MILITARY NATIONAL SECURITY SERVICE

Issue 1/2021

NATIONAL SECURITY REVIEW

BUDAPEST

Scientific Periodical of the
Military National Security Service

Responsible Publisher:

Lt. Gen. János Béres, PhD Director General
Chairman of the Scientific Board

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

E-mail: natsecreview@gmail.com
Webpage: http://www.knbsz.gov.hu

TABLE OF CONTENTS

THEORY OF NATIONAL SECURITY

ISTVÁN BANDI

A HISTORICAL OVERVIEW OF THE ROMANIAN SURVEILLANCE SERVICE FROM ITS ESTABLISHMENT AFTER WORLD WAR 2 TO THE REGIME CHANGE IN 1989 5

NIKOLETT KATALIN BÚS

THE LONG-TERM CORPORATE SUCCESS – SAFE COMPANY.....20

ÁGNES JOBST PHD

AN ALLY IN THE CROSSHAIRS? THE INTELLIGENCE COOPERATION BETWEEN THE GERMAN DEMOCRATIC REPUBLIC AND THE HUNGARIAN PEOPLE 'S REPUBLIC.....30

GEOPOLITICS

BERK CAN KOZAN

BURDEN SHARING: TO BE OR NOT TO BE.....44

FAISAL WARIKAT

SURVIVAL COMPARISON BETWEEN HAMAS AND HEZBOLLAH.....56

BENCE GÖBLYÖS

NATO'S RESPONSE FOR THE SOUTHERN CHALLENGES - NATO STRATEGIC DIRECTION SOUTH HUB 73

ANDRÁS NOVÁK

INTERNATIONAL PHYSICAL BARRIERS ALONG THE BALKAN MIGRATION ROUTE.....87

ÖMER AKYÜZ

TURKEY'S EUROPEAN UNION MEMBERSHIPS: DEVELOPMENTS, BENEFITS AND DRAWBACKS FOR BOTH SIDES 113

HAJNALKA SZILÁGYI-KISS

SITUATION OF IRAQI CHRISTIANS AS A SECURITY CHALLENGE 125

TIBOR SZILVÁGYI PHD
MILITARY UNMANNED AERIAL SYSTEMS AND THE NEW PARADIGM OF THE WARFARE 139

INFORMATION AND COMMUNICATION SECURITY

VERONIKA DEÁK
FINDING DIFFERENCES ON CYBER SECURITY BETWEEN PUBLIC AND PRIVATE SECTORS 169

PROF ZOLTÁN RAJNAI PHD – HAYA ALTALEB
RISK ASSESSMENTS METHODS AND CYBER VULNERABILITIES IN SCADA SYSTEMS 181

AGNES KEMENDI
E-COMMERCE SAFETY AND SECURITY IN THE INDUSTRY 4.0 ERA 195

ATTILA NÉMETH – SÁNDOR MAGYAR PHD
AN INVESTIGATION OF DATA USED TO SUPPORT CONTACT TRACING TO CURB THE SPREAD OF COVID-19 PANDEMIC FROM THE ASPECT OF POSSIBLE NATIONAL SECURITY APPLICATION (PART 2) 218

BÉLA PUSKÁS PHD – BENCE LÁZÁR
CYBER PROTECTION OVERVIEW 232

AUTHORS OF THIS ISSUE 244

CONDITIONS OF PUBLICATIONS 245

ISTVÁN BANDI

A HISTORICAL OVERVIEW OF THE ROMANIAN SURVEILLANCE SERVICE FROM ITS ESTABLISHMENT AFTER WORLD WAR 2 TO THE REGIME CHANGE IN 1989

Abstract

Part of the Romanian historical literature, citing memoirs of former members of the active-duty personnel, portrayed the intervention by external forces, namely the Soviet[1] and Hungarian special services as one of the greatest risks for communist Romania.[2] This security risk was articulated much earlier by the Romanian state security authorities.

After the Prague Spring in 1968, the leading cadres of the law enforcement agencies introduced a decision-making mechanism based on a new military doctrine. This was laid down in Decree 14/1972 on the organization of the national defense of the Socialist Republic of Romania, and was drafted in the spirit of national communism dictated by Nicolae Ceausescu. In this new legal framework, the term "fighting in enemy-occupied territory"[3] practically applied to enemies sought among the Allies (the Soviet Union and members of the Warsaw Pact). Thus, in addition to a supposed Hungarian intervention, the possibility of a Soviet intervention was also taken seriously. An analysis of the documents found in the archives of the former secret services (Archives of the National Inquiry Committee on the Documents of the Securitate – ACNSAS) and the that time Ministry Interior Border Guard's Surveillance Service can bring us closer to the clarification of this issue.

---

1 The present study does not examine the risk conditions for the intervention of Soviet agencies, not least because the material of the Romanian Surveillance Service does not show the security phenomenon referred to in the relevant literature. However, another organizational unit is designated as the UM 0110 military unit sign and materials from the Directorate for the Elimination of Threats from Socialist States provide a more nuanced picture of the Soviet threat.

2 WATTS, Larry: Ferește-mă doamne de prieteni, războiul clandestin al blocului sovietic cu România [Protect me, Lord, from my friends! The secret war of the Soviet bloc against Romania]. Bucharest, Editura RAO, 2012; WATTS, Larry: Here are some of them. România și sfârșitul războiului rece [The first will be last. Romania and the end of the Cold War], Bucharest, Editura RAO, 2013; MĂGUREANU, Virgil – STOENESCU, Alex Mihai: De la regimul comunist la regimul Iliescu. Virgil Măgureanu in dialogue with Alex Mihai Stoenescu [From the Communist Regime to the Iliescu Regime. Virgil Măgureanu in conversation with Alex Mihai Stoenescu], Bucharest, Editura RAO, 2008; STEFUREAC, Ioan Remus: Conflictul secret din spatele scenei România versus Rusia. 50 de ani de realități, mituri si incertitudini [The secret conflict behind the scenes. Romania versus Russia. 50 Years of Reality, Myth, and Uncertainty], Bucharest, Editura RAO, 2015.

3 This term is explained in more detail by researcher Mădălin Hodor in his dissertation: In 1989 a avut loc o diversiune militară executată de armata secretăa partidului [Military diversion carried out by the secret army of the party in 1989]. https://pressone.ro/istoricul-madalin-hodor-in-1989-a-avut-loc-o-diversiune-militara-executata-de-armata-secreta-a-partidului/ (downloaded 28 April 2019)

***Keywords*:** Romania, Communism, Hungarian minority, State Border Guard Service, Surveillance Service, Hungarian, refugees

Institutional background

After the end of World War 2, border protection was one of the priority tasks of the Romanian state. In the relatively short period of time leading up to the ratification of the Paris Peace Treaty, this area underwent fundamental changes. Complicating matters was the fact that, in a plastic international context, almost all of the neighboring states had put in place coercive measures. This study examines the trend of the phenomenon of illegal border violations in the period from 1947 to 1989 recorded by the Romanian Border Surveillance Service. In our short introduction, we aim to outline the most important professional policy and institutional organization decisions that also applied to the Hungarian-Romanian border section.

Along the Romanian-Hungarian joint border section in 1944, after the withdrawal of the front, border guard activity was conducted under Soviet military supervision. In the hinterland, in Northern Transylvania, a Soviet military administration was introduced from November 1944 to March 1945.[4] During the same period, the Romanian Border Guard underwent a major downsizing, reducing the number of border guard troops from 44,000 in August 1944 to 12,000 in April 1945, and removing several leading generals from command positions of the service branches.[5] In the countries 'liberated' by the Soviet Union, including Romania, defense and home affairs organizations, including the border guards, underwent permanent and fundamental restructuring under the direct supervision of the Allied Control Commission. The series of discharges and the uncertainty resulting from direct Soviet intervention were accompanied by a reduction in controls by border guards. Thus, the discipline of the dwindling border guard also disintegrated and it was not able to perform its task to the proper standard.[6]

A fundamental legal and organizational change was the publication of Decree No. 1259 of 21 June, based on Law 208, published in the Monitorul Oficial (Official Gazette) on 25 June 1947. Under the decree, border guards were transferred from the Ministry of Defense to the Ministry of the Interior and they remained there until 1960.

In the period from 1945 to the summer of 1947, professional decisions with extremely controversial legal backgrounds were made by the Romanian border guards, as large numbers of fugitives from the front returned to their homeland. As a result of the Romanian political decision, all those who left the territory of Transylvania were treated on the basis of the principle of collective guilt, as according

---

4 On the organization and operation of the Soviet military administration, see L. BALOGH, Béni: Changes in Empire in Transylvania and the Turnaround of 1944-1945; In: Our Time 2015/5. pp. 72-79. https://www.academia.edu/35747179/ (downloaded 28 April 2019)

5 NEAGOIE, Sever – VĂDUVA, Gheorghe – TENDER, Ilie: History of French and French Policies in the Front; Editura Scaiul, Bucharest, 2004, p. 337.

6 Ibid. p. 313.

to the relevant law they all continued to "serve Hitler's Germany".[7] Furthermore, due to the disorder of border relations, the masses of "black border traffic" were a serious problem for the border guards of both states.

From the second half of 1946, based on the ACC's permit and on the visa requirement between the two countries, the Romanian border guard authorities required a valid passport and a special permit issued by the Romanian ACC, as well as an entry or transit visa issued by the Romanian embassy. With reference to this, the Romanian authorities sent back many Szekler families with Romanian citizenship to Hungary, and persons of Hungarian nationality were transferred to Hungarian territory despite the relevant documents.[8] All those who could not officially cross the border to Romania – including those returning from the West from captivity, deportation, forced labor – tried to achieve their goal by avoiding the border guard authorities.[9] The Romanian Border Guard and the Border Surveillance Service, established in 1947, faced such challenges.

Organizational history review, analysis

The operations of the Surveillance Service were organically linked to the border guard organization. In 1947, after the Paris Peace Treaties and the coming into power by the communists,[10] the Border Surveillance Service (Serviciul de Informații Frontiere) was established within the Border Guard Headquarters then under the Ministry of Defense. It belonged under the direct command of Section II of the General Staff. In 1950, when it was reassigned to the Ministry of Interior it was a decoupled organizational unit of the Security Forces Headquarters. Between 1950 and 1960, the Surveillance Service operated under the direct command of the deputy minister of interior who was also in command of the Border Guard. Its primary task was to prevent border violations carried out in the border area settlements through the use of covert network techniques and thus support the Border Guard border security work. Structurally it was made up of departments, offices and teams, whose geographic distribution matched the organizational structure of the border guard.[11]

As provided by Council of Ministers Decree No. 159, the Border Guard Headquarters was moved from the Ministry of Interior to the Ministry of Armed Forces (MOAF)[12] on February 20, 1960, including the Surveillance Service, at the same time it continued its surveillance operations for another year based on joint cooperation regulations of the MOI and MOAF. Due to the new situation, the Surveillance Service lost access to the operational records of the Ministry of the

---

7 Monitorul Oficial (Official Gazette) No. 1945/17, Law Decree No. 50 of the Ministry of Justice.

8 MNL OL XIX-B-10 V-4. 574. 263/1946. 1. d. On expulsions from the Romanian border.

9 Ibid.

10 On December 30, 1947, the leaders of the Romanian Communist Party forced King Michael I of Romania to abdicate from the throne.

11 ACNSAS Fund D 013783/1. p. 306.

12 The Romanian Defense portfolio was, in the reporting period, between 1947 and 1989, called Ministry of National Defense until 1950, from 1950 to 1972 it was designated Ministry of Armed Forces, and from then on again Ministry of Defense. See: https://www.mapn.ro/repere_istorice/index.php (downloaded 28 April 2019)

Interior, as well as its previous training framework. To remedy the situation, Council of Ministers Decree No. 112 reassigned the Surveillance Service to the MOI as a decoupled separate organizational unit in 1961, and it continued to function as such until 1964 when, due to the restructuring of the MOI, its central command was assigned to Counter-Intelligence Directorate III of the MOI, and its regional units were assigned to the Securitate Directorates in the border regions. Based on the new organization chart, the regional officers of the Intelligence Service were tasked by the regional commanders of the Securitate, so they were placed in charge of all the covert operations in the border settlements and were less able to deal with their specifically border guard related surveillance duties. In 1967, the leadership of the MOAF sought to change this, asking to have the Surveillance Service to be assigned to them, because, as they said, information received did not satisfy the demand of the border guard for surveillance on SBI-s.[13] A decision was made in 1968 to assign the Surveillance Service to the Counterintelligence Directorate, and to have them perform their activities in the higher units of the organizational structure of the Headquarters of the Border Guard Troops.

In the early 1970s, the number of illegal border crossings increased on the border section with the Socialist Federal Republic of Yugoslavia. In order to address the issue, Order No. 5311 of the Chairman of the Leadership of the Securitate (the State Security Committee, Consiliul Securitatii Statului – CSS) ordered the reorganization based on which border security counter-intelligence officers from all over the country were concentrated on the southwestern section of the state border, operating under the county commander of the Securitate. The border counties which were not augmented with border protection counterintelligence officers had to man this task at the expense of their own active duty cadre. Their central professional control was the responsibility of the Military Counterintelligence Directorate No. IV. Under this concept, 36 counter-intelligence officers were assigned to ten county inspectorates, and covert surveillance of border violators was included in the operational records. In addition, these officers had a duty to provide support for the Militia[14] posts in the border zone, and also perform information and awareness-raising activities among the local population.[15] CSS Order No. 5311 did not include any instruction on what to do with individuals coming from non-border counties attempting to leave the country illegally, i.e. what preventive actions the competent county-level state security units should take. Both for the central and the regional units, the registration of individuals attempting to escape from the country and individuals illegally overstaying abroad, and the methodology of case-based processing of their files was regulated by MOI Order No. 00665 issued on 28 May, 1975, in compliance with Section 21 of Law No. 1972/132 on the organizational structure and functioning of the Ministry of Interior.[16] Thus, from 1968, the Surveillance Service was included in Counterintelligence Directorate III of the MOI and from 1976 it was reassigned to the Internal Intelligence Directorate.[17] Thus, a significant part of the former counterintelligence officers were transferred to Internal Intelligence Directorate No. I and to the county inspectorates of the Ministry of the Interior, respectively. Their distribution was as follows: Military Counter- Intelligence Directorate No. IV handed over 44 officers to the Internal

13 ACNSAS Fund D 013783/1, p. 307.
14 The police were called Militia in Romania in this period.
15 ACNSAS Fund D 013783/1, p. 308.
16 ACNSAS Fund D 013783/1, p. 296.
17 Ibid.

Intelligence Directorate I., 9 of them performed central control functions within Directorate No. I., 11 were transferred to Timiș County, 5 to Caraș-Severin County, 4 to Mehedinti County, 3 officers to Arad, Bihor and Constanța County each, 2 officers to Bucharest, and 1 officer to Brăila, Galati, Satu Mare and Tulcea County each. 14 additional counties received 1 officer each, while in the other 19 counties an officer of their own active duty personnel was designated and tasked with performing the functions of this specialty area.[18] With this transformation, the Headquarters of the Border Guard Troops, which in 1960 returned to the Ministry of Armed Forces[19] and the Surveillance Service, by being assigned to the MOI lost their direct synchronization opportunities in the internal affairs specialty area. For this very reason the Headquarters of the Border Guard Troops insisted that an organizational unit like the Surveillance Service was badly needed.[20]

Methodological measures and the involvement of all counties in prevention work did not improve statistics of border crimes. In effect, specialty area line work was still performed by the border counties and their supervisors, the department concerned of Military Counter-Intelligence No. IV. Ministerial order No. 00887 issued on 26 June 1976 extended the task of detecting and neutralizing individuals attempting to leave the country illegally and individuals overstaying abroad illegally to all operational organizational units. In effect, this order instructed all the specialized units of the Securitate and the Militia to take active measures. Within the Securitate, Internal Intelligence Directorate No. I was tasked with the mission-oriented coordination of the county and capital organizational units. The concept of this restructuring was placing the emphasis on prevention, that is escape from country starting in the central counties must be prevented.[21] With this measure, the Ministry of Interior achieved a state of affairs where the number of offenders did not increase significantly before 1979.[22]

---

18 The Headquarters of the Border Guard Troops remained within the organizational framework of the Ministry of National Defense until 1992.

19 ACNSAS Fund D 013783/1, p. 295v.

20 ACNSAS Fund D 013783/1, p. 311.

21 ACNSAS Fund D 013783/1, p. 315.

22 ACNSAS Fund D 013783/1, pp. 315-316. MG TABACARU, Dumitru: Report presented in October 1977 by the Ministry of the Interior; ACNSAS Fund D 013783/1.

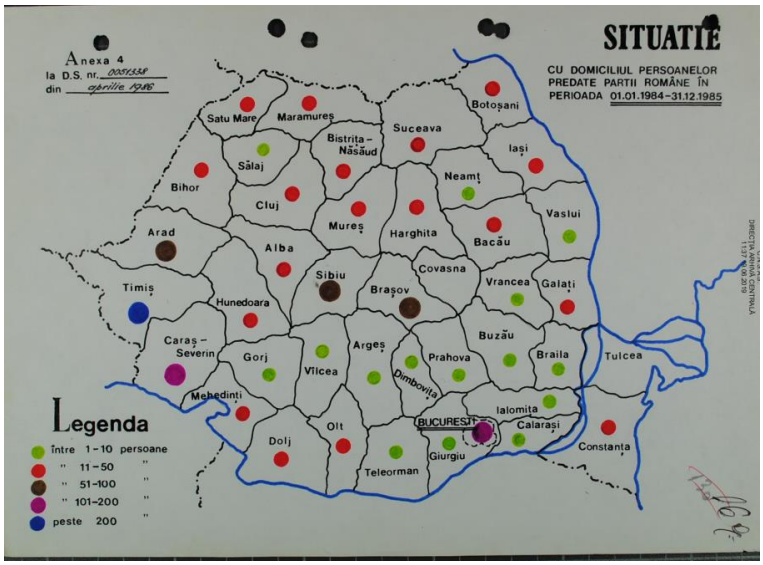

Figure 1. Legend: Number of individuals by domicile address returned between January 1984 and December 1985

green: 1-10 individuals
red: between 11-50 individuals
brown: between 50-100 individuals
purple: between 101-200 individuals
blue: over 200 individuals

The statement shows the trend that was characteristic of the first half of the seventies and eighties. Of the two border counties, Timisoara and Arad, mainly persons of German ethnic background, and more persons from the traditionally German-speaking counties (Sibiu, Brasov) left the country or returned by the border guard authorities of the neighboring states, respectively.

In the second half of the seventies, attempts hitherto not experienced were made to escape from the country. Among other instances, 7 people tried using a shunting locomotive to cross the state border illegally at the railway border crossing station of Jimbolia to get to Opština Kikinda in the then Yugoslavia. At the Timisoara and Naidăș border crossings station people tried to break through the barrier by car four times. In these attempts, decisive action was taken. The above cases are mentioned in Major General Tabacaru's 1977 summary report, stressing that although the number of attempts to cross the border illegally had decreased, attempts of a violent nature had appeared. Also in this report, foreign (Western) propaganda motivating the escape appears emphatically.[23] Ministerial Order No. 00887 also stated that firm neutralizing action would be taken against individuals engaged in political propaganda activities. Previously, political motivation was not taken into account in the phenomenon of leaving the country illegally. Among the foreign influencing organizations, Radio Free Europe and Amnesty International were mentioned. Secretary General Nicolae

[23] CEAUȘESCU, Nicolae: Cuvintul la adunarea activului de partid si a cadrelor de conducere din Ministerul de Interne; Editura Politica, 1978. p. 13.

Ceausescu strongly argued in 1978 that foreign services are behind a major part of the individuals leaving Romania illegally.[24] The secretary general of the party was still speaking about a downward trend, but in reality, this decrease in the number of incidents could not be detected in the statistical figures (See Infographic No. 1).

Hundreds of people illegally returning to Romania across the green border were subjected to a detailed interrogation process that revealed that those who had earlier left the country illegally in groups did not make any serious preparations before perpetrating their act. It is also worth emphasizing, because the relevant state security agencies had assumed that they would, through operational means, be informed about such preparations. Further it was found out that in most cases the reason for leaving the country illegally could be attributed to the desire to acquire wealth, to workplace conflicts and family problems, respectively.[25] To improve the situation a special briefing was held for the county Section I heads of departments and senior officers, within which new neutralization criteria such as prevention of subversive activities pursued by foreigners visiting Romania. A special briefing was held to improve cooperation between the Securitate and the Militia.[26]

In this context, the operational processing of individuals who earlier left the country illegally and returned; individuals who maintain contacts with foreign citizens, or regularly visit them; individuals who emigrated from Romania and conducted smear campaigns in the host country against their country of birth; the monitoring of the contacts in Romania of those who left the country, furthermore of those individuals who had left Romania earlier and returned there in possession of a new citizenship of a foreign country, also their family members and relatives. Special emphasis was placed on the operational processing of returnees in order to obtain information mainly on those living in refugee camps.[27]

In addition to operational methods, the Securitate placed great emphasis on information in order to curb the phenomenon of illegal emigration. Special briefings were held for the job centers, the Militia, members of the justice system, the press, the radio and the television. They initiated a social debate in the workers' communities, directly influencing the stakeholders and their environment along the educational and trade union line.[28]

By the end of the 1970s, Internal Intelligence Directorate No. I of the Ministry of the Interior, the Alien Administration Directorate and the National Headquarters of the Militia coordinated their activities to deal with the phenomenon of illegal border violators. The head of the Internal Intelligence Directorate No. I was responsible for coordinating the activities of this organization. This operational and organizational activity was marked by Major General Dumitru I. Tăbăcaru.[29]

---

24 ACNSAS Fund D 013783/1, p. 320.
25 ACNSAS Fund D 013783/1, p. 322.
26 ACNSAS Fund D 013783/1, pp. 331-332.
27 ACNSAS Fund D 013783/1, p. 314
28 ACNSAS Fund D 013783/1, p. 314.
29 DUMITRU I. Tăbăcaru was called up for military service in 1949. Graduated from Political Officer School No. 1 in Ineu (Arad county) and joined the Securitate in 1950. In the same year, he also attended military counter-intelligence training in Bucharest. As a freshly graduated lieutenant, his first position was at the MOI Military Counter-Intelligence Center.

Figure 2. Major General Dumitru Iancu Tăbăcaru[30]

As a result, the said departments have jointly developed the rules for cooperation with the border guard. In 1979, to enhance the control of the Yugoslav border section, the minister of interior ordered the transfer of 438 members of the Militia and the Securitate (31 officers, 310 non-commissioned officers and 97 rank and file soldiers), divided among 14 centers.[31] The leadership of the MOI was forced to take more and more actions by the escalating trend of outbound illegal border crossing. The repetitive orders provided for how the various directorates of the Ministry of the Interior could step up their operational and other preventive activities in the case of border violations. Among other things, this was provided for in MOI Order No. D/00129 1980, issued on 15 March.[32]

Since 1950, he has been teaching at the MOI Officer Training School No. 2. In 1954, he was transferred to the education department of the MOI Personnel Directorate as a first lieutenant. From 1957, as an operational officer, MOI Directorate III. Department No. 2 of Countering Churches. In 1960 he was sent to Moscow to take part in specialized training. After his return, from 1961 he worked in MOI Directorate No. III. as deputy head of Department No. 3 of countering adverse ideological influences in the intelligentsia, then after his promotion to the rank of Major he became head of that department. From 1963 he became Deputy Head of Directorate III of Internal Counter-Intelligence. He briefly moved from counter-espionage to intelligence and was appointed Deputy Chief of DGIE (Directorate General of Foreign Intelligence) in the rank of Lieutenant Colonel. From 1971 to 1977 he was the Deputy Head of Directorate I of Counter-Intelligence in the rank of Colonel, and from 1977 to 1980 he was the Head of the said Directorate in the rank of Major General. For the last two years of his career, he was Deputy Head of Internal Affairs of the Ministry of the Interior. Source: http://www.cnsas.ro/documente/cadrele_securitatii /TABACARU%20DUMITRU.pdf (downloaded 28 April 2019)

30 Source: ACNSAS Fund Cadre MAI 000077

31 ACNSAS Fund D 013783/1, p. 334.

32 ACNSAS Fund D 013783/1, p. 332.

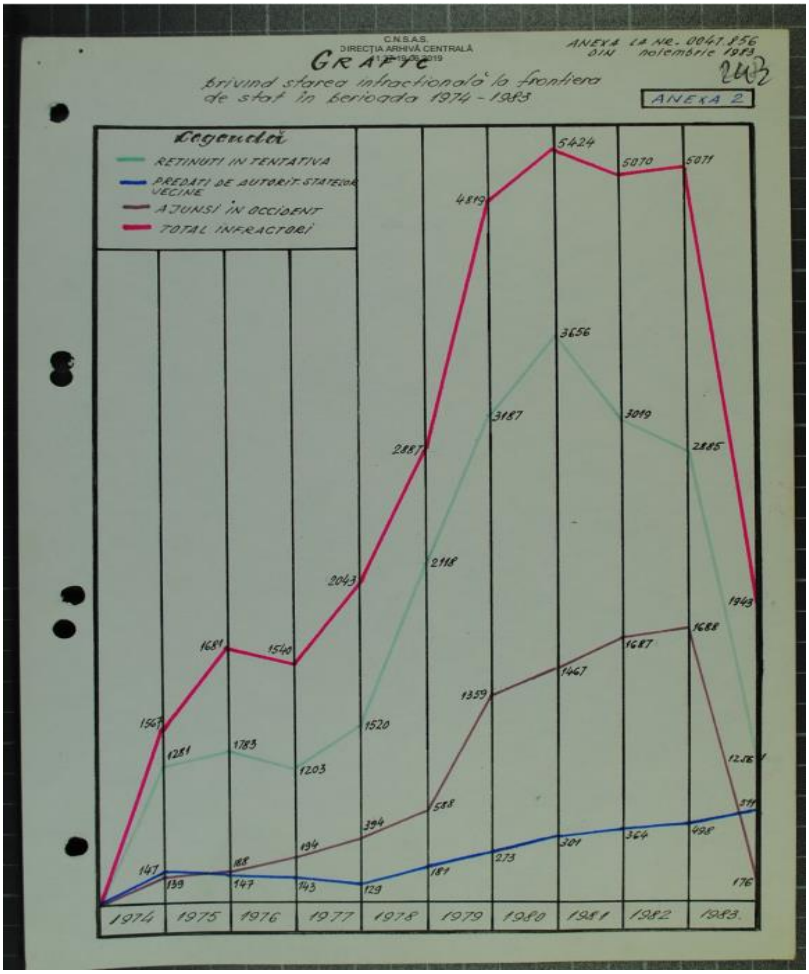

Figure 3: Infographics on border violations committed on the Romanian state border between 1974 and 1983[33]

Legend:
Green color – interdiction of SBI, under arrest
Blue – returned by the authorities of neighboring states
Brown – successful escape to the West
Red – total number of violators

From the mid-eighties, the emphasis in terms of perpetration shifted from the Yugoslav border section to the Hungarian border section. While between 1974 and 1983, 19629 cases of illegal border crossing were recorded towards SFR of Yugoslavia, the same period had 3055 cases of outbound border violation towards the Hungarian People's Republic. In the period mentioned a total of 32 800 documented cases were recorded on the national level: 21 565 persons were subject to criminal procedure, 8495 persons successfully crossed the borders, 2740 persons were subject to separate procedures as they were forcibly returned by the authorities of the

[33] Source: ACNSAS Fund D 013783/1, p. 284.

neighboring states.[34] Between 1981 and 1985, a total of 16412 cases were recorded, in which 14017 persons were of Romanian ethnic origin, 1272 were German, 649 Hungarian and 474 were of other ethnicity.[35]
In its annual summary report dated December 1984, Directorate No. I of Internal Intelligence mentioned for the first time that the number of Hungarian-speaking Romanian citizens going on a trip to Hungary via travel agencies and refusing to return to Romania had increased.[36] The downward trend in the number of illegal emigrations lasted from 1980 to 1985. In April 1986, according to the evaluation report of Directorate No. I of Internal Intelligence, under the supervision of the State Security Committee of the MOI it seemed that the number of instances of illegal emigration would stay at the level of the preceding period, but the number of provocative operations by foreign secret services – including those of the neighboring states – would increase, and the number of individuals attempting to flee from the country across the River Danube and of those who would attempt to flee from the country across the Romanian-Hungarian border. It was strongly indicated that the number of German-speaking Romanian citizens would show an increasing trend.[37]

In the first half of 1986, an extremely rapid change in the number of illegal state border crossing attempts took place, since the statistical figures indicated a 49% increase compared to the first half of 1985, and the direction also changed, instead of the Yugoslav border section now the Hungarian border section saw mare attempts at illegal border crossing.[38]

Colonel General Iulian Vlad,[39] operational chief of state security, described this as an alarming phenomenon and noted a serious setback in the line of state security prevention work.[40]

Figure 4. Colonel-General Iulian Vlad, the de facto chief of the Securitate[41]

[34] ACNSAS Fund D 013783/1, p. 243.
[35] ACNSAS Fund D 013783/1, p. 238.
[36] ACNSAS Fund D 013783/1, p. 197.
[37] ACNSAS Fund D 013783/1, p. 227.
[38] ACNSAS Fund D 013783/1, pp. 202-202v.
[39] ACNSAS Fund D 013783/1, p. 189.
[40] ACNSAS Fund D 013783/1, p. 188.
[41] Source: ACNSAS, Fund Cadre, Dossier 27753

The leadership of Directorate I of Internal Intelligence analyzed the situation and arrived at the conclusion that the county departments were not effective enough, the network-level detection was weak, and the records were not kept up to date, either. An interesting circumstance was noted, namely the fact that SBI-s arrested, interviewed and returned to, however they Romania by the Hungarian authorities told the Romanian authorities that German-speaking Romanian citizens were also interviewed by the Hungarian authorities, however they were released and advised to turn to the Embassy of the Federal Republic of Germany (FRG/West Germany) in Budapest.[42] Upon a proposal put forward by Major General Aron Bordea[43], Head of Directorate No. I of Internal Intelligence a new action plan named 'Borna' (Milestone) was put in place to handle the situation: all Militia posts in the border region were involved in detection efforts, all the agents employed in this line were given special training, the returnees were systematically interrogated and their activities were analyzed.[44]

Figure 5: Major General Aron Bordea[45]

[42] ACNSAS Fund D 013783/1 , pp. 189-190

[43] Aron Gh. Bordea began his public security career in 1951 as sergeant at the Ploiesti Regional Secretariat. Between 1951 and 1953, he first served as a sub-lieutenant and then as a lieutenant from 1953 to 1955 in Department No. 4. Between 1955 and 1959 he served as a team leader, then as bureau chief in the rank of first lieutenant. From 1959 he was a captain, and from 64 as a major, he was the head of department at the Prahova County Securitate Inspectorate. Since 1969 was the Deputy Head of the Dimbovita County Securitate Inspectorate. He completed the Securitate leadership training required for promotion and, from 1969 he was Deputy Chief of Operations in the rank of a lieutenant colonel. From 1973 he was the commander of the Securitate Inspectorate of the said county in the rank of colonel, and from 1979 he became a member of the general officer cadre as major general and headed the inspectorate of the said county. From 1980 to 1986 he was the head of the Directorate No. 1 of Counterintelligence, then in the last stage of his career from 1986 to the regime change in 1989 he was the head of the Directorate of Alien Registration, Supervision of Border Crossing Stations and Passport Control. http://www.cnsas.ro/documente/cadrele_securitatii/BORDEA%20ARON.pdf (downloaded: 28 April 2019)

[44] ACNSAS Fund D 013783/1, pp. 184-184v.

[45] Source: ACNSAS Fund Cadre MAI 000007

The efficiency of the measures that were supervised by Colonel Gheorghe E. Raţiu[46] from 1986 could not be measured, because since 1987 an intensive outflow of escapees was observed on the Hungarian border. While 3,630 incidents were registered in 1987, 13 638 were recorded in 1988, i.e., an increase of 376% occurred. A change in the destination of the illegal border crossings was clearly confirmed by statistical figures, as well as towards the Yugoslav FSR 2660, 1988, 1987, and recorded 4801 cases, while the Hungarian border in 1987, 915, in 1988 already 8703 people were in the statistics. The ethnic composition of the emigrants painted an even more obvious picture: in 1987, 2,704, in 1988, 6,142 Romanians, in 1987, 658, and in 1988, 6453 ethnic Hungarians were recorded.[47]

Figure 6: Colonel Gheorghe E. Raţiu[48]

1988 April new measures were taken to prevent the phenomenon thus 800 rank and file soldiers from the Army were reassigned with the permission of the Ministry of Defense to augment the patrolling of the Romanian-Hungarian border section. The briefing, training of the whole active-duty personnel of the border counties concerned, Satu Mare, Bihor and Arad was ordered to be held every ten days, also the briefing of the support and network staff, to be able to increase the number of line signalizations. At the central command level, with the involvement of the Headquarters of the Border Guard and MOI Directorates No. I of Internal Intelligence and No. IV of Military

---

46 In 1952, Gheorghe E. Raţiu began his state security career as a sub-lieutenant in the Valcea Regional Secretariat, Department No. 4. From 1954, as a lieutenant he was an operational officer of Department No. 3, from 1957 in the rank of first lieutenant he was a team leader of Section No. 3 and Deputy Head of Department. In 1965 he was promoted to the rank of captain, and in 1967 he was transferred to Olt county where he was assistant chief of the Securitate County Inspectorate. His career as a colonel continued in 1986 at Directorate No. I of Counterintelligence, first as Deputy Chief, then Chief of the Inspectorate until the downfall of the regime.

47 ACNSAS Fund D 013783/1, pp. 81-82

48 Source: ACNSAS Fund D 13414.

Counterintelligence assessment and analysis reports had to be prepared on the situation on a monthly basis.[49]

For the first time, in the first quarterly summary report of 1989 of MOI Directorate No I of Internal Intelligence mention was made of the fact that escapes from the country took place in an organized fashion, and special emphasis was placed on social support that was characteristic of these acts (i.e., support on the part of the local population in the border area, people smugglers were involved, foreign citizens rendered aid and assistance to the SBI-s). The report noted that the covert nature of organizing desertions increased (use of passwords, secret signals, using coded language during telephone calls in certain stages of these acts with the use of middle men who did not know the exact plan). Among the measures taken by Directorate No. I of Internal Intelligence, special emphasis was given to the detailed documentation of "foreign" citizens' activities and catching them in flagranti in the criminal act, since they believed that the phenomenon of desertions was presented by the foreign states and media in a way that was to the detriment of Romania's interests.[50]

As early as 1989, the critical level of the phenomenon had to be reported on a weekly basis. The line of work on the deserters was augmented by personnel from MOI Directorate IV of Investigation, to analyze the cases of individuals arrested and prosecuted and forcibly returned by neighboring states, respectively.[51] In their summary reports, the MOI's top leadership kept emphasizing Hungary's harmful activities. Until the last minute of the dictatorship, the Hungarian authorities met their obligation of forcible return, in compliance with the bilateral agreement between the two states, they returned 87 individuals to the Romanian border guard authorities as late as the second week of December.[52] Analysts of the Surveillance Service subjected all those who had been officially returned by neighboring states to intensive operational processing. The regional authorities reported weekly summary statements of persons handed over by neighboring states or arrested after illegal entry into Romania to both the secret service leadership and the leadership of the Communist Party of Romania. From these statistics we know that in the second week of December, *"96 individuals arrived [sic] from the Hungarian People's Republic (87 were returned by the Hungarian authorities, and nine entered Romania illegally). Of the returnees, 53 stayed in the territory of the neighboring state for less than 24 hours, 34 stayed there for 2 to 30 days and those who arrived illegally for a maximum of 25 days."*[53] Individuals received or apprehended by the border guards and Securitate were checked in the context of Operation Alpha. This practically meant that the Romanian counter-intelligence officers analyzed the action taken by the Hungarian institutions, focusing on their covert recruitment of the "deserters" and steps taken to redirect them to Romania. These investigations were given great emphasis by the Romanian state security leadership, but the results did not always support expectations. This was evidenced by the instruction personally given in December by Iulian Vlad to Colonel Gheorghe Rațiu, Chief of Directorate No. I of Internal Intelligence. The then chief of Romanian state security voiced outrage at the Alpha operations due to low efficiency, and instructed the chiefs of the directorates: *"Check through again everything that*

49 ACNSAS Fund D 013783/1, pp. 19v-120v.
50 ACNSAS Fund D 013783/1, p. 74.
51 ACNSAS Fund D 013783/1, p. 43.
52 ACNSAS Fund D 013783/1, p. 1.
53 ACNSAS Fund D 013783/1, p. 2.

was reported before 6 December 1989, compare the data of the «basic elements of the operational situation» with the instructions received and the tasks performed on this line! Subsequently, assess whether the instructions had been carried out, and if not, determine the cause of the failure to do so."[54] It can be seen from the text that the investigations conducted against individuals returned by neighboring states and against persons returning to Romania illegally across the border did not yield an operationally relevant, i.e., usable, result.

Conclusion

Based on the processed archival sources, one of the risk factors endangering the security of the Romanian state became visible to the contemporary Romanian secret services. The number of illegal border crossings was high from the early 1970s to the mid-1980s, especially on the Yugoslav border. A turning point appeared in the statistics in the mid-1980s, as the number of people leaving the Hungarian-Romanian border illegally exceeded the number of Yugoslav cases in the previous period. At the end of the eighties, a significant number of Hungarian-speaking Romanian citizens illegally crossing the border appeared in the statistics of border crimes, so linking this fact to the encouraging, informative and other news coverage in the Hungarian press and in the Hungarian language broadcasts of Radio Free Europe presented the scenario of foreign powers intervention for the Romanian services.

The recurring leitmotif of intervention by foreign powers was promulgated by historians like Alex Mihai Stoenescu, Larry Watts, Remus Ioan Ștefureac and the former state security senior officers of the dictatorship like Iulian Vlad, Virgil MAGUREANU, Costache Codrescu. These authors argue regularly that official intelligence (counter-intelligence, military intelligence) sources projected the image of impending aggression by certain foreign powers implying actions by the Soviet Union[55] and Hungary, which, as they believe, provide evidence of the fact of foreign intervention in the events in Timisoara in December 1989,[56] and a spectacular proof of foreign intervention is seen in the number of illegal border crossings.

