom-changing-face-djibouti?campaign=2087374&module=perpetual_scroll_0&pgtype=article (Download time: 26/11/2023)

BÁLINT PONGRÁCZ

RUSSIAN PRIVATE MILITARY CONTRACTORS IN THE CENTRAL AFRICAN REPUBLIC

Abstract

The Wagner Group's deployment to the Central African Republic is an exceptionally well-documented case of Russian interference in Sub-Saharan Africa, by means of private military companies (PMCs). The in-depth analysis of this case study reveals the complex nature of the Russian PMC-presence in the country and the multi-stakeholder rationale behind the phenomenon. This essay, the first in a series of three, introduces the Kremlin's incentives for the deployment of Russian PMCs in the Central African Republic. Consequent papers, published in later issues of this journal, deal with the Russian sub-state (II.) and local (III.) incentives respectively.

Keywords: Russia, Wagner Group, Central African Republic, Prigozhin, private military companies, mercenaries, Kremlin, foreign interference

INTRODUCTION

Two hours southwest of the capital of the Central African Republic (CAR) Bangui, there lie the ruins of the palace of the *last emperor of Africa*. The Berengo complex, once occupied by the country's self-proclaimed emperor Jean-Bedel Bokassa, has had peculiar new resident since 2018. Establishing their first training camp on the palace grounds, Russian private military contractors project their rapidly growing influence over the CAR from this base of operations.[1] The mounting human rights violations linked to the Russian military contractors justify the investigation of their presence in the CAR. However, other factors, such as the concurrent exploitation of the country's natural resources by Russian firms and the Wagner private military company's (PMC[2]) emergence in neighbouring Sudan and Niger, after their *coups d'état,* further amplify the need for the study of this unconventional method of Russian interference.[3,4]

1 KATZ, Brian – JONES, Seth G. – DOXSEE, Catrina – HARRINGTON, Nicholas: Moscow's Mercenary Wars: The Expansion of Russian Private Military Companies. Moscow's Mercenary Wars: The Expansion of Russian Private Military Companies, September 2020.

2 PONGRACZ, Bálint: What are the reasons for the presence of Russian private military companies on the African continent? *National Security Review,* 2023/1, pp. 80-106.

3 ARVANITIDIS, Barbara – ELBAGIR, Nima – MEZZOFIORE, Gianluca – QIBLAWI, Tamara: Exclusive: Evidence Emerges of Russia's Wagner Arming Militia Leader Battling Sudan's Army. CNN, 20 April 2023.

4 ARMSTRONG, Kathryn: Niger Coup: Wagner Taking Advantage of Instability – Antony Blinken. BBC News, 8 August 2023.

Additionally, taking into consideration the recent demise of Yevgeny Prigozhin – the owner of the Russian PMC operating in the CAR – it is especially timely to study this phenomenon as both policymakers and the academic community await developments on this ground.

This essay, subtitled *The Kremlin's Stake*, constitutes an effort to introduce and investigate the Russian state's incentive for deploying private military contractors to the Central African Republic. A further two essays are dedicated to elaborating on the perspectives of the other two stakeholders involved in the phenomenon, Yevgeny Prigozhin and the CAR government. Please note that the three essays in unison form a study whose overarching conclusion is attached to the final, third essay.

THE KREMLIN'S STAKE

According to Samuel Ramani, a recognised expert on Russian foreign policy in Africa, there are three distinct Russian objectives in the Central African Republic: undermining the French influence in the country, establishing Russian commercial interests and expanding the Kremlin's influence over the Central African region.[5] After a thorough review of the academic literature and the situation on the ground, these three objectives were found sufficiently broad to incorporate all major Russian goals and measures discussed by other scholars and analysts. Nonetheless, this study distinguishes between the objectives of the Russian state and the aims of Russian sub-state actors. Since the Russian commercial interests in the Central African Republic are in effect exclusively Prigozhin-linked, those are discussed separately in the second essay. [6] Meanwhile, this essay analyses the role of Russian private military contractors in the context of the Kremlin's objectives in the CAR. This endeavour requires *a priori* knowledge of the **modern history of the Central African Republic,** aiding the understanding of the complex domestic dynamics and the often-controversial role of foreign powers in the country. Only then, can the essay attend to the **(I.) Russian interference in the CAR** and the **(II.) Kremlin's aim at the Central African region.**

The Modern History of the Central African Republic

The Central African Republic was established in 1958 as a semi-autonomous state within the French Community (*Communauté française*), a post-colonial organisation comprised of France and her former African colonies.[7] The country gained full independence in 1960 and – with significant French support – David Dacko became the nation's first president.

---

5 RAMANI, Samuel: Russia's Strategy in the Central African Republic. Royal United Services Institute, 2021.

6 To be published at a later date in the consequent issue of this journal.

7 KALCK, Pierre: *Historical Dictionary of the Central African Republic*. Scarecrow Press, Lanham, Md. 2005.

After a period of five years, described by the general breakdown of political freedoms and the country's transition to a *de facto* single-party regime, Dacko was overthrown in the *Saint-Sylvestre coup d'état* by Jean-Bédel Bokassa.[8] President Bokassa, who famously crowned himself emperor and consequently renamed the country the Central African Empire in 1976, was the first leader of the CAR to establish diplomatic relations with the Soviet Union (USSR). Although the African nation received limited aid from the USSR, scholars agree that the CAR can under no circumstance be considered a Soviet client state at any point in history.[9] The persistence of French influence, however, is undeniable. In 1979, the French military launched Operation Barracuda, an armed intervention that deposed the increasingly violent Emperor Bokassa and restored Dacko to power and the country to a presidential republic.[10] After the French had re-imposed Dacko, the CAR ceased all diplomatic relations with the USSR.[11]

In less than two years, Dacko was overthrown a second time, by a military junta led by André Kolingba. However, under increasing pressure from France and the United States, Kolingba agreed to hold new elections, which he consequently lost to Ange-Félix Patassé. Patassé – who gained power in 1993 – presided over three mutinies, a number of unsuccessful coup attempts and an exponential growth of ethnic and religious tensions. In response to the deteriorating domestic security situation, President Patassé requested the help of the international community to maintain law and order ahead of the 1998 legislative and 1999 presidential elections. In April 1998 the United Nations deployed a 1350-man strong peacekeeping force designated MINURCA – the United Nations Mission in the Central African Republic.[12] Following the relatively peaceful elections, the mandate of MINURCA was extended to February 2000 with the intention to aid government efforts to collect and dispose of small arms circulating in the country. Despite its initial success, MINURCA failed to create lasting peace in the Central African Republic. Less than a year after the peacekeepers' departure, rebels sieged the capital, Bangui. Consequently, in 2003 General François Bozizé overthrew Patassé, who was deemed too weak to expel the rebels from the country. As a response to Bozizé's takeover, in 2004 the Central African Republic Bush War broke out, which saw government forces – at times supported by the French military[13] – clash with a number of rebel groups, most notably the Union of Democratic Forces for Unity. Without any tangible results, the Central African Republic Bush War gradually became a frozen conflict by 2007.

---

8 MARCUM, Anthony S. – BROWN, Jonathan N.: Overthrowing the 'Loyalty Norm': The Prevalence and Success of Coups in Small-Coalition Systems, 1950 to 1999. *The Journal of Conflict Resolution,* 2016/2, pp. 256-282.

9 RAMANI 2021.

10 BAXTER, Peter. *France in Centrafrique*. Casemate Publishers, 2011.

11 SANGO, Ndjoni: RCA-Russie: L'historique Des Relations Bilatérales. Ndjoni Sango, 24 October 2019.

12 N.a.: Resolution 1159, adopted by the Security Council at its 3867th meeting, on 27 March 1998. United Nations Digital Library, 1998.

13 ISSA, Jean-Magloire: Central African Govt Signs Peace Accord with Rebels. Reuters, 13 April 2007.

The conflict boiled over following the fraudulent re-election of Bozizé in 2011. During the Central African Republic Civil War – as the ongoing conflict became known – a coalition of predominantly Muslim rebels, known as the Séléka, forced Bozizé into exile. His successor, President Michel Djotodia, a former leader of Séléka, took office in 2013. Interesting to note, that Djotodia lived in the Soviet Union and studied at the People's Friendship University of Russia, however, this had no tangible impact on the – at the time still dormant – CAR-Russian relations.[14] The exchange of power did not mean the end of the civil war. As religious tensions created a new axis of confrontation, the new adversary of the Séléka became the coalition of Christian militias, known as anti-Balaka. The conflict between the two factions is estimated to have created over 300,000 internally displaced persons and was at the time feared to escalate into a genocide.[15] In an effort to contain the situation and to incorporate the rebels into the Central African Armed Forces, Djotodia dissolved the Séléka. However, many rebels refused to disarm and subsequently formed the rebel coalition, known as ex-Séléka.[16] In response to the failure of domestic efforts to slow the spread of violence, in late 2013 the UN created the African Union (AU) led MISCA – *the African-led International Support Mission to the Central African Republic* – which deployed 6,000 peacekeepers.[17] In parallel to MISCA, the French launched Operation Sangaris, the seventy military intervention of the former colonial power in the CAR.[18] MISCA later transformed and expanded into MINUSCA - the *United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic*.[19] Note that MINUSCA, unlike its predecessor, was not an AU-led mission, instead its operational planning was headed by French General Stéphane Marchenoir which further fueled neo-colonial accusations. After the resignation of Djotodia, – and the interim presidency of Catherine Samba-Panza, the first-ever female leader of the CAR – Faustin-Archange Touadéra won the 2016 presidential elections. Touadéra was the prime minister under Bozizé and allowed no representative of either ex-Séléka or anti-Balaka in the new government.

To summarize, despite countless foreign interventions – both military and political in nature –, a number of UN peacekeeping missions and 60 years of constant domestic efforts to establish peace and functional statehood in the country, by 2018, the Central African Republic had become a *de facto* failed state.

---

14 MATUSEVICH, Maxim: Russia in Africa: A Search for Continuity in a Post-Cold War Era. *Insight Turkey,* 2019/1, pp. 25-40.

15 N.a.: Central African Republic – Regional Situation Map. UNHCR Operational Data Portal (ODP), 2014.

16 MARONEY, Mikenna– DOWNIE, Richard: France to the Rescue (Again) in the Central African Republic. Www.csis.org, 6 December 2013.

17 N.a.: Resolution 2127, adopted by the Security Council at its 7072nd meeting, on 5 December 2013, United Nations Digital Library, 2013.

18 HÉMEZ, Maj. Rémy: Operation Sangaris a Case Study in Limited Military Intervention. Army University Press, 2016.

19 N.a.: Resolution 2588 (2021), adopted by the Security Council at its 8828th meeting, on 29 July 2021, United Nations Digital Library, 2021.

The country is partitioned with the government having control over only the capital and its neighbouring provinces, while various rebel groups – some ex-Séléka and anti-Balaka, while others non-affiliated – hold the Eastern regions, accounting for over two-thirds of the territory of the CAR. According to estimates by the United Nations, in 2018, over 60 per cent of the population – 2.9 million people – was in need of humanitarian assistance, while 600,000 people – 13% – were internally displaced and approximately an equal amount fled to neighbouring countries.[20]

RUSSIAN INTERFERENCE IN THE CAR

The principal objective of the Russian Federation in the Central African Republic is to challenge the historically strong French influence in the country.[21] This aim can be explained by a number of factors, the predominant of which is the competitive nature of state actors and their inherent pursuit of power.[22] The Russian objective to undermine the French influence in the CAR is best described as foreign interference. According to the U.S. Department of Homeland Security, *foreign interference* is defined as efforts taken by foreign governments in an attempt to undermine or manipulate the political discourse and economic position of a sovereign state.[23]

Hedging Strategy

The CAR's long history – of spiralling instability and the United Nations' and France's undeniable and numerous failures to creating lasting peace – has provided fertile soil for Russian interference. Following a playbook that it had previously implemented in Libya,[24] the Russian state used a hedging strategy in the CAR and established close relations with rival factions of the African nation, namely with President Touadéra and a number of rebel leaders.[25]

President Touadéra

Russia first gained the support of President Touadéra in 2018, when Moscow successfully lobbied the United Nations to partially lift its arms embargo against the CAR, emplaced in 2013. After blocking a French attempt to supply small arms seized in Somalia, Russia donated light weaponry to the Central African Armed Forces (FACA), with the first shipment arriving in mid-January 2018.[26]

---

20 N.a.: Displaced in the Central African Republic: One Family's Journey of 600 Kilometers – Central African Republic. OCHA, 5 July 2019.

21 RAMANI 2021.

22 DONNELLY, Jack. *Oxford Handbooks Online*. *The Ethics of Realism*. 2023. Reprint, Oxford University Press, 2008.

23 N.a.: Foreign Interference Taxonomy. U.S. Department of Homeland Security, 2018.

24 ARNOLD, Thomas D.: Exploiting Chaos: Russia in Libya. www.csis.org, 2020.

25 RAMANI 2021.

26 ROSS, Aaron: How Russia Moved into Central Africa. Reuters, 17 October 2018.

Alongside this freight of arms, Moscow sent 170 Russian "civilian instructors" to train FACA and other domestic security forces.[27] These instructors were later confirmed to be the first batch of Russian private military contractors arriving in the country.[28]

Rebel leaders

According to a CAR government spokesperson, shortly after their arrival, the Russian military experts met a number of rebel leaders.[29] This claim is substantiated by the sighting of a single-engine Cessna 182 aeroplane in rebel hotspots such as Birao, Bria and Kabo in February 2018.[30] The plane in question – identified by its tail number RA-67717 – is the property of Business Project (Бизнес Проджект), a Russian company associated with the owner of the Wagner PMC, Yevgeny Prigozhin.[31] The Kremlin's use of contractors in the efforts to establish backchannels with rebel groups can be explained by the plausible deniability of PMCs. For example, on the 16th of February 2018, Cessna RA-67717 landed in the rebel-held city of Aliando and its passengers met with Ali Darassa, the leader of the insurgency group known as Unity for Peace (UPC).[32] The UPC and its leader are sanctioned by the UN for murder, torture and other abuses of human rights and violations of international humanitarian law.[33] Consequently, Russia could not establish formal relations with Ali Darassa. However, a supposedly non-existent private military company could meet a warlord and by doing so be *"a way of implementing national interests without the direct involvement of the state"* to use Vladimir Putin's words.[34]

---

27 N.a.: Ответ заместителя директора Департамента информации и печати МИД России А.А.Кожина на вопрос СМИ о развитии сотрудничества между Российской Федерацией и Центральноафриканской Республикой. [Response of the Deputy Director of the Information and Press Department of the Russian Ministry of Foreign Affairs A.A. Kozhin to a media question about the development of cooperation between the Russian Federation and the Central African Republic.] Ministry of Foreign Affairs of the Russian Federation, 2018.