They all proclaimed the presentable version of the role the Securitate played in the events of 1989. An important part of this theory is the issue of foreign, namely Hungarian intervention, according to which theory Hungary played an active intelligence, what is more, military role in bringing down the Ceausescu regime.[57]

---

54 ACNSAS Fund D 013783/1.

55 The number of people crossing the Soviet-Romanian border illegally was negligible, so the question of intervention cannot be supported by the statistics of the Surveillance Service

56 SRI Preliminary Report on the Events of December. Part I (1/2), Timisoara, 1989: www.ceausescu.org/ceausescu_texts/revolutia/raportul-sri11.htm (downloaded 30 April 2021)

57 For more details, see István Bandi: The Question of Hungarian Intervention in the 1989 Romanian Revolution, in Betekintő (Insight), Year 14, Issue No 2, pp. 99-124. https://betekinto.hu/sites/default/files/betekinto-szamok/2020_2_bandi.pdf (downloaded 30 April 2021)

Bibliography:

- ACNSAS Fund Cadre MAI 000007
- ACNSAS Fund Cadre MAI 000077
- ACNSAS Fund D 013783/1.
- ACNSAS, Fund Cadre, Dossier 27753
- BANDI, István: The Question of Hungarian Intervention in the 1989 Romanian Revolution, in Betekintő (Insight), Year 14, Issue No 2, pp. 99-124. https://betekinto.hu/sites/default/files/betekinto-szamok/2020_2_bandi.pdf (downloaded 30 April 2021)
- CEAUȘESCU, Nicolae: Cuvintul la adunarea activului de partid si a cadrelor de conducere din Ministerul de Interne. Editura Politica, 1978.
- http://www.cnsas.ro/documente/cadrele_securitatii/TABACARU%20DUMITRU.pdf (downloaded 28 April 2019)
- https://pressone.ro/istoricul-madalin-hodor-in-1989-a-avut-loc-o-diversiune-militara-executata-de-armata-secreta-a-partidului/ (downloaded 28 April 2019)
- https://www.mapn.ro/repere_istorice/index.php (downloaded 30 April 2021)
- L. BALOGH, Béni: Changes in Empire in Transylvania and the Turnaround of 1944-1945; In: Our Time 2015/5. pp. 72-79. https://www.academia.edu/35747179/ (downloaded 28 April 2019)
- MĂGUREANU, Virgil – STOENESCU, Alex Mihai: De la regimul comunist la regimul Iliescu. Virgil Măgureanu in dialogue with Alex Mihai Stoenescu [From the Communist Regime to the Iliescu Regime. Virgil Măgureanu in conversation with Alex Mihai Stoenescu], Bucharest, Editura RAO, 2008.
- NEAGOIE, Sever – VĂDUVA, Gheorghe – TENDER, Ilie: History of French and French Policies in the Front; Editura Scaiul, Bucharest, 2004
- SRI Preliminary Report on the Events of December. Part I (1/2), Timisoara, 1989: www.ceausescu.org/ceausescu_texts/revolutia/raportul-sri11.htm (downloaded 30 April 2021)
- STEFUREAC, Ioan Remus: Conflictul secret din spatele scenei România versus Rusia. 50 de ani de realități, mituri si incertitudini [The secret conflict behind the scenes. Romania versus Russia. 50 Years of Reality, Myth, and Uncertainty], Bucharest, Editura RAO, 2015.
- WATTS, Larry: Ferește-mă doamne de prieteni, războiul clandestin al blocului sovietic cu România [Protect me, Lord, from my friends! The secret war of the Soviet bloc against Romania]. Bucharest, Editura RAO, 2012.
- WATTS, Larry: Here are some of them. România și sfârșitul războiului rece [The first will be last. Romania and the end of the Cold War], Bucharest, Editura RAO, 2013.

NIKOLETT KATALIN BÚS

THE LONG-TERM CORPORATE SUCCESS – SAFE COMPANY

Abstract

The author helps the organization understand where they stand on the road to an effective safety culture. Once we know this starting point, targeted measures can be taken to increase the level of security.
During her research, the author tried to make the leadership group to make a self-confession, for that purpose she prepared a safety awareness survey sheet. After evaluating the result, it was integrated into the organizational goal hierarchy as part of the Company's operational structure, sort of a safety awareness goal focus. A safe company can only succeed.

***Keywords*:** organizational culture, safety awareness survey, safe company, safety awareness

Introduction

I want to present the subject of my publication on the example of a large Hungarian company – without naming it. There has been a change in the top management of a large company that has been accompanied by an organizational transformation program aimed at laying the groundwork for increasing competitiveness. A lot of internal processes have been reviewed in the program. The results of the first analyses seemed to show that in many cases the processes were not related to each other according to the rules (in terms of quality assurance). In practice, however, it seemed to work well, but it also turned out that the Company owed it to an employee. In this analytic work, I formulated as my goal to help analyze the status of the specialty area within my sphere of responsibility.

The aim of the research, its investigation aspects

The basic aim of my research was to prove that competitiveness depends on the culture developed within the company, the attitudes and commitments of the leaders of the organizational unit. In my work, I have seen their shortcomings, however, there was no tool of such probative power in my hands to bring about change. I kept the organization under control through ongoing training, inspections, and annual regulatory reviews. I have identified that my personal commitment is not enough to prevent accidents at work. My common experience with accidents and injuries is that it is not a single factor that plays a role in their occurrence. Contrary to popular belief, a significant proportion of accidents do not depend on a single fault. The effect of several consecutive “cumulative” factors leads to the occurrence of an accident. Investigations and analyses following accidents often reveal that, in addition to the immediate cause of the accident, one or more events occurred prior to the accident that contributed to or were decisive in the development of the accident situation. At

this point in my work, I have to examine the behavior of the people involved and their contribution and responsibility in the development of the accident situation. In each case, reaching the leadership level - the shortcoming can be identified.

Research goals, hypotheses

The goal of my research is to explore the level of state-owned large enterprise safety culture on the senior and middle management levels based on empirical analysis, and will try to find an answer to the question of what action plan the leaders taking part in the survey can receive as a supplement to their performance assessment, what personal task can be set for a leader.

Research objectives	Research hypotheses
O1: The research seeks an answer to determine the level of safety culture in a state-owned enterprise.	H1: A safety awareness survey can be set up from the findings of the company's operations.
O2: The research seeks to answer the question of how business leaders can be encouraged to increase their safety performance.	H2: In the strategic planning of companies, it is necessary to present actions for the health and safety of employees as a separate element. H3: Corporate safety cannot be maintained without the leaders setting an example.

The material and method

In order to achieve my research goals, I processed the literature closely related to the topic and collected information on the methodologies for assessing the 'Safety Culture'.[1]

In addition to the factors set out in the guidelines, the functional framework of the organizational safety culture has also expanded in practice. Accordingly, the processes related to safety operate on different levels of the corporate hierarchy with different tasks and regulations, however, in their underlying content, the primary requirement is the widespread enforcement of safety awareness and the implementation of cooperation.[2]

My publications designed to provide literature background to introduce the knowledge of the frameworks, approaches through a survey conducted on corporate safety culture. Following the survey, proposals for action have been defined and identification of the program has been included in the corporate target hierarchy.

---

1 KERTAI-KISS, Ildikó: The organizational framework of safety culture, TAYLOR, Journal of Management and Organizational Sciences, 2015/3-4

2 LAZÁNYI, Kornelia: The Role of Safety Culture in Supporting the leaders' Decision Making; TAYLOR, Management and organization science journals, 2016/1

DuPont believes that the role of leadership in the transformation of the company's safety culture is extremely important and comprehensive.[3,4] I received no financial resources to prepare and carry out the project, so I continued my research on what theoretical implementations I could use and compile a survey myself. Questionnaire survey is the most commonly used research method in the social sciences. In a typical questionnaire survey, the researcher selects a sample and then takes a standardized questionnaire with each person included in the sample. I extended the scope of sampling to senior and middle management. A questionnaire survey is the best available method to collect original data to describe a population that is too large for direct observation. Careful probability sampling provides a sample that can be assumed to meet the characteristics of a larger population, and a carefully designed standardized questionnaire provides data on all respondents in the same format.[5]

Questionnaire surveys are also great for measuring the attitudes or orientations of a larger population. The questionnaire can be used as a specially designed tool to explore information for analysis, and an understanding of the underlying logic can be helpful at any time when interviewing people for data collection. The term questionnaire refers to a set of questions, but if we look at a questionnaire, we probably find at least as many statements in it as there are questions.[6] In this case, the questioner wants to know to what extent the respondent shares a certain attitude or view. Remszisz Likert, when he developed the Likert scale, in which he asks the respondent to choose one of the following alternatives: wholly agree, agree, do not agree, do not agree at all.[7]

In my survey, I identified the evaluation line according to the Likert scale[8] according to as a response.

My questions in the survey are brief, reflecting my commitment to clarity, accuracy, and expression of the importance of the topic. When compiling the series of questions, I tried to make the respondents answer quickly after reading the questions quickly. I tried to convey the inspiring effect of the questions and expressions in front of the respondents.

When compiling the questions of the survey sheet my intent was to obtain data ready for analysis and interpretation from the respondents.

---

3 https://prevenblog.com/en/what-can-we-learn-from-the-bradley-curve/ (downloaded 04 April 2020)

4 https://www.ehstoday.com/safety/article/21918409/safety-and-performance-excellence-behind-the-bradley-curve (downloaded 04 April 2020)

5 BABBIE, Earl R.: The Practice of Social Science Research; Balassi Publishing House, Budapest, 2001, ISBN 963 506 563 9

6 Ibid.

7 BROWN, JD: Likert items and scales of measurement? JALT Testing & Evaluation SIG Newsletter. 2011 March 15 pp.10-14. http://jalt.org/test/PDF/Brown34.pdf (downloaded 21 April 2020)

8 https://spssabc.hu/kutatasmodszertan/likert-skala-fogalma-elemzese/ (downloaded 21 April 2020)

The second part of the survey sheet is made up of closed questions which were mutually exclusive categories in response. My goal was to make the respondent rank the response categories.

The survey form was completed during one of the management meetings so non-response was ruled out. Respondents are essentially a random sample of the original sample, and thus a somewhat smaller random sample of the entire population. The management meeting provided an appropriate framework for completing the survey form and thus expected a high response rate. However, I determined before the start of the survey that an at least 50% response rate is acceptable so that the results and reports can be realized. A minimum of 60% response rate is good and a 70% response rate is excellent.[9] The result showed a 100% response rate.

During survey research it can be surmised that the survey tone / style / structure means the same to every respondent and that each response means the same, regardless of the respondent, so I conducted a pilot test before the questionnaire survey went live. The pilot test resulted in confirmed feedback that I made the best possible approach to the objective of determining the safety awareness status of the company.

As a result of my work, I prepared the following safety awareness survey sheet with input from my colleagues (Figures 1 and 2) **H1: A safety awareness survey can be set up from the findings typical of the company's operations.**

The survey form was completed during a company management meeting at an outside location. The willingness of the respondents was exemplary; it is summarized in Figure 1.

[9] https://journals.lib.pte.hu/index.php/mm/article/view/1717/1552 (downloaded 06 April 2020)

SAFETY AWARENESS SURVEY SHEET

Please tick one box only!

		Not at all	Not typically	Generally	Fully
1.	"Safety rides first!" Do you also live your everyday life, planning and executing your activities accordingly?	☐	☐	☐	☐
2.	Do you subscribe to the approach that work related accidents can be prevented?	☐	☐	☐	☐
3.	To what extent is labor safety present in your organizational unit?	☐	☐	☐	☐
4.	Do employees in your organization take part in setting health and safety goals, are their opinions reflected in these goals?	☐	☐	☐	☐
5.	When you notice a labor safety irregularity, do you stop irregular work performance?	☐	☐	☐	☐
6.	Are good labor safety practices, efforts appreciated in our Company?	☐	☐	☐	☐
7.	Does labor safety impact quality, productivity, profit?	☐	☐	☐	☐
8.	To what extent do you agree to middle management and work controllers taking preventive actions daily to ensure that safe work conditions, safe work activities are implemented?	☐	☐	☐	☐
9.	Are the Company's health and safety regulations comprehensible, easy to comply with, do they contribute to safe work?	☐	☐	☐	☐
10.	To what extent are labor safety regulations complied with in your organization?	☐	☐	☐	☐
11.	How well do you know work safety goals, results?	☐	☐	☐	☐
12.	Do you think the effectiveness of work safety aspects in your organization is satisfactory?	☐	☐	☐	☐
13.	To what extent do you consider it your own personal commitment, yourself to be empowered to take action for safe work?	☐	☐	☐	☐
14.	In meetings and briefings, are work safety aspects covered?	☐	☐	☐	☐
15.	Do you join investigations of work safety incidents, proposals for work safety, taking preventive actions?	☐	☐	☐	☐
16.	How regularly are you involved/do you take part in work safety audits, controls and site inspections?	☐	☐	☐	☐
17.	How effective do you think work safety inspections are (take into consideration their frequency, the thoroughness of the inspections, follow-up inspections, all forms of support that contribute to safer work)?	☐	☐	☐	☐
18.	Do you consider the work safety status of your workplace in light of work conditions?	☐	☐	☐	☐
19.	Does prevention appear in your activity?	☐	☐	☐	☐
20.	Do you have an opportunity to confer with your superiors regularly on work safety issues?	☐	☐	☐	☐
21.	Do you perceive the significance of employees not using personal protective equipment, what consequences may result from failure to use PPE?	☐	☐	☐	☐
22.	Do work controllers and leaders always have the time to inform or warn the employees of the work safety regulations, the importance of complying with them?	☐	☐	☐	☐
23.	To what extent do you think employees are satisfied with their work environment conditions?	☐	☐	☐	☐
24.	Can employees perform their jobs within the expected time limit while continuously complying with the required work safety regulations?	☐	☐	☐	☐

Figure 1: The front page of the safety awareness survey sheet
(Author's own edition)

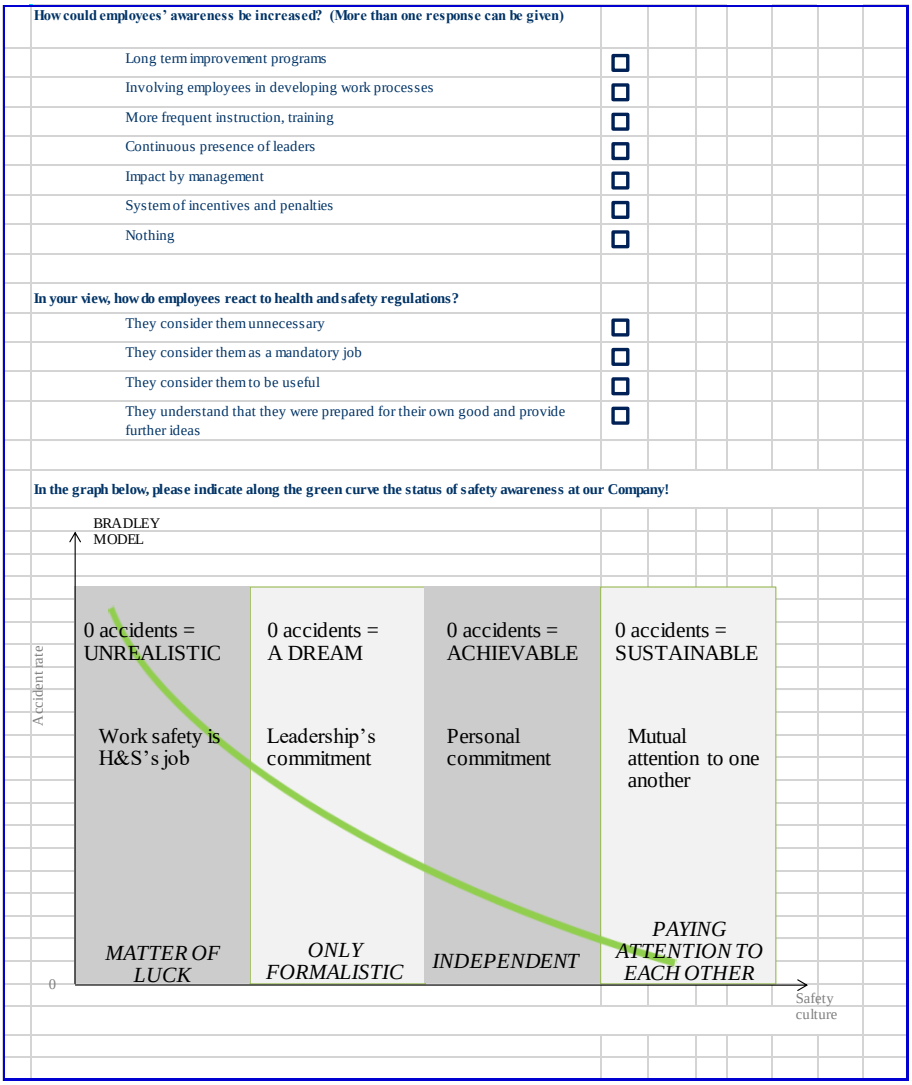

Figure 2: The back page of the safety awareness sheet
(Author's own edition)

The safety awareness questionnaire was completed by 28 people. Respondents were selected from the top and middle management levels of the Company. The result was determined for the percentage projection of the 4 categories given to the answers (not at all; not typical; in general; completely), which is shown in Figure 3, Figure 4 and illustrated visually.

Research results

		Answers	Not at all	Not typically	Generally	Fully	Not at all	Not typically	Generally	Fully
1.	"Safety rides first!" Do you also live your everyday life, planning and executing your activities accordingly?	28	0	4	13	11	0	14,29	46,43	**39,29**
2.	Do you subscribe to the approach that work related accidents can be prevented?	28	0	1	13	14	0	3,571	46,43	**50**
3.	To what extent is labor safety present in your organizational unit?	28	0	3	19	6	0	10,71	67,86	**21,43**
4.	Do employees in your organization take part in setting health and safety goals, are their opinions reflected in these goals?	28	3	10	12	3	10,71	35,71	42,86	**10,71**
5.	When you notice a labor safety irregularity, do you stop irregular work performance?	28	0	4	10	14	0	14,29	35,71	**50**
6.	Are good labor safety practices, efforts appreciated in our Company?	28	1	9	12	6	3,571	32,14	42,86	**21,43**
7.	Does labor safety impact quality, productivity, profit?	28	0	4	8	16	0	14,29	28,57	**57,14**
8.	To what extent do you agree to middle management and work controllers taking preventive actions daily to ensure that safe work conditions, safe work activities are implemented?	28	1	9	12	6	3,571	32,14	42,86	**21,43**
9.	Are the Company's health and safety regulations comprehensible, easy to comply with, do they contribute to safe work?	27	1	4	15	7	3,704	14,81	55,56	**25,93**
10.	To what extent are labor safety regulations complied with in your organization?	28	1	0	19	8	3,571	0	67,86	**28,57**
11.	How well do you know work safety goals, results?	28	1	3	16	8	3,571	10,71	57,14	**28,57**
12.	Do you think the effectiveness of work safety aspects in your organization is satisfactory?	28	1	3	21	3	3,571	10,71	75	**10,71**
13.	To what extent do you consider it your own personal commitment, yourself to be empowered to take action for safe work?	28	0	5	3	20	0	17,86	10,71	**71,43**
14.	In meetings and briefings, are work safety aspects covered?	28	2	5	15	6	7,143	17,86	53,57	**21,43**
15.	Do you join investigations of work safety incidents, proposals for work safety, taking preventive actions?	28	2	9	11	6	7,143	32,14	39,29	**21,43**
16.	How regularly are you involved/do you take part in work safety audits, controls and site inspections?	28	6	9	12	1	21,43	32,14	42,86	**3,571**
17.	How effective do you think work safety inspections are (take into consideration their frequency, the thoroughness of the inspections, follow-up inspections, all forms of support that contribute to safer work)?	26	1	12	10	3	3,846	46,15	38,46	**11,54**
18.	Do you consider the work safety status of your workplace in light of work conditions?	28	1	5	15	7	3,571	17,86	53,57	**25**
19.	Does prevention appear in your activity?	28	1	6	16	5	3,571	21,43	57,14	**17,86**
20.	Do you have an opportunity to confer with your superiors regularly on work safety issues?	28	3	9	13	3	10,71	32,14	46,43	**10,71**
21.	Do you perceive the significance of employees not using personal protective equipment, what consequences may result from failure to use PPE?	28	0	1	4	23	0	3,571	14,29	**82,14**
22.	Do work controllers and leaders always have the time to inform or warn the employees of the work safety regulations, the importance of complying with them?	28	1	7	19	1	3,571	25	67,86	**3,571**
23.	To what extent do you think employees are satisfied with their work environment conditions?	28	1	7	19	1	3,571	25	67,86	**3,571**
24.	Can employees perform their jobs within the expected time limit while continuously complying with the required work safety regulations?	27	3	5	12	7	11,11	18,52	44,44	**25,93**

Figure 3: The distribution of the answers in the safety awareness survey and their transformation into percentages
(Author's own edition)

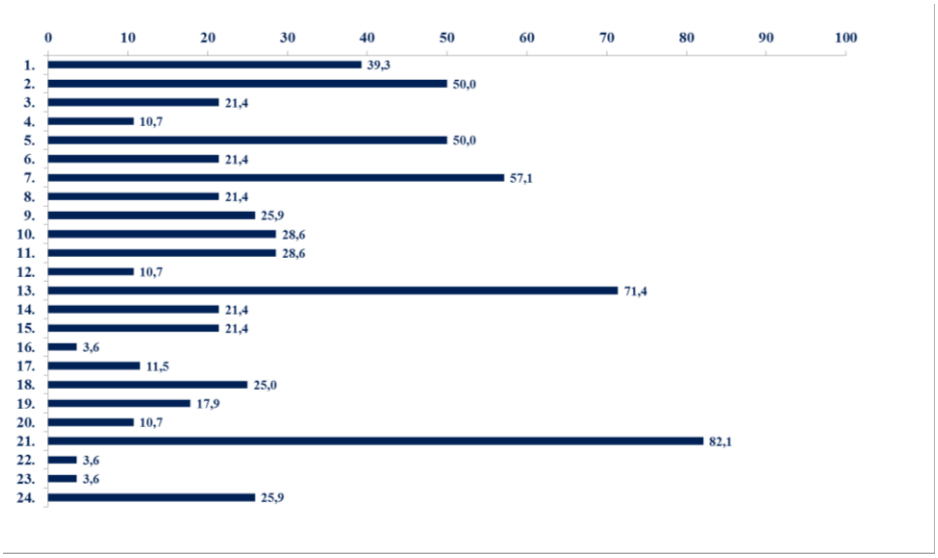

Figure 4: Distribution of safety awareness 1-24 questionnaire responses
(Author's own edition)

The most significant summary correlations established on the basis of the results of the questionnaire survey

By reading my words hidden in the questions from the evolution of the results. Two management "testimonies" can be identified for the most confirmed and the least valued statement of the results:
"As a manager, I don't have time to be there in the locations to regularly check, inform, warn to make an impact on improving conditions of the working environment."
Alternately:
"I agree that work related accidents can be prevented, for this I consistently prevent, do not tolerate the continuation of irregular work, work safety affects quality, productivity, profit. I am personally committed! "

I formulated both identified 'testimonies' in order to achieve a deep impact and a great impression among the respondents. Holding up a mirror, as it were, set up in the present situation to reflect their performance.

Based on my research results, I concluded that **H2: In the strategic planning of companies, it is necessary to display actions aimed at the health and safety of employees as a separate element.** Following the survey, I managed to identify two actions – which, by permission of the CEO I could supplement as part of the announced goal hierarchy (Table 1), so the evaluation criteria was included in their performance assessment. Setting a personal exemplary and "visible leader" is a fact that increases job safety in the operation of a large company, which makes the success of actions for the health and safety of employees.

Target focus		Indicator	Quantity	CEO	Technical area 1.	Technical area 2.	Technical area 3.
Safety awareness	Personal example/ visible leader	Promotions	pieces	x	x	x	x

Figure 5*: *Excerpt of the target hierarchy table according to the topic of the publication
(Author's own edition)

I sat with the directors of the specialty areas separately for a personal interview in which we reviewed survey results considering the provisions of the target hierarchy, we set individual directors' commitments. As a result, and to increase personal example, a visible leadership program was announced. **H 3: Corporate safety cannot be maintained without the personal example of management.**

The monitoring of the achievements recorded in the target hierarchy table, the evaluation of the set programs, and the reporting to the top management were within my area of responsibility.

Summary

In my publication, I proved that a safety awareness survey can be set up from the findings of the company's operations. I found that those who took part in the safety awareness survey are committed and identify their role in the operation of the organization, and corporate safety cannot be maintained without the personal example of its leaders. In the numerical assessment, the leaders could better identify their corporate performance, their preparedness in terms of safety culture. In the strategic planning of companies, it is necessary to display actions for the health and safety of employees as a separate element.

With the security awareness survey and its findings, I wished to demonstrate that a safe company can be established and operated, in which values and forms of conduct appear that as a result of an agreement between leaders and employees ensure primacy of safety over all other competing objectives, for the benefit of employee safety and environmental protection.

I do believe that attention paid to safety at work, resources, consistently structured procedures, can appear as a competitive advantage in an economic environment.

Bibliography:

- BABBIE, Earl: The Practice of Social Science Research, Balassi Publishing House, Budapest, 2001, ISBN 963 506 563 9
- BROWN, JD: Likert items and scales of measurement? JALT Testing & Evaluation SIG Newsletter. 2011 March 15 pp.10-14. http://jalt.org/test/PDF/Brown34.pdf (downloaded 21 April 2020)
- KERTAI-KISS, Ildikó: The organizational framework of safety culture; TAYLOR, Journal of Management and Organizational Sciences, 2015/3-4
- LAZÁNYI, Kornelia: The Role of Safety Culture in Supporting the leaders' Decision Making; TAYLOR, Management and organization science journals, Year 2016/1
- https://journals.lib.pte.hu/index.php/mm/article/view/1717/1552 (downloaded 06 April 2020)
- https://prevenblog.com/en/what-can-we-learn-from-the-bradley-curve/(downloaded 04 April 2020)
- https://spssabc.hu/kutatasmodszertan/likert-skala-fogalma-elemzese/ (downloaded 21 April 2020)
- https://www.ehstoday.com/safety/article/21918409/safety-and-performance-excellence-behind-the-bradley-curve (downloaded 04 April 2020)

ÁGNES JOBST PHD.

AN ALLY IN THE CROSSHAIRS? THE INTELLIGENCE COOPERATION BETWEEN THE GERMAN DEMOCRATIC REPUBLIC AND THE HUNGARIAN PEOPLE 'S REPUBLIC

Abstract

The Ministry of State Security, commonly known as the Stasi was the official state security service of the German Democratic Republic (GDR). The Main Directorate for Intelligence (Hauptverwaltung Aufklärung) was responsible for the espionage and for conducting covert operations in foreign countries. It has been described as one of the most effective intelligence agencies ever to have existed. One component of the successes was the extensive cooperation with its eastern "sister services". The Cooperation with the Hungarian Ministry of Home Affairs began after the Multilateral conference in Moscow in the spring of 1955, the first Agreement was signed in May 1958. Of particular mutual interest was the espionage against the Federal Republic of Germany (FRG), where active Hungarian immigrant organizations were functioning. The agreement was renewed in 1963 and 1981. At the same time, when Hungary stepped on the road of democratization in the second half of the 1960s, the political changes made the earlier ally a target. Unofficial co-workers of the operational group maintained by the Stasi in Hungary – originally for security of East German tourism – began to gathering information on several occasions about crucial Hungarian domestic and foreign affairs as well.

Keywords: GDR, Stasi, Hungarian People's Republic, Intelligence, Counter-espionage, GDR, Stasi, Hungary, Intelligence, Counterintelligence

The present study, divided into two parts, first reviews the intelligence cooperation between the German Democratic Republic (hereinafter: GDR) and the Hungarian People's Republic based on the agreements, the protocols of the preparatory work group meetings and on the summary reports. Following this, it continues to look at how Hungary, a former partner and ally, got into the crosshairs of the East German intelligence.

Intelligence cooperation between the German Democratic Republic and the Hungarian People's Republic

The leaders of the state security services, at a meeting held in Moscow between March 7 and 12, 1955 carried on consultations on the Intelligence coordination among the socialist countries, Marshal Ivan Serov, head of the Soviet secret service, the KGB, identified infiltration into the state, political, economic, and military organizations of the capitalist countries as a common goal. During the division of target countries, the Hungarian intelligence agencies were tasked with infiltrating the western countries dividing where a significant number of Hungarian emigrants lived. In this way, the focus of Hungarian intelligence was on the Federal Republic of Germany (hereinafter:

the FRG), Austria, France, Great Britain and the United States. The Minister of the Interior, László Piros, who headed the Hungarian delegation, reported on what had been said at the Moscow meeting at the meeting of the MDP Political Committee.[1] The Hungarian People's Republic and the GDR's state security agencies then signed the first agreement on cooperation, pursuant to which the Hungarian Ministry of the Interior delegated an operational unit to the eastern sector of the German capital. The intelligence *rezidentura* working against the FRG was established under the cover of the Hungarian Embassy in April 1955.[2] On 17 May 1955, Major Antal Fehérvári, Head of the East Berlin Operational Task Force, approached Erich Mielke, Deputy Head of the Ministry of State Security (hereinafter: MSS, commonly known as Stasi) for support.[3] He requested intelligence on the Hungarian émigré groups, their leaders, the Hungarian Section of Radio Free Europe, individuals *"on the payroll of hostile intelligence services working against the people's democracies"*, on the refugee camps in the western countries and on Hungarians living in East Berlin. The MSS only provided substantial intelligence on the refugee camps, furthermore gave information on Hungarians living in East Berlin and on their transit route to West Berlin. No substantive professional cooperation unfolded because up until then the East German had not paid any attention to Hungarian immigrants living in West Germany.

The uprising that broke out in the GDR on 17 June 1953, and the revolution in Hungary that broke out on 23 October 1956 called attention to the threats emerging from a lack of legitimacy of the political leadership, to the vulnerability of the states of the eastern bloc. The party leadership blamed the hostile foreign secret services and the "inciting activities" of the exile organisations working hand in hand with them for the outbreak of the uprising, therefore they tightened the cooperation with the secret services of the allied countries. The heads of state security of the Warsaw Pact member states met in Moscow in November 1957. In April 1958, Minister of the Interior Béla Biszku, referring to their November meeting, wrote a letter to the Minister of State Security Erich Mielke proposing to hold a bilateral meeting.[4] He suggested that the subject of the meeting be a common fight against the hostile centres in the FRG and West Berlin, and put forward a proposal for an exchange of information of a political, economic and military nature, falling in the interest of both countries. The meeting took place in Berlin, 19-22 May 1958. The members of the three-man Hungarian delegation were Minister of the Interior Béla Biszku, Police Colonel Jenő Hazai, Head of MOI II/2. (Counter-Intelligence) Directorate and Police

---

1 PALASIK, Mária: Organization and staff of the Intelligence Department, 1956–1962; Insights, 2011/2. pp. 4-5. www.betekinto.hu/2011_2_palasik (downloaded 20 December 2014)

2 ÁBTL 3.2.6. Rezidentura files. Organizational file for the Berlin rezidentura; JOBST, Ágnes: The operation of Stasi in Hungary. The relationship between East German and Hungarian state security 1955−1989; Jaffa Publishing House, Budapest, 2015. pp. 44-59. ISBN 9786155492471.

3 HERBSTRITT, Georg: The "Balkan File" of the GDR Ministry of State Security. Secret service measures against Hungarian immigration in West Germany; Historical Review, 2008/1. p. 111. In his study, Herbstritt refers to József Huszár covername as the first leader of the task force, which testifies that during this period of the Cold War, strict secretiveness was in place to protect the rezidentura even from intelligence personnel of friendly countries.

4 ÁBTL 1.11.12. Letter from Béla Biszku, Minister of the Interior, to Erich Mielke, Minister of State Security. April 3, 1958

Lieutenant Colonel István Móró, Head of MOI II/3. (Intelligence) Directorate. The German party was represented by Minister of State Security Erich Mielke, and Deputy Ministers Markus Wolf and Bruno Beater. Referring to the similarities between the geopolitical situations of their countries, i.e., directly neighbouring on countries of the opposing bloc, and in connection with that referring to the internal and external security, the signed a cooperation agreement including 16 points.[5] The main areas of cooperation identified by the Cold War logic were:

- exchange of information related to international organizations (NATO, the Socialist International, the international Trotskyist organizations, European Socialist Movement, churches);
- sharing of intelligence on the political parties and government agencies of the FRG, on the domestic policies of Austria, furthermore on the intelligence gathered on the diplomatic missions of the United States, the UK and the FRG;
- sharing of information on the agent situation with regard to the FRG and Austria;
- evaluation of the information shared;
- cooperation in the field of scientific and technical intelligence;
- exchange of information in the field of counter-intelligence: mainly for the secret services of the FRG, West Berlin and Austria, the US, the UK and France and the Hungarian immigrant organizations (Volksdeutsch groups, Hungarian Warriors' Comradely Union, Hungarian refugee offices). Development of covert operations based on the intelligence obtained;
- operational processing of Radio Free Europe;
- Operational processing of NATO training centres preparing armed diversion against the socialist countries armed diversion;
- fight against ideological diversion;
- processing of citizens (businessmen, professionals, tourists) of capitalist countries entering the territory of the GDR and the Hungarian People's Republic;
- detecting the activities of trusts;
- mutual assistance in carrying out illegal infiltrations (planting sleeper agents/cells), sharing of information obtained on hostile agents illegally infiltrated into the partner’s territory;
- participation of the GDR Ministry of State Security in the operational control of 1956 refugees of Hungarian nationality and citizenship intending to return to Hungary across East German territory;
- sharing resources of an agency with other party for the accomplishment of specific tasks, providing the data necessary for recruitment.
- cooperation in the field of operational technology;
- data service, making copies archival materials made before and after World War II.

[5] ÁBTL 1.11.12. 41-11-N-32/10-68. Protocol on operational cooperation between the Ministry of the Interior of the Hungarian People's Republic and the Ministry of State Security of the German Democratic Republic. March 19-22, 1958

The reports written in 1959 reports assessed the results of the cooperation all the way back to May 1958 to May, which was realised primarily in the area of sharing information, preparing background checks of Hungarian military immigrants living in the FRG, and granting assistance in covert operations.[6] The East Germans, in the context of the exchange of information, shared photographs and intelligence on the intelligence services of the USA, UK, and France operating in the FRG and West Berlin, on the state administration, domestic policy, counter-intelligence agencies of the FRG, and Institutes of Eastern Studies (Kremlinology), in addition they undertook language training of Hungarian intelligence officers planned for deployment in German-speaking countries.[7] In addition to the above, the Hungarian party also relied on their east German partner's assistance in the processing of the German ethnic minority in Hungary and in countering the West German intelligence. The Hungarian party shared information on Radio Free Europe, on the allied intelligence services operating in Austrian and German territories, on the interview techniques of the Austrian intelligence and counter-intelligence agencies, furthermore on Hungarian immigrants' organisations operating in the FRG. They shared their intelligence on the FRG Embassy staff accredited to Italy and Vatican, on the Jesuit Order, and on the agent situation in Austria,[8] and collected data on West German citizens entering Hungary.

A new situation came about on 13 August 1961, with the erection of the Berlin Wall, referred to as the "anti-fascist protective barrier" because the hermetic closure also made intelligence work more difficult in the German capital. The bilateral meeting held on 8-11 May 1963 in was attended by the six-member Hungarian delegation headed by Minister of Interior János Pap, its members were Deputy Minister of Interior József Galambos, Deputy Director General József Németi, Head of the Intelligence Directorate Vilmos Komornik, Head of the Counter-Intelligence Directorate Lajos Karasz, and Head of the Operational Technology Directorate Imre Markó. The four-member GDR delegation was headed by Minister for State Security Erich Mielke, its members were Deputy Minister for State Security Markus Wolf, Head of the Counter-Intelligence Division Werner Grünert and Head of the Operational Technology Division Herbert Hentschke.[9] The main focal areas of intelligence efforts continued to be the intelligence services of the FRG, the United States, the UK, and France, the Hungarian immigrant communities, Radio Free Europe, and the "training facilities used by diversionary groups supervised by NATO", but exchange of information in the area of political, military and economic intelligence gained increased importance. In connection with the last point it was agreed to mutually provide each other assistance in the organization and conduct of

---

6 ÁBTL 1.11.12. 11/109/59. Report on our relations with the state security agencies of the GDR. March 17, 1959; 63-540/1959. Report on the state of implementation of the agreement concluded in May 1958 between the Ministry of the Interior of the HPR and the Ministry of State Security of the GDR.

7 ÁBTL 1.11.12. 41-N-5519/62.

8 ÁBTL 1.11.12. 11/109/59. Report on our relations with the state security agencies of the GDR. March 17, 1959; Ibid., 63-540/1959. Report on the state of implementation of the agreement concluded in May 1958 between the Ministry of the Interior of the HPR and the Ministry of State Security of the GDR.

9 ÁBTL 1.11.12. 41-11-N-32 / 12-68. Protocol on cooperation between the Ministry of the Interior of the Hungarian People's Republic and the Ministry of State Security of the German Democratic Republic. May 11, 1963

fairs and international events, which involved the “processing” of participants coming from the capitalist countries. The new agreement also allowed the mutual “utilization” of Hungarian and East German citizens for operational purposes, that is, the transfer of assets.[10]

Although the crises of the Cold War era were followed by a détente of international tension, the emerging image of the enemy based on the content of the renewed agreements proved to be rather static. A unique episode of the cooperation was the extraction of the leaders of the Chilean Communist Party and their family members following the September 1973 military coup in Chile. The operation involving 8-10 persons was coordinated on the Hungarian side by Janos Berecz, Head of the Foreign Affairs Department of the HSWP, and by Markus Wolf, the East German intelligence chief.[11] The development of the new guidelines of operational cooperation took place in 1974.[12] A new element appeared in it, the monitoring of the Chinese "dissident and great power" foreign policy, the exchange of methodological studies in the field of operational psychology, and the changes in the classified administration of classified data and documents shared in the information exchange process. While previously only the classification of the information shared was indicated, the new administration rules stipulated that the information shared could not be further shared with other friendly countries without the permission of the originator of the information. However, the signing of the draft agreement of 1974 did not take place for unknown reasons.

The apropos of renegotiating cooperation was provided by events unfolding in Poland. An agreement broadly identical to the draft agreement of 1974 was signed in 1981. Political intelligence continued to focus on the United States and the FRG. Due to the strained Soviet-Chinese relations, a prominent role was given to China's foreign and domestic policies, and last but not least, to the reception in the West of the Soviet Union's new foreign policy. Increasing attention was paid to the economic area, to the EEC reforms and its relationship with the COMECON and to the appearance of Western banks in the socialist countries. During the preparation of the 1981 agreement, an evaluation of the information exchange with the Hungarian side was made. The staff of the Stasi considered the news materials shared with them in the 1960’s and 1970’s particularly helpful in the following areas:

---

10 At that time, the agent with the codename “Balaton” was handed over from the Hungarian side, who, being a former Colonel of the 2nd Directorate of the General Staff, had a good intelligence opportunity among the immigrant military officers living in the West ÁBTL 3.2.1. Bt-262/4. Work file of an agent codenamed "Balaton"

11 In the mid-1970s, the international coalition surrounding the rescue operation was unusual, in which the Austrian Ministry of Foreign Affairs and the Vatican took an active role due to the closure of the Chilean foreign missions of the socialist countries. The GDR undertook to accommodate 300, Poland 200 and Hungary 100 refugees from Chile. BStU MfS Abt. X. 2149.

12 ÁBTL 1.11.12. Without Registry Number. Agreement. Budapest, September 1974 dn The draft kept in Hungarian and German archives is missing the signature. Since only unsigned copies survive, it is dubious whether this agreement was ever signed or due to hopes of introducing SZOUD (automated) system the signatures were left out.