28 SIGNER, David: Wie Russland Afrikanische Krisenländer Infiltriert. Neue Zürcher Zeitung, 28 May 2018.

29 KIRILENKO, Anastasia: Blood Diamonds. Who Killed Russian Journalists in the CAR, and What Do Putin's Chef and St Petersburg Police Have to Do with It? The Insider, 2018.

30 Ibid.

31 KRUTOV, Mark: Важнейшее из искусств. Самолет Пригожина сняли в фильме 'Турист.' [The Most Important of the Arts. Prigozhin's Plane Filmed titled "The Tourist".] *Radio Svoboda*, 21 May 2021.

32 KIRILENKO 2018.

33 N.a.: ALI DARASSA. United Nations Security Council, 21 December 2021.

34 N.a.: Russia May Consider Establishing Private Military Companies. Sputnik International, 2012.

As a result of this hedging strategy, in a period of one year, Russia became an *"indispensable diplomatic arbiter in CAR"*[35], which materialised in the February 2019 peace agreement signed by President Touadéra and leaders of 14 rebel groups including Ali Darassa and numerous other warlord visited by Cessna RA-67717.[36]

Valery Zakharov

An additional dimension of the Russian state's strategy to use PMCs as deniable diplomats is the appointment of Valery Zakharov. Zakharov – the suspected passenger of Cessna RA-67717 – is a former Russian Federal Security Service (FSB) operative, who became the national security advisor to President Touadéra in unknown circumstances, sometime in 2018.[37] According to the U.S. Embassy in the Central African Republic, Zakharov is a Wagner Group employee tasked with the coordination of the PMC and various domestic actors – with considerable influence over the CAR's security-related decisions – with Russian state interests.[38] Openly admitting a Wagner employee to a high-ranking advisory role is a clear indicator of substantial Russian influence in the Central African Republic. Furthermore, it is an additional explanation of the presence of Russian PMCs in the country.

Soft Power

To support and reinforce its newly established foothold in the country, the Kremlin developed an elaborated information warfare network to project Russian soft power over the Central African Republic.[39] In its simplest form, soft power – as opposed to hard power – archives results by persuasion, rather than coercion.[40] In the Central African Republic, Russian soft power is utilised for two ends: for creating an anti-French narrative and establishing a pro-Russian sentiment. *"Russia is not just about arms [...] Security can come only when we change people's lives. We must create positive ground."* – explained Valrey Zakharov the rationale behind the Russian attempt at winning hearts and minds.[41]

---

35 RAMANI 2021.

36 N.a.: Accord Pour La Paix et La Réconciliation En Centrafrique. Centre for Humanitarian Dialogue, 2019.

37 N.a.: COUNCIL DECISION Amending Decision (CFSP) 2020/1999 Concerning Restrictive Measures against Serious Human Rights Violations and Abuses. Council of the European Union, 2021.

38 N.a.: U.S. Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization. U.S. Embassy in Central African Republic, 26 January 2023.

39 DUKHAN, Nathalia: Central African Republic: Ground Zero for Russian Influence in Central Africa. 2020.

40 NYE, Joseph S.: Soft Power. *Foreign Policy,* 1990/80, pp. 153-171.

41 HUON, Patricia – OSTROVSKY, Simon: Russia, the New Power in Central Africa. Coda Story, 19 December 2018.

Conventional methods of information warfare

The best-known example of Russian soft power projection in the CAR is *Radio Lengo Songo*, a radio station funded by the Russian state through its embassy in the country.[42] However, other media outlets, such as *Le Confident*, *Le Potentiel* and *Les Collines de l'Oubangui* have also received Russian state funding.[43] These news sources project anti-Western propaganda, blaming the UN and France for the prolonged conflict and despair in the CAR. Their common tactic is to amplify allegations – of questionable legitimacy – against peacekeepers, such as cases of alleged child rape committed by French troops during Operation Sangaris.[44] These efforts paint France and the UN as neo-colonial powers.[45]

Unconventional methods of information warfare

In addition to these conventional methods of information warfare, the Russian state made good use of Prigozhin's infamous *troll farm,* the Internet Research Agency (IRA) commonly known for its attempt to influence the 2016 US presidential elections.[46] Although the Facebook has taken down a large number of fake accounts directly linked to IRA operations in the region, the *troll farm* continues to assist the Kremlin's efforts to establish a pro-Russian sentiment in the Central African Republic.[47] The situation is further complicated by the IRA's recruitment of local journalists, bloggers and university students. Referencing local reports, the Centre for Information Resilience identified a loose network of IRA-linked local assets spreading anti-Western propaganda often by falsely portraying news sites, NGOs and pro-Russian groups on social media platforms.[48]

Cultural diplomacy

Other efforts aimed at establishing a pro-Russian sentiment in the CAR include Russian state-funded social and cultural events, such as a beauty pageant, *Miss Centrafrique*[49], a football tournament, the *Cup of Hope*[50] as well as numerous drawing and poetry competitions.[51]

---

42 SCHIPANI, Andres – PILLING, David – ADEOYE, Aanu: How Russia's Propaganda Machine Is Reshaping the African Narrative. Financial Times, 9 February 2023.

43 DUKHAN 2020.

44 N.a.: Panel Slams UN Failure over Child Sex Abuse – DW – 12/17/2015. dw.com, 2015.

45 THOMAS, Elise: Russian Disinformation in the Central African Republic. Centre for Information Resilience, 8 June 2022.

46 Ibid.

47 GLEICHER, Nathaniel: Removing More Coordinated Inauthentic Behavior from Russia. Meta, 30 October 2019.

48 THOMAS 2022.

49 HUON – OSTROVSKY 2018.

50 N.a.: How to Capture a State. Africa Defense Forum, 10 November 2022.

51 N.a.: Russian Influence on Show in C. African Beauty Contest. France 24, 12 December 2018.

Unsurprisingly, there is no evidence to suggest that private military contractors had an indispensable role in either one of these events, although it was Valery Zakharov who crowned the winner of the beauty pageant in 2018.[52] The effectiveness of these efforts is hard to measure, nonetheless, it is safe to assume that their impact dwarfs in comparison to the multidimensional information warfare conducted by Kremlin-funded radio networks and the Internet Research Agency's social media campaigns.

Conclusion

To summarise, in a period of one year, the Kremlin successfully established a foothold in the Central African Republic. By 2019, the Russian Federation had brokered an extensive peace treaty, imposed a Wagner employee as a national security advisor to President Touadéra, and created a large and multi-dimensional network of information warfare, projecting Russian soft power. In the light of these facts, it can be concluded that the Russian Federation successfully challenged the French influence in the CAR. Furthermore, it can be stated that the Russian private military contractors played a significant role in the Russian state's efforts to alienate the African nation from its former colonial overlord. The contractors' role in the Kremlin's hedging strategy – as military trainers and deniable diplomatic liaisons – constitutes a rationale for the Russian state's use of PMCs in the country. Nevertheless, it has been shown that the Russian efforts to project soft power in the CAR do not require the use of PMCs. Instead, the Russian information warfare campaign is conducted by another Prigozhin-linked entity: the Internet Research Agency.

THE KREMLIN'S AIM AT THE CENTRAL AFRICAN REGION

Having discussed how the Russian state has established its influence in the Central African Republic – and the large extent to which PMCs contributed to these efforts – it is appropriate to continue with the investigation of the Kremlin's efforts to reproduce the same effect on a regional scale. Considering that this paper is a single-subject case study concerned with the CAR, this effort might seem counterintuitive. However, the Russian state is suspected to be using the CAR as a springboard to expand its influence in the region.[53] Therefore, the investigation of this aspect of the Kremlin's foreign policy might reveal other Russian efforts taken in the Central African Republic that may or may not necessitate the deployment of Russian PMCs, thus providing relevant information for this research.

---

52 DOLEŚNIAK-HARCZUK, Olga: How the Wagner Group and Others Spread Propaganda in Africa. FakeHunter, 2023.

53 RAMANI 2021.

Russia's Pursuit of its Great Power posture

Scholars agree that the paramount reason for the Russian objective to establish some level of influence in the Central African region is the Kremlin's pursuit of its *Great Power posture*.[54] *"For the first time in 200 to 300 years, Russia faces the real danger that it could be relegated to the second or even the third tier of global powers"* – warned his compatriots the then newly appointed Russian Prime Minister, Vladimir Putin in 1999.[55] Recognising the distressing state of the country's economy and the turbulent domestic political landscape of post-Soviet Russia, Putin foreshadowed the nation's uphill struggle to remain a first-tier or even second-tier global power in the 21st century. By doing so, Putin outlined what many scholars believe to be the defining foreign policy doctrine of post-Soviet Russia, its pursuit of a "Great Power posture".[56] It is a difficult task to specify what the labels of first, second, and third-tier global powers entail, but according to Professor Andrei Kokoshin – the director of the Center for Advanced Studies of National Security of Russia at the Russian International Affairs Council (RIAC) and a full member of the Russian Academy of Science – these correlate with the status of superpower, great power and regional power, respectively.[57] Kokoshin explains that "*after the tragic dissolution of the Soviet Union"* the United States became the only superpower.[58] This "mono-superpower" is described by its robust economy and its foreign policy is distinguishable by the ability to *"project force to practically any corner of the world*".[59] In contrast, great powers can project influence – not power – to any corner of the world, while regional powers can only do so in their close vicinity. Kokoshin is reluctant to define the difference between power and influence in absolute terms, but he distinguishes the two by their relative magnitude to one another. To summarise Kokoshin's trisection, the United States of America is the only first-tier global power, second-tier powers are those which can project their influence globally, and third-tier powers are those which can do so over their neighbouring countries. Therefore, if Russia wants to challenge the American hegemony or even remain a second-tier global power – as Putin outlined in 1999 – it must be able to project at least influence – if not power – to distant regions of the world, including Central Africa. This indigenous Russian understanding of the Kremlin's pursuit of its Great Power posture has been accepted by Western analysts without significant alterations.[60] However, in addition, scholars like Besenyő and Siegle highlight the importance of the African continent in this Russian foreign policy doctrine.

---

54 SIEGLE, Joseph: Decoding Russia's Economic Engagements in Africa. Africa Center for Strategic Studies, 2023.

55 PUTIN, Vladimir: Russia at the Turn of the Millennium. Nezavisimaia gazeta, 1999.

56 SIEGLE 2022.

57 KOKOSHIN, Andrei: What Is Russia: A Superpower, a Great Power or a Regional Power. *International Affairs (Moscow),* 2002/6, pp. 100-125.

58 Ibid.

59 Ibid.

60 SIEGLE 2022.

They argue that Africa is an "attractive theatre" for Russia to further its claim for the title of first-tier global power because of the continent's vast size - accounting for 54 votes in the UN General Assembly and the – perceived or real – presence of a strong anti-colonial sentiment amongst African nations.[61,62] Moreover, in the past two years, the significance of the continent is expected to have further appreciated in the eyes of the Kremlin, due to Russia's increasing isolation within the international community, after its renewed invasion of Ukraine.

Autocracy Promotion

In order to achieve its desired influence in the Central African region, the Russian state has adopted a strategy of autocracy promotion.[63] As defined by Kästner, a foreign nation's deliberate attempts to conserve an autocratic regime or to slow down its democratisation constitute autocracy promotion.[64] Therefore, the Russian foreign policy in the Central African region does not focus on countries per se, instead, it creates reliable and long-term partnerships with indebted autocratic regimes whose grip on power is heavily promoted – if not ensured – by the Kremlin.[65] Russian autocracy promotion targets most Central African regimes, however, it is most prominent in the CAR, and therefore it is an ideal case study with regional implications. Autocracy promotion in practice can be relatively subtle - such as by means of diplomatic support – or outright kinetic – for example taking the form of a military intervention. In the Central African Republic, Russia utilised almost the full spectrum of autocracy promotion.

Support within the international community

As a permanent member of the Security Council, Russia has considerable power within the framework of the United Nations. Experts believe that the least intrusive way in which the Kremlin practises autocracy promotion is by hindering the effectiveness of UN sanctions against autocratic regimes it is allied with and by doing so projecting itself as *"the beleaguered regime's defender"*.[66] For example, in 2021, the Russian Federation blocked the appointment of UN experts to monitor and evaluate sanctions imposed on the Central African Republic.[67] This decision forestalled UN efforts to tighten the sanctions against the CAR's autocratic government, hence facilitating the regime's endurance.

---

61 BESENYŐ, János. The Africa Policy of Russia. *Terrorism and Political Violence*, 2019/1, pp. 132-153.

62 SIEGLE 2022.

63 RAMANI, Samuel: *Russia in Africa*: *Resurgent Great Power or Bellicose Pretender?* Reprint, Oxford University Press, 2023.

64 KÄSTNER, Antje: Autocracy Promotion. *The Handbook of Political, Social, and Economic Transformation*, 13 February 2019, pp. 411–415.

65 RAMANI 2023

66 SIEGLE 2022.

67 LEDERER, Byedithm: UN Diplomats: Russia Is Blocking Sanctions Experts in Africa. AP News, 30 September 2021.

Although, for the sake of due diligence, this aspect of autocracy promotion had to be noted, the Russian support of President Touadera's regime within the framework of the international community does not involve private military contractors. Therefore its relevance is limited in the context of this paper.

Information warfare

An alternative method of autocracy promotion is the use of soft power. As previously discussed the Russian state is familiar with both conventional and more unorthodox tools of information warfare, ranging from radio stations to troll farms and beauty pageants. According to the U.S. Africa Command, Russia was able to bolster support for President Touadera within the Central African Republic in a similar fashion and by utilising the same network of Moscow-funded local and cyber assets that it has used to create a pro-Russian and anti-Western sentiment.[68] Regarding the use of information warfare as a method of autocracy promotion, the same observation can be noted here as in the case of deploying the strategy as a tool of soft power projection with the aim to undermine the French influence in the country. The methods of Russian information warfare in the Central African Republic do not involve private military contractors, therefore this strategy cannot explain the presence of Russian PMCs in the country.