- the cooperation of the imperialist secret services (CIA, SIS, BND)[13] with intelligence services in developing countries;
- surveillance and processing of the diplomatic missions of the socialist countries in various countries, especially in the countries of the Third World;
- reorganization and operation of counter-intelligence agencies in African and Arab countries;
- the activities and staff of hostile radio stations (RFE/RL/SZER, RIAS)[14];
- methods of interviewing refugees in West German, Austrian, Italian and Turkish refugee camps.

We can form a picture of the cooperation in the 1980s based on the report of the Hungarian partner. The summary report on the years 1982-1988 of years found merely 7% (in figures: 279 of 1942) of the 250-350 pieces of intelligence shared by the East German colleagues annually to be useful, so the Hungarian evaluation of the exchange of intelligence is less positive.[15] It is uncertain whether this is due to the withholding of substantive information, or to a specific need for information now defined by national interests, or to other factors hidden in the background. The last meeting at department level on the subject of intelligence cooperation was held in Budapest, 18-22 June 1988. Summarizing the discussion, the experience of the Hungarian partner took the view that the talks *"have contributed positively to the correct identification of the intelligence targets and means under the current socio-political situation"*, that is, during the erosion of the regime.[16]

Hungary in the light of the Stasi reports, 1968 - 1981 - 1988

As the years in the heading indicate, the "mustering of troops" in the countries of the Eastern Bloc was given special significance in those fateful years; to see whether the partners are actually reliable and trustworthy allies. In the system of relations between the socialist countries, the question of the assessment of reforms was central. The Orthodox GDR party leadership viewed the Eastern Bloc's countries open to reforms, Poland, Czechoslovakia and Hungary, with great distrust. From the summer of 1964 on, the mission of the Stasi operational groups operating in Hungary was formally to "secure" East German tourism, but their tasking was extended to observation of the government agencies of the host country mandates the host country's government bodies, its domestic and foreign relations, public sentiment.[17] The rigid and partisan East German approach of the reports differed significantly from the Hungarian mentality. On 13 November 1975, for example, an unofficial co-worker of the Stasi, working in one of the Tourist agencies called attention to the fact that a Hungarian tour guide working with a group of East German tourists spoke at length about past centuries of Hungarian history, but said very little about the achievements

13 Central Intelligence Agency, Secret Intelligence Service, Bundesnachrichtendienst

14 Radio Free Europa/Radio Liberty; Radio in the American Sector – A radio station established in West Berlin on July 7, 1946, which operated until November 9, 1989, the fall of the Berlin Wall.

15 ÁBTL 1.11.4. 67-87-550/1988.

16 ÁBTL 1.11.4. 67-87-550/1988. Note on scientific and technical intelligence with the GDR. October 5, 1988

17 BStU MfS AIM 3812/92. Social contact codenamed "Erik" and BStU AIM 14770/89. Tl. II / 1-2. Archived personal material of an agent codenamed "Barbara Lubinski"

of the Hungarian working class after 1945.[18] The Western periodicals freely accessible in public libraries in Hungary did not escape their attention either, these were dangerous weapons of ideological loosening in the eyes of the Stasi employees.[19]

Prior to the deployment of the agents, their control officers drew up an employment plan for them, which set out in writing the areas in which they were required to report in writing. For example, the tasking of a GDR agent under the cover name "Horst Schwalbe", planted in Hungary in June 1986, included gathering information on the Hungarian political relations, the observation of current national and political events, the monitoring of large-scale events , the political and ideological diversion phenomena.[20] In September 1986, a college professor from Leipzig visited several Hungarian colleges, including the Department of Scientific Socialism at the Kálmán Kandó College of Electrical Engineering. Based on the exchange of experiences with college instructors, he reported the following phenomena of "ideological diversification":

- the curriculum included György Lukács's theory of labour, it was compared with the doctrines of the classical authors of Marxism,
- theories of advanced capitalism were included in the teaching of political economy,
- the history of the Hungarian labour movement between 1918 and 1975 was taken out of the curriculum.

Moreover, the staff of the department even stated unequivocally that Marxism-Leninism as an ideological subject is not of interest to students.[21] The reports of the operational group were summarized at the Embassy of the GDR in Budapest and were forwarded to the Ministry of Foreign Affairs of the GDR. In the next section of this paper, I present an analysis of the Country Reports submitted to the party leadership of the GDR in the summer of 1968 and in February 1988, and the protocols of the series of negotiations held in the early 1980's.

The circumstances of the drafting of the report dated 28 August 1968 were determined by the invasion of Czechoslovakia, therefore it placed great emphasis on public opinion related to the invasion, on the part played by prominent writers and members of the intelligentsia who criticised the political course of the party, on solidarity with the Prague Spring. However, in the main focus of the observation were the introduction of the New Economic Mechanism and the strengthening of relations with the Western states.[22] According to the critique formulated in regard of a new

---

18 BStU 12621/83. Archived personal material of an unofficial staff member codenamed "Bernd Thieme"

19 Ibid.; The task of inspecting Western press products available in Hungarian public libraries was also included in other agent reports. BStU MfS AIM 630/85. Bd. 1-5. Archived material of an agent codenamed "Steffen".

20 BStU MfS BV Potsdam KD LW 19 TI Bd 1-2. T. 2. Bd. 2.

21 BStU MfS Abt. X. 9.

22 The preparation for the transition from a central planning system to self-regulating, for competition-based market economy was coordinated by a working group of economic experts and functionaries headed by the secretary of the CC HSWP Economic Policy Department, Rezső Nyers. The basic principles of the reform were adopted by CC HSWP in November 1966. The reform introduced on January 1, 1968 increased the autonomy of companies.

approach to socialist plan economy, the introduction of the New Economic Mechanism led to the disdain of ideological indoctrination efforts.[23] The report devoted ten pages to Hungarian foreign policy ambitions. Since the FRG was perceived to be the main enemy of the GDR, the East Germans anxiously watched the strengthening of West German government and economic positions in Hungary.[24] The report took stock of the West German companies and cultural associations with representation offices in Hungary, including the organisations of deported ethnic German minority organizations, which were also considered to be the means of ideological loosening and stated with concern that the official Hungarian circles are open to establishing diplomatic relations with the FRG, which even friendship treaty concluded with the GDR could not prevent from happening.[25]

Although no similar report from 1981 survived, the documents of the talks preparing the Agreement in 1981 allow the reconstruction of the way Stasi leaders viewed contemporary Hungary. The extent of the shock caused by the Polish situation was indicated by the fact that Minister for State Security Erich Mielke, after 14 years, once again felt the need for a personal consultation, so he met his Hungarian counterparts in November 1981 in Budapest.[26] The events in Poland made both sides take stock of opposition groups operating in their respective countries.[27] The East German leadership paid great attention to the political and economic situation and stability of the partner countries. At a meeting held in Budapest on July 9, 1981, Deputy Minister of Security Lajos Karasz briefed the East German delegation on the situation in Hungary. The Stasi delegation next visited Budapest in November 1981, led by Army General Mielke. The purpose of the visit was to evaluate the cooperation since the meeting in Berlin at ministerial level in 1967, and to discuss future objectives. After discussing current issues of international life, the parties turned to talking about bilateral relations. This time it was Minister of Interior István Horváth who presented a briefing on the characteristics and difficulties of Hungarian domestic political life, and during this briefing he touched on state security measures taken against opposition forces. The leaders of East German state security services voiced their anxiety with regard to events in Poland, they were afraid lest a similar turn of events take place in Hungary. Minister for State Security Mielke's comments revealed a remarkably thorough knowledge of Hungarian opposition groupings.

---

23 The first high-level meeting on "the conceptual problems of the economic mechanism" was held at the Hungarian Academy of Sciences, 24 November 1965 and was followed by more public debates.

24 Coordination of the establishment of FRG's foreign trade representation in Budapest started in the wake of the decision of the Politburo of the Hungarian Socialist Workers' Party dated 25 August 1962. The Hungarian-West German trade treaty was signed on November 10, 1963, and the mutually opened trade representations also functioned as foreign missions. Diplomatic relations were actually established on 21 December 1973. MNL OL KÜM Secretariat XIX-jlr-56 (PJ) 1962.

25 BStU MfS ZAIG 5127.

26 BStU MfS ZAIG 5466. Notes about the consultation. Beratung 11-12. 11. 1981 Bp.

27 BStU MfS ZAIG 5466. This is the case with the Minister for MdI of UVR and for the MfS-MdI of UVR. Beratung 11-12. 11. 1981 Bp.

He urged strong actions to be taken against the distribution of Hungarian samizdat and immigrant publications, opposition events held in private residences and access of leading Hungarian opposition figures to Western media.[28] The issue of treating the opposition was once again raised in March 1982 during the visit in Hungary of a delegation of Department IX. (Investigation) of the Stasi. The guests had accurate knowledge of the opposition movements spreading among Hungarian youths, such as the Bush-communities founded by Piarist Priest György Bulányi,[29] equipment used to duplicate samizdat publications, the police raid carried out on the "Galamb Street Boutique" founded by László Rajk.[30] They considered it particularly dangerous that the samizdat publications now dealt not only with philosophical and historical issues, but expressed solidarity with the events in Poland and incited open resistance to the regime.[31] In regard of the police raid they did not fail to note and complain that the culprits got off with a simple fine. The pros and cons during the discussion outlined a differing understanding of the role of state security agencies. While opposition activities were punishable with prison sentences in the GDR, in Hungary it was by making publication impossible that the authorities tried to prevent the "second publicity" from gaining ground.[32]

In the second half of the 1980s, the crisis phenomena emerging in the Eastern Bloc countries highlighted the urgent need for reforming the socio-economic model. The Soviet policy urging East-West rapprochement also created favourable conditions for reform efforts in other countries of the communist alliance. Member States responded according to their national idiosyncrasies, level of development, not least their geopolitical situation and national interests; accordingly, perceptions of the need for reforms differed significantly. The various perceptions of the reforms brought about a radical transformation of the relationships within the alliance. The signs of the break-up of the bipolar world had been clearly outlined at the third follow-up meeting of the Conference on Security and Cooperation In Europe [hereinafter: CSCE] held between November 1986 and January 1989 in Vienna, in connection with which Foreign Minister Péter Várkonyi made the following observation: *"The dynamic changes in the international environment of the Vienna meeting have brought to light the divisions of interest within both NATO and the Warsaw Pact in terms of assessing Soviet reforms and the extent to which they support them. The disintegration of unity within the various groups has been a novelty in CSCE meetings, which have hitherto been more of a bloc-type negotiation, but were welcomed by many as the end of a period of special agreement between the great powers. […] Differences of opinion*

---

28 ÁBTL 1.11.1. 45-79/7/81. Report on the visit of the delegation of the Ministry of State Security of the German Democratic Republic to the Hungarian People's Republic on 12-13 November 1981; MfS ZAIG 5466 The name of the Minister for MdI is UVR and for Zusammenarbeit MfS – MdI is UVR. Beratung 11-12. 11. 1981.

29 The Piarist monk György Bulányi wanted to lay the foundations of an alternative society independent of state power with the Bush communities. Among other things, they opposed military service based on conscription.

30 The mother of László Rajk Jr., Júlia Rajk, distributed the samizdat publications in the rented council apartment in Galamb Street.

31 BStU MfS HA IX. 8740. Einige Bemerkungen zur gegenwärtigen Lage in der VR Ungarn (insbesondere zu den Aktivitäten oppositioneller Elemente). Berlin, 31 January 1983

32 The Hungarian political leadership placed great emphasis on maintaining a positive Western echo, the liberal image of Hungary typical of the Kádár era. The opposition sought to seize the opportunities arising from the situation.

and possible differences within the Warsaw Pact have been strong in the debate on economic issues, and in particular on human rights and humanitarian issues. These differences were more limited in military terms only. Although efforts were made on the part of the Soviets all along to overcome such problems throughout, there was a noticeable difference between the Soviet, Polish and Hungarian resolutions promoting the agreements and the more rigid GDR, Bulgarian and Romanian positions. The Czechoslovak position wavered between the two."[33]

The East German party leadership viewed the Hungarian reform efforts with resentment and suspicion. The leaders of the Socialist Unity Party of Germany argued that experimentation related to the leading role of the party should not be allowed in the immediate vicinity of West Germany.[34] They saw the guarantee of the survival of the second German state only in the unchanged maintenance of the economic and political model. When Anatoly Dobrinin, a senior member of the International Division of the Central Committee of the CPSU, discussed the issue of perestroika with Erich Honecker on February 5, 1987, the German party leader made it clear that he could not agree with Soviet policy in several regards.[35] During a session of the Central Committee of the Socialist Unity Party of Germany held on 7 February 1989, Minister of State Security Erich Mielke bluntly called renewal, perestroika and glasnost "the gravediggers of socialism".[36] The deepening of the break is indicated by the fact that the East German media first sifted the news about the events in Hungary and then banned the distribution in the GDR of the "Budapester Rundschau" covering Hungary in German.[37]

In December 1985, operational groups operating in Czechoslovakia, Bulgaria and Hungary were restructured.[38] The members of the groups up until then were recruited from the staff of Department VI responsible for securing tourism, now members of Department II for Counter-Intelligence were also delegated to the operational groups. In the wake of the decision, Lieutenant Colonel Herbert Heckerodt joined the Stasi operational group in Budapest in September 1986.[39] The official and unofficial co-workers were tasked with monitoring the political changes.

---

33 MNL OL XIX-jlr 93 d. Foreign Minister Péter Várkonyi's briefing to the Political Committee of the Hungarian Socialist People's Party on the follow-up meeting of the Conference on Security and Co-operation in Europe in Vienna. Budapest, January 27, 1989

34 KARNER, Stefan – KRAMER, Martin et al.: Der Kreml und die "Wende" 1989. Interne Analysen der sowjetischen Führung zum Fall der kommunistischen Regime. Documents; Studien Verlag, Innsbruck, 2014. p. 211. ISBN 9783706554138

35 ÁBTL 1.11.4. T-IX/1987. 67/9-4601/1987. BM III/I-6. Class. Recording.

36 SÜß, Walter: Staatssicherheit am Ende. Warum es den Mächtigen nicht gelang, 1989 eine Revolution verhindern. Ch. Links Verlag, Berlin, 1999. p. 178. ISBN 9783861531814

37 In 1988, in addition to the Hungarian edition of "Budapester Rundschau", the Soviet publications "Sputnik" and "Neue Zeit" and the Czechoslovak "Prager Volkszeitung" were banned in the GDR. See Das Sputnik-Verbot.

38 BStU MfS HA II/10. 286. Arbeitsordnung. Berlin, 1 August 1986

39 BStU MfS Abt. X. 1. BStI MfS Abt. X. 1804 Telegramm. Berlin, 8 November 1989

A summary report entitled "Reflections on the political stability of the Hungarian People's Republic at the turn of 1988/89" was prepared for the visit in Berlin by the new Secretary General of the HSWP Károly Grósz, on 8-9 September 1988.[40] Its authors compared their experiences in 1988 with the period before the 1956 revolution.[41] Although in their systematic comparison they came to the conclusion that the situation in 1988 was fundamentally different from the situation in 1956, that is to say there was no need to fear a counter-revolution breaking out at the end of the 1980's, all the same they did not in the long run preclude the threat of destabilization of the country. At its meeting on February 10-11, 1989, the Central Committee of the Hungarian Socialist Workers' Party adopted the multi-party system. The East Berlin leadership paid special attention to the breakdown of the party state, the separation of powers does and the retention of the leading role of the Hungarian Socialist Workers' Party. The disintegration of the monolithic unity of the Hungarian party leadership and the ideas concerning the integration of the opposition 's representations into the power system were carefully documented. The East German Ministry for State Security opened a file folder with the title "activities of anti-socialist forces in Hungary" on the Hungarian political transformation which it supplemented with a file-folder named "Alternative political forces and groups in Hungary", opened on the most important political organizations. Among intelligence materials gathered on the events of the opposition an appeal by FIDESZ issued on 30 March 1988 can be found as well as a detailed report on the session of the Hungarian Democratic Forum at the Cultural Centre of MOM (Hungarian Optical Works) on 19 November 1988.[42] The letter of the CC of the HSWP addressed to János Kádár, urging his resignation was translated into German, the party congresses and conferences of the HSWP and the personnel changes in the leading party units were reported on. The rehabilitation of the late Prime Minister Imre Nagy and his fellow martyrs raised visible concern.[43] The interesting thing about those reports is that it presents the process of regime change in Hungary from the point of view of a country that was an ally but couldn't be called a friend of Hungary. Given the amount of information gathered without sparing money and effort, the question of what they did with the information can rightly be raised. In April 1989, the GDR state security leaders' concerns were shared with the Deputy Chairman of the State Security Committee under the Council of Ministers of the USSR, who was also head of foreign intelligence. They called Major General Leonid Vladimirovich Shebarshin's attention to the fact that the legitimization of the activities of the opposition in Hungary and in Poland undermines the existing power structure and shakes the unity of the socialist camp.[44]

---

[40] BStU MfS HA II. 38877. Betrachtungen über einigen aktuellen Entwicklungen in der UVR Anfang 1989; Information on the application of the Hungarian Regulations to the month March 1989; Activities include alternative political groups and groups in Hungary. Budapest, April 7, 1989; MNL OL XIX-jlk 2552/89. 82. d.

[41] It is a remarkable coincidence that the meeting of the Central Committee of the Hungarian Socialist People's Party on February 10-11, 1989 also started from the premise that in 1956 the leadership's inability to renew led to a political explosion.

[42] The dossier contains a similar detailed report on the national conference of the MDF held at the Karl Marx University of Economics on 11-12 March 1989. BStU MfS Abt. X. 9.; BStU MfS HA II. 38877. Information on the Hungarian Conference on Hungarian Democratic Forums.

[43] The reburial of Imre Nagy and his fellow martyrs was decided at the meeting of the Political Committee of the Hungarian Socialist People's Party on November 29, 1988.

[44] BStU MfS Sec. Mittig 85. Hinweis. April 7, 1989.

Annus mirabilis – 1989/Wondrous year/

During Hungary's accession to the Refugee Convention, on 14 July, 1989 the operational groups in Budapest, Prague and Sofia were reorganized. Their control was taken over from Division VI (Security of Tourism) by Department 10 (Security of GDR diplomatic missions in friendly countries) of Division II (Counter-Intelligence).[45] The reorganization was justified by the domestic political changes taking place in certain friendly countries and the increase in the activities of the "counter-revolutionary" and "anti-socialist forces". As regards the processes related to the renewal of socialism, the counter-intelligence officer of the operational group in Budapest, Lieutenant-Colonel Herbert Heckerodt shifted the focus of the group's efforts from detecting opposition groups operating in friendly countries to revealing said groups' contacts in the GDR.[46]

Following the opening of the border on September 11, allied state security leaders held a meeting on September 14, 1989. Major General Ferenc Pallagi, Head of Hungarian State Security, personally received co-workers of Division VIII. (Observation, investigation) of the Stasi who arrived in Budapest. Talking to the head of the GDR delegation, Major General Coburger, he stated that the Hungarian authorities considered it unthinkable to interrupt the fruitful cooperation, which had a long history. The future areas of co-operation were identified as intelligence and counter-intelligence, and as regards the operations of the secret services, the consideration of national interests was emphasized. After the resignation of the Central Committee of the Socialist Unity Party of Germany, the heads of the operational groups in Prague, Sofia and Budapest, Colonels Gottschling, Fiedler and Heckerodt were called back to Berlin.[47] During the farewell from their partners in the host countries, as instructed, they had to indicate the intent to continue cooperation. After the disestablishment of the Ministry for State Security, the Office of National Security of the GDR took over on-going cases. A department for international relations was also created within the new institution the function of which was coordination of cooperation with foreign security agencies. The delegation of the GDR Office of National Security visited Hungary on 22 November 1989 to provide information about the GDR's political situation. Both partners agreed on the continuation of cooperation in the area of counter-intelligence.[48] The head of the German delegation, Major General Manfred Brückner announced the withdrawal of the GDR surveillance team operating in Hungary which he, somewhat euphemistically, called a "tourism security group".[49] In mid-December, the documents on the control of East German tourism in Hungary were collected and repatriated.[50] Lieutenant Colonel Rolf Isermemann, Head of Counter-Intelligence Department of the Office of National Security of the GDR and Colonel Herbert Heckenrodt, head of the operational group in Hungary, informed Colonel László Benkő, Head of the MOI III/II Counter-Intelligence Directorate that they were going

45 BStU MfS Abt. X. 1804. For the reorganization Erich Mielke Minister of State Security 13/89. s. was ordered.
46 BStU MfS HA II. 1700. Settlement and transfer of claims under the Staff Regulations
47 BStU MfS Abt. X. 1804 Telegramm. Berlin, 11 November 1989.
48 ÁBTL 1.11.1. 45-74/58/89. Report. Budapest, December 15, 1989.
49 ÁBTL 1.11.1. 45-74/47/89. Recording. Budapest, November 21, 1989.
50 MNL OL XIX-B-10. 1989. 00452/89. Notification. December 13, 1989.

to reduce the staff of their mission in Budapest to two officers.[51] The last daily operational brief of the Hungarian state security agencies dated December 29, 1989 gave an account of the reorganization of the German security services and on the destruction of intelligence documents on GDR-Hungarian cooperation dating back to the 1960's.[52]

Bibliography:

Historical Archives of State Security Services (ÁBTL)

- ÁBTL 1.11.4. BM III / I. Directorate documents. Information reports
- ÁBTL 1.11.1. Secretariat of Deputy Minister for State Security
- ÁBTL 1.11.12. Documents of the International Department of the Ministry of the Interior
- ÁBTL 2.7.1. Operational Daily Reports
- ÁBTL 3.2.1. Bt-262/4. Dossier of an agent codenamed "Balaton"
- ÁBTL 3.2.6. Rezidentura files. Organizational file for the Berlin rezidentura
- Country-wide Archives of the Hungarian National Archives (MNL OL)
- MNL OL XIX-j-l-k Documents of the Ministry of Foreign Affairs 1989. 83. d.
- MNL OL XIX-j-l-r Documents of the Secretariat of Foreign Affairs 1989. 93. d.
- The Bundesbeauftragte für die Unterlagen des Staatsicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik, Berlin (BStU)
- MfS AIM Archivierter IM-Vorgang
- MfS HA II. Spionageabwehr
- MfS HA IX. Untersuchungsorgan
- MfS Abt. X. Internationale Verbindungen
- MfS HA XVIII. Volkswirtschaft
- MfS Secretariat Mittig
- MfS ZAIG Zentrale Auswertungs- und Informationsgruppe

[51] ÁBTL 1.11.1. ÁBMHT 45-74/58/89.
[52] ÁBTL 2.7.1. NOIJ 253/4. December 29, 1989.

Published sources:

- JOBST, Ágnes: The operation of Stasi in Hungary. The relationship between East German and Hungarian state security 1955−1989; Budapest, 2015 Jaffa Publishing House. ISBN 9786155492471
- HERBSTRITT, Georg: The "Balkan File" of the GDR Ministry of State Security. Secret service measures against Hungarian immigration in West Germany; Historical Review, 2008/1. pp. 109-126.
- KARNER Stefan – KRAMER Martin et al.: Der Kreml und die "Wende" 1989. Interne Analysen der sowjetischen Führung zum Fall der kommunistischen Regime. Documents; Studien Verlag, Innsbruck, 2014. ISBN 9783706554138
- PALASIK, Mária: Organization and staff of the Intelligence Department, 1956–1962; Insights, 2011/2. www.betekinto.hu/2011_2_palasik (downloaded 20 December 2014)
- SÜß Walter: Staatssicherheit am Ende. Warum es den Mächtigen nicht gelang, 1989 eine Revolution verhindern. Ch. Links Verlag, Berlin, 1999. ISBN 9783861531814
- TANZSCHER, Monika: Die Stasi und die "Kaffeehaus-Czech Republic". Über die geheimdienstlichen Beziehungen der DDR zur Volksrepublik Ungarn; Horch und Gluck, Heft 27 1999/3. pp. 48-59.
- http://www.bstu.bund.de/DE/Wissen/DDRGeschichte/ Vorabend-der-Revolution/ 1988_Sputnik-Verbot/_node.html (downloaded: 25 Januray 2015)

BERK CAN KOZAN

BURDEN SHARING: TO BE OR NOT TO BE[1]

Abstract

NATO, established for military purposes at the beginning of the Cold War. However, at the end of the Cold War and the dissolution of the Soviet Union, NATO ceased to be a purely military-sized organization and became a unique multi-dimensional international structure. In this multi-dimensional concept of NATO, Turkey's place is far too important to be replaced by another country. Moreover, Turkey has hosted American nuclear weapons for decades under its NATO commitments. These weapons were deployed on Turkish lands as part of NATO's collective defence doctrine and were intended to prevent an invasion from the Warsaw Pact during the Cold War. However, NATO's contribution to Turkey's security is increasingly being questioned, and Turkey's position is becoming debatable at the time being. While Turkey has not been able to come under a real security umbrella like the other member states of NATO, Turkey has never experienced a process in which relations are questioned on this scale before. NATO, which was founded as a military alliance in self, has now become a major political platform. In this analysis, Turkey's membership to NATO and its position in the organization will be evaluated, mainly, over Tactical nuclear weapons.

Keywords: Turkey, NATO, nuclear weapons, U.S., Soviet Union, non-proliferation, deterrence, nuclear doctrine, disarmament, mutualy assured destruction, massive retaliation

Introduction

On the eve of nuclear weapons armistice talks or the signed non-proliferation agreements regarding the horizontal or vertical proliferation of nuclear weapons, particularly, between the United States of America and Russia outbreaks the importance of national security and enhances the role of deterrence strategies; as the one might be the witness almost after every launch of treaties.

However, besides the number of nuclear warheads in circulation, policies towards to or of nuclear weapons have always been profoundly striking the history. The nuclear arms race between the USA and USSR, during the cold war, reached an extraordinary level that tied with the balance of mutually assured destruction. Hence, this cluster of complexes entrenched the place of the role of nuclear weapons in the system of international relations. Herein, the starting point of the ignition was the everlasting rivalry between the USA and USSR.

[1] Hamlet, Act III, Scene I by William Shakespeare

The central core of these power struggle and the epicentre of competition was about geopolitical supremacy between superpower powers. Modern (geo-nuclear) strategies, usually, referred to George Kennan's vision which lightened the fuse of the containment policy. Kennan became the galvaniser of it and; hence the narrative started. Through his foresight and psychological inference, he simply defined how the containment policy should be towards USSR.

In his long telegram; USSR leaders were relentless, unstoppable and agnostic to the west; and, he believed that the Soviets endeavour to seek to expand their scope of control, referring to Norther Iran and Turkey that most possible potential areas of danger[2]. Moreover, George Kennan, in *"the sources of soviet conduct", bond his ideas with the character of USSR ideology. The author envisioned that "the agnosticism towards western world and components of Soviet foreign policy as embedded in the secretiveness, the lack of frankness, the duplicity, the wary suspiciousness and the basic unfriendliness of purpose; and, drew the thick line of competition between the USA and USSR."*[3] Thereby, Kennan proposed that the USSR had been heavily armed, so the outside world of communism frightened by. It was strongminded to spread communism, and thus no possible coexistence between the USSR and the USA could occur. However, the US was powerful than the USSR, and it could "contain" communism[4]. George Kennan's containment strategy was unquestionably defined the crisscross geographical supremacy. In some way, Kennan's strategy can be accepted as a geopolitical deterrence.

Therefore, the advent of nuclear weapons carried the deterrence theory joint with containment at the heart of the world's geography. To prove that, *"deterrence combined with containment was the strategy pursued by the West towards the Soviet Union throughout the Cold War."*[5] Hence, states shaped their policies and *"their race to develop and produce nuclear weapons and associated delivery systems became a central feature of that contest."*[6] However, when the US' nuclear weapons supremacy ended with USSR's explosion of the first nuclear weapon in 1949, the utilisation of using nuclear weapons mechanism changed steadily. Furthermore, in 1957, USSR announced the first intercontinental ballistic missile which was able to target anywhere on the earth face. The aftermath of this remarkable event, geo-nuclear deterrence gone out of the soil of these two superpowers swiftly and pulled states into the deterrence strategy. Shortly afterwards, deterrence strategies these developments have finally begun to enter into defence plans by states.

In the US, the Eisenhower administration's common belief was arming, and use of force to the deter Soviet Union and threaten it with total suppression. *"US officials believed this so-called "massive retaliation" concept, which sought to deter any Soviet*

---

2 KENNAN, G.: February 22, 1946 George Kennan's 'Long Telegram'; https://digitalarchive.wilsoncenter.org/document/116178.pdf (downloaded 04 April 2020)

3 KENNAN, G. F.: The Sources of Soviet Conduct; 1947, July, https://www.foreignaffairs.com/articles/russian-federation/1947-07-01/sources-soviet-conduct (downloaded 04 April 2020)

4 Ibid.

5 MATLARY, J. H.: Strategy: Deterrence, Containment, Coercion, and Confrontation; In: J. H. MATLARY (eds.): Hard Power in Hard Times, Palgrave Macmillan, 2018. pp. 23-45.

6 MICHEL, L. – PESU, M.: Strategic Deterrence Redux; Finnish Institute of International Affairs, Helsinki, 2019.

attack by threatening rapid escalation to general nuclear war, would be buttressed by deploying US nuclear weapons to Europe."[7] The reason why the Eisenhower had chosen massive retaliations got an edge over the USSR probably because the Soviet Union had a bigger army, and they threaten the vase domain. However, enormous retaliation's credibility was debatable. Leading scholars like Herman Kahn and Bernard Brodie crucially criticised the strategy that the doctrine is too aggressive and almost similar to the first strike. *"They thought that it was practically an invitation to the Soviets to precede any local aggression by a pre-emptive first strike on American bomber bases, eliminating the nuclear threat on the ground and forcing the United States into the land war it was unprepared to fight."*[8]

Eisenhower's "the new look policy" was abandoned after J.F. Kennedy, took the office in 1961. Improvements in technology, communications and transportation obsoleted the previous policy's credibility, and it had been changed by "flexible response". Flexible response allowed for political, logistical and military reciprocal deterrence, thereby allowing the United States to respond to attacks around the continuum of war, not only with nuclear weapons; it *"counted on a build-up of US and allied conventional forces to deter or, if necessary, defeat aggression on the level at which the Soviets chose to fight."*[9]

Nevertheless, the US deterrence strategy changed when USSR reached the nuclear weapons parity with the US. This nuclear equality brought mutually assured destruction. The MAD era began with J.F Kennedy administration and encompassed the Nixon and Reagan administration. However, the Cuban nuclear missiles crises showed mutual vulnerability, in contrast. MAD belligerents' (the US and USSR) military planners claimed that nuclear war could only be avoided if no party could anticipate a full-scale nuclear war. Because the threat's reputation is essential to this security, each side needed to spend considerable resources in its nuclear arsenals, even though it was not planned for use. *"The US and the Soviet Union, therefore, agreed to limit strategic defensive systems to preserve mutual retaliatory capability. Enshrined in the Anti-Ballistic Missile (ABM) Treaty of 1972, the stabilising effect of mutual vulnerability became integral to US-Soviet arms control in the twentieth century."*[10]

The MAD was modified under Jimmy Carter's administration and formed under the name of countervailing strategy. It stressed that the intended reaction to the Soviet offensive was no longer solely to strike Soviet population centres and cities, but instead to eliminate Soviet officials and invade strategic objectives in the expectation of a Soviet withdrawal until the Soviet Union was entirely defeated.[11] This strategy was reformed and developed to another definition of the MAD by Reagan

---

7 MICHEL, L. – PESU, M. op. cit.

8 MENAND, L.: Fat Man – Herman Kahn and the nuclear age; 2005. https://www.newyorker.com/magazine/2005/06/27/fat-man (downloaded 04 April 2020)

9 MICHEL, L. – PESU, M. op. cit.

10 WALLANDER, C. A.: Mutually Assured Stability: Establishing US-Russia Security Relations for a New Century; 2013. https://www.files.ethz.ch/isn/168169/mas_ib_atlanticcouncil.pdf (downloaded 04 April 2020)

11 WOOLF, A. F.: Nuclear Weapons in U.S. National Security Policy: Past, Prensent and Prospect. 2008. https://fas.org/sgp/crs/nuke/RL34226.pdf (downloaded 04 April 2020)

administration; this was strategic defence initiative; the goal was to construct space-based technologies to execute Soviet missiles before they hit the US in the space.

Doctrines including nuclear weapons, generally, collaborated with the USA. Although throughout the Cold War, nuclear deterrence doctrines were officially not accepted by USSR; however, due to security concerns more or less followed the same way of the power of deterrence of nuclear weapons. The USA's conventional hegemony and the dominancy of NATO can be shown as a reason for this.

The Cold War ended with the power of diplomacy. Indeed, the collapse of communism, economic crises in USSR, globalism, the global nuclear non-proliferation regimes and treaties regarding nuclear weapons and dissolution of USSR was in effect of this end. Moreover, after the Cold War, security strategies and concerns were completely changed, and states reacted new security axis; furthermore, states have begun to shape their policies accordingly. However, the expansion of NATO, the democratisation of Afghanistan and Iraq by the United States, the annexation of Crime by Russia, the modernisation of nuclear weapons in warehouses, the advance developments at the arms industry and the cancellation of the nuclear weapons proliferation agreements urges Russia and the United States, which now considers the heir of Soviets Union, to the edge of the new Cold War.

Despite all-above, whilst the Soviet Union was closing the gap with America in the nuclear arms race in the 1960s, the Soviet threat began to be felt more clearly both in Turkey and as in the United States. The Soviet Union increased its military presence and weapons capabilities along Turkey's eastern borders, and in the following years, relations with neighbouring countries began to intensify in all areas, including military cooperation. The growing military presence of the Soviet Union in NATO's peripheral area in terms of quality and quantity led to a greater emphasis on deterrence of nuclear power for the allies in general and Turkey in particular. Thus *"located in NATO's southern flank and sharing a long border with the Soviet Union, Turkey contributed extensively to the Alliance's deterrence strategy by providing military bases and facilities in this strategic region."*[12] In a sense, Turkey has made a significant contribution to reducing the threat to NATO's European allies by taking on the risk of the Soviet Union. But Turkey has not always found the support what it seeks.

Turkey as a part of NATO's Burden Sharing

NATO was born in the aftermath of the Second World War, when Europe was virtually destroyed and the strength of the USSR was feared. It is a strategic organisation in which the first step of the policy of containment of the USSR was created. While this drastic change in the international system was reflected in the foreign policies of the countries, it was instrumental in the reorganisation of Turkey's foreign relations. As a matter of fact, the main factor that dominated Turkey's foreign policy after the Second World War and gave it direction was the Soviet Union's

[12] KINACIOĞLU, M.: NATO-Turkey Relations: From Collective Defence to Collective Security; Turkish Foreign Policy, 2017. pp. 83-103.

territorial demands on Turkey,[13] which benefited from the gaps in the European instable position after the war. After the Soviet Union's policy towards Turkey changed according to frontline situations during the war, it gained its real character at the end of the war. Moreover, when the Soviet Union acquired first atomic weapon in 1949, its increased Turkey's security concerns. Hence, Turkey sought a solution against the Soviets expansionism, which meant the independence and territorial integrity of Turkey, and as a result, Turkey became a member of the NATO in 1952. Turkey's participation in the Korean War also played an important role in Turkey's admission to NATO. Therefore, as a part of the containment policy, Turkey has increased its importance in the Eastern Mediterranean and the Middle East. In defence of European NATO allies, Turkey's strategic advantages have allowed the US to mobilize its army and the weapons; hence, contain the Soviet Union.

On the other hand, the period when Turkey joined NATO also coincided within a period when the nuclear rivalry between the United States and USSR began to intensify. This ongoing rivalry in the nuclear arena has had repercussions for other NATO members. As a matter of fact, when the Soviet Union acquired the capability to strike the United States directly, NATO's European members began to question whether the United States could protect Europe against a possible Soviet attack at the expense of risking its territory. Furthermore, the conventional numerical superiority of the Soviet Union on the European continent has also led to another variety of the question that to what extent is possible to defend against a possible attack by USSR. As a result, deterrence seeking against the Soviet Union in Europe, due to the threat perception, the United States is committed to a policy of nuclear deterrence NATO in relation to the burden sharing.[14] Within the framework of NATO's decisions in 1957, the deployment of Thor and Jupiter missiles to the territory of various allies in Europe was deemed appropriate.[15] Thus, Turkey showed a special effort to take part in the Western Bloc and Turkey's regional position was an excellent strategic ground for the United States. The fact that, the Soviets became a massive nuclear power and their rapid progress in armament led the USA to find new allies to keep the Soviet Union within its cold-war borders via storing tactical nuclear bombs.

As a result, NATO strategies generally determined by the US since its establishment, *"the US first deployed nuclear weapons to Europe in September 1954 when the first weapons arrived in Britain. Within a decade, deployments spread to Germany, Italy, France, Turkey, the Netherlands, Greece, and Belgium, and in 1971 the deployment peaked with approximately 7,300 nuclear warheads deployed in Europe"*[16] under the NATO's nuclear umbrella.

---

13 BINNENDIJK, A.: The Russian-Turkish Bilateral Relationship: Managing Differences in an Uneasy Partnership; Turkey's Nationalist Course, Santa Monica,CA: RAND Corporation, 2020. p. 107.

14 ÜLGEN, S.: Turkey and The BomB; Carnegie Endowment for International Peace, Massachusetts Avenue, NW, 2012. https://carnegieendowment.org/files/Turkey_Bomb_Full_Text.pdf (downloaded 04 April 2020)

15 BERNSTEIN, B. J.: The Cuban Missile Crisis: Trading the Jupiters in Turkey? Political Science Quarterly, 1980. 95(1), pp. 97-125.

16 KRISTENSEN, H. M.: U.S. Nuclear Weapons in Europe A Review of Post-Cold War Policy, Force Levels, and War Planning. Washington: Natural Resources Defense Council, 2005.