Coup-proofing

In the absence of an outright Russian military intervention – similar to the French Operation Barracuda and Sangaris – the most kinetic method of autocracy promotion deployed by Moscow in the CAR is the coup-proofing of President Touadera's regime. However, this study discusses the Kremlin's on-the-ground efforts to aid and abet the survival of the Touadéra regime by coup-proofing it as a local incentive for the presence of Russian private military contractors in the Central African Republic. Therefore it is discussed in the third paper of this series.

Conclusion

To conclude, the Kremlin's overarching objective to reinforce its *Global Power posture* and its consequent desire to establish some level of Russian influence in the Central African region manifests itself in the form of autocracy promotion. It has been established that most forms of autocracy promotion do not provide an explanation for the presence of Russian PMCs in the CAR. However, the most direct form of autocracy promotion has been neglected in this essay as the coup-proofing of President Touadéra's regime is discussed in the third essay of this series.

---

[68] N.a.: CAR at Center of Russian Disinformation Effort. Africa Defense Forum, 29 March 2022.

Bibliography:

ARMSTRONG, Kathryn: Niger Coup: Wagner Taking Advantage of Instability – Antony Blinken. BBC News, 8 August 2023, Online: https://www.bbc.com/news/world-africa-66436797 (Download time: 04/13/2024)

ARNOLD, Thomas D.: Exploiting Chaos: Russia in Libya. www.csis.org, 2020, Online: https://www.csis.org/blogs/post-soviet-post/exploiting-chaos-russia-libya (Download time: 04/13/2024)

ARVANITIDIS, Barbara – ELBAGIR, Nima – MEZZOFIORE, Gianluca – QIBLAWI, Tamara: Exclusive: Evidence Emerges of Russia's Wagner Arming Militia Leader Battling Sudan's Army. CNN, 20 April 2023, Online: https://edition.cnn.com/2023/04/20/africa/wagner-sudan-russia-libya-intl/index.html (Download time: 04/13/2024)

BAXTER, Peter. *France in Centrafrique*. Casemate Publishers, 2011.

BESENYŐ, János. The Africa Policy of Russia. *Terrorism and Political Violence*, 2019/1, pp. 132-153. https://doi.org/10.1080/09546553.2018.1555976.

DOLEŚNIAK-HARCZUK, Olga: How the Wagner Group and Others Spread Propaganda in Africa. FakeHunter, 2023, Online: https://fake-hunter.pap.pl/node/96 (Download time: 04/13/2024)

DONNELLY, Jack. *Oxford Handbooks Online*. *The Ethics of Realism*. 2023. Reprint, Oxford University Press, 2008. https://doi.org/10.1093/oxfordhb/9780199219322.003.0008.

DUKHAN, Nathalia: Central African Republic: Ground Zero for Russian Influence in Central Africa. 2020, Online: https://www.atlanticcouncil.org/wp-content/uploads/2020/10/CAR-Russian-Influence-Final.pdf (Download time: 04/13/2024)

GLEICHER, Nathaniel: Removing More Coordinated Inauthentic Behavior from Russia. Meta, 30 October 2019, Online: https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-russia/ (Download time: 04/13/2024)

HÉMEZ, Maj. Rémy: Operation Sangaris a Case Study in Limited Military Intervention. Army University Press, 2016, Online: https://www.armyupress.army.mil/Portals/7/military-review/documents/Military-Review-20161231-art014.pdf (Download time : 04/13/2024)

HUON, Patricia – OSTROVSKY, Simon: Russia, the New Power in Central Africa. Coda Story, 19 December 2018, Online: https://www.codastory.com/disinformation/russia-new-power-central-africa/ (Download time: 04/13/2024)

ISSA, Jean-Magloire: Central African Govt Signs Peace Accord with Rebels. Reuters, 13 April 2007, Online: https://www.reuters.com/article/idUSL13397290 (Download time: 04/13/2024)

KALCK, Pierre: *Historical Dictionary of the Central African Republic*. Scarecrow Press, Lanham, Md. 2005.

KÄSTNER, Antje: Autocracy Promotion. *The Handbook of Political, Social, and Economic Transformation*, 13 February 2019, pp. 411–415. https://doi.org/10.1093/oso/9780198829911.003.0036.

KATZ, Brian – JONES, Seth G. – DOXSEE, Catrina – HARRINGTON, Nicholas: Moscow's Mercenary Wars: The Expansion of Russian Private Military Companies. Moscow's Mercenary Wars: The Expansion of Russian Private Military Companies, September 2020, Online: https://russianpmcs.csis.org/ (Download time: 04/13/2024)

KIRILENKO, Anastasia: Blood Diamonds. Who Killed Russian Journalists in the CAR, and What Do Putin's Chef and St Petersburg Police Have to Do with It? The Insider, 2018, Online: https://theins.ru/en/uncategorized/114123 (Download time: 04/13/2024)

KOKOSHIN, Andrei: What Is Russia: A Superpower, a Great Power or a Regional Power. *International Affairs (Moscow),* 2002/6, pp. 100-125, Online: https://ciaotest.cc.columbia.edu/olj/iarj/iarj_02_06a.html (Download time: 04/13/2024)

KRUTOV, Mark: Важнейшее из искусств. Самолет Пригожина сняли в фильме 'Турист.' *Радио Свобода*, 21 May 2021, Online: https://www.svoboda.org/a/samolet-prigozhina-film-turist/31265549.html (Download time: 04/13/2024)

LEDERER, Byedithm: UN Diplomats: Russia Is Blocking Sanctions Experts in Africa. AP News, 30 September 2021, Online: https://apnews.com/article/europe-middle-east-africa-russia-united-nations-5736d78d22ec648198dfab74600d9132 (Download time: 04/13/2024)

MARCUM, Anthony S. – BROWN, Jonathan N.: Overthrowing the 'Loyalty Norm': The Prevalence and Success of Coups in Small-Coalition Systems, 1950 to 1999. *The Journal of Conflict Resolution,* 2016/2, pp. 256-282, Online: https://www.jstor.org/stable/24755911 (Download time: 04/13/2024)

MARONEY, Mikenna– DOWNIE, Richard: France to the Rescue (Again) in the Central African Republic. Www.csis.org, 6 December 2013, Online: https://www.csis.org/analysis/france-rescue-again-central-african-republic (Download time: 04/13/2024)

MATUSEVICH, Maxim: Russia in Africa: A Search for Continuity in a Post-Cold War Era. *Insight Turkey,* 2019/1, pp. 25-40, Online: https://www.jstor.org/stable/26776045 (Download time: 04/13/2024)

N.a.: Accord Pour La Paix et La Réconciliation En Centrafrique. Centre for Humanitarian Dialogue, 2019, Online: https://www.hdcentre.org/wp-content/uploads/2019/02/Accord-pour-la-paix-et-la-r%C3%A9conciliation-en-Centrafrique.pdf (Download time: 04/13/2024)

N.a.: ALI DARASSA. United Nations Security Council, 21 December 2021, Online: https://www.un.org/securitycouncil/content/ali-darassa (Download time: 04/13/2024)

N.a.: CAR at Center of Russian Disinformation Effort. Africa Defense Forum, 29 March 2022, Online: https://adf-magazine.com/2022/03/car-at-center-of-russian-disinformation-effort/ (Download time: 04/13/2024)

N.a.: Central African Republic - Regional Situation Map. UNHCR Operational Data Portal (ODP), 2014, Online: https://data.unhcr.org/en/documents/details/32492 (Download time: 04/13/2024)

N.a.: COUNCIL DECISION Amending Decision (CFSP) 2020/1999 Concerning Restrictive Measures against Serious Human Rights Violations and Abuses. Council of the European Union, 2021, Online: https://data.consilium.europa.eu/doc/document/ST-14536-2021-INIT/en/pdf (Download time: 04/13/2024)

N.a.: Displaced in the Central African Republic: One Family's Journey of 600 Kilometers - Central African Republic. OCHA, 5 July 2019, Online: https://reliefweb.int/report/central-african-republic/displaced-central-african-republic-one-family-s-journey-600 (Download time: 04/13/2024)

N.a.: Foreign Interference Taxonomy. U.S. Department of Homeland Security, 2018, Online: https://www.cisa.gov/sites/default/files/publications/19_0717_cisa_foreign-influence-taxonomy.pdf (Download time: 04/13/2024)

N.a.: How to Capture a State. Africa Defense Forum, 10 November 2022, Online: https://adf-magazine.com/2022/11/how-to-capture-a-state/ (Download time: 04/13/2024)

N.a.: Panel Slams UN Failure over Child Sex Abuse – DW – 12/17/2015. dw.com, 2015, Online: https://www.dw.com/en/panel-slams-un-for-gross-institutional-failure-to-act-on-car-child-sex-allegations/a-18925783 (Download time: 04/13/2024)

N.a.: Resolution 1159, adopted by the Security Council at its 3867th meeting, on 27 March 1998. United Nations Digital Library, 1998, Online: https://digitallibrary.un.org/record/251948#record-files-collapse-header (Download time: 04/13/2024)

N.a.: Resolution 2127 (2013), adopted by the Security Council at its 7072nd meeting, on 5 December 2013, United Nations Digital Library, 2013, Online: https://digitallibrary.un.org/record/761853?ln=en (Download time: 04/13/2024)

N.a.: Resolution 2588 (2021), adopted by the Security Council at its 8828th meeting, on 29 July 2021, United Nations Digital Library, 2021, Online: https://digitallibrary.un.org/record/3933992?ln=en (Download time: 04/13/2024)

N.a.: Russia May Consider Establishing Private Military Companies. Sputnik International, 2012, Online: https://sputnikglobe.com/20120412/172789099.html (Download time: 04/13/2024)

N.a.: Russia's Strategic Goals in Africa. Africa Center for Strategic Studies, 2021, Online: https://africacenter.org/experts/joseph-siegle/russia-strategic-goals-africa/ (Download time: 04/13/2024)

N.a.: Russia's Use of Private Military Contractors. Africa Center for Strategic Studies, 2022, Online: https://africacenter.org/experts/russia-private-military-contractors/#_ednref2 (Download time: 04/13/2024)

N.a.: Russian Influence on Show in C. African Beauty Contest. France 24, 12 December 2018, Online: https://www.france24.com/en/20181212-russian-influence-show-c-african-beauty-contest (Download time: 04/13/2024)

N.a.: U.S. Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization. U.S. Embassy in Central African Republic, 26 January 2023, Online: https://cf.usembassy.gov/treasury-sanctions-russian-proxy-wagner-group-as-a-transnational-criminal-organization/ (Download time: 04/13/2024)

N.a.: Ответ заместителя директора Департамента информации и печати МИД России А.А.Кожина на вопрос СМИ о развитии сотрудничества между Российской Федерацией и Центральноафриканской Республикой. Ministry of Foreign Affairs of the Russian Federation, 2018. Online: https://archive.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3136399 (Download time: 04/13/2024)

NYE, Joseph S.: Soft Power. *Foreign Policy,* 1990/80, pp. 153-171. Online: https://www.jstor.org/stable/1148580 (Download time: 04/13/2024)

PONGRACZ, Bálint: WHAT ARE the REASONS for the PRESENCE of RUSSIAN PRIVATE MILITARY COMPANIES on the AFRICAN CONTINENT? *National Security Review,* 2023/1, pp. 80-106, Online: https://www.knbsz.gov.hu/hu/letoltes/szsz/2023_1_NSR.pdf (Download time: 04/13/2024)

PUTIN, Vladimir: Russia at the Turn of the Millennium. Nezavisimaia gazeta, 1999, Online: https://rl.talis.com/3/glasgow/items/7BACF97D-03C7-B04A-813B-5633F95A051D.html (Download time: 04/13/2024)

RAMANI, Samuel: *Russia in Africa*: *Resurgent Great Power or Bellicose Pretender?* Reprint, Oxford University Press, 2023. ISBN: 978-0197744598

RAMANI, Samuel: Russia's Strategy in the Central African Republic. Royal United Services Institute, 2021, Online: https://rusi.org/explore-our-research/publications/commentary/russias-strategy-central-african-republic (Download time: 04/13/2024)

ROSS, Aaron: How Russia Moved into Central Africa. Reuters, 17 October 2018, Online: https://www.reuters.com/article/us-africa-russia-insight-idUSKCN1MR0KA (Download time: 04/13/2024)

SANGO, Ndjoni: RCA-Russie: L'historique Des Relations Bilatérales. Ndjoni Sango, 24 October 2019, Online: https://ndjonisango.com/2019/10/24/rca-russie-lhistorique-des-relations-bilaterales/ (Download time: 04/13/2024)

SCHIPANI, Andres – PILLING, David – ADEOYE, Aanu: How Russia's Propaganda Machine Is Reshaping the African Narrative. Financial Times, 9 February 2023, Online: https://www.ft.com/content/d427c855-c665-4732-9dd1-3ae314464d12 (Download time: 04/13/2024)

SIEGLE, Joseph: Decoding Russia's Economic Engagements in Africa. Africa Center for Strategic Studies, 2023, Online: https://africacenter.org/spotlight/decoding-russia-economic-engagements-africa/ (Download time: 04/13/2024)

SIGNER, David: Wie Russland Afrikanische Krisenländer Infiltriert. Neue Zürcher Zeitung, 28 May 2018, Online: https://www.nzz.ch/international/wie-russland-afrikanische-krisenlaender-infiltriert-ld.1389297?reduced=true (Download time: 04/13/2024)

THOMAS, Elise: Russian Disinformation in the Central African Republic. Centre for Information Resilience, 8 June 2022, Online: https://www.info-res.org/post/russian-disinformation-in-the-central-african-republic (Download time: 04/13/2024)

VANESSA MARTINS

ROLE OF LOGISTICS IN DEFENCE ADMINISTRATION: AN OVERVIEW AMONG THE DIFFERENCES BETWEEN HUNGARY AND BRAZIL

Abstract

Logistics is a word to refer to the process of planning, implementing and controlling the raw material and resources' flow, but also the personnel, equipment, and it supplies in the civilian and the military perspectives. Defence administration, also known as defence management or defence administration management, refers to the strategic planning, organisation and coordination as well as to the oversight of defence-related activities within a country. It aims to develop and implement policies, plans and procedures to ensure the effective and efficient functioning of the defence capabilities of the nation. The primary goal of defence administration is to safeguard the nation's security and protect its interests. It is widely recognised that logistics and supply chains play a critical role in defence administration by ensuring the efficient and effective resources' flow, including personnel, information, supplies and equipment to support military operations. Logistics – encompassing the meticulous planning, execution and regulation of resources' flow into the domain of defence administration, and the strategic coordination, organisation and supervision of defence-related activities within a nation – represents a crucial and vital activity. This paper examines the logistics and the defence administration theories of two different nations such as Hungary and Brazil; while distinct nuances come to the fore. Hungary, as a landlocked country with unique geopolitical challenges, the logistics defence may focus on the cross-border transportation and strategic partnerships with neighbouring countries. In contrast, with its vast and diverse landscape, Brazil might prioritise logistics strategies that can address challenges, posed by expansive terrains and diverse climates. The aim of logistics in defence administration is linked to national security objectives in both Hungary and Brazil. While specific challenges and priorities may differ between the two countries, due to their geopolitical contexts, the effective logistics management is essential to maintain military readiness, fulfil alliance commitments, protect critical infrastructure and respond to emergencies or security threats. In addition to contributing to global and national security and stability.