As the strategic priority shifted from the overcrowded armies to the nuclear deterrence, Turkey, due to its geographical location, was considered a geopolitical country that shortened retaliation phase in a nuclear war against the Soviets. This, eventually, bring *"the deployment of Jupiter missiles in Turkey took place in 1961."*[17] For Turkey, the presence of nuclear weapons on its territory has been regarded for many years as an indication of the alliance's nuclear umbrella and solidarity with NATO and the United States against the Warsaw Pact countries. Also, Turkey has adopted the 'first use' strategy, which envisages NATO being the first party to apply for nuclear weapons when necessary; this means that, use of nuclear weapons before there is an attack.[18] On the contrary, the 'first use' emphasises that NATO could be the first to resort to nuclear weapons if all other options to protect allies against aggression are insufficient. However, the progress made by the Soviets in the field of missile technologies has also made the USA a beatable target. Thus, it seemed highly probable that a small conflict that started conventionally would rapidly escalate into a nuclear war and spread to the US lands. As a result, under the US leadership, the strategic concept of flexible response has adopted by the USA and changed NATO's strategic concept.[19]

American nuclear weapons deployed in Europe within the framework of NATO nuclear weapons sharing reached very high numbers in the middle of the Cold War period and gradually declined in the later stages. The reduction of American nuclear weapons that had been deployed in Europe began in the second half of the 1970s.[20] One might say that the first of the two major factors that triggered this reduction was the anti-nuclear power among the people of Europe and the INF agreement signed between the United States and the USSR in 1987. *"Thousands of more warheads were withdrawn beginning in late 1991, with additional withdrawals (totalling around 200) reportedly taking place as recently as 2008. Non-government sources estimate that a total of approximately 150 US warheads (B-61 gravity bombs) remain at storage sites in Germany, the Netherlands, Belgium, Italy, and Turkey."*[21]

According to Federation of American Scientists, these weapons are currently deployed in Belgium, the Netherlands, Germany and Italy, as well as in Turkey, within the framework of NATO Turkey continues to keep an estimated 50 weapons secretly deployed on its territory.[22] Nevertheless, Turkey supports the retention of arms on itinerary and expects other NATO countries to continue their tactical stewardship of nuclear weapons as part of the Alliance 's principle of burden-sharing. Turkey is hosting a B61 gravity bombs the Incirlik air force base near Adana; missiles scheduled for use by the US air force, with the others being delivered by the Turkish air force. Yet the Turkish air force does not have nuclear-mission aircraft approved. Moreover, a nuclear fighter wing at Incirlik is not permanently maintained by the United States.[23]

---

17 BERNSTEIN op. cit.

18 GERSON, M. S.: No First Use: The Next Step for U.S. Nuclear Policy; International Security, 2010. pp. 7-47.

19 LEGENDRE, T.: Military Change – Discord or Harmony? Copenhagen: Danish Institute for International Studies, 2011.

20 MICHEL – PESU op. cit.

21 Ibid.

22 KRISTENSEN, H. M.: U.S. Nuclear Weapons In Europe; Federation of American Scientists,Washington D.C. 2019.

23 ÜLGEN op. cit.

Strategies can be defined a long-term policies and goals developed by all actors in the international system to ensure their security. Because of the changing security environment in the international system has also changed the security needs of actors. Hence, actors have had to adapt to the new environment and develop new strategies to sustain their existence. As a defence organization, NATO has restructured by undergoing an organizational transformation process according to emerging or ongoing threats in the post-Cold War period, despite the disappearance of its anti-Warsaw Pact and has continued its existence with new tasks and fields of activity. Nonetheless, the dissolution of the Soviet Union the view of NATO, which had arguably excelled in conventional weapons, could undermine the strategy of use of nuclear weapons which has begun to be expressed afterwards.

However, it has not been possible for the alliance to take such a decision. As of the mid - the 1990s, it was predicted that European capitals would be within the range of nuclear warhead-bearing ballistic missiles that could come from the outside of Russian soil over a while. As a result of this assessment, in June 1996, NATO launched a comprehensive report of measures to counter such threats. The basic principle that emerged as a result of this report was to protect NATO's freedom of movement and to show that the alliance will not hesitate to threaten potential enemies with the use of weapons of mass destruction.[24] This is an indication that nuclear weapons will continue to be of the highest importance in NATO strategies. As a matter of fact, the NATO Strategic Concept documents adopted in 1999, 2010 and 2017 clearly emphasised importance of continuing the deployment of American nuclear weapons on the European continent.[25]

With the end of the Second World War, the international system underwent a fundamental structural change. The formation of the East-West bloc under the leadership of the two superpowers that emerged at the end of the Second World War and the formation of the relations between the two blocs in the form of the Cold War became the defining feature of the new international system. However, the collapse of the Warsaw Pact and after the Soviet Union's disintegration, many other NATO allies that had American nuclear tactical weapons withdrew the weapons from their country, but these weapons are still actively kept in Turkey. Although the probability of use is low, these weapons maintain their political influence under the name of the deterrence of nuclear weapons. Furthermore, in the troubled Middle East region, due to the confusion caused by the political changes in certain countries and the potential for nuclear weapons production due to the nuclear programs of some countries, tactical nuclear weapons are often still measured in terms of burden-sharing.

War on Geopolitics

The Soviet pressure addressed the Western European countries seek security. NATO arose as a defence organization by Western countries, with the United States of America's participation, against the increasing Soviet threat. While the collapse of the Eastern Bloc and the disintegration of the Soviet Union affected all structures in

---

[24] RUTHERFORD, I. P.: NATO's new strategic concept, nuclear weapons, and global zero; International Journal, 2011. pp. 463-482.

[25] https://www.nato.int/cps/en/natohq/opinions_168602.htm (downloaded 04 April 2020)

the international arena, NATO entered into an organizational transformation. It sought to adapt itself to the new period's conditions with the latest strategies and tasks it adopted. However, the end of the Cold War did not change Turkey's security needs regarding defence strategies. The oblivion of the Soviet military threat on, unlike Europe, did not mean sufficient for Turkey though ever since, NATO has formed Turkey-US relations.

Therefore, the importance and influence of Turkey's geopolitical position is a critical issue that needs to be parenthesis. Geopolitics has an impact on countries foreign policies and escalate the county's pace in international politics. Throughout the history, states where they control the strategic points, trade routes, chokes, straits, seas, religious centres, new water resources and has unearthed resources have always controlled the power centres and become dominant in the world politics. On the earth a few places have a particular geopolitical position as described above such as Turkey; she occupies peerless geography, lies at the junction of Europe and Asia.

As a peninsula, Turkey has surrender by three seas and contains two critical straits on them (Dardanelle and Istanbul). These straits only the gates where it opens to Black Sea from the Mediterranean Sea. Therefore, countries, where has a shore on the Black Sea, have to use these sea routes. Furthermore, thanks to Montreux strait talks, Turkey has a right to close these straits during the wartime; even though there are some specific rules regarding the transition of warships. Yet *"economically, the Black Sea is not very important for Turkey, but it controls the exit and entrance to the sea through the Turkish Straits."*[26]

Geopolitics cannot generate power politics alone. The aim of geopolitics is providing data to decision-makers; therefore, politics can be sustainable and maintainable. Thanks to its geography, Turkey has more than enough political options at the regional as well as at international level. With its powerful military (second largest in the NATO), youth population and strong nation's will, e.g., "in a survey carried out in 2015, 73 per cent of Turks were willing to battle for their country, ranking Turkey 12th out of the 64 countries surveyed and by far the highest among NATO member states,[27] Turkey plays a crucial role in the art of geopolitics.

In this respect, it becomes easy to understand why Turkey has been important for NATO. Turkey's membership to NATO was safety valve against USSR expansionist policies. Even before Turkey's membership to the Alliance *"it was argued that, in the event of a Soviet attack on Western Europe, if Turkey were a member of the Atlantic alliance United States bombers could attack the Trans-Caucasian oil fields, the industries of the Urals, and Russian supply lines from Turkish bases."*[28]

However, there have also been occasional crises within the NATO. Turkey has been disappointed by NATO or the United States at critical times. Due to the agreement reached between the Soviets and the United States on the Cuban crisis of

---

[26] WEZEMAN, S. T. – KUIMOVA, A.: Turkey And Black Sea Security; SIPRI, Solna, Sweden, 2018.

[27] Ibid.

[28] K, J. D.: Greece, Turkey, and N.A.T.O; The World Today, 1952. 8(4), pp. 162-169.

1962, the United States withdrew its Jupiter missiles. The NATO coalition was offended a major American partner, Turkey, militarily, economically and emotionally was affected by this situation.[29]

Also, one of the most prominent examples is undoubtedly the Cyprus issue. In 1964, the possibility of Turkey's warranted military operation in Cyprus caused a crisis. The crisis erupted with a letter from the United States, considered NATO's founding and most influential member. US President Lyndon B. Johnson, the "Johnson letter" written by Johnson implied that the USSR might intervene in a possible war with Turkey and that NATO would be reluctant to defend Turkey in such a situation.[30] Moreover, when the calendars were displayed in 1974, it was inevitable that the Turkish Armed Forces would act to bring peace to the island. Despite the passing of 10 years, the US attitude has not changed; *"in 1975, the US Congress decided to impose an arms embargo on Turkey"*[31]

There is no doubt that terrorism has invaded Turkey's agenda. However, Turkey did not get the support it expected from NATO. The civil war in Syria has posed significant threats to Turkey. Turkey has appealed to NATO to request a Patriot defence system. Expectations were that the Patriots would serve until the danger in Syria ended. But it didn't happen. US and Dutch missiles deployed to Turkey were withdrawn after a while, according to this demand. So, Turkey was alone in countering the air threat from Syria.[32]

Finally, Turkey agreed with Russia to purchase the S-400, one of the most advanced defence systems in the world.[33] NATO authorities initially approached Turkey's attempt to acquire the S400 with caution,[34] stating that it was an independent decision of a sovereign country. However, as Turkey's initiatives began to become official, the S400 systems would have a problem with integration with NATO systems and were asked not to be formally received. As a result, Turkey has been punished with kicked out from F35 air fighter program.

Today, Turkey still plays a vital role in the region and contributes to NATO policies. Moreover, Turkey sees NATO as an organisation that reinforces and enhances its westernisations well as the defence and security guarantees.[35] Since becoming a member of NATO, Turkey, with its powerful and crowded army, has served as a front-end protector for the Soviets. Since joining the NATO, Turkey's support for collective defence has contributed to the peaceful end of the East-West.

---

29 BERNSTEIN op. cit.

30 BOLUKBASI, S.: The Johnson Letter Revisited; Middle Eastern Studies, 1993. 29(3), pp. 505-525.

31 RUDNICK, D.: NATO and the Cyprus crisis Pressure groups versus power politics; The Commonwealth Journal of International Affairs, 1977. 67(226), pp. 182-190.

32 STEFANOVIC, D.: Turkey's perennial strategic importance and the S-400 Saga; 2019. https://www.aies.at/download/2019/AIES-Fokus-2019-10.pdf (downloaded 04 April 2020)

33 Ibid.

34 LINDGAARD, J. – PIEPER, M.: TURKEY'S NATO FUTURE: Between alliance dependency, Russia, and strategic autonomy; Copenhagen: Danish Institute for International Studies, 2020.

35 KINACIOĞLU op. cit.

Although the international security environment changed after the Cold War, NATO maintained its importance as an unchanging phenomenon of Turkey's foreign and security policy. Turkey has fulfilled all the responsibilities of alliance membership. Despite all the sacrifices Turkey has made, Turkey has not always seen the same response when it comes to its security.

Conclusion

The end of the Cold War has led to a strategic transformation of NATO's priorities. However, Turkey's geopolitical importance was not lost on the alliance's common interests. In the aftermath of the Cold War, several situations rendered Turkey's security dysfunctional. As Turkey tries to contribute to all of the alliance's military missions and strategic priorities with all its facilities and military capabilities, it is clear that differences between NATO allies arising from major structural problems in their approach to security issues have not disappeared. The Middle East-based security problems are seen as the alliance's reluctance to Turkey.

However, NATO's deterrence can be achieved collectively by all the capabilities and capabilities of the alliance, whether an ally has nuclear weapons or not, and by strengthening the spirit of solidarity. Moreover, only five countries still have American nuclear weapons among NATO allies. The United States, Britain and France also have their nuclear weapons. They also benefit from the alliance's nuclear deterrence, as the remaining NATO member states have U.S.-owned nuclear weapons on their territory. Turkey is one of these countries though the double standard applied to Turkey in all areas prevents this solidarity.

It is seen that the tactical nuclear weapons stationed in Turkey are of diplomatic-symbolic importance in the context of the relationship of trust between Turkey and the NATO alliance, rather than their defensive role. These bombs also have a political meaning in the context of NATO membership. It is bright and indisputable that nuclear weapons bring deterrence to Turkey. This situation has undoubtedly brought Turkey to a stronger position in the region. However, Turkey has made a great determination by choosing to be the target of these bombs. Turkey took the risk of becoming a target. However, it is considered that tactical nuclear weapons do not have inalienable importance in terms of Turkey's defence. In this context, when Turkey's security environment and defence priorities are taken into account, the more critical issues are missile defence needs and technology transfer which NATO members are reluctant show some respect. Furthermore, as Turkey comes under such a risk, NATO countries, especially the United States, are in a position to oppose even Turkey's acquisition of an air defence system. Finally, the “isolation policy” against Turkey is contrary to the spirit of the Union. Turkey is not a problem kid of NATO nor “so-called partner”, but a valuable member for 69 years.

Bibliography:

- BERNSTEIN, B. J.: The Cuban Missile Crisis: Trading the Jupiters in Turkey? Political Science Quarterly, 1980. 95(1), pp. 97-125.
- BINNENDIJK, A.: The Russian-Turkish Bilateral Relationship: Managing Differences in an Uneasy Partnership; Turkey's Nationalist Course, Santa Monica,CA: RAND Corporation, 2020. p. 107.
- BOLUKBASI, S.: The Johnson Letter Revisited; Middle Eastern Studies, 1993. 29(3), pp. 505-525.
- GERSON, M. S.: No First Use: The Next Step for U.S. Nuclear Policy; International Security, 2010. pp. 7-47.
- K, J. D.: Greece, Turkey, and N.A.T.O; The World Today, 1952. 8(4), pp. 162-169.
- KENNAN, G. F.: The Sources of Soviet Conduct; 1947, July, https://www.foreignaffairs.com/articles/russian-federation/1947-07-01/sources-soviet-conduct (downloaded 04 April 2020)
- KENNAN, G.: February 22, 1946 George Kennan's 'Long Telegram'; https://digitalarchive.wilsoncenter.org/document/116178.pdf (downloaded 04 April 2020)
- KINACIOĞLU, M.: NATO-Turkey Relations: From Collective Defence to Collective Security; Turkish Foreign Policy, 2017. pp. 83-103.
- KRISTENSEN, H. M.: U.S. Nuclear Weapons in Europe A Review of Post-Cold War Policy, Force Levels, and War Planning. Washington: Natural Resources Defense Council, 2005.
- KRISTENSEN, H. M.: U.S. Nuclear Weapons In Europe; Federation of American Scientists,Washington D.C. 2019.
- LEGENDRE, T.: Military Change – Discord or Harmony? Copenhagen: Danish Institute for International Studies, 2011.
- LINDGAARD, J. – PIEPER, M.: TURKEY'S NATO FUTURE: Between alliance dependency, Russia, and strategic autonomy; Copenhagen: Danish Institute for International Studies, 2020.
- MATLARY, J. H.: Strategy: Deterrence, Containment, Coercion, and Confrontation; In: J. H. MATLARY (eds.): Hard Power in Hard Times, Palgrave Macmillan, 2018. pp. 23-45.
- MENAND, L.: Fat Man – Herman Kahn and the nuclear age; 2005. https://www.newyorker.com/magazine/2005/06/27/fat-man (downloaded 04 April 2020)
- MICHEL, L. – PESU, M.: Strategic Deterrence Redux; Finnish Institute of International Affairs, Helsinki, 2019.

- RUDNICK, D.: NATO and the Cyprus crisis Pressure groups versus power politics; The Commonwealth Journal of International Affairs, 1977. 67(226), pp. 182-190.
- RUTHERFORD, I. P.: NATO's new strategic concept, nuclear weapons, and global zero; International Journal, 2011. pp. 463-482.
- STEFANOVIC, D.: Turkey's perennial strategic importance and the S-400 Saga; 2019. https://www.aies.at/download/2019/AIES-Fokus-2019-10.pdf (downloaded 04 April 2020)
- U.S. State Department. (n.d.): Strategic Defense Initiative (SDI), 1983. https://2001-2009.state.gov/r/pa/ho/time/rd/104253.htm (downloaded 04 April 2020)
- ÜLGEN, S.: Turkey and The BomB; Carnegie Endowment for International Peace, Massachusetts Avenue, NW, 2012. https://carnegieendowment.org/files/Turkey_Bomb_Full_Text.pdf (downloaded 04 April 2020)
- WALLANDER, C. A.: Mutually Assured Stability: Establishing US-Russia Security Relations for a New Century; 2013. https://www.files.ethz.ch/isn/168169/mas_ib_atlanticcouncil.pdf (downloaded 04 April 2020)
- WEZEMAN, S. T. – KUIMOVA, A.: Turkey And Black Sea Security; SIPRI, Solna, Sweden, 2018.
- WOOLF, A. F.: Nuclear Weapons in U.S. National Security Policy: Past, Prensent and Prospect. 2008. https://fas.org/sgp/crs/nuke/RL34226.pdf (downloaded 04 April 2020)
- https://www.nato.int/cps/en/natohq/opinions_168602.htm (downloaded 04 April 2020)

FAISAL WARIKAT

SURVIVAL COMPARISON BETWEEN HAMAS AND HEZBOLLAH

Abstract

Hamas and Hezbollah share common characteristics mainly that both of them survived an arrayed use of different methods to eliminate them but that strengthened them and kept them alive for more than 30 years.
This article compare Hamas and Hezbollah regarding their ability to survive. The used method is complex research methodology.
The main conclusion of this article is that Hezbollah is more resilient than Hamas and has more powers.

Keywords: Hamas, Hezbollah, Survival, semi-state actors.

Introduction

The survival of Hamas and Hezbollah is the academic research problem; given that most of the terrorist groups do not live more than 10 years.
The main objective of this article is to compare Hamas and Hezbollah in accordance with their survival. Comparative research methodologies seek for commonalities between the two entities, and try to explain how these entities could reach survival.
It is not an easy task to quantify survival and to compare between entities, though Chairman of the Communist Party of China Mao Tse-Tung used a scale from 0-10 to measure the power of the guerillas against their adversary. He applied the same factors on both sides' the guerillas and the incumbent government. The factors that Mao Tse-Tung thought about are:

a) appeal of a program: if the program is dynamic it can get 7 but if it has no program then 0;
b) popular support;
c) quality of troops;
d) military efficiency, in guerilla situations;
e) internal unity;
f) equipment;
g) operational terrain, is it favorable or not favorable;
h) operational area communications;
i) sanctuary.

But he measured these factors arbitrarily.[1]

[1] Mao TSE-TUNG: Quotations from Chariman Mao Tse-Tung; Rare Oriental Book Co. Aptos, California, 1966.

Method of analysis

This study is an analytical research that uses a mixed-methods approach of quantitative and qualitative designs, a questionnaire which was appropriate to the explanatory nature of the research to provide more significant in-depth data. The overall sample was composed of 300 respondents (200 males and 100 females). The sample size was calculated with a margin of error of 0.06. The survival was evaluated using an index of a 20 -item scale, developed by the researcher. The survey used a questionnaire that adopted a 5-point Likert scale (very high, high, medium, low, and very low) to measure the responses.

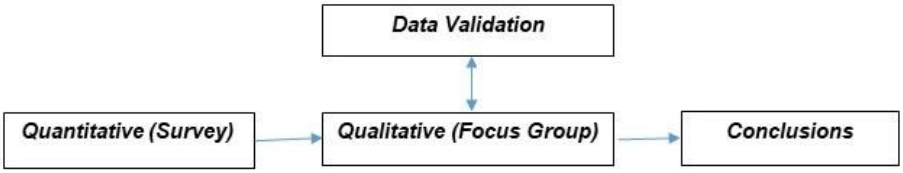

Figure 1: Method of analysis
(Author's own edition)

The demographic breakdown of the participants is based on age, gender, state of residence, occupation; the main areas were the Kingdom of Jordan, West Bank, Gaza Strip, Lebanon and Arab Israelis. Respondents' age between 20 and 30 years is 20%. Males represented 81.3% of the participants, 18.7% were females; the majority (85.5%) were employees from the civilian's bureaucracies, 20% from a security background, the rest are students and academics.

Gender	N	Percent %
Male	200	75
Female	100	25
Total	300	100

Figure 2: Distribution by Career
(Author's own edition)

Career	N	Percent %
Active or Retired civilian	100	33%
Active or Retired security	25	8
Academics	75	25
No Career	100	33
Total	300	100

Figure 3: Distribution by Residence
(Author's own edition)

Residence	N	Percent %
Jordan	100	33
Lebanon	35	12
West Bank	50	16
Gaza	100	33
Arab Israelis	15	6
Total	300	100

Figure 4: Distribution by Gender
(Author's own edition)

Age Interval	N	Percent %
Less than 20	1	0.5
21-30	49	11,5
31-40	100	33
41-	150	50
Total	300	100

Figure 5: Distribution by Age
(Author's own edition)

Variable	N	Min.	Max.	Mean	Std. Deviation
Age	300	19	68	39.54	7.71

Figure 6: Deviation in Age
(Author's own edition)

Validation of the instrument proceeded in two distinct phases. The initial phase involved a group of referees and expert arbitrators, who provided some comments on the tool. The second phase involved the implementation of a pilot study (N=30) to validate the survey using explanatory factor analysis. Factor loading for all items exceeded 0.60 (0.62 to 0.90).

The third way of validation was the use of focus groups, the focus group had a task to weigh the parameters that relate to the survival of semi-state groups in general and proper weight for both groups of Hamas and Hezbollah.

The reliability was tested using Cronbach's Alpha to ascertain the reliability and consistency of the survey. Cronbach's Alpha for the instrument sub-scales was between 0.81 and 0.78, indicating very good reliability and consistency, as indicated in Figure 7.

Sub-scale	No. of items	Alpha
Group Circle	10	0.84
State Circle	10	0.86
Community Circle	7	0.88
Other Groups Circle	9	0.81
Adversary Circle	4	0.76
Regional Circle	13	0.90
International Circle	6	0.86
Total	76	0.92

Figure 7: Reliability of knowledge transfer scale
(Author's own edition)

Data were analyzed using statistical package for social sciences (SPSS). The questionnaire items were rated on a 1–5 Likert scale (5=very high, 4=high, 3=medium, 2=low, 1= very low).
The following statistical techniques were employed: Standardized regression, T-test, One-way analysis of variance, Tukey test, Two-way analysis of variance, Cronbach's Alpha, and Factor Analysis; the mean score key is as shown in the following table:

No.	Mean score	Degree of Impact	Standard
1.	1 – 2.33	Low	One Standard Deviation below
2.	2.34 – 3.67	Moderate	Mean
3.	3.68 – 5	High	One Standard Deviation above

Figure 8: Mean Score Key
(Author's own edition)

3. Results of the research

3.1. Public Support

The impact of public support on Hamas' survival is more important than its impact on Hezbollah's, the mean score for public support on Hamas was four, while the mean for Hezbollah is 3.5

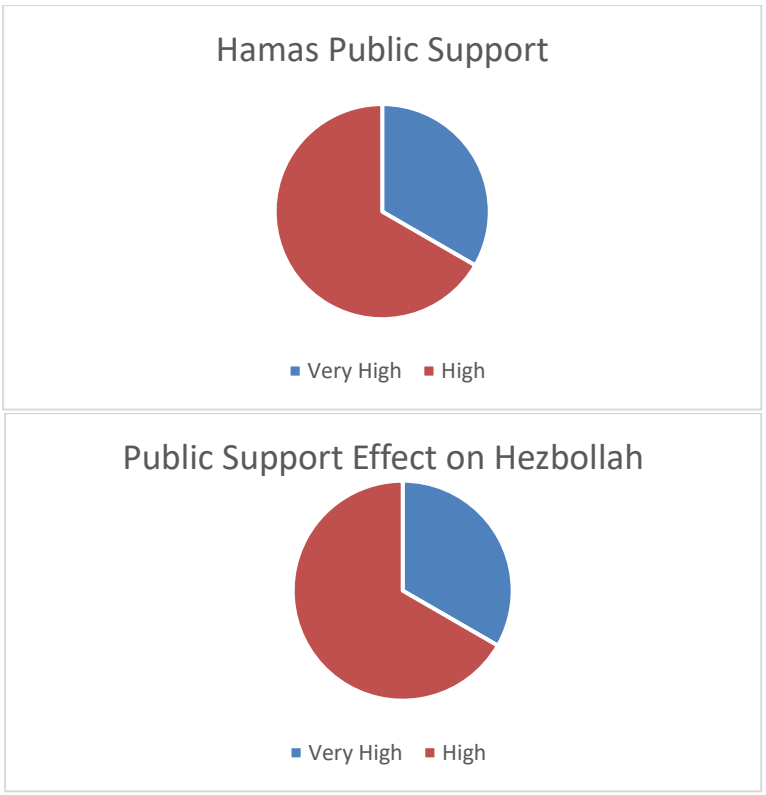

Figure 9: Public support effect on Hamas and Hezbollah
(Author's own edition)

The same view was validated by the Focus group that gave Hamas public support within the host nation, more impact than Hezbollah's, the focus group gave Hamas 4 and gave Hezbollah 3.5.

3.2. Military Capabilities

By the view of most respondents, Hezbollah has more military capabilities than Hamas. This finding is validated by historical analysis from the wars that erupted between Hamas and Hezbollah with Israel.

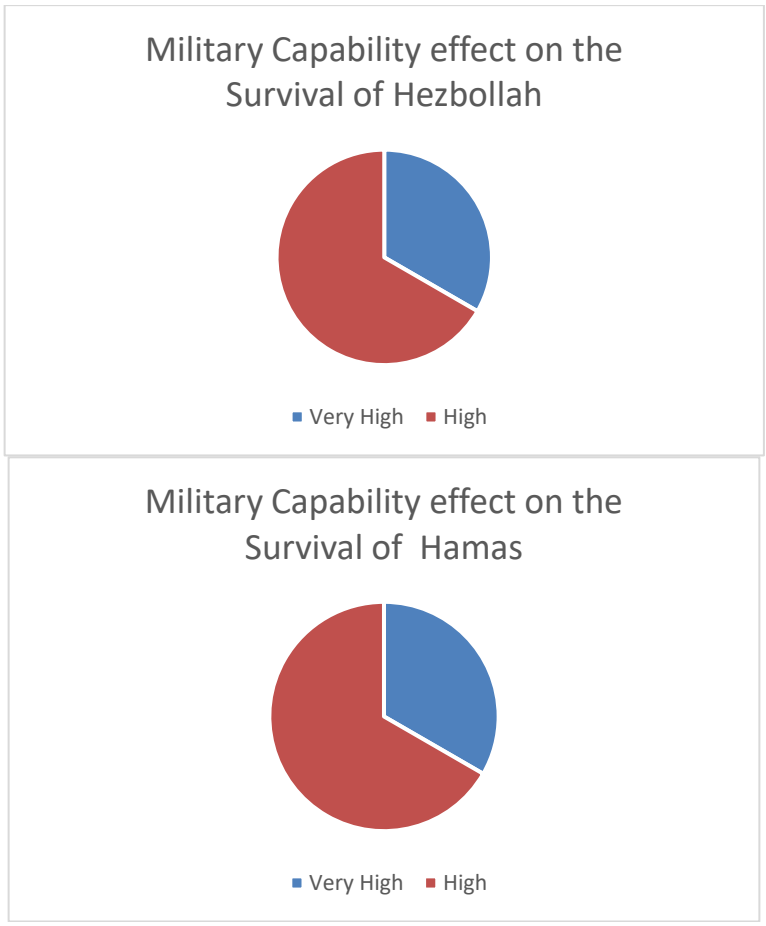

Figure 10: Military capability effect on Hezbollah and Hamas
(Author's own edition)

3.3. Ideology

The effect of ideology on Hezbollah's survival is more than its impact on Hamas, for any group to win, it needs weaponry, an ideology, and a motivating group[2]. Michael Freeman (2014) claims that ideology identifies" what *the problem is, who is the enemy, what solutions are, and what legitimate means are."*[3] Israelis assessed the nature of Hamas and that its strength lies in its ideology.

2 KHALAF, Shalah (IYAD, Abu): Palestine without an identity; Dar El-jaleel, 1996. p. 65
3 FREEMAN, Michael: Leadership Targeting of Terrorist Groups: A Strategic Assessment; CA Naval Postgraduate School, 2014

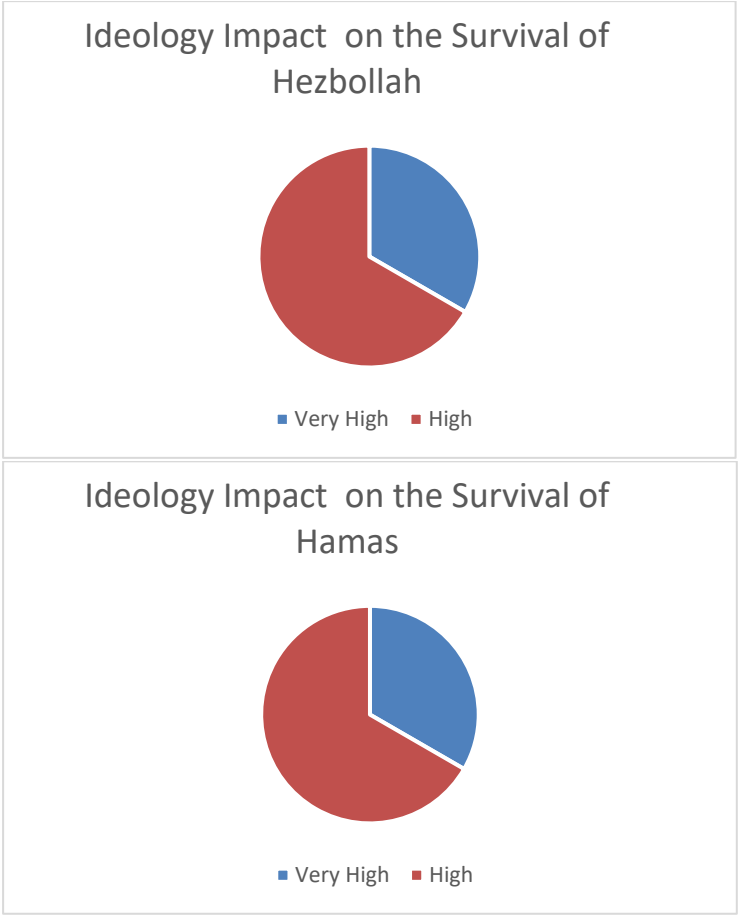

Figure 11: Ideology impact on the survival of Hezbollah and Hamas
(Author's own edition)

3.4. Organizational Structure

Hamas's organizational structure attributed more to the survival of the group more than Hezbollah's, the effect of organizational structure does not affect Hezbollah in serious means as it applies central hierarchy in the governance, while Hamas is a more networked organization.

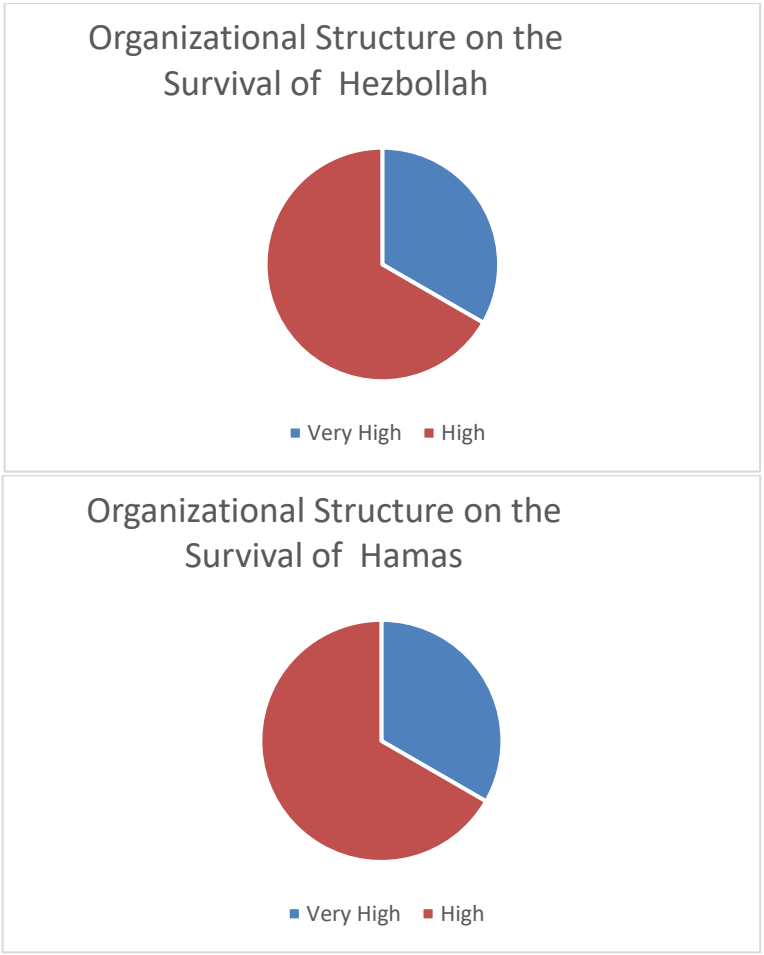

Figure 12: Organizational structure on the survival of Hezbollah and Hamas
(Author's own edition)

3.5. The operational security

The capability of Israeli security to penetrate Hamas is higher than its capabilities against Hezbollah's, Israel has a calm border with Hezbollah after the 2006 war except for operations against it inside Syria. Hamas was a bit more penetrated by Israeli security agencies as it stands on a high pressure especially from the Shabak[4].

[4] Shabak or sometimes called Shin Bet is the security organisation inside Israel which focuses on the internal security especially in Gaza and the West Bank.

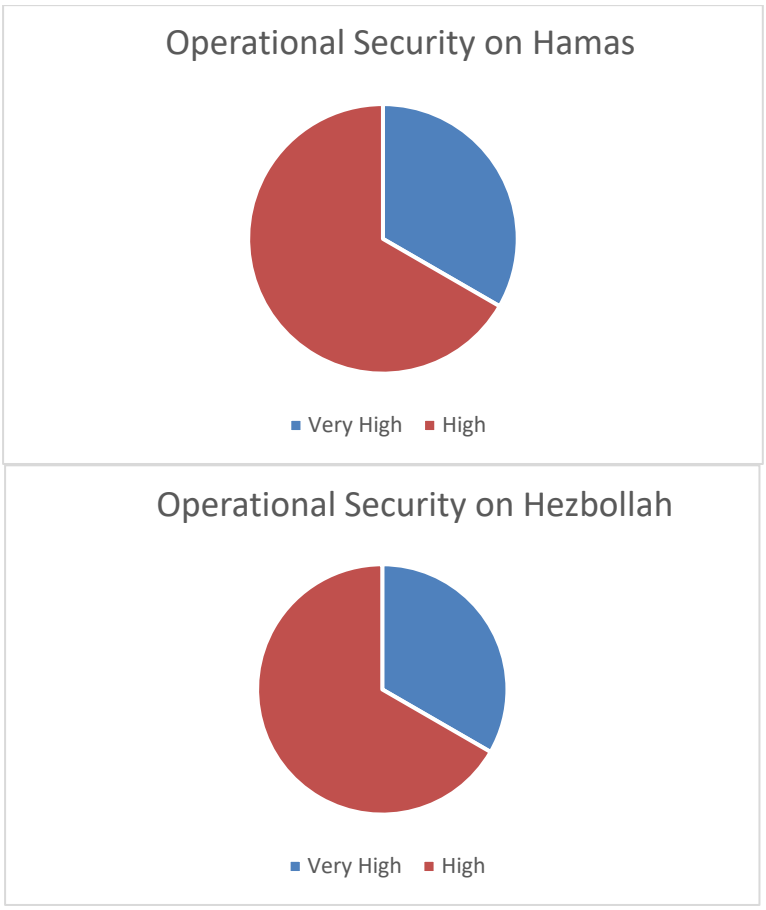

Figure 13: Operational security on Hamas and Hezbollah
(Author's own edition)

3.6. The Relationship with other groups

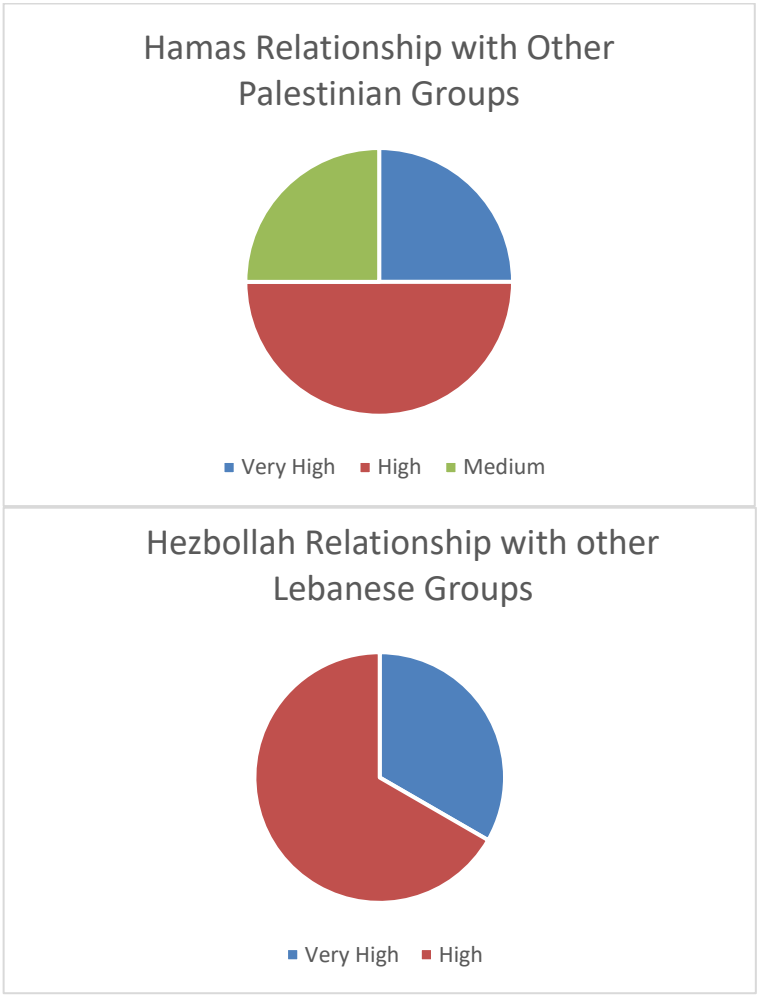

Figure 14: Hamas and Hezbollah relationship with other receiving country ethnics groups
(Author's own edition)

Hezbollah has more effective relationships inside Lebanon with 100% acknowledges this factor, while Hamas is less effective in this aspect, Hamas benefitted from its relationship with the Muslim Brotherhood, and with Hezbollah at the same time.

3.7. The weakness of the host state

The opinion of the participants was significantly important about the role in Hezbollah case, while in Hamas' case was divided.

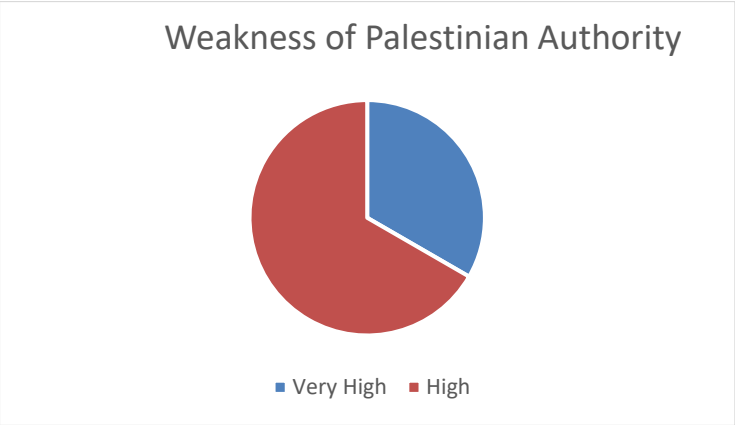

Figure 15: Weakness of Palestinian authority
(Author's own edition)

3.8. Foreign Regional support

The impact is almost preferable to Hezbollah with overwhelming support from Iran and Syria. Hamas is supported economically and militarily from Iran, also it has a limited political and economic support from Qatar and Turkey, and other parts of the world; however, the international circles are not in support of Hamas because of the limited borders that Hamas has with Israel and Egypt what limits its capabilities, in contrast to Hezbollah which has a porous border with Syria.