Keywords: Logistics, Defence Administration, Public Administration, Brazil, Hungary

Introduction

Logistics implicates the process of planning, implementing and controlling the efficient, effective flow and storage of goods, services, and the related information from the point of origin to point of consumption, for the purpose of conforming to customer requirements.

It comprises the management of raw materials' flow to finished goods through an organisation. Logistics means planning and organising activities that ensure that resources are in place, so that the process can be effectuated accordingly, in an efficient and effective manner.[1]

On the other hand, Logistics is responsible for maintaining and repairing military equipment to ensure operational readiness. Logistics could be also understood as a source of indication of the need to create alternative military equipment to serve certain areas, for example, forests and regions where rivers predominate. This includes routine maintenance as well as addressing damage incurred during operations. Other great examples are Logistics supporting military personnel's movement and well-being, including recruitment, training, and personnel management. Medical logistics ensures the availability of medical supplies, facilities and personnel to support the health and well-being of military personnel. Logistics plays a role in establishing and maintaining communication networks to facilitate the flow of information between different military units and command centres. Protecting sensitive information is crucial, and logistics helps establish secure systems and protocols for data management.

Lastly, collaborating with other nations on defence-related matters is essential, including military alliances, security agreements and cooperative efforts to address common challenges. Developing plans and capabilities to respond to crises, emergencies, or conflicts, both domestically and internationally are indispensable. In simple terms, Logistics is essential. It ensures that military forces are supplied, supported and sustained efficiently and on time. Effective logistics systems contribute to the overall readiness and success of military operations.

The Defence Logistics in Hungary

According to information available on the Hungary government website of the Ministry of Defence, the Hungarian Defence Forces General Staff Logistics Directorate (J-4) holds a departmental status within the Ministry of Defence. This organisation operates at the level of the Ministry and reports directly to the Chief of Defence of the Hungarian Defence Force (referred to as CHOD). The activities of the J-4 are overseen by the CHOD, and the Chief of the Directorate is responsible for leading the J-4, which comprises three distinct branches:

[1] MELLAT-PARAST, M. – SPILLAN, J. E.: Logistics and supply chain process integration as a source of competitive advantage: An empirical analysis. *The International Journal of Logistics Management*, 2014/2, p. 289-314.

Logistics, Operation Support, and Planning

The J-4 plays a crucial role by advising the CHOD and the Director of Staff (DOS) of the Hungarian Defence Forces General Staff on matters related to logistics. Additionally, it maintains communication with the civil administration of the Ministry of Defence and collaborates with other governmental organisations within its professional domain. The J-4 is responsible for strategic-level logistic planning and serves as the primary Point of Contact (POC) in bilateral and multilateral relations. concerning logistics at the strategic level. Furthermore, the J-4 actively engages in logistic coordination with NATO and the European Union, particularly in connection with international military tasks, related to consumer logistics.

The J-4 Division is responsible for managing the Defence Forces' Consumer Logistic System, preparing logistic decisions for the Chief of Defence (CHOD), and establishing military logistic requirements. It develops support plans for operations, coordinates logistic tasks for the Armed Forces, and oversees training and education programs for logistics personnel. Additionally, the J-4 provides analyses on budget management and represents Hungarian Defence Forces logistics in international forums, including NATO and EU discussions, ensuring efficient and effective logistics support.

The Logistics Branch plays a key role in ensuring efficient planning and execution of logistics within the Hungarian Defence Forces by advising the Chief of J-4 and CHOD on budgetary matters, coordinating both annual and long-term logistic budget planning, and analyzing essential budgetary aspects to support military readiness and effectiveness.

The Operation Support Branch focuses on strategic logistic planning for home defence operations, coordinating support for HDF units abroad, managing logistics for domestic and international exercises, planning Host Nation Support (HNS), and supporting disaster relief efforts. Meanwhile, the Planning Branch handles internal J-4 coordination, oversees logistic training and doctrine updates, and manages HNS issues at the defence staff level, including for the Strategic Airlift Capability (SAC) Programme. Together, these branches ensure the effective planning, coordination, and execution of logistics within the Hungarian Defence Forces.

The Defence Logistics in Brazil

Defence Logistics Base consists of an infrastructure centred on educational, scientific-technological and industrial capacity, capable of generating innovations and meeting all types of resource's demands for the defence system.[2] The Defence Logistics Policy Manual (PLD) serves as the Ministry of Defence's highest-level logistics planning document, guiding strategic planning to ensure the Armed Forces fulfill their constitutional and subsidiary roles.

---

2 Brick 2011.

Its objectives include reducing the technological gap with developed nations, minimizing international dependence on defence products, enhancing the Armed Forces' capacity to absorb mobilized resources, improving the efficiency and interoperability of logistics systems, and fostering societal awareness of national defence needs. As outlined in Manual MD 42 M–02, the policy aims to provide continuous logistical support from peacetime to war by ensuring resources are available in appropriate quantities, quality, timing, and locations. It emphasizes financial flexibility and acknowledges the unique characteristics of each Force without segregating Military Logistics into distinct systems.

Within the context of the Brazilian Army, from a doctrinal perspective, logistics are addressed in the C 100-10 Campaign Manual.[3] This manual underscores the strategic importance of military ground logistics. For example, the operational logistics covers critical areas including the supply of consumables (e.g., food, medications), ammunition, energy, spare parts, and maintenance of equipment and infrastructure. It also addresses health care for personnel and animals and emphasizes effective management through strategic planning and coordination. In defence equipment logistics, technological intelligence integrates innovation, manufacturing, mobilisation of civilian resources, personnel recruitment and training, and equipment management. These elements aim to enhance operational readiness, leverage advanced technologies, ensure resource availability, and maintain a skilled workforce to support both defence activities and transitions to civilian roles when needed.

Among the main logistical challenges that the Brazilian Army must adequately face is the need to supply detached platoons in distant corners of the Brazilian territory, and humanitarian missions in different regions of the world. Another challenge is to manage the logistics necessary to maintain investments in technologically complex systems and products of high strategic value, such as monitoring and surveillance systems to be used in the Brazilian border. Furthermore, formulating public policies and governmental initiatives grounded in territorial considerations proves pivotal for fostering regional development in the Amazon. Recognising the Brazilian Army's important role in ensuring that government actions and public policies are carried out effectively is essential. To improve the support system, especially in the Amazon area, they need to make important management changes, specifically in logistics and transportation systems. These steps are essential to make military operations in the area more flexible and effective.[4]

---

3 Manual de campanha: Logística militar terrestre. 2. ed. [Manual: Ground military Logistics.] Ministério da Defesa Exército, Comando de Operações Terrestres, Brasília, DF, 2003. C 100-10.

4 DA COSTA PEREIRA, A.: Logística da defesa: fundamentos da gestão de processos logísticos e transformação no Exército Brasileiro. [Defense logistics: fundamentals of logistics process management and transformation in the Brazilian Army.] *Coleção Meira Mattos: revista das ciências militares*, 2019/48, p. 301-320.

The importance of security related to Logistics Administration

Effective logistics systems are crucial for maintaining the defence capabilities of both Hungary and Brazil, ensuring the mobilisation, deployment, and support of military forces to address potential threats and safeguard national security. In Brazil, logistics is vital for managing its vast and diverse territory, enabling the Armed Forces to handle challenges like border security, anti-narcotics operations, and infrastructure protection. Hungary, as a NATO member, focuses on protecting critical infrastructure, such as transport hubs and communication networks, while adhering to NATO's logistics standards and ensuring resilience against threats like cyberattacks and sabotage.

Brazil's defence logistics supports its participation in international peacekeeping and humanitarian missions, adding complexity to its operations. Logistics management involves the efficient use of diverse infrastructure, including ports, roads, and airports, while coordinating with the Centre for Coordination of Logistics and Mobilization (CCLM) to streamline joint transport efforts. Hungary's logistics framework emphasizes NATO-aligned procedures to secure supply lines and routes in regions with potential threats, particularly where allied forces are deployed.

In both nations, logistics management plays a pivotal role in emergency response and crisis management, enhancing national resilience. Brazil's logistical capabilities are crucial for disaster relief and supporting civil authorities during floods and other crises, ensuring rapid and coordinated responses. Similarly, Hungary's logistics system facilitates swift mobilisation of resources for natural disasters and security crises. Overall, the effectiveness of logistical systems directly impacts the success of military operations, underscoring their essential role in national security strategies.

Conclusion

Defence logistics and technological innovation are crucial in shaping strategies to address evolving threats and opportunities while integrating with broader public policies and administrative frameworks. Both Brazil and Hungary illustrate how logistics systems must adapt to unique geographical and political contexts. Brazil's vast and varied landscape, including dense rainforests, urban centres, and coastal regions, requires a robust and flexible logistics network to navigate diverse terrains and environmental challenges. In contrast, Hungary, a landlocked European nation, emphasizes land-based transportation and interoperability with NATO forces, leveraging a well-developed regional infrastructure.

Brazil's defence logistics operations are extensive, supporting a larger military force and diverse international engagements, including UN peacekeeping and humanitarian missions. The nation relies on centralised command structures for planning, procurement, and coordination to manage the complexities of its vast territory.

Hungary, with a smaller military force, prioritises efficiency and cost-effectiveness, aligning its logistics closely with NATO frameworks. This focus on standardisation and joint operational readiness reflects Hungary's regional security priorities and allied commitments.

Both nations underscore the importance of integrating human, technological, scientific, and industrial resources into their defence logistics systems. Brazil's logistics must address the infrastructural challenges of remote regions like the Amazon, while Hungary benefits from Europe's advanced transportation networks to support military deployments. A comprehensive approach to logistics ensures readiness and resilience, adapting to each country's unique challenges and opportunities to sustain their defence capabilities effectively.

Bibliography:

BRICK, E. S.: A conceptual framework for defense logistics. *Gestão & Produção*, 2019/4, p. 2358-8586, DOI: 10.1590/0104-530X4062-19

BRICK, E. S.: *Base Logística de Defesa: conceituação, composição e dinâmica de funcionamento*. [Defense Logistics Base: conceptualization, composition and operating dynamics.] V Encontro Nacional da Associação Brasileira de Estudos de Defesa V ENABED, Fortaleza. 2011. Online: https://defesa.uff.br/wp-content/uploads/sites/342/2020/11/Base-Logstica-de-Defesa.pdf (Download time: 2023. 10. 05.)

DA COSTA PEREIRA, A.: Logística da defesa: fundamentos da gestão de processos logísticos e transformação no Exército Brasileiro. [Defense logistics: fundamentals of logistics process management and transformation in the Brazilian Army.] *Coleção Meira Mattos: revista das ciências militares*, 2019/48, p. 301-320. DOI: 10.22491/cmm.a018

MELLAT-PARAST, M. – SPILLAN, J. E.: Logistics and supply chain process integration as a source of competitive advantage: An empirical analysis. *The International Journal of Logistics Management*, 2014/2, p. 289-314. DOI: 10.1108/IJLM-07-2012-0066

N.a.: Doutrina de logística militar – Manual MD42-M-02. [Military logistics doctrine – MD42-M-02.] EMCFA, Brasília, DF: 2001.

N.a.: Manual de campanha: Logística militar terrestre. 2. ed. [Manual: Ground military Logistics.] Ministério da Defesa Exército, Comando de Operações Terrestres, Brasília, DF, 2003. C 100-10.

Portaria Normativa nº 614/MD, de 24 de outubro de 2002 (dispõe sobre a Doutrina de Logística Militar – MD 42-M-02) [Normative Ordinance No. 614/MD, of October 24, 2002 (provides for the Military Logistics Doctrine – MD 42-M-02)]

Portaria Normativa nº 1.890/MD, de 29 de dezembro de 2006 (dispõe sobre a Política de Logística de Defesa – PLD) [Normative Ordinance No. 1,890/MD, of December 29, 2006 (provides for the Defense Logistics Policy - PLD)]

SZEGEDI, Z. – PREZENSZKI, J.: Logisztika-menedzsment. [Logistics management.] Kossuth Kiadó, Budapest, 2010.

JÓZSEF ANDRÁS ÜVEGES

FORMS AND RISKS OF PERSONAL DATA APPEARING ON THE DARKWEB AND SURFACE WEB ILLEGALLY, NEGLIGENTLY OR INTENTIONALLY I.

Abstract

One of the most risky areas of our digital life is the internet communication and the sharing and the use of personal data, because the personal data of each user can be used against the person himself. Internet users generally do not expect their personal information to become public, but when it does happen, they are not prepared for the consequences of such a leak. Our personal data are traded daily by cybercriminal groups, and our miscreants may upload our personal data to social networks, in order to denigrate us. In the article, I present where and in what form our personal data appear in the digital space. This article presents the first part of the entire research, where we discuss the holistic approach employed to the subject matter, and we try to present its legal and methodological background.

Keywords: CyberSecurity, DarkWeb, DarkNet, SurfaceWeb

Introduction

Cybercrime and the electronic handling or using of the personal data are causing more and more problems in cyberspace present day. The transformation of the digital economy and society creates opportunities, challenges and naturally risks. The cyber protection, as well as the protection of our personal data are increasingly important, both socially and personally. In more and more cases, we see that the institutions and the authorities of the European Union – such as the European Commission, the European Union Cybersecurity Agency (ENISA), the computer emergency response team of the Union (Cert-EU[1]), or EUROPOL,[2] are drawing attention to the importance of cyber protection for the population and the businesses. ITGovernance's 2023 data also clearly illustrate this problem.

[1] The Computer Emergency Response Team for the EU institutions, bodies and agencies https://cert.europa.eu/

[2] European Police Office

	Organisation name	Sector	Location	Known records breached	Month of public disclosure
1	DarkBeam	Cyber security	UK	>3,800,000,000	September
2	Real Estate Wealth Network	Construction/ real estate	USA	1,523,776,691	December
3	Indian Council of Medical Research (ICMR)	Healthcare	India	815,000,000	October
4	Kid Security	IT services/ software	Kazakhstan	>300,000,000	November
5	Twitter (X)	IT services/ software	USA	>220,000,000	January
6	TuneFab	IT services/ software	Hong Kong	>151,000,000	December
7	Dori Media Group	Media	Israel	>100 TB*	December
8	Tigo	Telecoms	Hong Kong	>100,000,000	July
9	SAP SE Bulgaria	IT services/ software	Bulgaria	95,592,696	November
10	Luxottica Group	Manufacturing	Italy	70,000,000	May

Figure 1: IT Governance's 2023 data Top ten data breaches in 2023[3]

When using the Internet, we share personal data and other information, in some cases this happens automatically without our knowledge. A digital presence creates digital footprint,[4] which contains personal data. Unauthorized access to personal data or other information poses serious risks to all users.

In my article, I present and organize how and in what system our personal data are displayed in two different layers of the Internet. In addition, I present the results of our research, the purpose of which is to draw attention to the fact that unauthorized access to our personal data poses a serious security risk for us. In the research, we can also see that cybercriminals can do this in an easy way, since some of our personal data can be bought on the Internet.[5]

[3] Source: N.a.: List of Data Breaches and Dyber Attacks in 2023 – 8,214,886,660 records breached. IT Governance, 5 January 2024

[4] Decisively the traces generated in the online space are also called internet footprints, cyber or digital shadows. These virtual footprints are also created when using a mobile phone, coming into the field of view of biometric sensors, or when monitoring our internet habits. The essential element in this is that these signals can be linked to the pattern of our activity.

[5] N.a.: What is Digital Footprint? malwarebytes.com

A scientific problem

In different layers of the Internet, the personal data can be found in different ways and in different amounts and forms. While on the open Internet in the classical sense,[6] less and more imprecise data can be found, until then on the DeepWeb[7] and in the DarkWeb,[8] a large amount of active (valid) data can already be found, or it can even be purchased illegally (figure below).

The 2020 figure below clearly shows how high the demand for our data really is, and it is basically for information only;

Figure 2: How much do our data cost?[9]

How much do our data cost?

Credit card data: 6-20 USD
Scanned driving licence: 525 USD
Scanned passport: 5-15 USD
Subscription services: 0,5-8 USD
Personal data (full name, social security number, date of birth, email adress, mobile phone number): 0,5-10 USD
Selfie with the documents (passport, driving licence): 40-60 USD
Healthcare data: 1-30 USD
Online bankaccounts: 1-10% of the value
PayPal accounts: 50-500 USD

6 Surface web, visible web or the surface or visible part of the Internet. This is the part of the Internet that search engines can find, the indexed pages.

7 Part of the DeepWeb is an area that can be accessed through some kind of registration or identification. Our private online banking site and our password-protected cloud storage are the best examples of this.

8 In order to access the content here, we need an anonymous browser, which makes it impossible to identify our real identity and encodes our messages and activity.

9 Source: Dömös, Zsuzsanna: Ennyi pénzért árulják a személyes adatokat a sötét weben. 24.hu, 11. December 2020.

Average price for dark web data

Category	Product	Avg. dark web Price (USD)
Credit Card Data	Cloned Mastercard with PIN	$25
	Cloned American Express with PIN	$35
	Cloned VISA with PIN	$25
	Credit card details, account balance up to $1,000	$150
	Credit card details, account balance up to $5,000	$240
	Stolen online banking logins, minimum $100 on account	$40
	Stolen online banking logins, minimum $2,000 on account	$120
	Walmart account with credit card attached	$14
	Hacked (Global) credit card details with CVV	$35
	USA hacked credit card details with CVV	$17
	UK hacked credit card details with CVV	$20
	Canada hacked credit card details with CVV	$28
Payment Processing Services	Stolen PayPal account details, minimum $100	$30
	Stolen PayPal account details, minimum $1,000	$120
	Stolen PayPal account details, no balance	$14
	50 Hacked PayPal account logins	$200
	Hacked Western Union Account	$45
	Verified Stripe account with payment gateway	$1,000
Crypto Accounts	Hacked Coinbase verified account	$610
	Blockchain.com verified account	$310
Social Media	Hacked Facebook account	$65
	Hacked Instagram account	$45
	Hacked Twitter account	$35
	Hacked Gmail account	$80
Database Dumps	600k New Zealand emails	$10
	350k Czech emails	$10
	2.4 million Canada emails	$10
	4.78 million Mexico emails	$10
	380k Austria emails	$10
	USA Voter Database (various states)	$100

Figure 3: Types of data sold on DrakWeb[10]

From the figure above based on the 2024 data, it is clear that the price of our data shows an upward/growing trend. It is also clearly visible that a wide spectrum of our personal data is sold on marketplaces, operating on the DarkWeb.

[10] Source: N.a.: How much is your data worth? The complete breakdown for 2024. invisibly.com, 13 July 2021.

Typically, personal data is leaked on the SurfaceWeb, as a result of human negligence, while on the DarkWeb, it is due to intentional damage. To this end, it is necessary to emphasize, present and systematize the manner and form in which personal data are disclosed in the two layers.

The figure (below) clearly shows, as described, why my research only makes sense in these two layers.

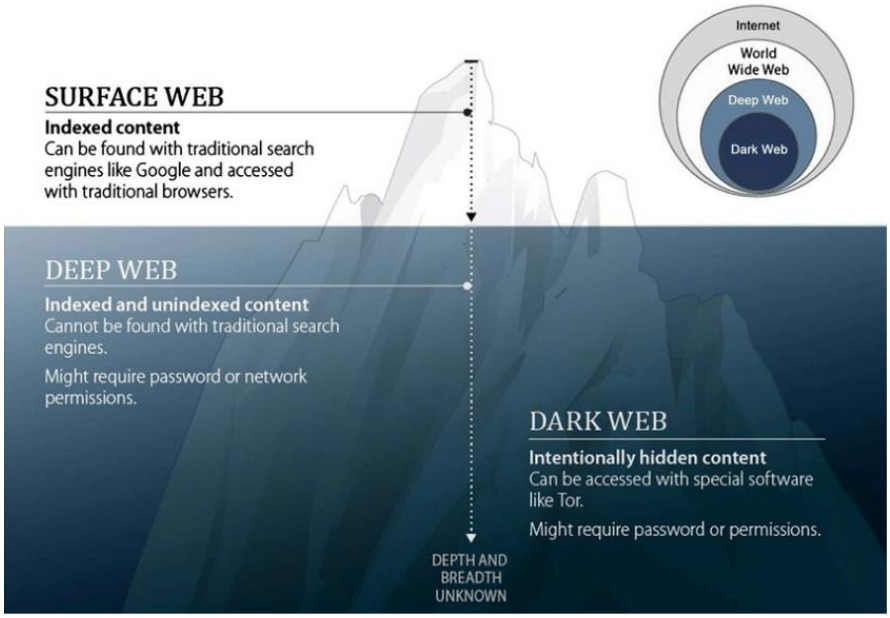

Figure 4: Internet layers[11]

Demarcation

During my research, I examined only two of the three layers of the Internet. In the case of the DeepWeb, I did not conduct research, as in my opinion, the examination of SurfaceWeb and DarkWeb clearly show the risks and differences. The DeepWeb, which is the hidden part of the Internet, is basically not relevant for the research, banks store data here, and our correspondence is also located here, hidden from unauthorized observers.[12]

[11] BESHIRI, Arbër – SUSURI, Arsim: Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. *Journal of Computer and Communications*, 2019/3

[12] NAZAH, Saiba – HUDA, Shamsul – ABAWAJY, Jemal – HASSAN, Mohammad Mehedi: Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. *IEEE ACCESS*, 2020/8

I also emphasize that it is not basically doxing[13] presentation is the aim of the research. Our personal data can be obtained by simple internet searches, browsing social media sites, and they can also be removed from our IT devices, by using unauthorized methods, in addition to social engineering[14] techniques the attackers can use. But the goal of doxxing is typically to embarrass, blackmail, or harass the victim or the targeted business. In the course of our research, I searched and examined openly accessible personal data to a limited extent.[15] In summary, the figure below shows in the most tangible way that SurfaceWeb and DarkWeb are the best targets for research.

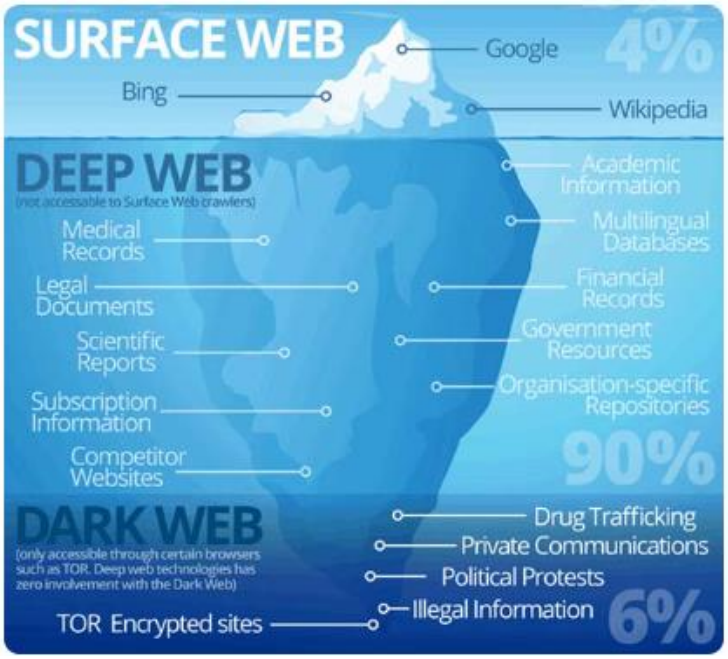

Figure 5: Internet layer percentage distribution[16]

[13] Doxxing or doxing in general: collection and public publication of previously secret or difficult-to-access personal information.

[14] The social engineering refers to all techniques aimed at talking a target into revealing sensitive information or performing a specific action for illegitimate reasons. Hackers are aware that the weakest point of any defense system is the worker. The social engineering attack method is also based on this fact. The method allows cybercriminals to manipulate the person (target) in such a way that victims do not adhere to security or other business security process protocols, thereby allowing malicious activities or leakage of sensitive information.

[15] SNYDER, Peter – DOERFLER, Periwinkle – KANICH, Chris – MCCOY, Damon: Fifteen minutes of unwanted fame: detecting and characterizing doxing. Lecture: *IMC '17: Proceedings of the 2017 Internet Measurement Conference*, 01 November 2017

[16] N.a.: Dark Web: What's under the Surface? threatcop,com, 4 January 2022

Hypothesis

In my opinion, in the vast majority of cases, personal data appear on SurfaceWeb, due to human negligence or are leaked, due to a lack of information security knowledge. On the other hand, personal data, leaked/sold on the DarkWeb or leaked in a pre-planned manner, pose a major risk for both businesses and private individuals (natural persons). Basically, personal data appear in data groups or in the form of data combinations, since their illegal use is only possible in this way.

Clarification

In order to ensure that no open questions arise in the case of the contents of our study, we clarify several terms and present the legal and technical environment of the research.
Due to the easier interpretation, it is necessary to clarify the legal environment (law and decree), as well as IT concepts, since the research covers the topic by overlapping these two fields.

Legislation

Internet searches can sometimes have legal consequences. The legal environment of my research and article is primarily the general data protection regulation (GDPR)[17] and the Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Privacy Act"),[18] as well as the Act C of 2012 on the Criminal Code[19] define.

The general framework of data protection in the territory of the EEA member states is regulated by the GDPR, with the exception of criminal, national defense and national security data management or control, bacause in this case, this area is the regulatory competence of the member states.

It should be noted, however, that in the case of criminal data processing, uniform EU principles also apply.[20] If these laws are violated, it is primarily related to the misuse of personal data.

---

17 The European Parliament and the Council (EU) 2016/679 Decree on the protection of natural persons with regard to the management of personal data and the free flow of such data, as well as the 95/46/EK on the repeal of the Directive.

18 ct CXII of 2011 on the Right Informational Self- Determination and on Freedom of Information.

19 Act C of 2012 on the Criminal Code.

20 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

In this case, the Criminal Code 219. § may arise as an applicable legal defense In this case, the legal object of the crime is the The Fundamental Law of Hungary Article VI. (3-4),[21] the right to the protection of personal data declared in paragraph 1, and the legal situation is a framework provision, the background legislation of which is the GDPR, as well as the Privacy Act.

Such sectoral legislation can be, for example, in the field of healthcare on the management and protection of healthcare and related personal data 1997. XLVII. Law, which establishes a framework for the management of health data, or the Labor Code, which contains provisions regarding biometric data for employees.[22] This study is basically talking about abuses when someone deliberately violates one of the legal provisions on the protection of personal data and handles personal data without authorization or for a purpose other than for the purpose of making a profit or causing significant damage to interests, or even if he fails to observe or enforce data security measures.

Criminal Code – 219. § Abuse of personal data

Regarding data obtained illegally on the Internet, two major sub-areas can be identified, but there are many Criminal Codes we know the type of crime within its scope (No. 1 Annex). Offenders commit a crime when they enter an IT network without authorization,[23] as well as when the personal data obtained from it are handled, that is they misuse this personal data.

A Criminal Code 219. § on the basis of which, in violation of the legal provisions on the protection or management of personal data, for the purpose of making a profit or causing significant damage to interests, handles personal data without authorization or contrary to the purpose, or fails to take measures for the security of the data, shall be punished with imprisonment up to one year. Whoever violates the legal provisions on the protection or handling of personal data does not comply with his obligation to inform the data subject, and thus significantly harms the interests of another person or others. It is considered a classified case, committing this with special personal data, in which case, it is punishable by imprisonment up to two years. Another qualifying factor is if you did it as an official or using a public commission, in which case, the penalty is three years.