3.9. The Role of Israel

The respondents gave a significant role for Israel to preserve Hamas, while the role is against Hezbollah is evident.

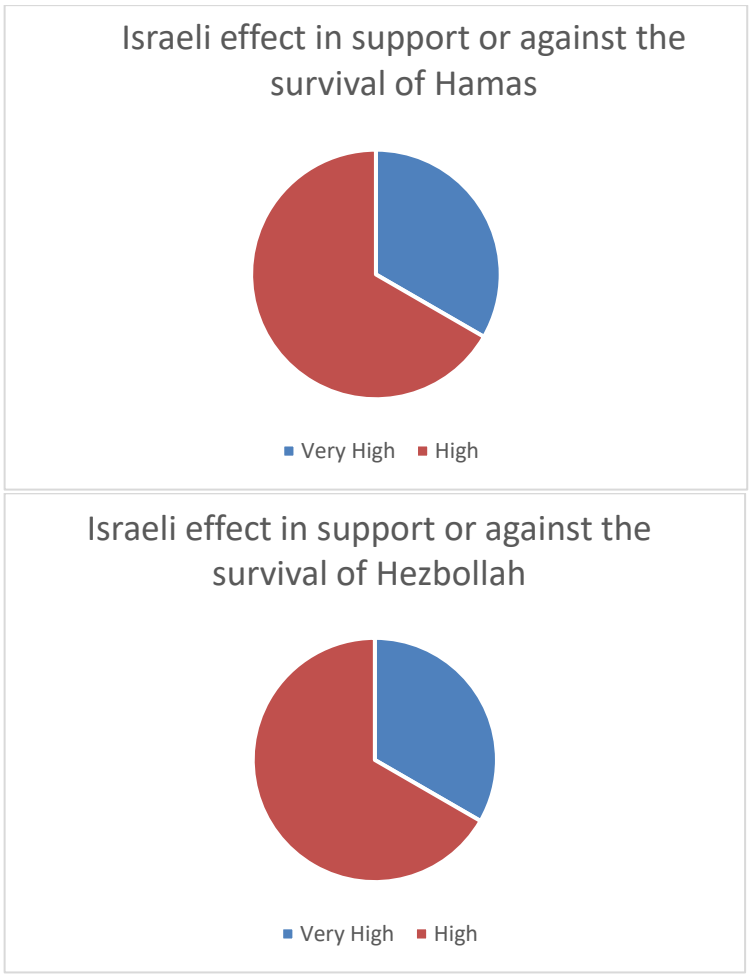

Figure 16: Israeli effect in support or against the survival Hamas and Hezbollah
(Author's own edition)

3.10. Other findings

Based on the results of the survey, the following table displays the mean score of the findings of the survey that establish a comparison between both groups dependent on the surveyed sample.

Factor	Hamas	Hezbollah
Public Support	4	3
Ideology	3	4
Military Capabilities	2	4
Financial Assets	2	4
Organizational Structure	3	3
Maturity	5	5

Operational Security	4	5
Relations with Other groups	3	4
Regional support	4	3
Israel Effect	4	3
International Support	3	4
Total	36	43

Figure 17: The Mean Scores of Survival Circles
(Author's own edition)

4. Focus Group Results

Two focus groups of 10 experts were created to assess the factors of survival's weights, give a comparable weigh to Hamas and Hezbollah. They also give weight to some factors that cannot be judged by surveys. One of the main objectives of the focus group is to approve the model of survival circles. Another focus group is going to be held in Hungary next year to ascertain the results.

Factor	***Weight/ Focus Group 1***
Size	3
Ideology	3
Military capabilities	3
Financial Assets	3
Maturity	3
State sponsorship	3
Public support	6
Host State weakness	6
Other Groups support	3
International support	3
Adversary calculation	4
Total weight	40

Figure 18: Wight of the parameters
(Author's own edition)

Activity	HAMAS	Hezbollah	Remarks
Size	A	A	Both of them are more than 5000
Ideology	A	A	Both have the highest ideology which is a blend of religious and nationalistic
Military capabilities	B	A	Both groups have military experience in wars with Israel and with internal competitors
Maturity	A	A	They started from similar dates in the 1980s, Hezbollah from 1983, while Hamas from 1987
Financial Assets	B	A	Resources of Hamas are more monitored by Israel in contrast to Hezbollah
Host state weakness	A	A	Lebanon is partially influenced by Hezbollah because of the political game and alliances with the FPM, regarding Hamas the PA lost the battle with Hamas in 2007
Topography	A	A	The topography of Gaza is difficult for invaders because of the high density of population, tunnels, a high percentage of collateral damage, in Lebanon it is a little bit easier for aerial attacks, but for ground forces, there is a battlefield prepared
Social support	A	B	Hamas has high support inside Gaza, while Hezbollah has less support because of his external endeavors
Iran sponsorship	B	A	Iran supports both groups, but its assistance to Hezbollah far outweighs its assistance to Hamas
Israel Calculations	B	A	Israel monitors both groups, but its dealings with Hamas is more threatening because of proximity
International pressure	A	B	The pressure over Hamas is more than the pressure over Hezbollah because of Hezbollah political alliances inside the government
Other groups support	B	A	Hezbollah has more connections with militant groups
Total	32	35	

Figure 19: Focus Group weights
(Author's own edition)

The focus groups were asked to give a grade for each factor in the comparison between Hamas and Hezbollah, for this task, A=3, B=2, C=1;

Factor	*Weight*	*Hezbollah*	*Hamas*
Groups Resilience	15	15	13
The community circle	6	5	6
The State Circle	6	6	6
The Regional Circle	6	6	4
The Other Groups Circle	3	3	2
International Circle	3	2	2
Israeli Calculations	4	3	2
Total	43	40	35

Figure 20: Weights of aggregate factors
(Author's own edition)

5. Comparison

Hezbollah has better chances of survival more than Hamas. The survey shows Hezbollah had 43 while Hamas Has 36 points.
The focus groups validated the result with similar numbers which gave Hezbollah 40 and Hamas 35. This result is depicted in the following chart:

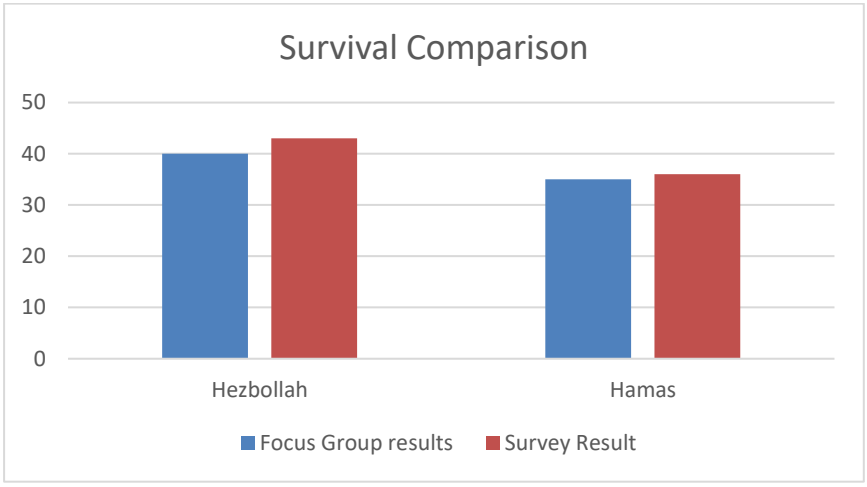

Figure 21: Comparison of survival between Hamas and Hezbollah
(Author's own edition)

The results can be explained by their semi-state character which yield host state weakness, public support to the group, international support, the presence of regional support, the size of the group, and its engagement in administrative and political matters within the state.

6. Conclusions

The main conclusion is that Hezbollah is more survivable than Hamas. The semi-state character of both groups is the main variable that keeps both groups alive, semi-state means that the host state is weaker to dominate them, 75% of the respondents agree that the weakness of the Lebanese state is an instrumental element to the thrive of Hezbollah, more results prove the same to Hamas.
Public support for the groups is enough to remain alive with about 25%, which is earned by their capabilities to provide socio-economic services, and having a political branch and ideology, also they use a model called golden trinity of resistance which is captured by Hezbollah, and Hamas similar to the Clausewitzian trinity of war,
Israel is not fully capable of defeating neither Hamas nor Hezbollah mainly because of their nonmaterial component that is their ideology that attracts supporters, especially when the fight is against Israel which give them the needed legitimacy and reasons to their survival.
Research studies show that nationalist and religious groups have more endurance than other groups like left or right-wing groups. Some attribute the reason for the staying in power of sacred or spiritually based motivation. Hamas is a blend of religious part and national liberation movements. However, this research proves that religious groups have a problem to implement their agendas outside their home state.

Hezbollah is more survivable than Hamas, even if the economic situation worsens in Lebanon. Hezbollah can survive the crises as it has its own resources.
Another indicator in the survey for the semi-state character is the public support both groups enjoy, and the legitimacy they managed they earn within their host states and even with their enemy which is Israel.
Hezbollah has its media outlets like al-Manar TV, generators for electricity called the al-Hadi company, water wells, TV subscriptions, while Hamas governs Gaza with de-facto governments with services ranging from security to municipal duties.

The adversary calculation is a new term, that has to be taken into account, in this account, a 'bone breaking point' is the threshold that instigates the reaction and triggers the resolve of the enemy, as long as, the groups acts below that point, they might get limited forgiveness and maneuver of play is allowed. Committed by both groups is to play under the critical threshold with Israel and to keep low level intensity of conflict with Israel whenever it is needed.

Bibliography:

- BARTELS, Knud: The Center of Gravity; in: An Anthology of Doctrinal Papers (Carlisle Barracks, PA: Department of Military Strategy, Planning, and Operations, US Army War College, 1994.
- CLAUSEWITZ, Carl von: On War; edited and translated by Michael Howard and Peter Paret, Princeton University Press, Princeton, 1976. pp. 75-77.
- EIKMEIER, Dale C.: COG Analysis; Military Review, July-August 2004, (downloaded 17 February 2006)
- FARRELL, Theo: Constructivist Security Studies: Portrait of a Research Program; International Studies Review 2002/1. p. 49, http://www.jstor.org/stable/3186274 (downloaded 17 October 2020)
- FREEMAN, Michael: Leadership Targeting of Terrorist Groups: A Strategic Assessment; CA Naval Postgraduate School, 2014.
- Guardian: Hezbollah Leader: We regrert the two kidnapping that led to war with Israel; 28 August 2006. https://www.theguardian.com/world/2006/aug/28/syria.israel (downloaded 17 October 2020)
- KHALAF, Shalah (IYAD, Abu): Palestine without an identity; Dar El-jaleel, 1996.
- Mao TSE-TUNG: Quotations from Chariman Mao Tse-Tung; Rare Oriental Book Co. Aptos, California, 1966.
- RICHARD, Davis: Hamas, Popular Support and War in the Middle East: Insurgency in the Holy Land; Routledge, London, 2016.
- SCHNAUBELT et al.: Vulnerability Assessment Pocket Guide; 2014. https://www.rand.org/content/dam/rand/pubs/tools/TL100/TL129/RAND_TL129.pdf (downloaded 17 October 2020)
- STRANGE, Joseph – IRON, Richard: Centers of Gravity & Critical Vulnerabilities; Marine Corps War College, Quantico, Virginia, 1996. pp.1-12.
- United Nations Security Council Resolution 1559: Calls upon all remaining foreign forces to withdraw from Lebanon; Calls for the disbanding and disarmament of all Lebanese and non-Lebanese militias; Supports the extension of the control of the Government of Lebanon over all Lebanese territory, 2004.
- WARIKAT, Faisal: Circles of survivability of Terrorist Groups; National Security Review, 2020/1. pp. 129-147.

BENCE GÖBLYÖS

NATO'S RESPONSE FOR THE SOUTHERN CHALLENGES - NATO STRATEGIC DIRECTION SOUTH HUB

Abstract

One of NATO's youngest elements was inaugurated and commenced its work in 2018. Its establishment was the output of a very long process, in which Southern NATO members tried and convinced the rest of the Alliance of the importance of security challenges emanating from the Southern strategic direction. In this essay I am looking for the major motives behind the establishment of this new Hub. Also, I try to identify those fields in which a proper-working Hub can assist the Alliance achieving its goals. During my research I found that the Hub's success greatly depends on the way the member states handle it. After a turbulent decade, an information centre like this can be a great help to assist the Alliance to project stability, but recent processes may jeopardize the capabilities of the Hub. There are severe strategic divergencies within the Alliance, and now, during the COVID-19 pandemic it will be hard to maintain the capabilities and contributions while a race for resources can be expected between the Eastern and Southern directions.

Keywords: NATO, Hub, Middle East, Northern Africa, MENA, Southern direction

Introduction

The aim of this essay is to introduce the leading drivers behind the creation of NATO Strategic Direction – South Hub and to explain its main purpose. It is in my interest to expand the existing literature about this new element, as during my research I realized that about the Hub and stability projecting elements there are only a very few publications.

One of NATO's youngest element's aims is to improve the Alliance's awareness about its southern neighbourhood. I will examine the basic functions of the Hub and I will make an effort to evaluate the advantages of it and the challenges it faces.

The method of my research was based on open-source information. Besides these, I had the luck to consult with Hungarian, Italian and other international staff members due to my recent deployment, and gather some extra, but still unclassified information.

In my essay, I will firstly provide a brief overview of the main milestones leading to the creation of the Hub. Then I will explain why a new element was needed in NATO's structure. Before explaining the main processes and security threats that Hub can assist NATO's goals, I briefly explain the expression projecting stability. Finally, I shortly give a clue about the Hub's inner structure before introducing the main

effects of the latest important report that was created in order to provide a possible blueprint for the Alliance's next decade.

Modern history of the Southern strategic direction

Back in the Cold War era, NATO had a fairly clear and obvious purpose and threat perception. After the collapse of the Soviet Union and the disintegration of the Warsaw Pact, NATO, as a surprised victor, had to seek for new tasks and verification of its own existence. Then history happened and the Alliance found itself facing with a new set of threats and crises close to its borders. The transforming NATO's history since then is basically about adaptation to a rapidly changing security environment and is striving to provide proper answers to these challenges. Besides others, the events on the Western Balkans, the appearance, evolution and golden age of international terrorism, then clandestine adversary activities in the cyberspace, the Arab Spring, the events in Eastern Ukraine and on Crimea made it a must for the Alliance to improve itself, create or develop certain capabilities to counter challenges that are far beyond conventional, Article V operations.[1] Since the very beginning of the existence of this Alliance, the main focus point of strategic thinking was the menace posed by eastern actor(s), namingly the Soviet Union. Therefore, the guiding principle of channeling the capacity building, deterrence, prevention, preemption and collective defence measures and efforts was always the Eastern threat, most notably in the Baltics, Poland and nowadays in Romania and Bulgaria.[2]

Nevertheless, the Southern allies have been trying to draw the attention of the Alliance to the fact that countering the Eastern threat is not the only action that NATO has to deal with. The importance of the menace posed by the threats and risks from the Southern direction is being stressed by these South European allies, most notably Italy. As Italian researcher and former diplomat, Alessandro Minuto-Rizzo states, the recognition of the importance of the Southern strategic direction by NATO is the outcome of a very long process. In 1999, the representatives of Italy were more than satisfied that in the end of the Washington summit, they succeeded to force one sentence in the declaration about the Mediterranean region. Today the importance of the Southern neighbourhood seems to be acknowledged and shared. The president of the NATO Defense College Foundation underlines that despite Italy being one of the major players in this process, they failed to contribute with a complex vision or action plan regarding the Arab world and the Mediterranean region. As all the Southern allies failed to do so as well, we can hardly point out a strategic vision regarding the Southern flank of NATO in its strategic concepts or decision-making processes. Therefore, the one robust other direction received greater support pushed by the United States of America – the Eastern one. The USA is historically less interested in the issues with NATO's Southern neighbourhood.[3]

---

1 The North Atlantic Treaty. Article V. https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=en (downloaded 13 August 2020)

2 AVERSANO STABILE, Andrea: NATO's 70th Birthday: Family Matters at Stake pp. 2-3.

3 MINUTO-RIZZO, Alessandro: The 'Nebulous' Naples Hub: Is There a Strategic Direction for the South? https://www.ispionline.it/en/pubblicazione/nebulous-naples-hub-there-strategic-direction-south-20928 (downloaded 27 October 2020)

The Alliance, however, did not remain fully passive in this direction. It conducted active cooperation and neighbourhood policy with the state-level actors of this region. Most importantly, the Mediterranean Dialogue was initiated in 1994 and started its activities in the next year. It was founded by NATO and five external countries, Egypt, Israel, Mauritania, Morocco and Tunisia, and they were later joined by Jordan and Algeria. The main purpose of this cooperation is the development of good relations with these states and mutual confidence-building. Upon this scheme, the Istanbul Cooperation Initiative was formed by NATO in 2004, and it consist of Bahrain, Qatar, Kuwait and the United Arab Emirates. [4]

Why a Hub is needed?

The main drivers behind the creation of this new element in NATO's structure are the new security challenges, the need of the projection of stability and the willingness and capabilities to conduct out of area operations in accordance with the 2010 Strategic Concept of the Alliance, titled Active Engagement, Modern Defence.

From the Eastern direction the threats, risks and challenges can be more precisely identified. Hence collective defence and deterrence here as the main tools are stressed.[5] This cannot be told about the Southern direction, though. Since the middle of the last decade, the southern allies were louder than before urging the Alliance to pay closer attention to the Southern flank and to elaborate solutions to counter the more complex, faceless, but as serious threats as on the East. The then-defence minister of Italy, Roberta Pinotti highlighted: personally she, the chief of general staff of the Italian Armed Forces and Italy's permanent representative to NATO strongly encouraged the Alliance to take steps and to create a new element in NATO's structure in order to counter the menaces emerging from the South more effectively and comprehensively.[6]

The main tools in the Alliance's toolset to deal with the challenges of the South are NATO's newly (mostly since the beforementioned Strategic Concept came into force in 2010) embraced cooperative security approach, application of various soft power capabilities and stability projection. The territory of NATO's Southern strategic direction is quite similar to the enlarged Mediterraneum of the Italian geopolitics.[7] This includes all Africa, north from the Equator, the so-called arc of instability, which spans from Morocco to Afghanistan, the Persian Gulf and the Western shores of the Black Sea. This territory involves land and sea, and, of course, airspace. One can simply understand that NATO can build trust among its Southern members in order to contribute to the countering of the Eastern threat, if their voice is

---

4 BASAGNI, Laura – BRANDSMA, Charlotte – LESSER, Ian – LÉTÉ, Bruno: The Future of NATO's Mediterranean Dialogue – Perspectives on security, strategy and partnership. https://www.gmfus.org/publications/future-natos-mediterranean-dialogue (downloaded 29 October 2020)

5 TARDY, Thierry: The risks of NATO's maladaptation. p. 7.

6 ANSAMED: NATO Hub in Naples 'particularly important' – Pinotti http://www.ansamed.info/ansamed/en/news/sections/generalnews/2017/02/15/nato-hub-in-naples-particularly-important-pinotti_61bddeb3-91c6-46d7-a549-d3dd315fe845.html (downloaded 02 november 2020)

7 Mediterraneo allargato

heard in the Alliance, and the Northern/Eastern partners also acknowledge the Southern threat. The different perception of threat causes some severe strategic divergencies within the Alliance.[8]

At the time the summit was held in the summer of 2016 in Warsaw (the first summit held in one of the capitals of the former Warsaw pact states) it became obvious that the events taking place South of the Alliance's borders can severely damage the member states' interests. Islamist terrorist attacks in the territory of the European allies, the seemingly endless conflicts in North Africa and the Middle East, uncontrolled mass influx of migrants made it to the headlines when it came to security at that time. Two major, symbolic incidents happened in November of 2015. On the 13th a suicide bomber committed a terrorist attack in a night club in France. Almost 100 innocent civilians died in this attack. The other major incident happened not even a fortnight later: on the 24th a Russian bomber jet was shot down by Turkish air defence after the violation of their (and therefore NATO's) airspace. The downed bomber was a Sukhoi Su-24. As I mentioned before, these incidents were symbolic as the two major threats on the Euro-Atlantic peace and way of life incarnated. Not to be nostalgic, but even terrorism is not what it used to be. As in the beginning of our millenary terrorism was quite different. As this is not the main topic of this essay, I would not elaborate this statement more, but one can be sure about the fact that prevention is way harder nowadays as the terrorists are hardly or not at all linked to 'regular' terrorist organizations (that use internet and dark web professionally) and they are seemingly integrated in the Western societies. Unfortunately, we have seen several attacks of this kind in the last decade. The other case shows the conventional, usual threat posed by the Russian Federation. However, the Russian threat also evolved. Russia now, besides the conventional threat, uses hybrid warfare and masters in disinformation. The Southern threat is usually related to migration, trafficking in human beings, weak or failed states, terrorist organizations, while the Eastern challenge posed by Russia used to be conventional, Article V-based deterrence, prevention, pre-emption and posture. Compared to this, nowadays Russia applies hybrid and cyber warfare, builds and develops A2/AD[9] capabilities in Northern Africa and at the Black Sea in order to destabilize NATO's Southern neighbourhood also. It has lesser importance on our topic now, but in this period of time, besides Syria and Libya, Iran's suspected nuclear programme was also a concern, while the insecurity was not eased by the United States. All in all, now we cannot declare that Russia is 'only' a conventional threat from the East, nor can we say that non-state, complex threats and terrorism come from the South.

Dealing with security challenges arisen from the South perfectly fits in the Strategic Concept endorsed by the Alliance in 2010, as cooperative security became the third main pillar of the Alliance alongside with collective defence and crisis management.[10]

---

8 Ziya Meral: NATO and its Southern Flank. p. 85.

9 Anti Access, Area Denial

10 Active Engagement, Modern Defence – Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. p. 8. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf (downloaded 12 november 2020)

The main topic of the summit in Warsaw in 2016 was the Islamic State, of course and the ways and means that can be used to counter the threats it poses. It also became clear that the tools NATO possesses are not necessarily satisfactory to counter the Southern challenges. It was a bit far ago, but every stakeholder can remember the failure of the exodus of NATO from Iraq. The local security sector was, simply put, not ready to take over the responsibilities that were previously taken by the Allies. Using an effective and developed analysis and assessment to assist decision-making processes would probably very usefully preventing premature decisions. Two very important tools in the toolset of NATO's holistic approach, namingly defence capacity building and security sector reform can be effectively supported by an element like the Hub.[11]

As during the Cold War era, the main threat was posed by a single player from a definite direction, today the challenges we need to counter are faceless and all around. Only one of the problems with this is that given these threats, the member states can have shockingly different threat perceptions and therefore different strategic visions. [12] These divergencies can be seen between the Eastern and Southern member states, as they assess the existing threats severely differently. The Eastern and Northern states are considering the Russian threat from the East as the ultimate menace, while the interests of the Southern allies are more endangered by the threats experienced from the Southern direction, through the Mediterranean Sea, from the Middle East and Africa.[13]

In the last decade, the most important events that caused severe turbulence in the security of the North Atlantic Alliance both rooted from the southern strategic direction. The birth and emergence of the Islamic State was preceded by the Arab Spring in the beginning of the decade. The storms accompanying this spring did not bring fresh air and the MENA[14] region now nor more stable, neither more secure. It is fractioned by several political, societal, religious assets, and that causes challenge in various fields of security. In these circumstances, Islam radicalism can address those youngsters that have no other option to break out of their situation, as social mobility is nearly non-existent. Those living in these underdeveloped regions can be described with poverty, struggle to access drinking water, low education and high fertility, while their state does not function in various places or only partially does, while these groups are not (strongly) represented politically. NATO should create capabilities to get inputs also from these groups, as the information gathered from here can be valuable in a good functioning early warning system.[15]

---

11 MARRONE, Alessandro: What's new on NATO's Southern flank – Security threats and the Alliance's role after the Warsaw Summit. pp. 1-2. https://www.baks.bund.de/de/node/1558 (downloaded 12 november 2020)

12 REFLECTION GROUP: NATO 2030: United for a New Era pp. 8-9. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf (downloaded 09 december 2020)

13 Jean-Loup SAMAAN: Outflanked? NATO's Southern Hub and the Struggle for its Middle East Strategy. p. 63.

14 Middle East and North Africa

15 DIBENEDETTO, Alessandra Giada: Projecting Stability to the South: The Role of NATO Strategic Direction – South Hub. p. 2. http://cesi-italia.org/contents/Conf.Report%20Projecting%20Stability%20to%20the%20South_compressed.pdf (downloaded 16 november 2020)

Projection of stability

Nevertheless, the expression projecting stability is known since the middle of the 1990s, we, today still have no doctrines, but not even a working definition of it. According to Zoltán Szenes, 'the stability is a state or condition in which a country, government or society is able to create a situation in which they can mitigate the risk of a possible conflict. Projection is an activity that is conducted by the Alliance upon the request of the partner country or international organization in order to promote stability and increase security.'[16]

As it can be derived from the Strategic Concept of 2010, one of the major tasks of the Alliance regarding the Southern threat is the projecting of stability. In the toolset of projecting stability there are various tools, including conducting training missions. The aim of these can be the training of local security forces, or even training of public administration members or creating the culture of good governance. During these kinds of activities, it is vital to apply the principle of subsidiarity. The created Hub is responsible for providing these missions with the needed advice and information, and also to collect, handle, disseminate, share and assess the information received from these. It is important to highlight that when we talk about information in connection with the Hub, we mean open-source information, and not intelligence-provided. ISR[17] capabilities are also vital, but those are not the Hub's responsibility.[18]

The category of projecting stability can bear somewhat deeper cooperation also, like sharing intelligence inputs, strategic know-how, joint trainings, operations or missions or even preparation for accession to NATO. Of course, this would be hard to envisage in the case of the states of the MENA region, but we already saw common operations with ICI members.[19]

The birth of the Hub

On the 15th of February, 2017, NATO Secretary General, Jens Stoltenberg held a press conference in which he announced the decision about creating the Hub. After the ministerial level session of the North Atlantic Council, the Secretary General underlined that the Alliance has never ever faced that complex security challenges in the post-bipolar era as then, and this is the case highly because of the instability of the MENA region. It is of utmost importance to project stability and to improve the capabilities that can counter terrorist threats, he added. He also told that the Hub is

---

16 Translated by the author, originally: „*A stabilitás (stability) a NATO szerint egy olyan helyzet, állapot, ahol egy ország, kormány vagy társadalom képes olyan feltételeket teremteni, amelyek csökkentik a konfliktusok kialakulásának potenciális veszélyét. A kivetítés (projecting) olyan tevékenység, amelyet a Szövetség az érintett partnerország vagy nemzetközi szervezet kérése alapján végez, hogy elősegítse a stabilitást, növelje a biztonságot."* SZENES, Zoltán: A NATO új politikája: Stabilitás Kivetítése a Déli Régióba. p. 8.

17 Intelligence, Surveillance and Reconnaissance

18 DIBENEDETTO, Alessandra Giada: NATO's Hub and the Alliance's Engagement towards the South. https://cesi-italia.org/en/articoli/903/natos-hub-and-the-alliances-engagement-towards-the-south (downloaded 17 november 2020)

19 SZENES op. cit.

just one, but very important tool in the Alliance's Southern framework. NATO Response Forces, effective planning and training and ISR capabilities are other important tools in this comprehensive approach. The Hub about to be created does not aim to command high-profile operations, because the Alliance already has the institutions for that. The Secretary General highlighted three major areas:

- gathering, disseminating and assessing information,
- improving situational awareness in the area of interest,
- coordination of different resources, activities, and approaches.[20]

The location of this new element is also symbolic. However, all the member states can be affected by the events of the MENA area, the most severe effects can be detected in the Southern allies. Those states that have shores washed by the Mediterranean Sea faced international terrorism, human trafficking or an influx of mass migration. Therefore, it was obvious that the new Hub would open in one of the southern allies, at an existing NATO premise. The new Hub is located in the very same building as the Joint Forces Command, in Naples. Its logo shows the territory in which the Hub is about to operate. This territory has no shape borders in the logo, but we can assume that this is not just about style: The Alliance is flexible with the boundaries of this territory, as the challenges it will face probably will be hard to even locate, and maybe they can emerge from the outside of this area. However, this area is quite immense, five countries are to be highlighted in this territory due to their special relations with the Alliance or because of their strategic importance in the Southern neighbourhood. These are Iraq, Jordan, Libya, Syria and Tunisia. If we look at this territory, we can say that the vast majority of NATO's current operations are conducted in the highlighted area.

The legal basis of the creation of the new Hub is to be found in the second Article of the North Atlantic Treaty:
'The Parties will contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions, by bringing about a better understanding of the principles upon which these institutions are founded, and by promoting conditions of stability and well-being. They will seek to eliminate conflict in their international economic policies and will encourage economic collaboration between any or all of them.'[21]

Main bodies of the Hub

The amount of information of the internal structure of the Hub is quite limited, but getting in touch with members of it helped to get some insight of the inner cells. The Knowledge Management and Engagement is responsible for overseeing the overall activities of the Hub, and for enable the coordination and information flow between the commandment and the elements of the individual cells, and functions under the directions of the deputy director. The Comprehensive Research and Analysis Section monitors the outstanding, evolving and in-future security challenges and crises. It collects, shares and assesses information. The Engagement Coordination

[20] NATO: Press conference. https://www.nato.int/cps/en/natohq/opinions_141109.htm (downloaded 08 december 2020)
[21] The North Atlantic Treaty. Article II

Section serves as a coordinating body which aims to synchronize the efforts conducted by the interested players in the area and seeks to prevent or eliminate unnecessary parallel activities. The Civilian-Military Engagement & Coordination Section is the section vital in civilian-military cooperation and a cornerstone of getting the information from the population in order to enable for the Hub and the Alliance itself to get a proper situational awareness.[22]

Connect, Consult, Coordinate

One of the most important purpose of the Hub is to create a forum for the interested actors regarding the Southern neighbourhood. The interested playes, international organizations, non-governmental organizations, experts and NATO can connect to one and other. Getting the involved parties to the table and get them to initiate talks and consultation is vital in order to prevent the escalation of a possible conflict. Using a proper early warning system helps to settle the differences and conflicts of interests in a peaceful, sustainable manner. The third major task of the Hub is the coordination. This is about coordinating the actions to be taken in order to reach optimal use of resources.[23]

During the Warsaw summit and in the NATO 2030 programme (to be introduced later) the 360° approach is mentioned. The meaning of this is that threats and challenges can be expected from any possible direction, somewhat undermining the southern and eastern threat perceptions. The idea would be to get the Alliance ready to respond to these challenges. We can also say that this means that the Alliance (rhetorically) acknowledges the importance of the Southern threats. One action worth mentioning is that NATO made its AWACS (Airborne Warning and Control System) available for the U.S.-led coalition's efforts against the Islamic State. This was based upon the recognition of the fact that a direct confrontation would have backfired for NATO. The Alliance also has some measures to counterterrorism. This, however, does not primarily mean armed NATO operations in counterterrorism actions, but the training of local security forces and aiding these countries in any agreed way in order to eliminate the factors that feed these terrorist organizations. As a direct involvement would easily end up in a turmoil with an uncertain result, and local authorities might have bigger acceptance in these cases, NATO's most important role is defence capacity building.[24]

According to the Hub's former director, Gen. Brig. Ignazio Lax, the most dangerous threats and challenges from the South are the spreading of radical ideologies, mass migration, climate change, smuggling of drugs, piracy, demography, corruption, water scarcity, poverty, epidemics, international organized crime groups and bad governance. The Hub's most important role according to him is to analyse, assess these challenges and identify their roots. The Hub, of course, must examine

---

22 SGUAITAMATTI, Elisa: NATO's new Strategic Direction South Hub in Naples: Strategy and Balkan Activities. http://www.balkanalysis.com/blog/2018/01/08/natos-new-strategic-direction-south-hub-in-naples-strategy-and-balkan-activities/ (downloaded 11 december 2020)

23 DIBENEDETTO, Alessandra Giada: NATO's Hub and the Alliance's Engagement towards the South.

24 MARRONE op. cit. p. 2.

those threats that affect European security with special attention. He underlined that the Hub needs to collect, assess and share the common knowledge about the area in question, and to provide a forum for the interested parties (international organizations, states, non-state actors) in order to synchronize the efforts, they make and coordinate their actions for the sake of effectiveness.[25]

The Hub has a sophisticated website available. Here, the outsider can get a little bit of an insight to the Hub's activities. Members of the Hub regularly pay visits to stakeholders in the MENA area, they have conferences time to time, in the COVID-19 situation they hold regular webinars, they release weekly newsletters, while also some high-quality publications can be also accessed on this page.[26]

As Giray Sadik underlined: reality has far exceeded the thought that hybrid threats can only emerge from the East and terrorism only from the South. This tendency can be seen in Russia's strengthening presence in the MENA region. According to the researcher the Alliance's actions must be based on common understanding and willingness, as the lack of these can be a serious sign for the external actors about the thought weakness and of the Alliance. As the threats and challenges, that we need to face are getting more and more complex, while the boundaries are getting blurred between local and international, civilian and military, state and non-state actors and roots, it is of utmost importance that the approach taken is comprehensive. Not only horizontally, but also in the meaning of different sectors. The Alliance need to cooperate with local authorities, other state actors, international organizations, non-governmental organizations and local societies.[27]

Andrea Margelletti underlines that the two most important things are the political will and the operational capabilities, when we talk about the Southern threat. According to him, the Alliance need to seek real collective measures based on consensus in order to act effectively, because if this criterium is not met, then it's not only the southern allies, but also the whole Alliance what has to face unwanted challenges.[28]

There are several active players in the area already. The majority of these actors share a common goal, but their ways can vary. NATO (or more precisely, the Hub) is a key element in coordinating these diverse efforts and helping the creation of certain action plans, what can be followed by these actors, and unnecessary costs can be avoided, also fiscally, in human resources and efforts. In this, it is very important to have a proper situational awareness about the southern neighbourhood, but also a certain awareness about NATO's motives and goals in the region for the external actors. As mentioned before, the Hub might also have great responsibility in bringing the region's people closer to the Hub. If the Hub wants to contribute to the elaboration of effective strategies or even shorter-term plans, then it needs to develop deeper understanding about the societies in the area in question.[29]

---

25 DIBENEDETTO, Alessandra Giada: Projecting Stability to the South. p. 5.
26 www.thesouthernhub.org (downloaded 14 december 2020)
27 DIBENEDETTO, Alessandra Giada: Projecting Stability to the South. p. 14.
28 Ibid. p. 15.
29 Ibid. pp. 16-18.

The 2018 Brussels summit and the Package on the South

The world's leading press outlets were busy debating U.S. President, Donald J. Trump's resolute speech and his proposal about burden sharing (increment of defense spending to 4% compared to the yearly GDP),[30] but regarding our topic, the main event of the 2018 Brussels summit is the endorsement of NATO's Package on the South. It includes several political and practical recommendations, and it declared that the Alliance need to strengthen its resilience against menace emerging from the South and need to improve deterrence.[31]

Package on the South includes the need for a more robust deterrence to the South, strengthening the crisis management operations and improving the resilience against security threats, involving terrorism. Beyond these, Mediterranean Dialogue and Istanbul Cooperation Initiative need to be strengthened also. In the summit declaration it was also announced that the Hub reached its operational capacity and commenced its work. It is also written that the Hub will help the Alliance to properly handle the Southern strategic direction's challenges alongside with partner states and international organizations. The most important tools doing so are gathering, handling, sharing, assessing and analyzing information.[32]

NATO 2030

In December, 2020, the final report of a reflection group appointed by the Secretary General was published. This working group was tasked to elaborate recommendations for the Alliance. It mostly contains political recommendations and has not yet been accepted in any way, as things stand now it is just a draft for a blueprint for the next decade of the Alliance. It contains 138 recommendations, and 4 of them are about the southern strategic direction. These are:

- *'NATO must articulate a consistent, clear, coherent approach to the South, addressing both the traditional threats emanating from this region like terrorism and new risks, including the growing presence of Russia, and to a lesser extent China. The relationship between multiple frameworks and activities (Projecting Stability, Framework for the South, Defence Capacity Building, Partnerships) needs to be defined more effectively – with ownership of different portfolios clearly allocated as they are in areas such as the Eastern and Northern flanks.*
- *NATO must therefore maintain political focus on building up military preparedness and response for the Southern/Mediterranean flank, in particular by revising and delivering its Advance Plans and strengthening the Hub for the South at JFC Naples. In this context, the Mediterranean region has to remain free to Allied navigation as a prerequisite to sustaining a military effort across Alliance territory.*

---

30 SZENES, Zoltán: Transzatlanti „Super Bowl" p. 44.

31 DIBENEDETTO, Alessandra Giada: NATO's Hub and the Alliance's Engagement towards the South.

32 NATO: Brussels Summit Declaration. https://www.nato.int/cps/en/natohq/official_texts_156624.htm (downloaded 19 december 2020)

- *NATO should strengthen ties and cooperation, especially with the EU, […] [i]t should engage more with partners in the South, regional organisations, including African Union (AU), League of Arab States (LOAS), Organisation of Islamic Cooperation (OIC), Gulf Cooperation Council (GCC) and via continued out-reach out to international organisations, including the United Nations, to establish a cooperative security network across the region.*
- *NATO should increase the frequency of political consultations, including at the NAC level, on the South. Allies with specialist understandings and/or greater engagement should be asked to brief the NAC more frequently. NATO's aims, engagement and actions in the South must do more to incorporate the impact of Russian and Chinese presence, interests, and activities. In this context, NATO's Russia policy should be updated to include a Mediterranean component.'*[33]

The reflection group thinks that nowadays there are no clear distinctions between the Eastern and Southern threat, therefore a 360° approach is more likely to be effectively used. However, they underline that the challenges from the Southern direction will get more and more important in the coming decade. The document also declares that adversary activities of Russia, and to a lesser extent, China can be detected in the area, and this can undermine the security of the Alliance. This document brings some kind of strategy or at least identifies some tasks as hardly seen before. As it was mentioned before, this document cannot be viewed as an official strategy of the Alliance. In this part, Hub is not mentioned, but we can see that in the summary of the working group's thoughts about the South, once again they underline the Hub's tasks: '*The Alliance has agreed that its approach in the South includes: building the capacity of and engaging southern partners and neighbours; increasing Alliance awareness and risk monitoring; increasing Alliance resilience and responsiveness to security threatsand challenges arising from the South; working with the EU, African Union and other regional and international organisations, where relevant.'*[34]

Summary

From its creation, the Hub possesses strictly limited resources. It can be said not only about the financing, but also the manning. This situation surely did not improve as the COVID-19 struck in the end of 2019. I believe that the Hub has some serious potential, but as things stand, it is far from the peak of its capacity and capabilities. Hub can be one very important body of the Alliance in raising situational awareness about emerging threats. It also has to be said that this statement will be true only if the member states agree on allocating some more resources to this element. To reach this, the member states need to recognize the importance of the Hub as the most important element when it comes to security challenges approaching from the Southern neighbourhood. We can assume that the Southern members will promote this, as they

[33] Reflection Group op. cit. pp. 34-35.
[34] Ibid.

faced serious challenges in the middle of the last decade. The southern allies need to convince the northern and the eastern members, and maybe even the United States.[35]

Connection, consultation, coordination. This is the mission of the Hub. Indirectly, the Hub's most important role is to create a stable, secure southern neighbourhood in order to prevent these crises having an effect within the borders of the Alliance. Because of this, NATO needs to be active in defence capacity building, and even in security sector reforms. During the actions taken in accordance with Package on the South, the Alliance needs to take on a holistic approach which means it should involve military, law enforcement, and a lot of other, civilian measures to effectively counter the complexity of these challenges. To do this, the involvement of military, law enforcement, public administration experts, non-governmental organizations and local actors is a must. NATO also needs to improve its cooperation with other international organizations, firstly, but not exclusively with the European and the African Union, and it has to improve the existing efforts, like the Mediterranean Dialogue or the Istanbul Cooperation Initiative, as they had some results, but only limited. The Alliance even has to consider creating new frameworks in which Hub can provide some valuable assistance.