What is important to emphasize is that the crime can be committed intentionally. A crime committed for profit can only be committed with direct intent.

---

21 *"Everyone shall have the right to the protection of his or her personal data, as well as to access and disseminate data of public interest."*

22 Act I of 2012 on the Labor Code, 11.§

23 Criminal Code. 423.§ – Information system or data breach

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information – operational activity

In the case of operational – law enforcement, national defense or national security – operations, the Criminal Code. 219.§and the CXII of 2011. which fills it with content, that is means CXII of 2011 I have to break its rules in order for our action to be considered based on this legal fact. If the act is committed in connection with special data (for example, in connection with health or criminal data), in that case, the judgment is more severe, and even if all this is done in an official personal capacity. There was no reference to criminal liability for the research, so in this study we also anonymized all data, in order not to cause significant harm to any person by publishing their personal data found on the DarkWeb. We did not use classified data in our research either, as our research activities are not national security activities or operation. The anonymized data are presented so that the reader can better understand the significance of the risk.

European Union Data Protection Regulation (GDPR)

If the personal data are not handled by CXII of 2011, (that is not related to activities aimed at law enforcement, national defense or national security), the case falls under the scope of the rules of the GDPR. In this case, we can handle personal data during our research, in compliance with the principles contained in Article 5 of the GDPR (purpose limitation, etc.), and we must be able to legitimately refer to one of the legal bases in Article 6 (1), in order to hanlde this personal data (collection, storage, publication), according to the legal requirements. In this case, during our research, we either have to ask for the consent of the data subjects (there is little chance that the data subjects of the personal data sold on the DarkWeb would give us such consent), or we can process this data by citing our legitimate interest. In this case, it is doubtful that our research interest would override the interests, rights and freedoms of the data subjects, if personal data were published, especially given that we can present the results of our research with anonymized data. As a result, during the research, we did not store (we did not save on a hard drive) the acquired data, we only used them during the anonymization procedure.

In the case of special data, Article 9 (1) of the GDPR clearly prohibits the processing of data, and these personal data can only be processed if we can legally refer to one of the exceptions in Article 9 (2), and we comply with Article 6 (1) of one of the legal bases listed in paragraph, During our research, in this case as well. I chose the publication method of anonymizing personal data.

With this procedure, on the one hand, I do not violate the provisions on data protection, on the other hand, we do not exhaust the Civil Code. 219, since anonymized data are not subject to either the GDPR or the Infotv. as long as they remain anonymized. That is why it is very important that during the research the anonymization was carried out in such a way that it was final, that is the re-identification of the persons involved could not take place.

The fundamental law of Hungary

The right to the protection of personal data is fundamentally and decisively the right of everyone (every person). The Constitutional Court 15/1991. (IV. 13.) decision defines the right to data protection as the right to informational self-determination. This is derived from the provisions of the constitution regarding human dignity, as well as from the right to the protection of personal data also mentioned in the previous constitution. The fundamental Law of Hungary VI. Article (3 mentions the fundamental right to the protection of personal data. According to the above-mentioned Constitutional Court decision, according to the content of the right to informational self-determination, everyone decides on the use of their personal data.

Act V of 2013 on the Civil Code

The Act V of 2013 on the Civil Code (2:43. §) includes the protection of personal data and the right to image and sound recording are among the named personality rights.

Computer abuse

It is more commonly known as the information system[24] fraud committed using.[25]

Some research so far

Many scientific articles have been written on the subject, since the problem did not appear recently. A study on the subject was already published in 2010, where the author emphasizes how it is necessary to protect our personal data during electronic trading in the United States of America. As well as how the protection of personal data affects electronic commerce. In his conclusion, he emphasizes that the proper protection of personal data greatly contributes to the functioning of proper digital commerce.[26]

Some studies have already examined the relationship between financial abuse and personal data. According to the conclusion of this 2019 study, your personal information is becoming a seller on the DarkWeb, and this should no longer be treated as a possibility, but as a fact. Evidence from their analysis shows that some use this data to grow their businesses, while others just pass it on. The analysis conducted through the study highlights the fact that there is an increasing demand for personal data in various online illegal trading forums. Larger players in the market are providing more and more services and goods to carry out illegal activities.

---

[24] Tools that ensure the automatic processing, management, storage and transmission of data.

[25] Criminal Code 375. § – crime defined by.

[26] PANNAH, Em: Cybersecurity in Electronic Commerce: *Effect of Safeguarding Personal Data on Identity Theft*. ProQuest Dissertations&Theses, University of Maryland University College, November 2010.

Understanding these implications is of great practical importance in terms of protecting personal data and keeping sensitive data secure. In addition, continuous monitoring of the illegal market is vital for cybersecurity experts and law enforcement personnel to be aware of the growing scale of online threats.[27]

It is also important to highlight that the research shows a dichotomy, as the handling of personal data basically takes place on the DeepWeb, under legal or controlled conditions (96% of Internet content is located here). However, the illegal part is on the DarkWeb, which is a relatively bottleneck of the Internet from the point of view of its use.

According to a study published by the United States Air Force Command, DarkWeb users (assuming they use TOR) are two (2) million people/day out of nearly 3.2 billion users (0.625% of global users). Which is a negligible amount in terms of percentage, but if you look at the numbers, it is still high, since many people out of the 2 million people carry out their illegal activities on a daily basis. The data of the study also confirm the results of our research, according to which the search in the upper layer of the Internet is meaningless, while in the second layer we can get a clear picture of the types of data distributed. The samples taken from the third layer show the actual risks and their extent.[28]

A scientific article is also being prepared in the context of Hungary, in which the misuse of personal data and the criminal consequences are analyzed. Attila Péterfalvi and Dániel Eszteri's article *"The criminal law protection of personal data in Hungary and the related practice of the National Data Protection and Freedom of Information Authority" present the criminal law protection of personal data in the Hungarian legal system, and discuss the main criminal substantive legal provisions related to personal data".* Many scientific works have also been produced regarding the DarkWeb and the DeepWeb, although in several cases concepts are mixed up, especially in the case of the DeepWeb and the information found on the DarkWeb about the fact that they were uploaded to the mentioned layer by legal/illegal means.[29,30,31]

In some studies, the DarkWeb is considered a part of the DeepWeb, where clearly illegal activity takes place. Or the DarkWeb provides the opportunity for various organizations and national security services to carry out covert operations against each other.

---

27 VARGAS, Vanesa-Madalina: The new economic good: Your own personal data. An integrative analysis of the Dark Web. Lecture: *Proceedings of the International Conference on Business Excellence*, 2019/1, pp. 1216-1226.

28 COLE, Jeremy: Dark Web 101. Air&Space Power Journal En Español, Air University, Maxwell AFB, AL, 1 March 2016.

29 BARTLETT, Jamie: Infiltrating *'The Dark Net,' Where Criminals, Trolls And Extremists Reign*. NPR. 03 June 2015.

30 CIANCAGLINI, Vincenzo – BALDUZZI, Marco – MCARDLE, Robert – RÖSLER, Martin: *Below the Surface: Exploring the Deep Web*. Trend Micro, Incorporated, 2015

31 JARDINE, Eric: *The Dark Web Dilemma: Tor, Anonymity and Online Policing.* Global Commission on Internet Governance, 2015/21.

According to Kristin Finkl's article, this layer can be well described as an operation space, literally as follows: *"Just as criminals can rely upon the anonymity of the Dark Web, so too can the law enforcement, military, and intelligence communities. They may, for example, use it to conduct online surveillance and sting operations and to maintain anonymous tip lines. Anonymity in the Dark Web can be used to shield officials from identification and hacking by adversaries. It can also be used to conduct a clandestine or covert computer network operation such as taking down a website or a denial of service attack, or to intercept communications. Reportedly, officials are continuously working on expanding techniques to deanonymize activity on the Dark Web and identify malicious actors online."*[32]

In other research, DarkWeb and DarkNet are synonymous with each other, and this area is clearly part of DeepWeb. Quoted verbatim: *„However, there are large sections of the Internet that is unindexed and hidden from the normal search engines. These concealed part of the Internet is Deep Web which is estimated to make up about 96 precent of the WWW. Within the Deep Web a subset that is mostly used for illicit purpose is the Dark Web or Dark Net."*[33]

Research

Purpose of research

The purpose of our research is to present the form and distribution of personal data on the Internet, and to prove my hypothesis. I will also present the effectiveness of the search types, and I will also organize the personal data found according to their type.

Research parameters and environment

Research security

The cyber security environment of the research was designed as follows. The reason for this is that in the last phase of the research, the content on the DarkWeb was not censored at all, its content was not checked, that is it cannot be ruled out that our IT network will be damaged or that we may become victims of fraud.

VPN and TOR

During the search, we used VPN and TOR network at the same time *(Onion Over VPN).* The Onion Routing Project was created by the United States Naval Research Laboratory like a tool for anonymously communicating online in the middle 90's, and the Onion Router was further developed by the Defense Advanced Research Projects Agency in 1997 (Weimann).

---

32 FINKLEA, Kristin. M.: *Dark Web*. CRS report, Congressional Research Service, 10 March 2017, pp. 1-16.

33 NAZAH – HUDA – ABAWAJY – HASSAN 2020.

Tor was also used to protect the communications of the American military. The Tor network became operational in 2003 and since 2006 it has been maintained and improved by the Tor Project Inc.

The encryption protocol of the VPN service does not allow infected content to find the IP address on the Internet, hiding the IP address does not allow malicious operators to reveal the TOR client. That is, we used the TOR browser through the VPN channel.

TAILS

The Amnesic Incognito Live System (TAILS) is the unique Debian-based version of Linuz, which does not leave trail on the computer. This operational system can be used gratis, and can be activated also from the USB drive. TAILS cannot save cookies or files to your hard drive without directly requesting it. You also don't run the risk of browsers "paged" the data to the backend.

All TAILS web traffic automatically flows through Tor. If the operating system detects non-anonymous connections, it automatically blocks them. TAILS also has built-in modules such as a text editor and email client, which means it can do more than just browse the web.[34] We did not use this method during the research, as based on my practical experience, ToR Over VPN also provides adequate security.

Anonymity

During the research, I tried to ensure that the presented data could not be linked to companies or individuals. That's why I deleted the names of the companies, their contact information and the names of the employees, as well as their personal data, on the screenshots. The names of the companies are not relevant information regarding the results of the research. In addition, it is important to note that without anonymization, I can cause reputation destruction even if I want to.

Research data protection legal compliance

During the research, we had to meet the requirements of the GDPR, that is I could only manage personal data in a way that complied with the basic principles of the GDPR. Even with reference to the research, I cannot disclose personal data in the case of which I cannot prove their legality, and I must act fairly and transparently throughout the research.

Keyword search

In the first step of my research, I used a keyword search to observe what search results I could get.

[34] TAILS can be downloaded from tails.boum.org.

During the search, I searched for the keywords ”Stolen social security numbers”, ”ID card number”, ”ID number”, ”personal data” using the Google engine. As expected, I found results and sponsored cyber security articles that of course did not contain personal information. From this, it can be concluded that keyword search on the open Internet is a completely ineffective method. This is because a search engine is a program or application that searches for information in some Internet environment based on conditions set by a specific user. Internet search engines typically consist of two parts, one of which collects information,[35] and the other organizes. During the systematization, the indexer analyzes the pre-indexed pages and then associates metadata with them, with the help of which he sets up an order according to relevance based on the search criteria. When the user starts a search, the search engine uses the index to select the pages that meet the criteria, ranks them based on the meta information associated with them, and lists them according to relevance among all the results. Also, it can be assumed that the illegal data manager does not use an indexed website to sell his/her product.

If we look at the following examples as a keyword search, the following partial results are generated:

Personal data:	697 000 000 million hits (0,39 s);
ID card number:	5 020 000 000 hits (0,43 s);
Stolen social security numbers:	109 000 000 hits (0,47 s).

Figure 6: Search on Google
(Source: Author’s own collection)

It is clear from the data of the three examples above that an open search performed with the Google engine (performed with a browser) does not yield any appreciable results, which would violate any law. Basically, we get pages that can be linked to the keywords (in some relation) as a result.

[35] Robot or web crawler.

Search by/on social networks

In the second step of the research, I conducted an observation on a social network. Social networks store a lot of uploaded personal data. We found out during our research (No. 2 annex), that the following personal data are posted on social networks in feeds or uploaded albums as follows:

Surname and first name[36]

(Occurrence: screenshot of ID card, document proving educational qualification, certificate proving absoltidorium, Hungarian uniform, birth certificate, driver's license, OKJ qualification document, machine operator's license, court summons, police report, internet quiz or game results post). These data are relatively easy to obtain, little abuse can be committed with them independently, so their risk factor is LOW.

Date of birth

(Occurrence: document certifying educational qualification, certificate certifying absoltidorium, birth certificate, court summons, police report).

Document proving educational qualification

(Occurrence: photo of OKJ certificate, BsC or MsC diploma with all data according to the content requirements). Their usability has a LOW risk, as basically these data are less likely to be abused.

Biometric data[37]

Basically, the route (GPS data), blood pressure, other physiological data measured with an IoT device during some kind of sports performance. For law enforcement officers, the combination of the first two data and the route data poses a CRITICAL risk, as organized criminals can abuse personnel by using them. The best example of this is the scandal that happened in 2018, during which a student became a national security risk. Mobile devices or applications are used to track staff training. Millions of people do this every day. On the other hand, a 20-year-old Australian student discovered the location of bases used by military forces and intelligence services by studying heat maps. ZDNet wrote a detailed case study about the problem.[38]

---

36 Also first name, birth name, maiden name.

37 All personal data relating to the physical, physiological or behavioral characteristics of a natural person obtained through specific technical procedures that enable or confirm the unique identification of a natural person, such as facial image or dactyloscopic data.