It is also important to note that the beforementioned strategic divergencies based on different threat perceptions do exist. While a common posture would be very important, it is very probable that on the short run, the member states' contributions will not rise due to the coming economic struggles caused by the effects of COVID-19 pandemic. And if the contributions will not grow, the Southern and Eastern strategic direction will 'compete' for resources and therefore every dollar (or euro), every man and every bit of an effort will be fought for. If the Hub will not get the resources needed, it will be nothing else than a pose. A pose for the external world (especially for the Southern neighbour states, the European and the African Union) and a pose for the southern allies miming that the Alliance do care about Southern threats. In other words: if the Hub will be only another element that consumes money and human resources in the eye of political and military leaders that brings no benefits, this prophecy will be self-fulfilling.

To sum up, the idea behind the creation of the Hub was to create an information centre that has all the relevant information about the Southern strategic direction that can serve as a forum for consultation and cooperation, where the interested players can optimize their efforts, while the unnecessary redundancies can be avoided. Whether the Hub can live up to the expectations, time will tell, but as always, it's up to the member states. If the Southern strategic direction will grow up in importance for the Alliance right next to the Eastern flank, not only in rhetorics, Hub can be a highly successful element of the Alliance, but not only for NATO's joy, but also for the states of the region.[36]

---

35 CALMELS, Christelle: NATO's 360-degree approach to security: alliance cohesion and adaptation after Crimean crisis. pp. 1-6.

36 NATO: Press conference. https://www.nato.int/cps/en/natohq/opinions_141109.htm (downloaded 08 december 2020)

Bibliography:

- ANSAMED: NATO Hub in Naples 'particularly important' – Pinotti; http://www.ansamed.info/ansamed/en/news/sections/generalnews/2017/02/15/nato-hub-in-naples-particularly-important-pinotti_61bddeb3-91c6-46d7-a549-d3dd315fe845.html (downloaded 02 november 2020)
- AVERSANO STABILE, Andrea: NATO's 70th Birthday: Family Matters at Stake. Rome, 2019, Istituto Affari Internazionali. ISSN 2280 6164
- BASAGNI, Laura – BRANDSMA, Charlotte – LESSER – Ian –LÉTÉ, Bruno: The Future of NATO's Mediterranean Dialogue – Perspectives on security, strategy and partnership; https://www.gmfus.org/publications/future-natos-mediterranean-dialogue (downloaded 29 October 2020)
- CALMELS, Christelle: NATO's 360-degree approach to security: alliance cohesion and adaptation after Crimean crisis; European Security, 2020. 29. vol. 4. pp. 416-435. ISSN 0966-2839
- DIBENEDETTO, Alessandra Giada: NATO's Hub and the Alliance's Engagement towards the South; https://cesi-italia.org/en/articoli/903/natos-hub-and-the-alliances-engagement-towards-the-south (downloaded 17 november 2020)
- DIBENEDETTO, Alessandra Giada: Projecting Stability to the South: The Role of NATO Strategic Direction – South Hub; http://cesi-italia.org/contents/Conf.Report%20Projecting%20Stability%20to%20the%20South_compressed.pdf (downloaded 16 november 2020)
- MARRONE, Alessandro: What's new on NATO's Southern flank – Security threats and the Alliance's role after the Warsaw Summit; https://www.baks.bund.de/de/node/1558 (downloaded 12 november 2020)
- MERAL, Ziya: NATO and its Southern Flank; Whitehall Papers, 2019. vol. 95. 1. pp. 81-90
- MINUTO-RIZZO, Alessandro: The 'Nebulous' Naples Hub: Is There a Strategic Direction for the South? https://www.ispionline.it/en/pubblicazione/nebulous-naples-hub-there-strategic-direction-south-20928 (downloaded 27 October 2020)
- NATO: Active Engagement, Modern Defence – Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization; https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf (downloaded 12 november 2020)
- NATO: Brussels Summit Declaration; https://www.nato.int/cps/en/natohq/official_texts_156624.htm (downloaded 19 december 2020)
- NATO: Press conference;https://www.nato.int/cps/en/natohq/opinions_141109.htm (downloaded 08 december 2020)

- NATO: The North Atlantic Treaty. Article V. https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=en (downloaded 13 August 2020)
- REFLECTION GROUP: NATO 2030: United for a New Era; https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf (downloaded 09 december 2020)
- SAMAAN Jean-Loup: Outflanked? NATO's Southern Hub and the Struggle for its Middle East Strategy. In: The International Spectator, 2018. 53. vol. 4. pp. 58-74. ISSN 0393-2729
- SGUAITAMATTI, Elisa: NATO's new Strategic Direction South Hub in Naples: Strategy and Balkan Activities. http://www.balkanalysis.com/blog/2018/01/08/natos-new-strategic-direction-south-hub-in-naples-strategy-and-balkan-activities/ (downloaded 11 december 2020)
- SZENES, Zoltán: A NATO új politikája: Stabilitás Kivetítése a Déli Régióba. Honvédségi Szemle, 2019/2. pp. 6-26. ISSN 2060-1506
- SZENES, Zoltán: Transzatlanti „Super Bowl"; Hadtudomány, 2018/3-4. pp. 43-65. ISSN 1215-4121
- TARDY, Thierry: The risks of NATO's maladaptation. In: European Security, 2020/3. pp. 275-300. ISSN 0966-2839
- www.thesouthernhub.org (downloaded 14 december 2020)

ANDRÁS NOVÁK

INTERNATIONAL PHYSICAL BARRIERS ALONG THE BALKAN MIGRATION ROUTE

Abstract

One of the most considerable migration routes was the Western Balkan corridors in 2015 according to the Frontex data. The area went through a (re) borderization process, a transformation of borders. Hungary was the first country, which started building border fences, Northern-Northern-Macedonia, Croatia and Slovenia followed this in the Balkan.
Beside the physical building operations changes were observable on the borderlands of the area's countries. Violent appearances increased towards the border-crossing people. Many people experienced physical violence or verbal abuse.
It did not manage to bring the migration crisis to an end despite the construction of the technical border locks. Pursued fugitives found themselves in another prison in the Balkan transit zones while escaping the war. The COVID-19 epidemic and the severe measures surrounding it in 2020 supplied another aggressive treatment against refugees. I analyze the details of these international technical border locks.

Keywords: borderization, Border Violence Monitoring Network, international closing of the border, migration route, Balkan area, border fence, physical abuse, verbal abuse, COVID-19, coronavirus, route, act of terrorism, exodus, border protection, not-detonating lock, migration, decree, safety closing of the border, illegal border crossing, danger, migration politics, terrorist organization, ISIS, Syrian, Afghan, Iraqi, community, right of asylum, application, technology, wire netting, keeping, building operations, transport, national defence, minister, presidents, physical obstacle, measures, electric fence, camcorder, heat camera, night-vision equipment, system, smartprocuring, minor offence, soldiers, base, migration pressure, migration crisis, electric shock, accident, immigration prohibition, refugee camp, Serbia, Northern-Macedonia, South-Hungary, Slovenia, Greece, Croatia, Central Asia, European Union, Turkey, Syria, internal political conflict, media, drones, weapon, fugitive families, Syrian conflict, geographical conditions, migrant pressure, human smuggling, crime, face recogniser system, compulsory provision, authorities, Morocco, corn patrolling, prison, United States, Mexico

In 2015, one of the most significant migratory routes was the Western Balkan Route according to Frontex's data.[1] From this year on, the area went through a process called (re)borderization due to which its borders shifted remarkably.[2] The first country to have started building a border fence was Hungary that was followed by Northern-Macedonia, Croatia and Slovenia only a few weeks later.

[1] Frontex 2020. https://frontex.europa.eu/publications/frontex-releases-risk-analysis-for-2020-vp0TZ7 (downloaded 16 November 2020)

[2] Border Violence Monitoring Network: The Balkan route – Background. 2020. https://www.borderviolence.eu/background/ (downloaded 16 November 2020)

Besides the construction of physical barriers, one could notice significant changes in the policies referring to the handling of migration on the borderlines of the countries mentioned above. As the Border Violence Monitoring Network notes, violence against migrants started to become more and more frequent. Many of them gave accounts about physical abuse, some mentioned verbal attacks, others complained about their belongings, such as their mobile phones, having been taken away from them.

With the construction of physical barriers, the migratory crisis has not been entirely resolved; instead, the migratory routes started to shift. According to the Border Violence Monitoring Network's accounts, as more barriers were built, violence was also on the rise.[3] People trying to escape war and persecution in their home countries found themselves in another trap in the Balkan transit zones. The pandemic raging through the entire world in the year of 2020 only aggravated the situation as the restrictions and rules gave way to more cruelty and aggression against the migrants already having been put into an unfortunate situation.[4] The figure below shows the main migratory routes and the barriers that were built until 2019 May in the Balkan Region.

Figure 1: The main migratory routes and barriers in the Balkan Region[5]

(Remark: In the Figure Northern-Macedonia is not indicated under her internationally recognised constitutional name.)

[3] Ibid.
[4] Ibid.
[5] Source: Ibid.

Physical barriers: definition, history and types

In the terminology of the military, obstruction of movement means the hindrance, delay or complete halt of the powers of the enemy.[6] The coordinated obstruction of movement has always played an important role in military action; however, its importance has been recently on the rise in other areas as well, such as the handling of migration. According to Dr. Kovács Zoltán, physical barriers can first and foremost be utilized for preventing terror events. Many believe physical barriers are the solution to the problem of uncontrolled mass migration.[7] With these barriers, it is possible to force migrants to only enter through controlled border checkpoints and therefore, to offer a solution to the most pressing issues in illegal migration. Additionally, with carefully devised and implemented barriers, it is not only possible to prevent unauthorized personnel from crossing the border, but also to keep illegal cargo outside one's legal territory.[8]

When defining physical barriers, we are following the work of Zoltán Kovács. In his line of work, he first goes on to explore the term 'obstacle' and 'barrier' and then uses them as the basis for the definition. As such, he defines physical barriers as *"physical materials, tools and buildings of combat that are created and utilized for military purposes and then used to destroy the enemy, halt, derail or delay its action in order to support our own groups in the destruction of the forces and tools of the enemy or to provide sufficient time for other types of activities"*.[9] Consequently, building a physical barrier can have multiple goals, one being to avert or slow down the movement of certain groups of people. It does not come with surprise then those physical barriers have become indispensable in border protection.

There are several methods for border protection. Obstruction of movement can be fulfilled by utilizing physical barriers among which we distinguish explosive and non-explosive barriers. Explosive barriers used to be popular in border protection, an example of such solution was the Iron Curtain during the Cold War. This however has become outdated mostly due to the high maintenance costs associated with such barrier. Moreover, the possibility of an explosion appeared as a constant humanitarian threat. Besides physical barriers, border protection can be enhanced by using artificial or natural obstacles.[10] Due to the rising tendency of being on the defensive against non-traditional threats, however, non-explosive barriers are gaining more and more momentum.[11]

Following military terminology, there are three major types of non-explosive barriers: barriers against military vehicles, against infantry and against descent. When further breaking down barriers against infantry, we encounter two types: electric and

---

6 VARGA, Zs. (2018a): A mozgásakadályozás lehetőségei az illegális migráció megakadályozása érdekében; Műszaki Katonai Közlöny, 2018/2. pp. 277-306.

7 KOVÁCS, Z.: A mozgásakadályozás korszerű eszközei, anyagai; Műszaki Katonai Közlöny, 2018/1.

8 Ibid.

9 KOVÁCS, Z.: A műszakizár-rendszer felépítésének lehetőségei a Magyar Honvédségben a NATO elvek és vonatkozó nemzetközi egyezmények tükrében; PhD értekezés, Budapest, 2004. p. 20.

10 VARGA (2018a) op. cit.

11 KOVÁCS (2018) op. cit.

wire barriers. Wires fences can be movable or immovable. These cannot always be used in border protection. Nonetheless, with the careful consideration of the surroundings of the area to be protected, the expected migratory pressure and the financial resources available, they can be perfectly utilized when devising a nation's border protection system.[12] Moreover, another aspect of physical barriers is gaining importance besides durability and protection: the speed of installation.[13] As for the type of the area, some type of fence is preferred on land, whereas constant patrolling is the most common way of protection on water.[14]

As we have previously alluded to it, there are two major types of obstacles: artificial and natural. One can encounter several examples in history where humankind built and used some kind of a natural obstacle. One of the first obstacles utilized by humans is the fact in itself that they attempted to choose a place of living that offered shelter and protection against the enemy. As the need for enhanced protection grew – and the potential of natural barriers capped and deteriorated – humans started to turn to artificial barriers. One of the first constructions to be called as s physical barrier can be found back in 8000 BC. The ancient city of Jericho, for example, was surrounded by a thick wall that was supposed to provide protection against any intruders.[15] Similarly, a wall was built around the Roman Empire in the first century. The wall called the limes was then expanded throughout the centuries that followed.[16] The world's longest border protection piece is the Great Wall of China. It runs on the Northern border of China and is more than 7,000 kilometers long. Its external layer is constructed from brick and stone; on the inside they used stamped mud and breakstone.[17] Building these barriers required a significant amount of resource and time.

One of the turning points in border protection was the invention of gunpowder that is often used in a complementary way with physical barriers. Such an instance was the siege of Buda in 1686 when the Turkish forces utilized well-prepared explosive and non-explosive physical barriers as part of a complicated system.[18] Later on, dugouts and other tools, such as the 'spanyolbak' became popular due to their mobility. During World War I., wire fences were especially popular as an example of non-explosive barriers. The most commonly utilized wire fences were made of easily manageable, collapsible and convertible elements.[19] Another special type of wire fence is the electric fence. Electric fences were installed by the so-called 'electrogroups'. During World War II., explosive barriers started to gain more prominence. This, however, did not mean that non-explosive or natural barriers were

12 VARGA (2018a) op. cit.
13 KOVÁCS (2018) op. cit.
14 VARGA (2018a) op. cit.
15 BAKOS, T.: A hadi mozgás- és manőverakadályozás kialakulása, fejlődése; Műszaki Katonai Közlöny, 2018/1. pp. 319-334.
16 BESENYŐ, J. Security preconditions: Understanding migratory routes; Journal of Security and Sustainability Issues, 2016. pp. 5-26. http://jssidoi.org/jssi/uploads/papers/21/Besenyo_Security_preconditions_understanding_migratory_routes.pdf (downloaded 16 November 2020)
17 VARGA, Zs. (2018b) A határvédelmi objektumok, létesítmények, eszközök fejlődésének történeti áttekintése; Műszaki Katonai Közlöny, 2018/1. pp. 287-318.
18 BAKOS (2018) op. cit.
19 Ibid.

not used at all – quite the opposite. Wire fences were still built the same way as during World War I. Additionally, the two types of barriers were often combined.

The brief historical overview above exemplifies an important point: physical barriers have been used by humanity for several thousand years. Initially, humans were reliant on natural barriers; later on, as necessities started to shift, artificial barriers started to gain momentum. Physical barriers – as we have also seen in ancient times – can be utilized for military as well as humanitarian purposes, such as the handling of migration. Both explosive and non-explosive barriers evolved remarkably during the two world wars and continue to develop in recent days.

The Southern border in Hungary

In 2015, Hungary started to build a border fence on its Southern border with the aim of shutting down its Hungarian-Serbian and Hungarian-Croatian "green border". According to the official documents of Magyar Közlöny, the measures implemented were put in place *"in order to handle the significant pressure caused by migration."*[20] The due date for the construction was set for November 30th, 2015. It is important to note that the original intention for the barrier was to serve temporarily and was built by the Hungarian Army. Due to the high construction and maintenance costs, however, some question the temporary nature of the border fence.[21]

The Hungarian fence – background and context

According to the data of Frontex, in 2015, one of the most significant migratory routes was the Western Balkan Route. An unprecedented number of migrants arrived via this route to the region with the intention of getting to Western Europe. As cruel wars and conflicts raged across some parts of the African continent and the Middle East, many left the region in hope of a better future. In 2015 alone over 764,000 illegal border crossings were registered. This number was sixteen times higher as the one in 2014.[22]

---

20 Magyar Közlöny, 2015. június 17. http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK15083.pdf (downloaded 16 November 2020)

21 BALLA J. – KUI L.: A határőrizeti célú ideiglenes biztonsági határzár és határőrizetre gyakorolt hatásai; Hadtudományi Szemle 2017/1.

22 Frontex (2020) op. cit.

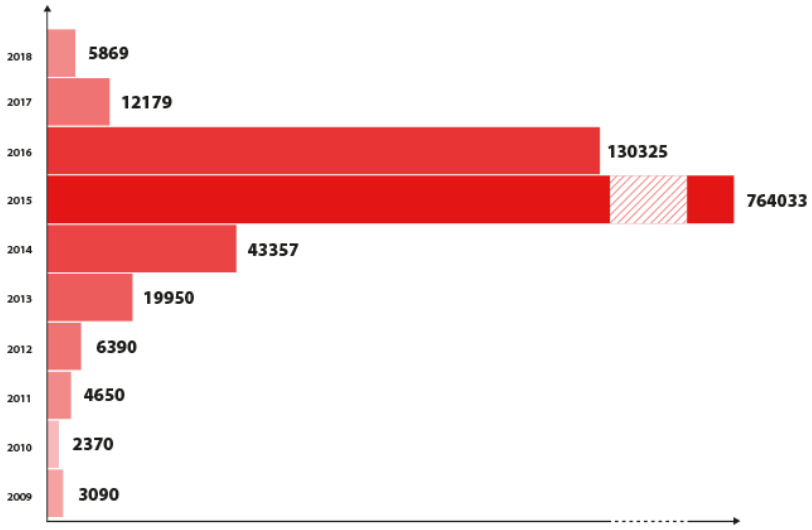

Figure 2: The number of illegal border crossings on the Western Balkan Route between 2009-2018[23]

The influx of migrants, however, brought about some concern as well. Besides refugees, many migrants arrived as well in hope of economical gains. Moreover, terrorists could also sneak into Europe as part of the migration flow.[24] Experts have attempted to raise attention to this problem on several occasions given the complexity of the issue at hand.[25] In his work János Besenyő acknowledges the importance of the migration of Muslim individuals, as they enrich cultures, but the author also warns against the frequency of people taking advantage of Europe's flexible migration policy Additionally, some organizations are sending individuals in an organized manner with malicious intent to execute unacceptable missions abroad. According to Besenyő, ISIS (Iraqi and Levant Islamic State or the Iraqi and Syrian Islamic State) poses a serious threat that should be taken very seriously. Besenyő et. al. (2016) adds that as the tools available for the spreading of information grows, the threat they pose also rises.[26] ISIS for example is knowingly utilizing the features of Twitter in order to effectively and quickly spread its messages to a wide audience.

Most of the migrants are Syrian, Afghan and Iraqi. They first reach the shores of Greece, and then proceed to Hungary or Croatia through Northern-Macedonia and Serbia. Usually, their final destination is Western Europe. Between January and June of 2015, between 100 and 1750 individuals were caught a day on average on the

---

23 Source: Frontex (2020) op. cit.

24 VARGA (2018a) op. cit.

25 BESENYŐ (2015) op. cit.

26 BESENYŐ J. – PRANTNER Z. – SPEIDL B. – VOGEL D.: Az Iszlám Állam – Terrorizmus 2.0. Történet, ideológia, propaganda; Honvéd Vezérkar Tudományos Kutatóhely, Kossuth Kiadó, Budapest, 2016. ISBN: 978-963-09-8441-6.

borders.[27] These people were detained because they illegally tried to cross the green borders. Most of these incidents occurred on the Hungarian-Serbian border. The majority of migrants, however, did not intend to settle in Hungary. As János Besenyő (2016) comments, in Hungary, there is not a well-established Islam community that could have assisted the settlement of these people. Consequently, they moved forward to Austria and Germany where they applied for asylum.[28]

Given the escalating nature of the migration crisis, mayor of a Hungarian town, László Toroczkai, was the first to propose the idea of a border fence. In his town, Ásotthalom, there were accounts that mentioned groups of migrants of about 10-30 people crossing their town all day long that is situated only 10 kilometers away from the border.[29] Eventually, the Hungarian government decided to build the Southern border fence on June 15th, 2015. The construction was based on the governmental order numbered 1401/2015. (VI. 17.) In this document, they proposed the construction of a 175-kilometer-long and 4 meters high temporary border fence.[30]

The construction of the Hungarian Southern border fence

The construction of the physical barrier – officially named the temporary security barrier for border surveillance purposes – on the Southern border of Hungary started with the construction of a 175-meter-long prototype barrier. It took place in the town of Mórahalom and was executed by the Hungarian Army. The prototype was built with the intention of experimenting with and evaluating different construction technologies. Eventually, it was decided to use 4-meter high, steel pillars based on concrete. The pillars were inserted into the ground by mechanical force, which was followed by the placement of wire fence on top. In certain areas, however, so-called NATO wire rollers were installed that became known in Hungarian as 'GYODA' being an acronym for 'gyorstelepítésű drótakadály' (quickly installed wire obstacle). During the construction of the prototype, the process of marking the territory and its cleaning from vegetation were started already.[31]

As the next phase of the construction, they started to build the primary barrier. A four-story wire roller-based system was built: three rollers were placed vertically on a concrete iron, and the fourth was placed on a Y-shaped extension cord. Even though this establishment was capable of fulfilling the primary function of the barrier – to prevent illegal migration –, the construction of the main element was still ahead. As Zsolt Varga (who also participated in the planning and devising of the border fence) discussed it in his line of work, the construction of a three-meter-high fence

---

27 https://web.archive.org/web/20150911223211/http://www.police.hu/hirek-es-informaciok/hatarinfo/elfogott-migransok-szama-lekerdezes?honap%5Bvalue%5D%5Byear%5D=2015&honap%5Bvalue%5D%5Bmonth%5D=8 (downloaded 16 November 2020)

28 BESENYŐ, J.: Not the invention of ISIS: Terrorists among immigrants; Journal of security and sustainability issues, 2015/1. pp. 5-20.

29 SERDÜLT, V.: Kerítést építene a határon Toroczkai; origo.hu, 2015.01.22. https://www.origo.hu/itthon/20150122-keritest-epitene-a-hataron-toroczkai.html (downloaded 16 November 2020)

30 Magyar Közlöny, 2015. június 17. op. cit.

31 VARGA (2018a) op. cit.

was up next. Its supporting barrels were placed 1.5 meter deep into the ground. On top, they placed a wire net.[32] According to the government order from July 31st, 2015, a 50,000 to 300,000 forint-fine (141 to 846 euros) must be paid if someone were to enter the zone of the construction area illegally, obstruct the construction process or drive an unmanned airplane into the area.[33] Later on, a need for crossing the fence emerged for several purposes, for instance for patrolling, maintenance or rescue operations. Therefore, gates were installed in the border fence at several points.[34]

Figure 3: Physical barriers on Hungary's Southern border[35]

The implementation of the border fence was split between three organizations. BN Holding Ltd. was responsible for ordering raw materials, manufacture the elements of the fence, provide tools and implement certain parts of the border fence. HM EI Ltd. ensured certain conditions were met at the site of the construction and also took part in patrolling and delivering. The third party, the Hungarian Army contributed to the preparatory phase of the construction and was responsible for the majority of the actual implementation.[36]

Eventually, a 170-kilometer-long border fence was built on the Hungarian-Serbian border. In total 21 different technical solutions were utilized in the construction. As a result, however, the migration crisis has not been resolved, but the

---

32 VARGA (2018a) op. cit.

33 Magyar Közlöny, 2015. június 17. http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK15083.pdf (downloaded 16 November 2020)

34 VARGA (2018a) op. cit.

35 Source: ZIVANOVIC, Maja: Hungarian Border 'Smart Fence' Violates Rights, Says NGO; Balkan Insight, 04 July 2017, https://balkaninsight.com/2017/07/04/hungarian-smart-fence-opposes-eu-values-ngo-says-07-04-2017-1/ (downloaded 16 november 2020)

36 BALLA – KUI (2017) op. cit.

migratory routes shifted. Several illegal border-crossing attempts were made on the Hungarian-Croatian border this time. Therefore, a need for a Hungarian-Croatian border fence emerged. The second phase of the construction of the Hungarian Southern border fence started. According to István Simicskó defense minister, the goal was to build 10-kilometer-long sections of the fence daily with the contribution of 3800 soldiers.[37] Since the Drava River functioned as a natural obstacle, there was no need to build a fence on the entirety of the borderline on the Hungarian-Croatian border.[38] In the end, a 132-long border fence was built utilizing 43 different technical solutions.[39] The construction was completed on October 16th, 2015. This date marked the day when the closure of the Hungarian Southern border was realized. The Hungarian Government spent over 12 billion forints (nearly 34 million euros) on the construction.[40]

Figure 4: Hungarian physical barriers[41]

The efficiency of the border fence and the construction of the second line of defense

According to data collected by the Hungarian police, the number of illegal migrants decreased significantly following the construction of the border fence.

37 Valasz.hu**:** Simicskó bedobta magát: napi 10 km kerítés, 3800 katona a határnál**;** 2015. http://valasz.hu/itthon/simicsko-bedobta-magat-napi-10-km-kerites-3800-katona-a-hatarnal-115007 (downloaded 16 November 2020)

38 VARGA (2018a) op. cit.

39 BALLA – KUI (2017) op. cit.

40 BARANYAI G.**:** Tizenkétmilliárd forintból épült a fizikai határzár**;** Magyar Idők**,** 2015**.** https://www.magyaridok.hu/belfold/ezzel-sikerult-megvedeni-magyarorszagot-79549/ (downloaded 16 November 2020)

41 Source: SMITH, Saphora: Go Bach to Where You Came From' retraces reverse refugee route; NBC News, 25 August 2018, https://www.nbcnews.com/news/world/go-back-where-you-came-retraces-reverse-refugee-route-n903081 (downloaded 16 november 2020)

Instead of thousands, only about a dozen cases emerged where action was necessary.[42] However, violation of the rules kept occurring. One instance happened in August of 2015, when an individual damaged the fence by cutting his way through it near the town of Ásotthalom. As a result, the government decided to strengthen the protection at the border.

On January 19th, 2016, Reuters wrote about the Hungarian government's intentions of expanding the border fence to the Hungarian-Romanian border should the migratory route shift in that direction from the Hungarian-Croatian borderline. In this article, Hungarian Minister of Foreign Affairs said: *"In case there is a need for a fence there, we will be ready for the construction the next day"*.[43]

Eventually, Hungarian Prime Minister Viktor Orbán announced in August 2016 that they were going to strengthen the border fence on the Hungarian-Serbian border. This meant that a completely new line of protection was going to be built up running alongside the one they already implemented. The newest technologies were to be used. *"As an addition to the temporary security barrier, a second line of fence is going to be built within the borderline of the country and will be equipped with an electric security system"* – said Sándor Pintér former Minister of Interior Affairs in a letter dated September 13th 2016.[44]

Figure 5: Hungarian physical barriers[45]

---

42 http://www.police.hu/hirek-es-informaciok/hatarinfo/elfogott-migransok-szama-lekerdezes 2020. november 14. (Downloaded 16 November 2020)

43 THAN, K. – PAWLAK, J.: Hungary ready to erect anti-migrant fence on Romanian border; Reuters, 2016. https://uk.reuters.com/article/us-europe-migrants-hungary-minister-idUKKCN0UX284 (downloaded 16 November 2020)

44 Parlament.hu: Pintér Sándor levele. 2020. https://www.parlament.hu/irom40/11844/11844-0001.pdf (downloaded 16 November 2020)

45 BBC News: Hungary MEP suggests using pig heads to deter refugees; https://www.bbc.com/news/world-europe-37158330 (downloaded 16 november 2020)

As part of the second line of defense, modern technologies, such as thermographic cameras, night vision systems, spotlights and video cameras were included. This new, strengthened system could not be easily damaged for example by cutting.[46] In the intelligent system, there is 900-voltage running that is not dangerous for humans. It is, however, capable of sending an immediate signal to the center in case an illegal attempt to cross or destroy the fence is noticed.[47] In his work, Varga[48] (2018) details what exactly was built into the intelligent alarm system:

- a cable running in the fence that is equipped with sensors on every 10-15 centimeters;
- 111 thermographic – and 297 motion sensor cameras equipped with laser;
- high-power spotlights for nocturnal activities;
- a communication system;
- an acoustic alarm system equipped with speakers on every 300 meters.

The smart fence is capable of immediately noticing intrusion and notifying the respective centers. (Mórahalom or Bácsbokod). Moreover, when a violation occurs, the spotlights turn on and the acoustic system warns the intruder in multiple languages. (English, Serbian, Arabic, Farsi, Urdu). In the meantime, individuals on patrol duty can monitor the events through the cameras attached to the system that can move in multiple directions. The person on patrol duty closest to the location is notified through radio and can arrive on the spot within a few minutes.[49]

As these areas of border surveillance tend to be located at quite distant locations, a need for community bases emerged. These buildings are not only convenient for the personnel on duty, but is also ensures that quick action can be taken as well as smooth transportation.

---

46 Magyar Idők: Bakondi György: erősebb kerítés épül a déli határon; 2017. https://www.magyaridok.hu/belfold/bakondi-gyorgy-erosebb-kerites-epul-deli-hataron-1346074/ (downloaded 16 November 2020)

47 Delmagyar.hu: Áram alá kerül az okoskerítés, üzemelhet az intelligens jelzőrendszer a magyar-szerb határon; 2017. https://www.delmagyar.hu/szeged-es-kornyeke/aram-ala-kerul-az-okoskerites-uzemelhet-az-intelligens-jelzorendszer-a-magyar-szerb-hataron-1299955/ (downloaded 16 November 2020)

48 VARGA (2018a) op. cit.

49 Ibid.

Figure 6: The community base on the Hungarian Southern border[50]

The exact amounts of money spent on the construction of the Hungarian Southern border is not known, however, the total costs in 2015 could have been over 84 billion forints and over a 100 billion in 2016.[51] The construction of the second line of defense in 2017 could have meant an additional few billion forints. Taking all these information into account, Balla and Kui (2017) notes that the border fence cannot be considered temporary. In reality, a permanent system was carefully devised and later implemented.

The most important pieces of information about the Hungarian border fence:

- a 170-kilometer-long fence was built on the Hungarian-Serbian border, out of which 122,6 kilometers shut the border completely and the remaining 47,4 kilometers were realized using specific solutions that accounted for the special geographical conditions
- a 132-kilometer-long fence was built on the Hungarian-Croatian border, out of which 105,5 kilometers shut the border completely, the remaining 26,2 kilometers was realized with other technical solutions

---

[50] Source: SZÉKELY, Tamás: Hungary Builds Four New Soldier Barrack to Strengthen Border Protection in The South; Hungary today, 21 March 2017

[51] BALLA – KUI (2017) op. cit.

- on all border crossing points (Röszke-I., Röszke-II., Ásotthalom, Bácsalmás, Hercegszántó, Udvar, Beremend, Drávaszabolcs, Barcs, Berzence, Letenye-I., Letenye-II.), they were prepared to shut the borders with mobile obstacles if necessary.[52]

International examples of physical barriers

The borderline between Greece and Turkey

Greek authorities decided to shut their border with Turkey in the year of 2012. A 10.5-kilometer-long border fence was constructed with the purpose of handling the intensifying migratory flow.[53] Later this year, a 4-meter-high fence of six elements was built in two rows with a concrete base. One of them runs on the borderline directly and the other one on the Greek side.

Figure 7: Refugees on the Greek - North-Macedonian border[54]

Besides the construction of the physical barrier on the border, Greek authorities paid special attention to enhanced patrolling. As a result, the number of illegal migrants arriving into the country decreased significantly. At the same time, it is important to note that a phenomenon commonly occurring at other borders could be detected here as well: instead of stopping the migratory flow, the fence shifted the

52 VARGA (2018a) op. cit.

53 BESENYŐ, J.: Fences and Border Protection: The Question of Establishing Technical Barriers in Europe; Academic and Applied Research in Military and Public Management Science, 2017/1. pp. 77-87.

54 PÁLFI, Rita: Európai Bizottság: az EU nem bukhat meg kétszer; Euronews, 05 March 2020, https://hu.euronews.com/2020/03/04/europai-bizottsag-az-eu-nem-bukhat-meg-ketszer (downloaded 16 november 2020)

route to another direction. Instead of the Greece-Turkey border, some of the migrants started to attempt border crossings at the Bulgarian-Turkish border.[55]

The borderline between Bulgaria and Turkey

The number of migrants arriving to Bulgaria skyrocketed from 2012 to 2013. According to estimates, the figures were ten times higher than the in the previous year.[56] The majority of migrants arrived from Syria. Consequently, the government decided to build a border fence on Bulgaria's Southeastern border. The plan was to build a 166-kilometer-long physical barrier, out of which 33 kilometers were realized by 2015 and another 100 kilometers by 2016. In terms of the technical parameters, the fence was 3 meters high and had been equipped with a camera system. The wire fence lies in a concrete base and was mostly financially supported by EUROSUR (European Border Surveillance System).[57]

Figure 8: Bulgaria built a fence at the Greek border[58]

According to data obtained by Frontex, the number of illegal migrants went down by 84% from 2015 to 2016. It is also important to point out that the construction of the border fence was not the only factor that had contributed to this change in migration. Besides building a fence, special attention was given to the appropriate allocation and deployment of human resources. In other words, more than 1500 military personnel were ordered for service at the border. Additionally, Bulgarian authorities strengthened collaboration with Turkish organizations. Having approached the issue from various angles, the results discussed above were achieved.

---

55 Ibid.
56 Ibid.
57 Ibid.
58 GAFFEY, Conor: Bulgaria Ready to Stend 1,000 Troops to Secure Turkish Border; 18 September 2015, https://www.newsweek.com/bulgaria-ready-send-1000-troops-secure-turkish-border-373755 (downloaded 16 november 2020)

The borderline between Greece and Northern-Macedonia

The borderline running between Greece and Northern-Macedonia was also affected by the migration crisis of 2015. Due to the intensifying migratory flow, Northern-Macedonia ordered enhanced border surveillance in November 2015. The Northern-Macedonian military was responsible for the majority of the construction work. According to The Guardian, some of the military personnel were attacked by migrants during the initial phase of the construction. The article went on to discuss the possible underlying reasons why this event took place and concluded that an electrical accident suffered by a Moroccan man while travelling on top of a train might have contributed to the escalating emotions.[59]

Figure 9: North-Macedonian patrol on duty at the Greek border (near Idomeni)[60]

On top of the construction work, border surveillance measures were also implemented. These introduced a migration ban on Afghan, Pakistani, Iranian and African migrants. Moreover, immigration rules were tightened for Syrian and Iraqi immigrants. These measures, however, resulted in a chaotic and heavily frustrated situation: several thousand migrants were trapped in migration camps. In a few weeks, Europe's biggest refugee camp was born where chaos and exasperation took over.[61] The situation was not resolved until May 2016 when over 8,500 refugees were released. In the meantime, the construction of a second line of border fence started on the Greek - Northern-Macedonian border. The intention was to come up with a long-term solution for the migration crisis.[62]

---

59 The Guardian: Migrants attack Northern-Macedonian police as construction of Greek border fence begins; 2015. https://www.theguardian.com/world/2015/nov/29/migrants-attack-macedonian-police-as-construction-of-greek-border-fence-begins (downloaded 16 November 2020)

60 BBC News: Second fence under construction at North-Macedonia - Greece border; 12 February 2016, https://www.bbc.com/news/av/world-europe-35564444 (downloaded 16 November 2020)

61 Ibid.

62 Ibid.

Figure 10: North-Macedonian police officers on duty at the Greek border (near Idomeni)[63]

The borderline between Slovenia and Croatia

Following the construction of the physical barrier on Hungary's Southern border, other countries started to experience heavier migration into their territories. As migratory routes shifted, more and more migrants appeared in countries like Slovenia and Croatia. By November 2015, the construction of a wire fence was underway and was successfully completed by the promised deadline.

Figure 11: Workers build a fence in Slovenia near the River Kolpa in August 2019[64]

---

63 ALOIS B.: Rite&Reason: Using to stop migration is pointless; The Irish Times, 12 April 2016, https://www.irishtimes.com/opinion/rite-reason-using-fences-to-stop-migration-is-pointless-1.2606416 (downloaded 16 november 2020)

64 Reuters: Slovenia erects more border fence to curb migrant inflow. 2019. https://fr.reuters.com/article/instant-article/idUSKCN1VC19Q (downloaded 16 November 2020)

A few years later, construction was underway once again on the Slovenian-Croatian border. According to Reuters (2019), the number of migrants rose significantly from the year of 2018 to 2019, by 56% respectively.[65] As a result, the Slovenian government entered into a contract with a Serbian company to build a 40-kilometer-long border fence.

The border fence is approximately 2.5 meters high and runs along the Kolpa River – a natural barrier on the borderline of the two countries. In an interview the spokesperson of the Slovenian Ministry of Interior said that the border fence was to be constructed temporarily in order to lessen illegal migration and to ensure the safety of their citizens.[66]

Since 2015, a physical barrier was put in place on 196 kilometers in total on the Slovenian-Croatian border. In 2020, the Slovenian government announced they would strengthen their border surveillance. Once again, they cited the rising number of illegal border crossings as the underlying reason for the construction and talked about the fence as a temporarily solution.[67] According to their plans, a 40-kilometer-long section is going to be added to the already existing barrier. Among the information disclosed in April, however, there was no mention regarding the exact location of this new border fence.

Figure 12: Border fence on the Slovenian-Croatian border[68]

65 Ibid.
66 Ibid.
67 Infomigrants: Slovenia to erect more fences along Croatia border to curb illegal crossings. 2020a. https://www.infomigrants.net/en/post/24123/slovenia-to-erect-more-fences-along-croatia-border-to-curb-illegal-crossings (downloaded 16 November 2020)
68 Ibid.

The borderline between Serbia and Northern-Macedonia

In May 2020, the media wrote about the wire fence that was started to be built on the borderline of Serbia and Northern-Macedonia. A few months prior to the beginning of the construction, migration on the Balkan Route – from the Middle East and Middle Asia to Europe – rose significantly. In an interview a Serbian politician said, *"we believe the fence is going to provide further protection for non-EU countries against the influx of migrants that can become massive again on the Balkan Route"*. The mayor added that the construction of the border fence is part of a deal with the European Union.[69]

A couple of months later, the spokesperson of the European Union denied the existence of such deal and added that despite the significant amounts of financial aid provided by the EU for the handling of migration in the Western Balkan Region, this money does not support the construction of any kind of border fence.[70]

Figure 13: Fense between Turkey and Syria[71]

The borderline between Turkey and Syria

The border between Turkey and Syria is somewhat over 900 kilometers long. Since 2011, internal armed conflicts have been constant in Syria. As a result of the civil war, people have been leaving the country in hope of a better future. In order to

---

69 Infomigrants: Serbia building barbed-wire border fence, media reports. 2020b. https://www.infomigrants.net/en/post/26791/serbia-building-barbed-wire-border-fence-media-reports (downloaded 16 November 2020)

70 Meta.mk: EU: Building wire fence on border between Northern-Macedonia and Serbia not part of the agreement with Serbia. 2020. https://meta.mk/en/eu-building-wire-fence-on-border-between-macedonia-and-serbia-not-part-of-the-agreement-with-serbia/ (downloaded 16 November 2020)

71 India Blooms: World in Photos: Aug. 20, 2020, https://www.indiablooms.com/photos-details/W/5725/world-in-photos-aug-20-2020.html (downloaded 16 november 2020)

control this process, construction of a border fence began in 2015 that was supposed to be implemented on the entirety of the border. It was announced by the media in the spring of 2018 that a 764-kilometer-long section has been completed.[72] Part of it, 564 kilometers, was built by a company named TOKI that is supported by the Turkish State. Another 200 kilometers was financed by Turkish governorates. With the completion of this physical barrier of over 750 kilometers, the Turkish-Syrian border fence has become the third longest in the world with the Great Wall of China being the first and the American-Mexican border fence the second.[73]

In this system of physical barrier, various physical elements have been implemented, such as concrete walls, patrolling roads and surveillance towers. The concrete walls are 2 meters wide and 3 meters tall. On top, a 1-meter-high wire fence was placed.[74] Additionally, the wall has been equipped with smart solutions. For instance, thermographic cameras, remotely controllable arms system, drone surveillance systems and light systems with sensors.

Figure 14: The wall between Turkey and Syria near the city of Gaziantep[75]

Due to the construction of this large-scale physical barrier, several families trying to escape from their own homes find themselves trapped in refugee camps at the border. Some of them are forced to find alternative solutions. As it has been said

---

72 NationalNews: Syria-Turkey border wall completed. 2018. https://www.thenationalnews.com/world/mena/syria-turkey-border-wall-completed-1.738637 (downloaded 16 November 2020)

73 Hürriyet Daily News: Turkey-Syria border wall to be completed by spring; 2017. https://www.hurriyetdailynews.com/turkey-syria-border-wall-to-be-completed-by-spring-124303 (downloaded 16 November 2020)

74 Daily Sabah: Turkey finishes construction of 764-km security wall on Syria border; 2018. https://www.dailysabah.com/war-on-terror/2018/06/09/turkey-finishes-construction-of-764-km-security-wall-on-syria-border (downloaded 16 November 2020)

75 KOCH Alex: US officials meet Turkish counterparts on potential safe passage in northern Syria; Foreign Brief, 5 August 2019, https://www.foreignbrief.com/daily-news/us-officials-meet-turkish-counterparts-on-potential-safe-passage-in-northern-syria/ (downloaded 16 November 2020)

in an article by Reuters, the border wall has become a type of symbol for the people on the run. There are some that seek shelter nearby the wall instead of the refugee camps. There, they build their own safe spaces. Their only concern is about the time when the war reaches the border area. Then, they say, they have no idea where to go.[76]

The borderline between Spain and Morocco

The main migratory route within the area went through the desert in North Africa towards the enclaves of Ceuta and Melilla, two Spanish enclaves on Moroccan territory.[77] These two cities have been under migratory pressure since the 1990s.[78] Both territories are of strategic importance, under Spanish rule, located on Africa's Northern shore.[79] Due to their geographical positions, they belong to a route preferred by migrants over the more dangerous route to Europe via the Mediterranean Sea. The Spanish government in alliance with the Moroccan authorities and other African countries has made several attempts – sometimes quite cruel – to halt migration on this route. One of these attempts included the construction of a large-scale radar- and fence system.[80]

In 1993, Ceuta built an 8.2 kilometer-long and 3 meters high border fence. Additional construction began two years later: the fence was extended to 6 meters high.[81] Moreover, a road with surveillance towers was built alongside the fence for patrolling purposes.[82] Akin to the phenomenon that occurred on Hungary's Southern border, migrants started to use a different route: this time towards the town of Melilla. As a result, a 12-kilometer-long border fence was built there. The physical closure of the Southern border of the European Union was fulfilled.[83] Given the strong migratory pressure, it was decided to build a fence of 3 rows (there is a 3-meters-high one in between two fences of 6 meters).[84] Approximately, construction cost 60 million euros. The country with the most border surveillance expenditures between 2007 and 2010 was Spain among the countries of the European Union. It spent 120 million euros during this time frame.

---

76 Reuters: For Syrians fleeing Idlib, Turkish border wall becomes symbol of their plight. 2020. https://www.reuters.com/article/us-syria-security-wall-idUSKCN20K2MQ (downloaded 16 November 2020)

77 BESENYŐ, J.: Nyugat-Szahara és a migráció; Afrika tanulmányok, 2011/3. pp. 34-45.

78 BESENYŐ (2017) op. cit.

79 VARGA (2018a) op. cit.

80 BESENYŐ (2011) op. cit.

81 BESENYŐ (2017) op. cit.

82 VARGA (2018a) op. cit.

83 BESENYŐ (2017) op. cit.

84 VARGA (2018a) op. cit.

Figure 15: Spanish police are using a crane to help illegal immigrants (2019-09-02)[85]

During the 2014-15-migration crisis, Ceuta and Melilla – similarly to other countries – have often experienced instances of illegal border crossing. What is more, human trafficking and other illegal activities were being reported, as well.[86] In December 2019, news came according to which the Spanish government was going to renovate the physical borders at Ceuta and Melilla. They were going to dismantle the existing system and build face recognition technology into the new one.[87] There were more than 32 million euros allocated for the project that had the purpose of holding back illegal migration.

Additionally, Spain introduced several new rules and regulations: patrolling in cooperation with the Moroccan authorities, strengthened maritime patrolling at Gibraltar and the imprisonment of migrants.[88]

The borderline between the United States and Mexico

One of the most controversial and talked-about aspects of American politics is the issue of migration with a special attention to the Mexican-US borderline. There is a 3200-kilometer-long borderline in between the two countries with two natural barriers: the Colorado and the Rio Grande Rivers. Moreover, the area is scattered with deserts, sand dunes and hills that further serve as factors hindering physical movement in the area. In case of the American-Mexican borderline, it is important to note that it

---

85 MACGREGOR, Marion: Spain: Migrants hide among toxic ash and broken glass in attempt to reach mainland; 23 February 2021, https://www.infomigrants.net/fr/post/30427/spain-migrants-hide-among-toxic-ash-and-broken-glass-in-attempt-to-reach-mainland (downloaded 16 March 2021)

86 BESENYŐ (2017) op. cit.

87 GUESSOUS, H.: Spain Modernizes Security Fences at Ceuta, Melilla borders; 2019. https://www.moroccoworldnews.com/2019/12/288197/spain-fences-ceuta-melilla-borders/ (downloaded 16 November 2020)

88 BESENYŐ (2011) op. cit.

not only functions as a crossing point for humans, but it is also a significant place of trade in between the two nations. A recurring problem is the trade of illegal products, such as drugs.[89] Nonetheless, illegal migration remains the greatest issue, which is mostly due to the low standard of living and the rising population in Mexico.

The construction of the physical barrier of the area started in 2006. Various fence systems were implemented on the third of the entire borderline. In total the border fence stretches 1100 kilometers long on the American-Mexican borderline. Construction was finished between the areas of California and Arizona in 2010. Then, they continued in Texas. In his campaign in 2016, president Donald Trump promised to build a border fence on the entirety of the border in case he is elected. Even though this promise was never fulfilled, a significant part of the physical barrier was rebuilt and another 32 kilometers were added during his presidency.

After careful consideration of the geographical conditions of the area mentioned above, the fence was constructed using several different solutions. They implemented steel pillars based in concrete and covered it with metal in the desert areas.[90] As the area is also scattered with sand dunes, they also had to implement clever solution: they invented a so-called "moving fence" that was able to follow the movement of the sand dunes.

The border fence is 3 meters high on average and is equipped with smart solutions, such as thermographic cameras and underground sensors. At certain intervals, the fence was built in two or three rows for further security. The main goal of the construction of the American-Mexican physical barrier was to halt illegal drug trafficking and handle the enormous migratory flow.

Figure 16: The American-Mexican border fence in August 2019[91]

89 VARGA (2018a) op. cit.
90 Ibid.
91 SPAGAT, Elliot: Homeland Security to repair damage created by border wall; PBSO News Hour, 30 April 2021

Bibliography:

- 213/2015. (VII. 31.) Korm. rendelet a határőrizeti célú ideiglenes biztonsági határzár építésén dolgozók védelméről, továbbá az államhatárról szóló törvény szerinti közérdekű használati joggal összefüggő kártalanításról szóló 211/2015. (VII. 23.) Korm. rendelet módosításáról – Magyar Közlöny 2015. 112. szám, 2015. július 31.
- A rendkívüli bevándorlási nyomás kezelése érdekében szükséges egyes intézkedésekről szóló 1401/2015. (VI. 17.) Korm. határozat, Magyar Közlöny 83. szám.
- ALOIS B.: Rite&Reason: Using to stop migration is pointless; The Irish Times, 12 April 2016, https://www.irishtimes.com/opinion/rite-reason-using-fences-to-stop-migration-is-pointless-1.2606416 (downloaded 16 november 2020)
- BAKOS, T.: A hadi mozgás- és manőverakadályozás kialakulása, fejlődése; Műszaki Katonai Közlöny, 2018/1. pp. 319-334.
- BALLA J. – KUI L.: A határőrizeti célú ideiglenes biztonsági határzár és határőrizetre gyakorolt hatásai; Hadtudományi Szemle 2017/1.
- BARANYAI G.: Tizenkétmilliárd forintból épült a fizikai határzár; Magyar Idők, 2015. https://www.magyaridok.hu/belfold/ezzel-sikerult-megvedeni-magyarorszagot-79549/ (downloaded 16 November 2020)
- BBC News: Hungary MEP suggests using pig heads to deter refugees; https://www.bbc.com/news/world-europe-37158330 (downloaded 16 november 2020)
- BESENYŐ, J.: Nyugat-Szahara és a migráció; Afrika tanulmányok, 2011/3. pp. 34-45.
- BESENYŐ, J.: Not the invention of ISIS: Terrorists among immigrants; Journal of security and sustainability issues, 2015/1. pp. 5-20.
- BESENYŐ, J. Security preconditions: Understanding migratory routes; Journal of Security and Sustainability Issues, 2016. pp. 5-26. http://jssidoi.org/jssi/uploads/papers/21/Besenyo_Security_preconditions_understanding_migratory_routes.pdf (downloaded 16 November 2020)
- BESENYŐ J. – PRANTNER Z. – SPEIDL B. – VOGEL D.: Az Iszlám Állam – Terrorizmus 2.0. Történet, ideológia, propaganda; Honvéd Vezérkar Tudományos Kutatóhely, Kossuth Kiadó, Budapest, 2016. ISBN: 978-963-09-8441-6.
- BESENYŐ, J.: Fences and Border Protection: The Question of Establishing Technical Barriers in Europe; Academic and Applied Research in Military and Public Management Science, 2017/1. pp. 77-87.
- Border Violence Monitoring Network: The Balkan route – Background. 2020. https://www.borderviolence.eu/background/ (downloaded 16 November 2020)

- Daily Sabah: Turkey finishes construction of 764-km security wall on Syria border; 2018. https://www.dailysabah.com/war-on-terror/2018/06/09/turkey-finishes-construction-of-764-km-security-wall-on-syria-border (downloaded 16 November 2020)
- Delmagyar.hu: Áram alá kerül az okoskerítés, üzemelhet az intelligens jelzőrendszer a magyar-szerb határon; 2017. https://www.delmagyar.hu/szeged-es-kornyeke/aram-ala-kerul-az-okoskerites-uzemelhet-az-intelligens-jelzorendszer-a-magyar-szerb-hataron-1299955/ (downloaded 16 November 2020)
- Frontex 2020. https://frontex.europa.eu/publications/frontex-releases-risk-analysis-for-2020-vp0TZ7 (downloaded 16 November 2020)
- GAFFEY, Conor: Bulgaria Ready to Stend 1,000 Troops to Secure Turkish Border; 18 September 2015, https://www.newsweek.com/bulgaria-ready-send-1000-troops-secure-turkish-border-373755 (downloaded 16 november 2020)
- GUESSOUS, H.: Spain Modernizes Security Fences at Ceuta, Melilla borders; 2019. https://www.moroccoworldnews.com/2019/12/288197/spain-fences-ceuta-melilla-borders/ (downloaded 16 November 2020)
- https://2015-2019.kormany.hu/hu/honvedelmi-miniszterium/fotok/elkeszultek-a-hatarvedelmi-bazisok (downloaded 16 November 2020)
- http://www.police.hu/hirek-es-informaciok/hatarinfo/elfogott-migransok-szama-lekerdezes 2020. november 14. (Downloaded 16 November 2020)
- https://web.archive.org/web/20150911223211/http://www.police.hu/hirek-es-informaciok/hatarinfo/elfogott-migransok-szama-lekerdezes?honap%5Bvalue%5D%5Byear%5D=2015&honap%5Bvalue%5D%5Bmonth%5D=8 (downloaded 16 November 2020)
- Hürriyet Daily News: Turkey-Syria border wall to be completed by spring; 2017. https://www.hurriyetdailynews.com/turkey-syria-border-wall-to-be-completed-by-spring-124303 (downloaded 16 November 2020)
- India Blooms: World in Photos: Aug. 20, 2020, https://www.indiablooms.com/photos-details/W/5725/world-in-photos-aug-20-2020.html (downloaded 16 november 2020)
- Infomigrants: Slovenia to erect more fences along Croatia border to curb illegal crossings. 2020. https://www.infomigrants.net/en/post/24123/slovenia-to-erect-more-fences-along-croatia-border-to-curb-illegal-crossings (downloaded 16 November 2020)
- Infomigrants: Serbia building barbed-wire border fence, media reports. 2020. https://www.infomigrants.net/en/post/26791/serbia-building-barbed-wire-border-fence-media-reports (downloaded 16 November 2020)
- KOCH Alex: US officials meet Turkish counterparts on potential safe passage in northern Syria; Foreign Brief, 5 August 2019, https://www.foreignbrief.com/daily-news/us-officials-meet-turkish-counterparts-on-potential-safe-passage-in-northern-syria/ (downloaded 16 November 2020)

- KOVÁCS, Z.: A műszakizár-rendszer felépítésének lehetőségei a Magyar Honvédségben a NATO elvek és vonatkozó nemzetközi egyezmények tükrében; PhD értekezés, Budapest, 2004. p. 20.
- KOVÁCS, Z.: A mozgásakadályozás korszerű eszközei, anyagai; Műszaki Katonai Közlöny, 2018/1.
- MACGREGOR, Marion: Spain: Migrants hide among toxic ash and broken glass in attempt to reach mainland; 23 February 2021, https://www.infomigrants.net/fr/post/30427/spain-migrants-hide-among-toxic-ash-and-broken-glass-in-attempt-to-reach-mainland (downloaded 16 March 2021)
- Magyar Idők: Bakondi György: erősebb kerítés épül a déli határon; 2017. https://www.magyaridok.hu/belfold/bakondi-gyorgy-erosebb-kerites-epul-deli-hataron-1346074/ (downloaded 16 November 2020)
- Magyar Közlöny, 2015. június 17. http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK15083.pdf (downloaded 16 November 2020)
- Meta.mk: EU: Building wire fence on border between Macedonia and Serbia not part of the agreement with Serbia. 2020. https://meta.mk/en/eu-building-wire-fence-on-border-between-macedonia-and-serbia-not-part-of-the-agreement-with-serbia/ (downloaded 16 November 2020)
- National News: Syria-Turkey border wall completed. 2018. https://www.thenationalnews.com/world/mena/syria-turkey-border-wall-completed-1.738637 (downloaded 16 November 2020)
- PÁLFI, Rita: Európai Bizottság: az EU nem bukhat meg kétszer; Euronews, 05 March 2020, https://hu.euronews.com/2020/03/04/europai-bizottsag-az-eu-nem-bukhat-meg-ketszer (downloaded 16 november 2020)
- Parlament.hu: Pintér Sándor levele. 2020. https://www.parlament.hu/irom40/11844/11844-0001.pdf (downloaded 16 November 2020)
- Reuters: Slovenia erects more border fence to curb migrant inflow. 2019. https://fr.reuters.com/article/instant-article/idUSKCN1VC19Q (downloaded 16 November 2020)
- Reuters: For Syrians fleeing Idlib, Turkish border wall becomes symbol of their plight. 2020. https://www.reuters.com/article/us-syria-security-wall-idUSKCN20K2MQ (downloaded 16 November 2020)
- SMITH, Saphora: Go Bach to Where You Came From' retraces reverse refugee route; NBC News, 25 August 2018, https://www.nbcnews.com/news/world/go-back-where-you-came-retraces-reverse-refugee-route-n903081 (downloaded 16 november 2020)
- SERDÜLT, V. Kerítést építene a határon Toroczkai; 2015. https://www.origo.hu/itthon/20150122-keritest-epitene-a-hataron-toroczkai.html (downloaded 16 November 2020)

- SPAGAT, Elliot: Homeland Security to repair damage created by border wall; PBSO News Hour, 30 April 2021
- SZÉKELY, Tamás: Hungary Builds Four New Soldier Barrack to Strengthen Border Protection in The South; Hungary today, 21 March 2017
- THAN, K. – PAWLAK, J.: Hungary ready to erect anti-migrant fence on Romanian border; Reuters, 2016. https://uk.reuters.com/article/us-europe-migrants-hungary-minister-idUKKCN0UX284 (downloaded 16 November 2020)
- The Guardian: Migrants attack Macedonian police as construction of Greek border fence begins; 2015. https://www.theguardian.com/world/2015/nov/29/migrants-attack-macedonian-police-as-construction-of-greek-border-fence-begins (downloaded 16 November 2020)
- Valasz.hu: Simicskó bedobta magát: napi 10 km kerítés, 3800 katona a határnál; 2015. http://valasz.hu/itthon/simicsko-bedobta-magat-napi-10-km-kerites-3800-katona-a-hatarnal-115007 (downloaded 16 November 2020)
- VARGA, Zs.: A mozgásakadályozás lehetőségei az illegális migráció megakadályozása érdekében; Műszaki Katonai Közlöny, 2018/2. pp. 277-306.
- VARGA, Zs.: A határvédelmi objektumok, létesítmények, eszközök fejlődésének történeti áttekintése; Műszaki Katonai Közlöny, 2018/1. pp. 287-318.
- ZIVANOVIC, Maja: Hungarian Border 'Smart Fence' Violates Rights, Says NGO; Balkan Insight, 04 July 2017, https://balkaninsight.com/2017/07/04/hungarian-smart-fence-opposes-eu-values-ngo-says-07-04-2017-1/ (downloaded 16 november 2020)

ÖMER AKYÜZ

TURKEY'S EUROPEAN UNION MEMBERSHIPS: DEVELOPMENTS, BENEFITS AND DRAWBACKS FOR BOTH SIDES

Abstract

Study has been conducted in order to assess "sui generis" European Union membership process of Turkey that officially started with Association Agreement in 1963. Beside the historical array of the events, I have intended to examine the nature of the relationships and the impediments multidimensionally based on political and economic aspects. I have begun to put in order historical developments dating back to the Migration of Tribes (B.C.375) and Ottoman State era (1299-1918) in the study in order to touch upon to the depth of relationship between Europe and Turkish nation. However, I have continued with 20th century developments like First World War, Second World War, the evolution of European Union, foundation of the Republic of Turkey under Mustafa Kemal Atatürk on 29 October 1923 based on Western democracy and the continuing prominent developments reaching our time. In addition, I have classified the hot topics that were seen as the most important obstacle in front of the membership from both sides. Hence, I have tried to assess the process of Turkish membership of European Union objectively, calculating the benefits and drawbacks of probable membership of Turkey for both of the actors. Since Turkey's European Union membership process is a mysterious, attracting, rich topic and my intention was to shed a light on the topic by projecting both European and Turkish point of view in this study.

***Keywords*:** membership, policies, obstacle, history, Turkey, negotiations, European Union

Introduction

The evolution of the European Union as a supranational regional organisation and the relations between the EU and Turkey have long been an attention catching issue on the agenda of the world. The next steps and decisions the EU and Turkey will take on their partnership, will play a crucial role in the power of both the EU and Turkey in acting on the world stage. Their approaches to each other will be determinant in building a constructive relationship.

In my paper, I am going to give the historical background of Turkish-European relationships and Turkey-EU relationship as well to show how bounded two actors are. Hence, I am going to discuss the hot topics to be considered as an obstacle to Turkey's EU membership originating from both the European Union and Turkey sides. Moreover, I will take into account the benefits and drawbacks of being member of the European Union both for my home country and the EU itself. The hot topics and arguments are scientific; however, the paper also includes my point of view subjectively which is between social constructivism and realism.

1. EU-Turkey Relations: History and Developments

The current relationship between the EU and Turkey can be understood better through understanding the heritage of historical ties and developments between Turkey and Europe as a whole. This relationship in the history dates back to migration of tribes around 375-500 B.Sc. with the migration of various societies towards Europe which basically shapes todays European mosaic as a result of Hunnic Turks which divided Roman Empire into two parts as western and eastern. Nevertheless, the real communication and interaction starts with the Turkish influx into the Anatolia around the middle of eleventh century reached its momentum with the rise of Ottoman Empire through lands conquered until the doors of Vienna. However, although being a member of Concert of Europe, the Ottoman Empire turned out to be named as "the Sick man of Europe" due to various internal and external reasons like overseas explorations, enlightenment and scientific improvement, strengthening of European states and backwardness, religious control and veto on scientific researches, bad governance in ruling ground in the inside started falling since mid-eighteenth century while European states increased their power vigorously which will prevent the rivals to catch up with them easily in long term. Thus, in the WW1 Ottoman Empire has collapsed as a result of defeat against the entente powers in his alliance with Germany, Austria-Hungary in 1918. Resulted with the victory, Turkish Independence War, had taken place against Triple Entente and Greece between 1919-1922 under the leadership of Mustafa Kemal Atatürk provided the foundation of Turkish Republic starting from 23 April 1920 with the opening of Turkish Grand National Assembly under Western-oriented democratic principles. On the other hand, Europe had faced a huge internal turmoil due to Great Depression, dictatorships and revisionist ambitions under Hitler and Mussolini until the end of WW2 (1939-1945) which was the bloodiest war due to the technological improvements which left traumas in the mind of humanity like holocaust and nuclear bomb against Japan.

Turkish ruling elite lead by İsmet İnönü had put a great deal of effort to stay away from this war and resist both ideological pressures of Russia and fascist oppression of Germany and Italy and invitations from other side mainly by Winston Churchill. As the War resulted with the victory of USA, UK, Russia, France, ended the fascist regimes and turned the global system into a bipolar one pioneered by Russia and the USA. After the war ended, the United Nations were founded on 24 October 1945 instead of failing League of Nations and on 4 April 1949 North Atlantic Treaty Organization has been founded under the leadership of USA in order to realise the containment policy against Russia. On the other hand, Turkey had passed to the multi-party system in the end of 1940s as the commitment in its constitution envisaged although she has been founded as a Republic in 1920. However, European struggle of democracy ever since Magna Carta (1215) cannot be compared with Turkish struggle since first Ottoman Constitution of Kanuni Esasi (1876). Turkey has become a member to NATO in order to consolidate its own security showing her commitment to democratic values despite the Ottoman heritage, Muslim population and Turkish identity while most of the neighbours ruled by different versions of monarchy.

Besides the security concern against communist Russia, another concern in Europe was the creation of peace and welfare within the continent among Western European states. The idea of controlling and regulating coal and steel production of the states under a centralized authority prevailed among others which came up with

the Schuman Plan under the leadership of Robert Schumann and Jean Monnet. This plan paved the way to the creation of European Coal and Steel Community with the Treaty of Paris (1951) with the memberships of France, Germany, Italy, Netherlands, Belgium and Luxembourg in 1952. This cooperation among these states enabled this community to evolve into European Union through various founding agreements historically, Treaty of Rome (1957) founding the European Economic Community, Maastricht Treaty (1993) founding the European Union, Amsterdam Treaty (1997), Treaty of Nice (2007) and Lisbon treaty (2009). Through these treaties, the European Coal and Steel Community turned into European Economic Community, European Community and finally it gained the title of European Union in 1993 with Maastricht Treaty and its three-pillar structure. With the fall of the Berlin Wall in 1989 the victory of Western democracy over Soviet's communism, "the End of History" as Fukuyama puts it, sparked off enlargement towards Eastern Europe till Balkans through Greece (1981) and Bulgaria (2007) over time. The main stimuli behind these treaties were to create a peaceful environment and economic cooperation through a trading bloc then to have a spill over effect into other areas of the cooperation. Throughout the history of that creation, this economic based cooperation expanded into other areas of partnership such as political, social, defence, juridical areas which has both international and supranational features. Today, the European Union is a Political and Economic entity which provides free movement of goods, services, people and capital within 27 members and takes decisions at supranational level, having effects on national level either directly or indirectly.

Moreover, the creation of Eurozone in 1999 enabled Europe to have the second biggest reserve currency as Euro today after Dollar of US beside having stable financial system, robust economy against shocks and crisis with eased trade conditions among Member States. Today, European Union has evolved into a multidimensional political entity with 27 of its members (UK's Brexit) and 435 million of population as the biggest trading bloc on Earth. It has become a giant super power in the world as a result of pioneering democracy, human rights and related values EU has evolved into very successful "Soft Power". *"If a superpower is a political entity that can consistently project military, economic, and soft power trans-continentally with a reasonable chance of success, the EU surely qualifies. Its power, moreover, is likely to remain entrenched for at least another generation, regardless of the outcome of current European crises. In sum, Europe is the "invisible superpower" in contemporary world politics."*[1]

European Commission, European Parliament and European Council are the most important three institutions who are aiming at converging and serving the interest of these 27 members simultaneously, which is a very highly difficult task. Embeddedness, cooperation and commitment for over 60 years and its global effects over the less developed countries, helping the spread of democratic values and indirect effects over the under developed countries in Asia, Africa and Middle East proves that EU is quite successful so far although it has faced several crises such as 2008 Financial Crisis, 2015 European Debt Crisis, Migration Crisis in 2010s and Brexit in 2020. Although the EU Member States envisaged and entitled to create a Common Foreign

[1] MORAVCSIK Andrew: Europe is still a Superpower; 2017 https://foreignpolicy.com/2017/04/13/europe-is-still-a-superpower/ (downloaded 11 november 2020)

and Security Policy since the 1970s through Three Pillar Structure (CFSP), Lisbon Treaty (WEU) and Common Security Defence Policy, military deployments mostly stayed on national levels. Hence, since most of the EU members are also NATO members that has paved way to focus more on economy and political integration and embeddedness rather than military one. In addition, EU has been taken active role in the UN led or NATO led Peacekeeping operations for example Bosnia and Herzegovina and Democratic Republic of Congo which the EU mission took over the UN mission force in the former one. *"With its contribution of 38% of the UN budget, the EU has been the single largest benefactor to the UN budget. It also provided the largest contingent of peacekeepers to the UN peacekeeping."*[2]

On the other hand, today, Turkey with 85 million of population whose 99% of Muslims and young people creates a bridge between Asia and Europe continents as the neighbour of the European Union in her South-eastern borders. Turkey is geopolitically located in a very crucial point surrounded by many important countries like Iran, Syria, Iraq, Azerbaijan (Nakhchivan), Armenia, Georgia, Bulgaria, Greece. Moreover, she has been surrounded by three seas: Mediterranean Sea, Black Sea and Aegean Sea. Aegean Sea and Black Sea are connected into each other through Bosphorus and Dardanelles straits. Given this location in the World makes Turkey both very attractive country for economy and trade yet risky due to the fragile governance risk in its neighbours created for instance by the wars in Iraq and Syria. Turkey has followed the Western Democracy's path since its foundation through memberships in UN, NATO, Council of Europe, Organisation for Economic Cooperation and Development (OECD) and with her eagerness to be member of the European Union although her democracy has been intervened by military twice in 1960 and 1980.

Turkey's relation with Europe formally started with the signing of Association Agreement in 1963 known as Ankara Agreement with European Economic Community. However, this agreement was initially based on economic relations it had also hidden part related to full membership. *"However, the agreement already raised hopes for more, mainly due to this formulation: 'As soon as the operation of this agreement has advanced far enough […] the Contracting parties shall examine the possibility of the accession of Turkey to the Community'21 ."*[3] Following these years, Turkey had been kept waiting in the EU for 33 years until the decision of the Custom Union with European Union in 1996. Customs Union has increased the enthusiasm within the country regarding the full membership in the EU. Although it was limited to industrial and processed agricultural products, it has been hoped that Customs Union will create further economic integration and it is going to open the road towards the full membership as a result of the spill over effect. Three years later, Turkey was granted candidacy for full membership in Helsinki Summits by European Council in 1999. In the light of that enthusiasm, Turkey enacted various constitutional changes, decreasing the efficiency of the military on the governance in security council, treating military elite as a consultant body. *"Since Spring 2002, two extensive constitutional*

---

2 STELMACH, Alice – BEMBA Magali: EU Contribution to UN Peacekeeping; 2016. https://ippjournal.wordpress.com/2016/03/17/eu-contribution-to-un-peacekeeping/ (downloaded 11 november 2020)

3 HAUGE, Hanna-Lisa – ERALP, Atila – WESSESLS, Wolfgang– SELAY BEDIR, Nurdan: Feuture Working Paper – Mapping milestones and periods of past EU-TurkeyThe Future of EU-Turkey relations; 2016. p. 11.

amendments and eight harmonization packages, which include fundamental changes in domestic policy and throughout Turkish society, were enacted."[4]AK Party (Justice and Development Party) has created stability in democracy with their victory in 2002 and country left the coalition party-system phase behind. As, Recep Tayyip Erdoğan the Prime Minister of the time puts it, the full membership was the national goal of the country. Following these improvements in the country, the accession talks have started in 2005 but the enthusiasm in Turkey had faded away due to waiting for quite a long time on the door of the EU, and very small progress was made in accession talks between 2005-2010 and totally stopped between 2010-2013. By the end of 2014, the numbers of opened chapters were 14 out of 35 and just one of them was being closed provisionally. Due to long awaited process and membership, limited customs union, instability in the Turkish bordering country in Syria as a result of Arab Spring (2011) and problems with Greece, and "Privileged Partnership" offered by France and Germany in addition to Financial Crisis in 2009 and following debt crisis have only resented Turkey and pushed her on EU sceptic side. In addition, in 2018, the EU has enacted provisions related to Balkan countries increased the hope for Turkey, but Turkey had its worst assessment ever since the start of the talks in 2005: *"The Council notes that Turkey has been moving further away from the European Union. Turkey's accession negotiations have therefore effectively come to a standstill and no further chapters can be considered for opening or closing and no further work towards the modernization of the EU-Turkey Customs Union is foreseen."*[5] Thus, the main reason for that decision in addition to others is the increasing the term of the state of emergency by three months after the defeat of failed coup d'état in Turkey (2016) until 2021. That decision was claiming that the various levels of freedom were going to be censored and prevented which is against the Copenhagen criteria.

2. Turkey's Perspective: Hot topics, Advantages and Disadvantages of European Membership

2.1. Cyprus Issue and So-Called Minority Problems

To start with, Turkey has always been relatively enthusiastic about becoming a full member of the European Union despite its volatile relations throughout its membership history. However, there are hot topics which make the country more sceptical about EU membership such as Cyprus issue and Aegean Islands issue with Greece, Financial Crisis and following problems in the EU and so-called minority problems. These issues mainly make the country consider the possible repercussions of EU membership and reduces its enthusiasm.

First of all, Turkey's intervention into the Cyprus issue in 1974 was a definitely necessary move due to the island's geopolitical and demographic importance. Turkey felt compelled to protect its own nationals. However, before this intervention, an alternative has been tried such as governing the island as a whole under the

---

4 ASLAN, Hatice: Turkey and the EU – the inner-Turkish Debate, Conflicting Ideologies, Harmonization and Change; Fredrich Ebert Stiftung. Europäische Politik, Bonn, Germany, 2006. p. 1.

5 Council of the European Union: Enlargement and Stabilisation and Association Process – Council conclusions; June 26, 2018, http://www.consilium.europa.eu/media/35863/st10555-en18.pdf (downloaded 11 november 2020)

constitutional bid with proportional allocation of power in 1960 with foundation of the Republic of Cyprus. Nevertheless, a coup d'état took place on Greek side in 1974 in order to tie the island into Greece (Enosis) prompted Turkey to interfere in the island. Since then, the only country recognized the Northern Cyprus as a state is Turkey and the Southern Cyprus's accession to the EU without resolving the problem in the island brought the situation into a deadlock in 2004. *"In April 2004, in two separately held referenda, the Turkish Cypriots voted with overwhelming majority in favour of a reunification plan under the auspices of the UN. The Greek Cypriots rejected this plan in their own referendum. Nevertheless, in May 2004 the Republic of Cyprus was granted full EU membership while the Turkish Cypriots were denied membership status (TDN, 4.9.2005)."*[6] Under these conditions, Greek Cypriots' having welfare with the accession and not having any driving force for solution, makes the solution impossible and it is Turkey's national issue that's why I think there is no probable solution to that problem without willingness of both sides. In addition to that, 12 important islands in Aegean Sea have been delivered to Greece in 1947 which are very close to the Anatolian Turkish mainland and strategically important for Turkey's security. That unfair submission, short proximity and unable provision of disarmament of these islands has resented Turkey and created distrust against the EU.

Secondly, there is so called minority issue that is popularly addressed Kurdish Issue. Turkey, has a population 99% of which is Muslim and there is no part of people in Turkish and Ottoman State has been regarded as a minority. In the foundation of Turkish Republic everybody given the same constitutional rights both in 1921 and 1924 constitutions as a Turkish citizen regardless of his/her origin. Moreover, according to the Lausanne Treaty, only the religios groups in Turkey have been accepted as minorities.

Keep everything aside, Turkey is a country that has suffered from terrorism ever since 1984 by PKK (Kurdistan Worker's Party) and over 30000 people died and around 20000 of them were PKK members and the rest were civilians, public officers and military officers. Turkey has faced many traumas throughout time and losses were not only civilians but also economic, social, political losses were real. In addition, peaceful resolution process started by AKP between 2009-2015 in order to leave violence and terrorism, use legal political representation but even then, loosened conditions were being used as preparation for higher violence targeted terrorist actions. *"In the "terrorist incidents" between June 7, 2015 and January 21, 2017, 596 civilians, 580 soldiers and 311 police died."*[7] The request of the European Commission of changing the definition from "Turkish" to "Türkiyeli" is unacceptable and against the Turkish constitution. These efforts can only be seen creating divisions within the Turkish citizens and threatening unitary integration of the state.

---

6 ASLAN op. cit. p. 5.

7 Diken: Terör bilançosu: 7 Haziran 2015'ten bu yana 596 sivil, 580 asker, 311 polis hayatını kaybetti; 2017. http://www.diken.com.tr/teror-bilancosu-7-haziran-2015ten-bu-yana-596-sivil-580-asker-311-polis-hayatini-kaybetti/ (downloaded 11 november 2020)

2.2. Benefits and Drawbacks

To begin with, Turkey's expected benefits and drawbacks of the EU full membership are highly discussed. Speaking on political aspect, Turkey with her population of over 85 million of people is going to get the largest share of seats in European Parliament according to proportional seat allocation. With the help of that power and back up by the power of EU, Turkey can pursue its foreign policy goals as a more credible unitary power with relatively soft power support of the Union. Thus, it can increase its chances of being a regional power in her struggle with Iran, Israel and Saudi Arabia and being a role model for other countries whose democracies are more fragile and unstable. Secondly, with the conditions of Copenhagen Criteria, Turkish political institutions can increase their commitments to democracy, rule of law, decreasing corruption and nepotism through their membership obligations. Thirdly, the European Parliament, European Commission and European Council can perform as a forum to solve the Cyprus problem and Agean continental shelf crisis with Greece. In addition to that, ongoing turmoil in Syria, Nagorno Karabagh, Iraq and Nuclear problems with Iran can be solved easier because both EU's soft power beside the military capability and Turkey's accession to the Union as a country makes EU more friendly and Turkey more respected neighbour.

Secondly, Turkey has dual economic system, modernized economic system on the side and agricultural labour-based economy on the other side as in the case of Central and Eastern European countries of EU. *"Figure 6 indicates that the EU has the largest share of the world's economic production. Also, with its nearly 40% share of world trade in terms of both merchandise and commercial services, the EU takes first place in the list of world trading powers. The currency used by 15 of the 27 EU members, the euro, is among the most important currencies in the world."*[8] Targeted aid and loan to be received beside the annual budget will be quite helpful to transform the economy by increasing the high-tech and education policies of the Union, providing the labour to be more skilled for business environment. In addition, it will increase the competitiveness and innovation among Small and Medium sized Enterprises (SMEs) contributing to increased level of technology and merchandise will make the market more attractive for FDI from within and outside the Union. *"In this context, the EU accounts for 41.3% of total exports and 33.4% of total imports of Turkey. On the other hand, Turkey is an important trade partner of the EU according to the foreign trade statistics of the EU, indicating that in 2020 Turkey ranks sixth at imports and exports of the EU with shares of 3.7% and 3.6% respectively."*[9] With the membership and total execution of Customs Union, Turkey can increase its volume of trade and can have more and more strong currency with being a member of Eurozone as well. Being a member of Eurozone provides a strong, nonfluctuating second largest reserve currency, no exchange rate among Member States and easy use for the consumers across the member countries will also protect the economy against the crisis and shocks. Lastly, free movement of goods, services, people, and capital will enable business expansions from the inside to outside and vice versa.

---

8 ABDI, Pehlivan: Turkey's membership in the European Union analyzing potential benefits and drawbacks; Monterey, California. Naval Postgraduate School, Monterey, California, USA, 2008. p. 49.