38 OSBORNE, Charlie: Pentagon bans military from using GPS apps and fitness trackers. ZDNET, 18 August 2018.

Litigation materials/partially anonymized litigation materials

In the course of the research, the uploaded document of a litigation case (in png format) was found in three cases. A divorce case, a patent case, and a package of expert documents brought in a child custody case, and the corresponding court decision. The uploaded materials were contained in the news feeds, the purpose of the upload was, according to the posts, a deliberate activity, in order for the opposite parties to carry out a discrediting campaign due to their perceived or real grievances. The uploads are CRITICAL risk factors, as the names and data of witnesses, government officials (judges, lawyers, prosecutors) are or may be included on the documents.

Invoices and purchase data for products purchased online

There is a LOW risk of leaking said data, even though it may be linked to a name or a name and date of birth during posting. Basically, our financial data is not included on the blocks and printed payment blocks. It is a MEDIUM risk if you provide information with the help of these and in combination with our client's photo gallery about our existential situation. Because as a result, we can become targets of organized criminal groups.

The above results are data that their owner clearly shared independently without external pressure as a result of wrong settings or possibly in the case of a discrediting campaign. We do not include the data that appears on the data sheets operated by the social portals, as they are only visible to a closed group.

Complex SurfaceWeb search

During the more complex research, we searched on SurfaceNet for news whose results or consequences appear on the DarkWeb interfaces, and then presented the results with the help of screenshots. In the third step, we searched for the terms ”personal data breach” and ”personal data leak” that produced results that could be linked to the leakage of personal data. Although, similar to the first step, the search did not yield concrete results, it did point to those incidents in which personal data were also affected. In other words, the following information can be extracted in this way:

- incident time (informative data for further the research);
- the company of which hacker group (authoritative data for further research);
- what was the leaked information (relevance indicator for further research);
- who is affected in the incident (authoritative data for further research).

On the basis of the data obtained above, it is possible to filter out which major company had a cyber security incident and/or which hacker group managed to gain access to a large amount of personal data during an incident during the period under review. In this case, we would have two options. In the first case, the affected/victim can be contacted and informed about what personal data has been made public.

However, the data obtained from here cannot be considered primary data, since we have no insight into what actually came out. Therefore, if possible, the investigation should be continued on the electronic interface operated by the hacker group, which basically cannot be found on the open internet due to anonymity.

During the research, the hacker groups use screenshots to prove that they have the mentioned data files. Buyers/interested parties can use the screen photos to evaluate whether they will purchase the mentioned data files.

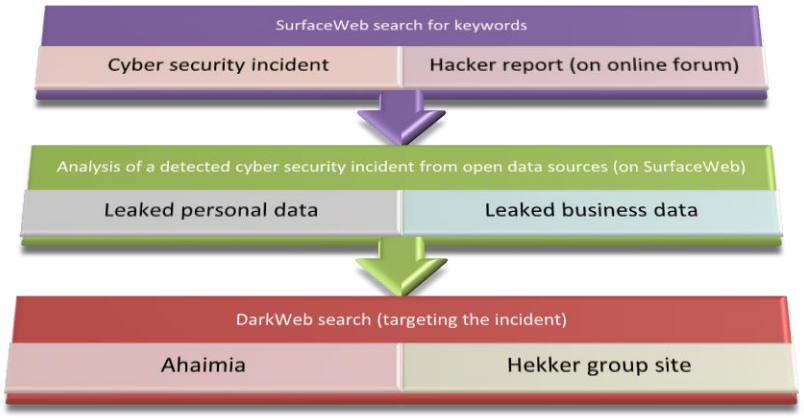

Figure 7: Way of the search
(Autor's own edition)

We emphasize that these groups usually have Telegram and Twitter accounts on the open internet, where they sometimes post their attacks. In the case of hacker groups, there are also cases with a negligible number of occurrences when they post personal data about each other during the rivalry.

A good example of this is when members of BreachForums and OnniForums accused each other of leaking personal data. According to unconfirmed information, the details of BreachForums members were posted by the rival group. Furthermore, tweets from the official Twitter account of OnniForums claimed responsibility for the attack. Another tweet from the same forum claims that they were also involved in an attack on another hacking forum, which was a group known as 'Exposed'. Notably, in May 2022, a partial database was leaked on ExposedForum, containing the data of 460,000 members of RaidForums, which have now been seized. It is clear from the above incident that the rival groups are practically in constant conflict with each other, where the primary goal is to damage the credit of the other. The authenticity of the above information should be treated with reservations, as the motivation is to discredit the other group. Thus, it cannot be ruled out that these databases do not contain real data.

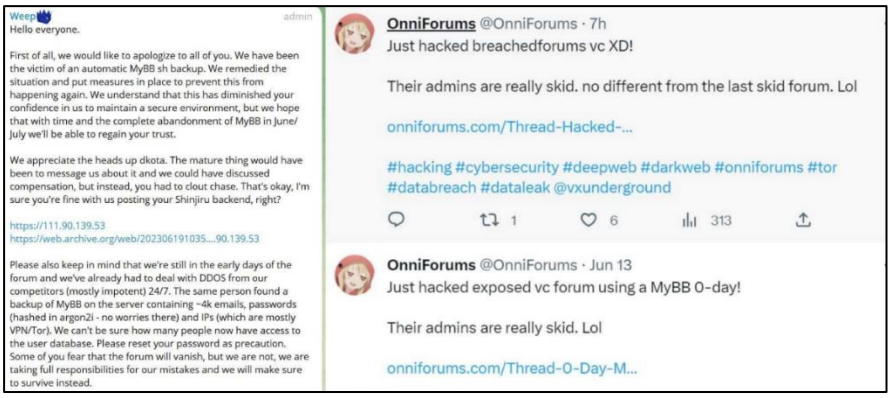

Figure 8: OmniForums post
Source: SocialMedia account post

After the analysis, it can be determined that according to OmniForums posts, login keys, usernames, email addresses, IP addresses, password extracts, registration dates, members' last visits and posts, number of posts and last activity were exposed.

Summary

Keywords can almost always be formulated in relation to the thing to be searched for. These are important aids during the search. Searching in this way, can be simple or complex. In the latter case, we can use a special search term to speed up the search and narrow down the set of results. We use search spaces during the keyword search. These are websites whose search engine maintains its own database. In these, each keyword has one or more URLs. This database is updated from time to time by the website's search engine. I present the deeper and practical results of my research in the next section, which is organically connected to my current article. In my next analysis, I will present the types of data found on DarkWeb's commercial platforms with the help of screenshots.

No. 1 annex

Crimes that can be committed in the Hungarian digital ecosystem:

- 204.§ Child pornography
- 219.§ Abuse of personal data
- 220.§ Misuse of public data
- 222.§ Harassment [39]
- 223.§ Violation of privacy
- 224.§ Breach of confidentiality of…
- 226.§ Defamation
- 226/A.§ Making a false audio or image recording suitable for defamation
- 226/B.§ Making public a false audio or image recording suitable for defamation hozatala
- 227.§ Defamation
- 265.§ Abuse of classified data
- 360.§ Organization of illegal gambling
- 375.§ Fraud committed using an information system
- 385.§ Violation of copyright or copyright related rights
- Criminal Code 423. according to section, information system or data violation (data manipulation).

[39] Cyberbullying: Such activity in cyberspace (harassment), which is distinguished from single abuse or other conflict situations by three factors. Basically, it has a strong, negatively influencing effect, so the victim of bullying cannot live his life because of the activities of the bully. Secondly, bullying is repeated at irregular intervals, the abuser regularly returns to the victim and repeats the act, be it physical, verbal or sexual activity. The third criterion is a shift in the balance of power: during bullying, the abusing party always has more power (has more money, is stronger, has more friends, is louder), and he flaunts this during the bullying.

No. 2 annex

Social network monitoring - partial results - with manual retrieval -396 clients.

During the monitoring, I examined 396 Facebook clients on the basis of what personal data can be found in the person's news feed [40], or in their posts. Clients with an evaluable result are included in the list. The investigation does not cover whether the user shared it by mistake or on purpose, nor what personal data are included in the shared contact information. The search was limited to personal data uploaded in text (or clearly legible in a picture), the data does not contain conclusions.

Found data types:

- NKE certificate from the public administration examination (name, mother's name, exam part qualification, details of exam committee members, exam date) - uploaded photo;
- Cambridge language exam result (with name, uploaded diploma image, diploma number and ID) - uploaded photo;
- National Health Insurance Fund Department of Individual Equality Affairs form;
- Complete documentation of divorce proceedings (name, witnesses, special personal data);
- Founded Hungarian identity card (photographed on both sides without anonymization);
- Patent lawsuit file with details of the plaintiff and defendant;
- Birth and health data of the child born (name, birth weight, mother's name, document number);
- Own biometric data related to sports activities;
- Place of stay (check-in from an event, tourist/hospitality facility);on-line térben vásárolt termékek számlái, vásárlási adatai (vásárló adataival);
- Own sports performance (name, biometric data, place of residence, route traveled, hobbies);
- Military discharge letter [41] (name, name of military unit);
- Application certificate (name, address, results achieved);
- Certificate of award certifying charitable activity (name, name of activity);
- EMMI award and diploma for social work (name, recipient, donor, sample signature, date of donation, reason for donation);
- Class photo from military secondary school (names, date of graduation, institution identifiers);
- List of members of my terminated military unit, date of demobilization.

From the results above, it can be seen that users share the personal data of third parties in several cases. Of course, in such a way that the person did not give his consent to this, but basically he does not know about it either[42].

[40] September 2023 – December 2023.

[41] A soldier who has/her completed his/her service and received obsit.

[42] On the shared pictures, the users do not tag the people in the given picture.

In the list above, it can be seen that in two cases, this was presumably done intentionally by the use, in order to damage the reputation of the party with the opposite interest. In the case of the patent lawsuit, the legal documents contained a lot of personal data, and the victim and the alleged infringer could be clearly identified.

In the case of the demolition lawsuit, personal data were also published that the victim presented, in order to discredit the person who committed the perceived or real harm.

The above data can be particularly well used for data enrichment, which can facilitate further cyber attacks for hackers.

Bibliography:

BARTLETT, Jamie: Infiltrating *'The Dark Net,' Where Criminals, Trolls And Extremists Reign*. NPR. 03 June 2015, Online: https://www.npr.org/sections/alltechconsidered/2015/06/03/411476653/infiltrating-the-dark-net-where-criminals-trolls-and-extremists-reign (Download time: 16/01/2024)

BESHIRI, Arbër – SUSURI, Arsim: Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. *Journal of Computer and Communications*, 2019/3, DOI: 10.4236/jcc.2019.73004

CIANCAGLINI, Vincenzo – BALDUZZI, Marco – MCARDLE, Robert – RÖSLER, Martin: *Below the Surface: Exploring the Deep Web*. Trend Micro, Incorporated, 2015, Online: https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf (Download time: 16/01/2024)

COLE, Jeremy: Dark Web 101. Air&Space Power Journal En Español, Air University, Maxwell AFB, AL, 1 March 2016. Online: https://apps.dtic.mil/sti/pdfs/AD1005862.pdf (Download time: 16/01/2024)

DÖMÖS, Zsuzsanna: Ennyi pénzért árulják a személyes adatokat a sötét weben. 24.hu, 11. December 2020, Online: https://24.hu/tech/2020/12/11/kaspersky-szemelyes-adatok-dark-web-erteke-adatlopas/ (Download time: 16/01/2024)

FINKLEA, Kristin. M.: *Dark Web*. CRS report, Congressional Research Service, 10 March 2017, pp. 1-16, Online: https://sgp.fas.org/crs/misc/R44101.pdf (Download time: 16/01/2024)

JARDINE, Eric: *The Dark Web Dilemma: Tor, Anonymity and Online Policing.* Global Commission on Internet Governance, 2015/21. Online: https://www.cigionline.org/sites/default/files/no.21.pdf (Download time: 16/01/2024)

KAVALLIEROS, Dimitros – MYTTAS, Dimittros – KREMITSIS, Emmanouil – LISSARIS, Euthimios – GIATAGANAS, Georgios – DARRA, Eleni: Using the Dark Web. In: AKHGAR, Babak – GERCKE, Marco – VROCHIDIS, Stefanos – GIBSON, Helen (eds.): *Dark Web Investigation*. Springer Cham, January 2021, pp. 27-48. DOI: 10.1007/978-3-030-55343-2_2

N.a.: Dark Web: What's under the Surface? threatcop,com, 4 January 2022, Online: https://threatcop.com/blog/surface-web-dark-web-and-deep-web/ (Download time: 16/01/2024)

N.a.: How much is your data worth? The complete breakdown for 2024, invisibly.com, 13 July 2021, Online: https://www.invisibly.com/learn-blog/how-much-is-data-worth/ (Download time: 16/01/2024)

N.a.: List of Data Breaches and Dyber Attacks in 2023 – 8,214,886,660 records breached. IT Governance, 5 January 2024, Online: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023#top-data-breach-stats (Download time: 16/01/2024)

N.a.: What is Digital Footprint? malwarebytes.com, n.d. Online: https://www.malwarebytes.com/cybersecurity/basics/digital-footprint (Download time: 16/01/2024)

NAZAH, Saiba – HUDA, Shamsul – ABAWAJY, Jemal – HASSAN, Mohammad Mehedi: Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. *IEEE ACCESS*, 2020/8, DOI: 10.1109/ACCESS.2020.3024198

OSBORNE, Charlie: Pentagon bans military from using GPS apps and fitness trackers. ZDNET, 18 August 2018. https://www.zdnet.com/article/pentagon-bans-military-from-using-devices-with-gps/ (Download time: 16/01/2024)

PANNAH, Em: Cybersecurity in Electronic Commerce: *Effect of Safeguarding Personal Data on Identity Theft*. ProQuest Dissertations&Theses, University of Maryland University College, November 2010, Online: https://www.proquest.com/openview/472b719e9fa49dc82954ac68d7d215f0/1?pq-origsite=gscholar&cbl=18750 (Download time: 16/01/2024)

SNYDER, Peter – DOERFLER, Periwinkle – KANICH, Chris – MCCOY, Damon: Fifteen minutes of unwanted fame: detecting and characterizing doxing. Lecture: *IMC '17: Proceedings of the 2017 Internet Measurement Conference*, 01 November 2017, pp. 432-444. DOI: 10.1145/3131365.3131385

ÜVEGES, András József: A kriptopénzek árnyékában. [In the shade of cryptocurrencies.] Felderítő Szemle, 2018/1, pp 162-169.

VARGAS, Vanesa-Madalina: The new economic good: Your own personal data. An integrative analysis of the Dark Web. Lecture: *Proceedings of the International Conference on Business Excellence*, 2019/1, pp. 1216-1226. DOI: 10.2478/picbe-2019-0107

Principles, laws and government decisions:

Act C of 2012 on the Criminal Code.

Act V of 2013 on the Civil Code.

Act CXII of 2011 on the Right Informational Self- Determination and on Freedom of Information.

The European Parliament and the Council (EU) 2016/679 Decree on the protection of natural persons with regard to the management of personal data and the free flow of such data, as well as the 95/46/EK on the repeal of the Directive.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHAAct I of 2012 on the Labor Code.

The Constitutional Court 15/1991. (IV. 13.) The use of personal data and the personal identification number.

AUTHORS OF THIS ISSUE

ALEXANDRU MALACENCO PhD (in history), is a researcher at the State University of Moldova, Chişinău;

ANDRÁS JÓZSEF ÜVEGES is a PhD student of the Doctoral School of Military Engineering of the as well as a scientific associate of the National Security Institute of the University of Public Service, Budapest;

BÁLINT PONGRÁCZ is an MA student at the Royal King's College, London;

DORKA HORVÁTH is an MA student at the Faculty of Public Governance and International Studies, University of Public Service, Budapest;

IMRE DOBÁK PhD is an Associate Professor, University of Public Service, Civilian National Security Department, Budapest;

ISTVÁN BANDI is a researcher of the Historic Archives of the State Security Services, Budapest;

ISTVÁN SOLTI PhD is an Assistant Professor, University of Public Service, Civilian National Security Department, Budapest;

PÉTER POMOGÁCS is a PhD student of the Doctoral School of Security Studies of the University of Public Service, Budapest;

TAMÁS DRUSZA is a PhD student of the Doctoral School of Law Enforcement at Ludovika University of Public Service, Budapest;

VANESSA MARTINS is a Brasilian PhD Candidate in Military Science, at the Doctoral school of Military Sciences at the University opf Public Service, Budapest.

PROOFREADERS OF THIS ISSUE

PROF. JÓZSEF KIS-BENEDEK is a former Hungarian military intelligence officer, security expert, and doctor of military sciences. A retired colonel and a doctor of military sciences;

FERENC KAISER PHD is an associate professor at the Department of International Security Studies, Faculty of Military Science and Defence Officer Training, National University of Public Service;

BÉLA PUSKÁS PHD is a cyber- and IT security expert at the Military National Security Institute of the University of Public Service.

CONDITIONS OF PUBLISHING IN THE NATIONAL SECURITY REVIEW

Ethical requirements:

- The written work (“article”) has not yet been published elsewhere in this form.
- The written work (“article”) is the exclusive intellectual property of the author(s), which is confirmed by completing and signing the author's (authors’) statement.
- The written work (“article”) is correct, retrievable and researchable, includes all the references specified in the author's guide.
- The written work (“article”) contains a bibliography (which includes a list of cited literature, a list of Internet materials with download times).
- The written work (“article”) reflects the author(s) own opinion, which by definition does not necessarily coincide with the position, standpoint and/or opinion of the Military National Security Service of Hungary.
- The manuscript must under no circumstances contain racist, xenophobic or extremist statements.

Publication information:

- Please send the manuscript in electronic form to the e-mail address natsecrev@knbsz.gov.hu.
- An author's fee may be paid for articles accepted for publication provided an agreement would be reached concerning the payment with the author's declaration.
- Manuscripts are always proofread by the Editorial Board. (Articles to be published in the publication are proofread by competent employees of the Service with academic degrees or other subject matter experts.)
- The Editorial Board – taking into account the reviewers' opinions – reserves the right not to publish manuscripts deemed unsuitable for publication without justification.
- Anyone can publish in the publication whose writing the Editorial Board deems suitable for publication in the Review, as well as for publication on the Internet, based on the ethics, content and formal requirements.
- Please attach to the manuscript the name, rank, position or job title of the author or authors, permanent address, telephone and internet contact details, and their ORCID and MTMT identifiers – if they have the latter.

Content requirements:

- In accordance with the nature of the periodicals, we publish writings – studies, articles and other topics and materials – that process and analyze scientific questions related to national defense, primarily national security, intelligence, reconnaissance, military security and security policy.

- The written work to be published must be logical, clear, coherent and well-structured – it must have an introduction, discussion and conclusion.
- The formulation of the Author's own concept related to the topic should be understandable, and the conclusions should be well-founded, supported by arguments and data.

Formal requirements:

- The length of the author's manuscripts should preferably not exceed one “author's sheet” (40,000 characters), however, taking into account the content and topic of the manuscript, after an individual (responsible publisher) evaluation, longer articles may also be published.
- The manuscript should be written in letter-type Calibri Light 12-point font, double-spaced, and images and figures should be edited in a processable format (.jpg or .tif) "in line with the text".
- A short content summary (Abstract/Summary) must be attached to the article, maximum 10-12 lines, in Hungarian and English – the short content summary must be written in E/3 person and not be the same as the introduction of the main text.
- Three to five keywords are required for the article, in Hungarian and English, after the Abstract.
- The Authors are required to send the title of the article also in English.
- In social sciences, please use the usual numbered reference in the citations footnote method. (In the editing of the journal, ISO 690:2021 "Information and documentation. Guidelines for bibliographic references and citations of information sources" and ISO 4:1984 "Information and documentation. Bibliographic description and reference. Rules for abbreviating bibliographical terms" are the guiding standards indicated in the descriptions below (with deviations. In case the author does not use the standards or the attached aid, the author may be asked to revise the manuscript.)
- For numbers longer than four digits, use the CTRL-SHIFT-SPACE (non-breaking) space, not the plain space or period; e.g. 430,000. (This is not necessary for four-digit numbers.)
- In the case of quotation marks, we use the English version (”...”), not the Hungarian („...”) versions.
- Use internal quotation marks (»...«) for the quoted part within the quoted text – "beginning of quotation »internal quotation« end of quotation.".
- If we also need a parenthesis within a bracketed part (...), then the square bracket [...] is used.
- Foreign terms and abbreviations must be explained in the footnotes for the first time in the written work (example: WFP – UN World Food Program).

Requirements for figures, sketches, maps, diagrams and other attachments:

- When editing figures, tables, diagrams, and pictures that contain essential information belonging to the article, it is necessary to number them – for example, Figure 1 - and give them a title, as well as indicate in a footnote the source of the illustration or the fact of own editing.
- It is the responsibility of the author to edit the figures and tables, the illustrations should be named in an identifiable way without formatting that impairs the quality of the manuscript. The recommended resolution should be at least 300 dpi.
- The publication of a figure taken from another publication must be authorized by the author, and the source must be clearly indicated in his/her own text.
- Data in foreign languages must be translated into English.
- The publisher may, at its own discretion, waive the publication of illustrations with no informational value, of a quality that may not be suitable for publication, or of an uncertain source.

Please observe the followings when quoting and making footnotes:

- Serial numbers given as superscripts after citations within the text refer to notes, which must be given in the order of their appearance in the text. (These notes may contain citations.)
- The footnote number is typically placed after the punctuation mark that ends the part of the sentence or sentence.
- Additional and explanatory additions not directly related to the text should also be included in footnotes.
- If several works were to be cited in the text, only one superscript number should be used, and the works should be separated by semicolons in the footnote.
- The first citation must contain at least (if available): author's last name - lowercase - first name: Address. Publisher, place of publication, year of publication as specified in the bibliographic references, as well as the page number of the quoted part. (In the case of several authors, the names of the authors must be separated from each other by using a long hyphen.)
- The first citation must contain at least (if available): the author's last name and the first name (the latter in minuscule), as well as: title, publisher, place of publication, year of publication, as they are given in the bibliographic references, and the page number of the cited part. (In the case of several authors, the names of the authors must be separated from each other by using a long hyphen.)
- In the case of three or more author(s), in the footnote, after the first author's name, the “et al.” (et alii – and others) abbreviation must be used and the names of all authors must be written in the bibliography.

- After the first citation, subsequent citations must contain the following: last name of the author(s) – in minuscule – year of publication, page number. (If there is a work cited in the manuscript with the same last name and publication year, the first letter of the first name must also be used – e.g. Szabó M. 2014, 9.)
- If the author is unknown, the “n.a.” abbreviation must be used.
- If the year of publication is unknown, the abbreviation "n.d." must be used.
- If the place of publication is unknown, the "n.p." abbreviation must be used.
- If the publisher is unknown, "n.p." abbreviation must be used
- If the referenced work was published in a language written in other than the Latin alphabet (e.g. Russian or Chinese), the author must also transcribe the title of the referenced work into Latin letters.
- During the direct repeated summons following the first summons, the “Ibid.“ abbreviation must be used.

List of bibliographical references:

- In the list of bibliographic references, please enter the references in the alphabetical order of the first data element.
- If the referenced work has an ISBN number, please indicate it after entering the bibliographic data.
- If the article has an ISSN or DOI identifier, please indicate it after entering the bibliographic data.

The main types of quotations are as follows:

TYPE OF WORK REFERRED TO	FIRST REFERENCE IN TEXT	FURTHER REFERENCE IN TEXT	BIBLIOGRAPHY REFERENCE
Single-authored work	ÁCS, Tibor: *On the military culture of the reform era*. Zrínyi Publishing House, Budapest, 2005, p. 34.	ÁCS 2005, 34.	ÁCS, Tibor: *On the military culture of the reform era*. Zrínyi Publishing House, Budapest, 2005. ISBN 963 9276 45 6
A work by two or three authors	SZENES, Zoltán – SIPOSNÉ KECSKEMÉTHY, Klára: *NATO 4.0 and Hungary*. Zrínyi Publishing House, Budapest, 2019, p. 55.	SZENES – SIPOSNÉ 2019, 55.	SZENES, Zoltán –SIPOSNÉ KECSKEMÉTHY, Klára: *NATO 4.0 and Hungary*. Zrínyi Publishing House, Budapest, 2019. ISBN 978 963 327 770 6
Edited work	BEREK, Lajos: The basics of military science research. In: SZILÁGYI, Tivadar (ed.): *Selections*. Zrínyi Miklós Military Academy, Budapest, 1994, p. 33.	BEREK 1994, 33.	BEREK, Lajos: The basics of military science research. In: SZILÁGYI, Tivadar (ed.): *Selections*. Zrínyi Miklós Military Academy, Budapest, 1994, pp. 31-50.

TYPE OF WORK REFERRED TO	FIRST REFERENCE IN TEXT	FURTHER REFERENCE IN TEXT	BIBLIOGRAPHY REFERENCE
Journal (printed)	KOVÁCS, Jenő: The roots of the new Hungarian military science, the conceptual problems of its development. *Új Honvédségi Szemle*, 1993/6, p. 6.	KOVÁCS 1993, 6.	KOVÁCS, Jenő: The roots of the new Hungarian military science, the conceptual problems of its development. *Új Honvédségi Szemle*, 6/1993, pp. 1-7. ISSN 1216-7436
Journal (electronic)	FORGÁCS, Balázs: Histography of the concept of war culture II. *Hadtudományi Szemle*, 2009/3, p. 4.	FORGÁCS 2009, 4.	FORGÁCS, Balázs: Histography of the concept of war culture II. *Hadtudományi Szemle*, 2009/3, pp.1-8. Online: https://epa.oszk.hu/02400/02463/00006/pdf/EPA02463_hadtudomanyi_szemle_2009_3_001-008.pdf (Download time: 02/20/2024)
Electronic content	ABRAMS, Lawrence: Ransomware attack at German hospital leads to death of patient. Bleepingcomputer, Bleepingcomputer September 17, 2020.	ABRAMS 2020.	ABRAMS, Lawrence: Ransomware attack at German hospital leads to death of patient. Bleepingcomputer, 2020. szeptember 17. Online: https://www.bleepingcomputer.com/news/security/ransomware-attackat-german-hospital-leads-to-death-of-patient/ (Download time: 02/20/2024)
	N.a.: Operation Ghost Stories. fbi.gov, 10/31/2011.	Operation Ghost Stories 2011.	N.a.: Operation Ghost Stories. fbi.gov, 10/31/2011. Online: https://www.fbi.gov/news/stories/operation-ghost-stories-inside-therussian-spy-case (Download time: 02/20/2024)

TYPE OF WORK REFERRED TO	FIRST REFERENCE IN TEXT	FURTHER REFERENCE IN TEXT	BIBLIOGRAPHY REFERENCE
Doctoral theses, theses, papers	SOMKUTI, Bálint: *The fourth generation of warfare: new opportunities for asserting interests*. PhD dissertation. Doctoral School of Military Sciences, National Public Service University, 2012, p. 95.	SOMKUTI 2012, 95.	SOMKUTI, Bálint: *The fourth generation of warfare: new opportunities for asserting interests*. PhD dissertation. Doctoral School of Military Sciences, National Public Service University, 2012. DOI: 10.17625/NKE.2012.019
Conference	HOLCZINGER, Norbert: Sustainable development and financing. Lecture: *Sustainable development in development policy – 20 years of Hungarian EU membership*. National University of Public Service, Ludovika, Budapest, 23 April 2024.	HOLCZINGER 2024.	HOLCZINGER, Norbert: Sustainable development and financing. Lecture*: Sustainable development in development policy – 20 years of Hungarian EU membership*. National University of Public Service, Ludovika, Budapest, 23 April 2024. Online: https://kfi.uni-nke.hu/hirek/2024/04/29/fenntarthato-fejlodes-a-fejlesztespolitikaban (Download time: 02/20/2024)

TYPE OF WORK REFERRED TO	FIRST REFERENCE IN TEXT	FURTHER REFERENCE IN TEXT	BIBLIOGRAPHY REFERENCE
Law	Act V of 2013 on the Civil Code	Ptk. Section 183 or Ptk. Section 183, paragraph (1). or Ptk. Section 183, paragraphs (1)–(3).	Act V of 2013 on the Civil Code
Ordinance	100/2009. (V. 8.) Government decree on the detailed rules for authorizing certain uses of orphan works	100/2009. (V. 8.) Government decree	100/2009. (V. 8.) Government decree on the detailed rules for authorizing certain uses of orphan works
Decision	1100/1997. (IX. 30.) Government decision on the review of our copyright legislation	1100/1997. (IX. 30.) Government decision	1100/1997. (IX. 30.) Government decision on the review of our copyright legislation