9 Republic of Turkey, Ministery of Trade, 2020, https://www.trade.gov.tr/turkey-and-eu/turkey-and-the-eu (downloaded 11 november 2020)

Lastly, the binding rules and tradition of freedom will enable Turkish civil society have increased rights of freedom, expression and which I think it is basic for the robust democracy institution to work within the state unless it doesn't go towards anarchy and terrorism. In addition, with free movement of goods, services, people, and capital, Turkish citizens will be able to travel, work, study and have more skilled and talented workforce through benefiting from high level of education and trainings in Europe. Lastly, increased welfare, social and security protection will enable state and society and democratic institutions work hand in hand properly.

In contrast to benefits, there might be expected some drawbacks as a result of being an EU member for Turkey. From political point of view, there are two important concepts at stake: sovereignty and national identity. By becoming a member, Turkey is going to transfer part of its power to the EU institutions namely EU Commission and the Parliament. From that moment Turkey's chance of movement as a single actor is going to be reduced. Taking into consideration of its differences from the rest of the EU countries like religion, location, domestic dynamics in what degree these policies can be compatible with Turkish national interests. Secondly, the probable change of the constitution definition of identity to ethnic based one from Atatürk's Nationalism namely from "Turkish" to "Türkiyeli" can only pose a threat to state's unitary order and makes the country weaker. Lastly, unfair allocation of 12 Aegean islands that are very close to Turkish national mainland to Greece in 1947 and accession of Southern Cypriots to EU before the solution the problems in the island in 2004 makes one think that if these problems are going to discussed and solve in fair environment within the EU. On the other hand, Turkey is concerned about last longing membership and Brexit of UK that what if that leave is being followed by the other member states. Turkey increased its bilateral relations with single actors outside the EU as well. These two increased the idea that Turkey can be better off without EU since the entity's future is uncertain. *" [The] EU is portrayed badly in Turkey. People are made to think Turkey's problems will be over when it joins the Union. That is not true. It is awkward to expect the EU to solve Turkey's internal and external problems. It has grown too much and too fast. Turkey will not be destroyed if we stay out of it. We need to think a lot before approaching this entity that cannot even guarantee its existence for another next twenty year."*[10]

Secondly from economic point of view, it is obvious that the quality of goods belongs to the EU, technology, innovation, skilled labour, industry is better however Turkish economy is steadily improving since 2001 crisis. *"While many European countries have been unable to recover from the financial problems, the Turkish economy grew by 9.2% in 2010, and 8.5% in 2011, thus distinguishing itself as the fastest growing economy in the world. (OSEC 2012, 1-3)."*[11] Opening of the Turkish market without the increase of level of Turkish economic indicators like industry, labour force, innovation, technology will totally disrupt the Turkish economy and industry as in the example of Greece. On the other hand, being a member of Eurozone, will prevent act independently against crisis and fluctuations through not being able

[10] AKSU, Kenan: Turkey-EU Relations: Beyond membership; army, religion, and energy; Thesis submitted for the degree of Doctor of Philosophy. Department of Politics, Goldsmiths College University of London, England, 2015. p. 45.

[11] MODEBADZE, Valeri – SAYIN, Mehmet Fatih: Why Turkey should join the European Union: Arguments in favor of Turkish membership; Journal of Liberty and International Affairs, Institute for Research and European Studies, 2015/2. p. 2.

to use the devaluation, deciding interest rates. Moreover, that will make the country dependent on the decisions taken by European Central Bank in Frankfurt. Thus, the 2008 Financial Crisis and 2012 European debt crisis made the country sceptical about the membership because at the time Turkey was doing very well as mentioned above recovering quickly from the 2008 crisis.

Lastly, in Turkey laicism is in force rather than the secularism which means that state and religious matters are separated but the religion and religious practices are in the control of the state. That practice has taken place since the establishment in order to prevent misinterpretation of religion and use for different means like radicalism or terrorism that another fact should be taking into consideration by policymakers otherwise freedom may turn into something unintended.

3. EU's Perspective: Hot topics, Advantages and Disadvantages of European Membership

3.1. Religion

In the beginning, currently EU has 12.5 million of Muslim citizens and probable candidates like Albania and Bosnia Herzegovina have also Muslim population. Nevertheless, taking into consideration large country like Turkey whose %99 of her Muslim country they may fear that the European mosaic can be broken with the inclusion of Turkey, thus radical Islam may diffuse all over the Europe or Turkey with Islamic population portrayed as an invader. First of all, there is no religion on Earth established can be portrayed or identified with terrorism. Terrorist acts of any group, by any religious justification usage of terror as a means can't be accepted. The main reason that problem that continues for 10 centuries between Eastern world and Western world is that, Eastern world knows more about Western religion, culture and practices than Western knows about Eastern. The most fascinating book I have read about Islam is Hz. Muhammed (s.a.v.) written by Karen Armstrong explains the birth of religion on social and political circumstances of the time in a very objective and scientific way. I believe that both sides should meet and learn more about each other so that "Clash of Cilizations" as Samuel Huntington puts it can be prevented. Turkey, both as a government and society against the sharia law. Turkey's constitutional acceptance of religion as an individual matter and commitment to the democracy since its foundation is quite a proof that religion is not a threat for the European Union.

3.2. Benefits and Drawbacks

There are mainly four areas that can benefit population and economy, geography, and security. Firstly, young, dynamic population of Turkey can easily be beneficial remedy for the aging population of Europe as an alternative workforce. However, with the proper transition process Turkish labour force can easily be incorporated into European economy. The total working age population (15-64 years) is expected to fall by 20.8 million between 2005 and 2030.[12] The fertility rate in Europe is extremely low. It is below the threshold needed to renew the population.

[12] VALVERDE, Santiago Carbó: The determinance in bank margins in European banking, Journal of Banking&Finance, 2007/7, p. 248.

Because of the low birth rates European countries will face serious socioeconomic problems in the future: *"aging could cause potential annual growth in GNP in Europe to fall from 2-2.25% to 1,25% in 2040."*[13] Secondly, as Turkey economically improving since 2001 and became an attractive market for the FDI from the outer world it can help to increase its poor growth rate of the European Union. In addition, the European Union is dependent on the Russian oil after the Ukraine crisis, made the authorities reconsider its options. As I see it and generally agreed, Turkey is the best possible option to diversify the EU's energy supply and provide its energy security. Through membership and supply of Caspian gas through Turkish border can relieve European authorities in a great degree. Thirdly, with the fall of Berlin Wall and enlargement European Union has become an international actor. With the inlusion of Turkey, the EU can increase its sphere of influence towards the Middle East and can affect the new neighbouring countries through union's neighbourhood policy which serves for EU's strategic interest, peace and stable performance. Besides that, having Turkey as a member state break the understanding of EU as a Christian club and it can be a proper example for the rest of the neighbouring countries that can motivate them to take actions in line with the Western democracy. Thirdly, Turkey can be a reliable ally with having second largest army capabilities within the NATO. Thus, the south-eastern borders of the continent will naturally be protected by the Turkey's membership.

On the other hand, mentioning the drawbacks, Turkey's economic transformation requires both financial and technical assistance. The real thing is that, there is a gap between EU and Turkey from the point of competitiveness, innovation and level of skilled labour obviously. However, accomplishing this difficult task can be mutually beneficial for both sides in the long term. Secondly, the fear is that population influx towards Europe as in case of France feared during the Spain's accession. *"When negotiations for the accession of Spain to the European Economic Community were launched, France in particular feared that it would be invaded by Spanish workers looking for employment but in reality, this never happened. In 1960s and 1970s, Spanish economy started to grow and many Spaniards who had migrated in large numbers to Germany and France began returning to Spain."*[14]

In my opinion once the welfare and good living conditions exhibited people will not find migrating attractive due to its difficulties like culture, language and new social life. Lastly and the most important one is that Common Foreign and Security Policy. Turkey's membership is going to protect the continent's South-Eastern borders but these will be new European Union external borders at the same time. Ongoing civil war in Syria, fragile government in Iraq, nuclear problem question in Iran, conflict over Nagorno Karabagh between Azerbaijan and Armenia, fragile Russian-Georgian relations can probably make the policymakers think twice. Yes, leaders might think of it as dangerous to confront with these problems and issues but stability achieved through neighbourhood and enlargement policies within the neighbour states motivating actors in the direction of the Western Democratic way can help to the slowdown of the migration influx from internally struggling countries.

---

[13] Ibid. p. 4.
[14] Ibid.

Conclusion

In my opinion, Turkey's membership can be beneficial for both sides once it has been handled from social constructivist point of view. Turkey's dynamics are way more different dynamics and geographical necessities must be understood by the European Union and there must be clear and open communications. However, Turkey's Cyprus issue, national identity and sovereignty are the most important issues that have to be approached sensitively.

To sum up, I am in favour of Turkish EU membership only and only if Turkey's internal dynamics, concerns and mentality is being understood, national unity and interests are respected by European Union member states and institutions. Unless actors understand each other and converge their interests all the benefits can be reversed.

I believe that even if Turkey doesn't become a member will play a major role in the area and will not lose its part of sovereignty, mobility and bilateral independent policies with third actors. *"Turkey has spent the last several years improving its relationships with various other non-EU countries, in particular the Middle East and the United States. Given its new economic and strategic potential, Turkey no longer needs to rely on EU acceptance to prove that it is a modernized country on the international market."*[15] Turkey, taking into accounts all of its features, cannot be ignored and the future can only be shaped through constructivist approach of both sides and I believe that, Turkey's ties with Europe is deeper than the ones with US, although they are not alternative to one another. I believe that through Turkey's membership, the European Union can be highly influential and successful in spreading its values to the region and being a stabilizer factor in the Middle East, which would enlarge peace and prosperity coverage as foreseen by the initial phase of the evolution of the EU.

Bibliography:

- ABDI, Pehlivan: Turkey's membership in the European Union analyzing potential benefits and drawbacks; Monterey, California. Naval Postgraduate School, Monterey, California, USA, 2008.
- AKSU, Kenan: Turkey-EU Relations: Beyond membership; army, religion, and energy; Thesis submitted for the degree of Doctor of Philosophy. Department of Politics, Goldsmiths College University of London, England, 2015.
- ASLAN, Hatice: Turkey and the EU – the inner-Turkish Debate, Conflicting Ideologies, Harmonization and Change; Fredrich Ebert Stiftung. Europäische Politik, Bonn, Germany, 2006.

[15] CAMPBELL, Madison – DEMARTINO, Elisa: Disadvantages to Turkey's EU Accession: Turkish Perspective; Claremont-UC Undergraduate Research Conference on the European Union, Vol. 2012, Article 5. http://scholarship.claremont.edu/urceu/vol2012/iss1/5 (downloaded 11 november 2020)

- CAMPBELL, Madison – DEMARTINO, Elisa: Disadvantages to Turkey's EU Accession: Turkish Perspective; Claremont-UC Undergraduate Research Conference on the European Union, Vol. 2012, Article 5. http://scholarship.claremont.edu/urceu/vol2012/iss1/5 (downloaded 11 november 2020)
- Council of the European Union: Enlargement and Stabilisation and Association Process – Council conclusions; June 26, 2018, http://www.consilium.europa.eu/ media/35863/st10555-en18.pdf (downloaded 11 november 2020)
- Diken: Terör bilançosu: 7 Haziran 2015'ten bu yana 596 sivil, 580 asker, 311 polis hayatını kaybetti; 2017. http://www.diken.com.tr/teror-bilancosu-7-haziran-2015ten-bu-yana-596-sivil-580-asker-311-polis-hayatini-kaybetti/ (downloaded 11 november 2020)
- HAUGE, Hanna-Lisa – ERALP, Atila – WESSESLS, Wolfgang– SELAY BEDIR, Nurdan: Feuture Working Paper – Mapping milestones and periods of past EU-TurkeyThe Future of EU-Turkey relations; 2016.
- MODEBADZE, Valeri – SAYIN, Mehmet Fatih: Why Turkey should join the European Union: Arguments in favor of Turkish membership; Journal of Liberty and International Affairs, Institute for Research and European Studies, 2015/2.
- MORAVCSIK Andrew: Europe is still a Superpower; 2017 https://foreignpolicy.com/2017/04/13/europe-is-still-a-superpower/ (downloaded 11 november 2020)
- Republic of Turkey, Ministery of Trade, 2020, https://www.trade.gov.tr/turkey-and-eu/turkey-and-the-eu (downloaded 11 november 2020)
- STELMACH, Alice – BEMBA Magali: EU Contribution to UN Peacekeeping; 2016. https://ippjournal.wordpress.com/2016/03/17/eu-contribution-to-un-peacekeeping/ (downloaded 11 november 2020)
- VALVERDE, Santiago Carbó: The determinance in bank margins in European banking, Journal of Banking&Finance, 2007/7

HAJNALKA SZILÁGYI-KISS

SITUATION OF IRAQI CHRISTIANS AS A SECURITY CHALLENGE

Abstract

The article intends to investigate Iraq, a state in the middle of Eurasia, in the centre of conflicts in the Middle East. The region is the cradle of Judaism, Christianity and Islam, but also the main arena of their opposition.
Today's Iraq is the area of River Tigris and Euphrates region where the beginning of civilization dates back. Both the Islamic cultural circle, the regional powers, but also the global superpowers try to gain dominance.
The safety of this area is crucial for everyone. How and by what means can Hungary contribute to the security of the region?

Keywords: Middle-East, Iraq, geopolitics, security, Hungary Helps Program

Introduction

One of the oldest continuous Christian communities of the world is Christians in Iraq, in the region between Tigris and Euphrates rivers, historically known as Mesopotamia, which is often called the cradle of civilization. Christianity was brought to Iraq in the 1st century. These territories are also known from the Bible, mainly from the Book of Genesis.[1] Today it is one of the powder kegs in the world.

One of the basic needs of a person is the wish to live in safety, without fear. The root of the Latin term "cura" refers to anxiety, fear, while "se" means, as a privative suffix: without. That is, the original content of our word security (securitas) is that a person is safe if he can live without fear, so the person is not in danger. Although danger perception is subjective, as someone who is not objectively in danger can also perceive something as a threat. It is important, however, to realise that besides the individual's worries, there is also a community perception when we study a larger group or a mass of people. It is important to distinguish between real or perceived threats when addressing human security issues. Politics is the collection of activities aimed at leading the society and the state; acquiring and keeping power; and a system of related principles. Security policy, as the term itself suggests, focuses on security processes. Politics must be an instrument which establishes and maintains security within human communities, states and the international systems as a whole. About security policy - as it is also indicated by the wording - it is worthwhile to think as the policy to be linked to security processes. Politics must be a tool for creating and maintaining security between human communities, states and the international systems they create. If there is a challenge or a sense of danger on the part of a group of people, in most cases there is a real basis for it, and the cause and the search for a

[1] LOZANO, Maria ed. (2021): The Christions of Iraq, Resource: Aid to the Church in Need; p. 10. www.acninternational.org, (downloaded 27 December 2020)

solution must be addressed, even if it is hidden.[2] This paper addresses the vulnerabilities of Iraqi Christians who live in the vicinity of paramilitary, fanatical, Islamist terrorist groups. Life in Iraq is not only for them is an everyday challenge nowadays. ISIS has been defeated, but it continues to live in cells.

Geopolitical situation of Iraq

Iraq's geographical location and its vulnerable position affect the behaviour of the main geostrategic players. Brzezinski classified Iraq as a geopolitical pillar because it can provide access either to a few economically and politically dominant areas or to important resources, that is why it is important to the United States, European Union and the surrounding regional powers. Iraq is located in the middle of Eurasia, surrounded by three regional powers (Turkey, Iran and Saudi Arabia) that have a strong impact on groups affiliating with them, often on a "divide and rule" basis. It is in both Turkey's and Iran's interest to preserve the unity of Iraq. The rationale for this policy is the presence of a Kurdish autonomous entity in Northern Iraq; as a large number of Kurds live in both countries, the break-up of Iraq might lead to increased demands for an independent Kurdish state. These factors could transform an internal crisis in Iraq into a major regional or international conflict.

As early as the 1970s, the U.S. saw the Kurds in northern Iraq as a potential tool which might weaken Saddam Hussein's regime, which was then classified as a hostile force. In 2003, the Kurdish Peshmerga provided significant assistance to the U.S. forces in the Iraqi war and later in the fight against ISIS, but they knew that the disintegration of the Middle East state system would have unpredictable consequences. Similarly to the neighbours of Iraq, the U.S. has also been interested in the stability of the northern Iraqi region, and could not support the aspiration of the Kurds to create an independent Kurdistan.[3]

Compared to the United States, Europe has always had stronger economic ties with the Middle East. This is because Europe consumes more crude oil and natural gas, which are strategic raw materials, from this region than the USA. To ensure stability in the South, the EU is signing joint declarations, bilateral and multilateral agreements with multiple Mediterranean countries, including Iraq.

ISIS terrorist attacks made Europe and the world understand that a war waged at NATO's frontier directly impacts European and global security. The United Nations have sought to curb violent inter- and intrastate conflicts in the past 60 years. To achieve this goal, they usually relied on peacekeeping measures, and in most cases only intervened once the conflict was over. By this moment, the opposing sides had already caused significant damage to each other and to the international community trying to assist. The devastation caused by the IS is the most serious current security policy challenge.

---

[2] SZILÁGYI-KISS, Hajnalka: Irakban Magyarország segít; In: UJHÁZI, Lóránd et. al. (eds.): Budapest-jelentés a keresztényüldözésről; 2020. p. 321.

[3] CSICSMANN, László: A kurd államiság esélyei a Közel-Keleten a geopolitikai rivalizálás tükrében; Regio, 2018/1. pp. 24-51. www.regio.tk.mta.hu/index.php/regio/article/view/201/pdf_181 (downloaded 26 December 2020) p. 27.

Security challenges of Iraq

Religious-ethnic fragmentation is typical of Iraq. The three largest religious, ethnic groups in Iraq are Shiite Arabs (58-63%), Sunni Arabs (17%) and Sunni Kurds (about 15-20%). Ethnic Kurds live in the Kurdish Regional Government (KRG) which is their autonomous territory in the North. The rest of the population is Turkmen, Yezidi, Shabak, Kakai, Bedouin, Romani, Assyrian, Circassian, Persian and Sabean-Mandean. This 5% of the nearly 40 million population is almost 2 million people. Among this, Christian population was about 250.000 in 2019.[4] Most of the Christians still speak Aramaic which is the language spoken by Jesus Christ. It is the oldest continuously spoken language in the world.[5]

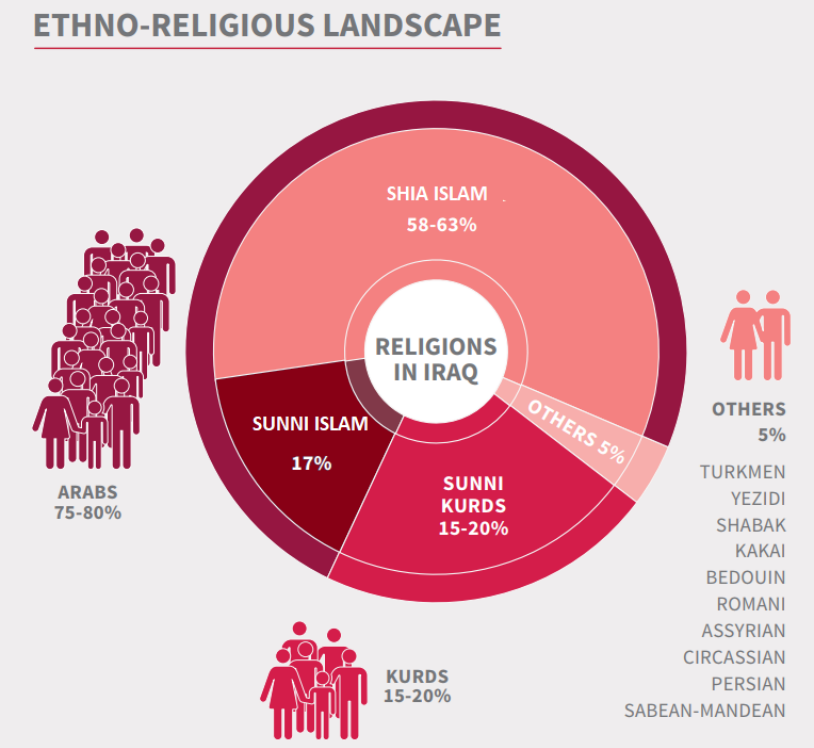

Figure 1: Ethno-religious landscape of Iraq[6]

[4] Chaldean Archbishop Warda of Erbil told ACN in 2019: *"In the years prior to 2003, we numbered as many as one-and-a-half million – six percent of Iraq's population. Today, there are perhaps as few as 250,000 of us le Maybe less. "* ACN International: Aid to the Church in Need: Iraq in 2019. p. 14. www.acninternational.org/regional-activity/middle-east/iraq/ (downloaded 27 december 2020)

[5] NRC Iraq: Iraqi Christian Foundation: Brief Summary on Iraqi Christians, 2019. p. 1. http://iraqichristianfoundation.org/ (downloaded 04 March 2021)

[6] Source: LOZANO op. cit. p. 9.

In all locations where Christians live, the territory of Nineveh Plains falls into Iraq's disputed territories claimed by both the KRG and the Central Government in Baghdad. At the moment Baghdad controls the area.[7] From the emergence of Islam (for almost fourteen centuries) there has been a conflict between Islam and Christianity. These conflicts often led to serious armed conflicts. Hostilities were sometimes motivated by religion, however, much more often related to politics, power, economy or other considerations. Neither side can be blamed unilaterally for these conflicts. *"Each side is looked upon by the other as a culture very different in terms of its crucial elements; a threatening, alien entity entirely different from 'us'; it is the source of constant danger and is likely to attack us at any moment."*[8]

Between 1958 and 2003, the country's government was largely in the hands of a few authoritarian military leaders. After the overthrow of Saddam Hussein's regime in 2003, the new Iraqi governments were unable to stabilize the security situation of the country. After the fall of Saddam Hussein, the army was disbanded, and the soldiers discharged, and extremists filled this power vacuum which led to a flare up of the Sunni–Shiite sectarian conflict. Other ethnic-religious fault lines also intensified and clashes between militias of the three major social groups became regular occurrences. The 2005 Iraqi constitution only guaranteed the rights of minorities and free religious practice in principle, as it also specified that no law could conflict with Islamic regulations.[9] Therefore, Christians have been pushed into the background in all areas of life, their access to public services has been curtailed, their labour market position and the security of their property have deteriorated. In the absence of efficient Iraqi armed forces, the U.S. military was entrusted with policing tasks. This act provoked Shiite and Sunni paramilitary formations alike and led to an increase in the number of attacks against the U.S. and coalition forces. One of the consequences of the rising number of casualties was that U.S. public opinion turned against the presence of American troops in Iraq.

After the withdrawal of coalition troops, in December 2011, the Iraqi civil war immediately intensified. In addition to the armed clashes along the Sunni–Shiite religious fault line, the northern Kurdish territories also announced their intention to secede from the central government. The situation of Christians in Kurdistan has always been more favourable, as they received more seats in the local legislature. In 2012, the Kurdish Government declared the religious neutrality of schools and equality between denominations in school education.

The Islamic State (IS), which seceded from the al-Qaeda terrorist organisation and became independent in April 2013, took advantage of this power vacuum and achieved rapid success. They captured Mosul, the most important city in northern Iraq, on 10 June 2014, and a month later Abu Bakr Al-Baghdadi declared the foundation of the World Caliphate. IS took control of significant Kurdish and Christian-populated

---

7 Ibid.

8 FISCHL, Vilmos: Islamic Civilization and its influence on the World Today; National Security Review, Budapest, 2018/1. p. 10. https://www.knbsz.gov.hu/hu/letoltes/szsz/2018_1_NSR.pdf (downloaded 02 March 2021)

9 KÓRÉ, András: The Security Situations of Christians in Iraq and Syria in 2018. In: KALÓ, József – UJHÁZI, Lóránd (eds.): Budapest Report on Christian Persecution 2018; Budapest, Dialóg Campus Kiadó, 2018. p. 69.

areas of northern Iraq and the Nineveh Plains. The Shiite population of these territories and those Sunnis, who did not support IS were also victimised by the terrorist organisation. The situation of the various religious minorities, including the Christians, was even worse and they were forced to pay a special tax if they did not convert to Islam. Attacks on holy places, kidnappings, and brutal executions were frequent. Violence against women, slavery, trafficking in human beings and organs have also become almost commonplace. Because of the atrocities, even Pope Francis called for armed intervention, while the Holy See opposed it. More and more researchers had come to the opinion that while the presence of the terrorist organisation is unacceptable, yet the Iraqi state could easily weaken after the disappearance of the IS because the minimal cohesion created by the presence of a "common enemy" would also disappear. [10]

Internal security issues also have an impact on foreign policy and security in the region. Security policy is a set of political goals, strategies and related instruments that create the conditions for maintaining peace, preventing wars, tackling threats and hazards, and defending the country. In the 1980s, Barry Buzan and his colleagues strived to address the military, political, economic, social, and environmental aspects separately in the context of security challenges. The focus of the present paper is on Iraq, the threat to the Christian minorities living there and the impact of this situation on Europe, including Hungary. Based on Buzan's theory the challenges are most pronounced in the social and military sectors in Iraq. Tensions between ethnic, religious groups and tribes are significant there. The spiritual life of Arabs is fundamentally determined by their sense of tribal unity, which is manifested in the appreciation of the traditions, virtues of the ancestors, the nurturing of common values, and strong alienation from and cooperation against strangers. Religion plays only a secondary role to these folk moral values. The region is the cradle of Judaism, Christianity and Islam, but there are also tensions arising from them. The region's current borders reflect British and French interests around the time of the First World War. So these borders disregard the religious, cultural and ethnic make-up of these territories. As a consequence, the population of the new countries could not identify itself with a framework that had been imposed upon them. Therefore, once conflicts over repressed cultural differences surfaced, they could not be controlled. The goal has always been to preserve the identity which holds the group together, which, if compromised, is perceived by the group as a security threat.[11]

When examining the military field, the militaristic nature of Arab society reveals the attraction of Iraqi Muslims towards violent conflict. Traditional Islamic thinking divides the world into a house of peace (Dar al-Islam) and a house of war (Dar al-Harb). The latter includes areas where Islam is not an official state religion. The "holy war" (jihad) is obligatory for every faithful Muslim in the so-called "houses of war" areas so they can spread the religion of the Prophet Muhammad. The fight between them will go on until Islam proves to be victorious. As a result of this thinking and after the territorial conquest, Islam also easily spread in the territory of contemporary Iraq. Although these principles are only upheld by radical and extremist advocates,

---

[10] UJHÁZI, Lóránd: A keresztények biztonsági helyzete Irakban, „korszakváltás" a vatikáni diplomáciában; Szakmai Szemle, 2015/3. p. 54.

[11] GAZDAG, Ferenc – REMEK, Éva: A biztonsági tanulmányok alapjai; Budapest, Dialóg Campus Kiadó, 2018. p. 23., SZILÁGYI-KISS, Hajnalka: Irakban Magyarország segít; In: UJHÁZI, Lóránd et. al. (eds.): Budapest-jelentés a kereszténygyüldözésről; 2020. p. 324.

mention should be made of the fact that they are also deep rooted in that division of Islam which is followed by the vast majority of its believers.[12] Terrorist assassins usually take advantage of upheavals and dismantle the existing security system. They do this to provide the desperate population with a feeling of a false order and security in a state which is dominated by fear. Then they exploit these circumstances to further their interests. The definition of a terrorist act is *"the premeditated use of violence or threats thereof with the intent to attempt to intimidate the government, society, for religious, political or ideological purposes"*.[13] Terrorist groups built up a network with all the important supporting institutions for now, but it is important to make a distinction between the terrorist network of institutions and the Islam believers. It is necessary to emphasize, that the war on terror is not to be interpreted as fight against the entire East or the Muslims. It is a war against the institutions of terror (political groups, arms trafficking, training camps, banks involved in money laundering and the terrorists themselves), „*all of which, in line with the ideas rooted in radical, political or militant Islam, engage in actions leading to terrorist attacks by pursuing their political interests"*.[14]

Situation of the Iraqi Christians

Iraqi Christians live together in peace with other communities mostly in the North in the Nineveh Plains, Erbíl, Dohuk, Sulaymanyah and Kirkuk where they were settled historically. Many Christians moved to Baghdad and Basra in the 70ies because of economically or security reasons, but nearly all of them moved back up to the north due to the intimidation of ISIS.

12 FISCHL op. cit. p. 12.

13 RESPERGER, István: Biztonsági kihívások, kockázatok, fenyegetések és ezek hatása Magyarországra 2030-ig; Felderítő Szemle, 2013/3. p. 27.

14 FISCHL op. cit. p. 6., HARAI, Dénes: The cult of violence and the protection of civilization. Social issues and sociological implications of the fight against terrorism; (Manuscriptinternal use) Zrínyi Miklós Nemzetvédelmi Egyetem; 2008. p. 4.

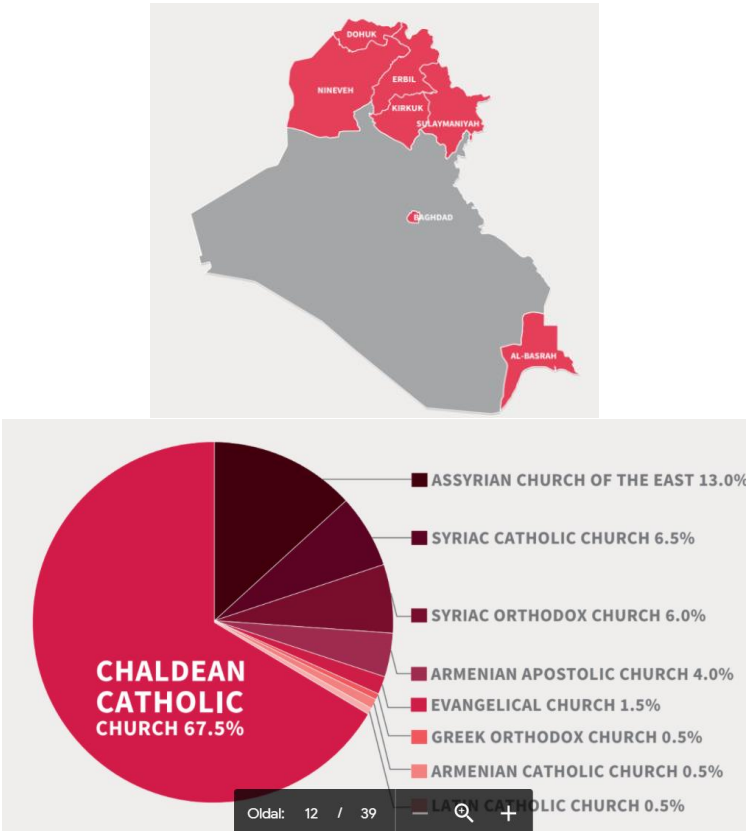

Figure 2: Christians in Iraq[15]

The two most significant and oldest Christian groups in Iraq are the Apostolic Catholic Assyrian Church of the East and the Chaldean Catholic Church. The head of the former church is Patriarch Mar Gewargis III, while the leader of the latter is Patriarch Louis I Raphael Sako. The Assyrian Church is most closely connected to the territory of modern-day Iraq. According to the traditions of this church, it was founded by Saint Thomas the Apostle. After the Council of Ephesus in 431, they separated theologically from the universal church, due to the influence of Patriarch Nestor of Constantinople. The Chaldean Catholic Church stems from the Assyrian Church of the East. Its history starts in the middle of the 16th century when Johanna Sulaka, the newly elected patriarch, travelled to Rome, to receive the pallium from Pope Julius III, who appointed him as the patriarch of Mosul.[16] This event took place on February 20 1553. In addition to these churches, the Antioch Orthodox, the Syrian

15 Source: LOZANO op. cit. pp. 11-12.

16 WAGNER, Péter – SZALAI, Máté (eds.): A többség-kisebbség dinamika szerepe a közel-keleti konfliktusokban; 2019. p. 36. www.kki.hu/wp-content/uploads/2019/07/0726_kki_mena_tanulmanykotet_fin.pdf (downloaded 02 March 2021)

Jacobite, the Syriac Catholic and the Armenian Apostolic Orthodox Churches are all present in Iraq.[17]

In recent years, the religious composition in Iraq has changed significantly, and the Christian community is under constant threat. In the movie, "*Theirs is the Kingdom of Heaven",*[18] Archbishop Nicodemus, the Syriac Orthodox Metropolitan of Iraq, stated: *"ISIS has occupied our villages in bright daylight before the eyes of the whole world. No one did anything. No one defended us. ISIS took away our history, our country and our money. They took everything from us, but they could not take our God away. It is impossible to live a dignified life if we are not safe, if we are not protected. Our upbringing is not about fighting. We were raised to learn and to teach others. At the very least, the UN should declare the villages of Iraqi Christians protected villages. Why is this so hard to say? If the root is cut, the tree dies. The root of all Christianity is here in Iraq. Help us, protect us in our own country!"* If the security of Iraqi Christians is shaken, this will influence the immediate and wider environment alike.

According to the EU Report on the Situation of Human Rights and Democracy in 2019, the human rights situation in Iraq was still challenging. The main issues were connected to the wave of protests and violence that began in October 2019. Among the other challenges, the report highlights hostility against ethnic and religious minorities, barriers preventing the return of displaced persons, the poor condition of IDP (Internally Displaced Person) camps, lack of justice, the practices of the death penalty and torture as well as rape.

Up-to-date research published by the Aid to the Church in Need (ACN) shows that 2 out of 3 people in Iraq are currently unemployed, and the unemployment rate among Christians is even higher, especially among young people. Often nobody has a job and face living difficulties. 6 million people need external help. ACI, which is an internationally recognised and respected charity organisation, is a leading international donor supporting the Iraqi Christians. ACN is supported by the Committee for the Reconstruction of the Nineveh Plains, which was established on 27 March 2017. This committee works in close cooperation with the Christian (Chaldean, Syriac Catholic and Syriac Orthodox) churches in Iraq to ensure that this ancient Christian community can survive the current challenging times.

According to the Nineveh Reconstruction Committee, 14,000 families, approximately 90,000 people, fled to Erbil from Mosul and the Nineveh Plains when ISIS started intimidations and terrorist attacks from 1st August 2004. The area of the Kurdish Regional Government seemed to be the safest place in Iraq that time.

Father Georges Jahola describes the situation as *"Of course, not everything is positive yet. The problems in our country are enormous. One thing is certain: if Christians from all over the world hadn't been so generous in helping our people,*

---

17 UJHÁZI op. cit. p. 55.

18 A documentary by Beatrix Siklósi, which presents the fate of persecuted Christians of Northern Iraq and the work of Christian churches. www.youtube.com/watch?v=ogcozTJ2fcI (downloaded 20 December 2020)

there would be no one left here."[19]. Like ACN, the Hungarian Government considers the reconstruction of churches and residential buildings to be paramount, as this is the only way to ensure that Iraqi Christians remain in place. A report, based on research carried out in 2019 and published in June 2020, shows the consequences of the rise and fall of the IS and the persecution of Christians on the Nineveh Plains. In 2003, the number of Christians in Iraq was 1.5 million and they made up 5% of the population. By 2020, the number of Iraqi Christians has dropped to 120,000, a 92% decline. The number of Christians living on the Nineveh Plains also decreased from 102,000 in 2014 to 36,000. The same report also forecasts that by 2024, if we do nothing, the number of Christians in Iraq could fall to just 23,000.

Religious activity is particularly important for the inhabitants of the Nineveh Plains. 70% of Christians who live here attend religious ceremonies at least once a week, and only 4% of the entire population of the region define themselves as "non-religious". The community and cultural life of these communities are built around the church, and with the paralysis of state and welfare institutions, Christian organisations have to fill the void by providing social, educational and cultural services to the population. The survey's respondents classify the lack of stability and security, unemployment, corruption, religious exclusion, poverty, lack of health care, and their damaged or burnt-out homes and church buildings amongst their biggest challenges. 57% of Iraqi Christians living on the Nineveh Plains have already considered emigration, 35% wanted to leave Iraq within five years. 64% of them have an immediate family member who lives in another country. 24% of Christians were negatively affected by the activities of various militias or other hostile groups. 87% of them do not feel safe, while 67% think it is "likely" or "very likely" that IS or a similar terrorist group will return within the next five years. Half of the respondents agreed that "Christianity has no future in Iraq".[20]

The consequence of the destruction of ISIS in Iraq

Destruction of ISIS[21] caused massive destruction in the environment, economy, culture and society in the whole population of Iraq. Between 2014 and 2019 73,083 people were killed, 62 schools were completely destroyed, 15,011 houses were damaged (partially or completely destroyed, burned). From this total, 14,828 houses require reconstruction.

---

19 Source: Nineveh Reconstruction Committee, https://www.nrciraq.org/nineveh-reconstruction-committee/iraq-in-2019/ (downloaded 04 March 2021)

20 SZILÁGYI-KISS op. cit. p. 331.

21 3 years of war from 2014-2017. The major military operations are finished in late 2017, but the humanitarian crisis is still not over.

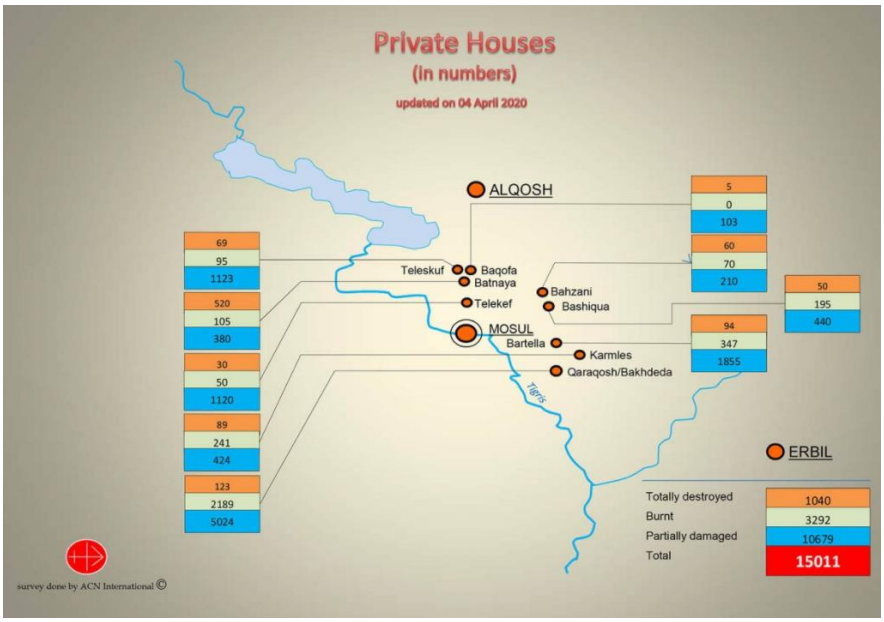

Figure 3: The situation of private houses in the Nineveh Plains[22]

Out of these, 8,166 houses (54.4% on 3 September 2020) have already been completed due to the efforts of international organisations. Currently, another 290 houses are under renovation. Based on calculations made on 4 April 2020, the renovation of 15,011 private homes alone will cost a total of $ 260,410,810.

[22] Source: Nineveh Reconstruction Committee op. cit.

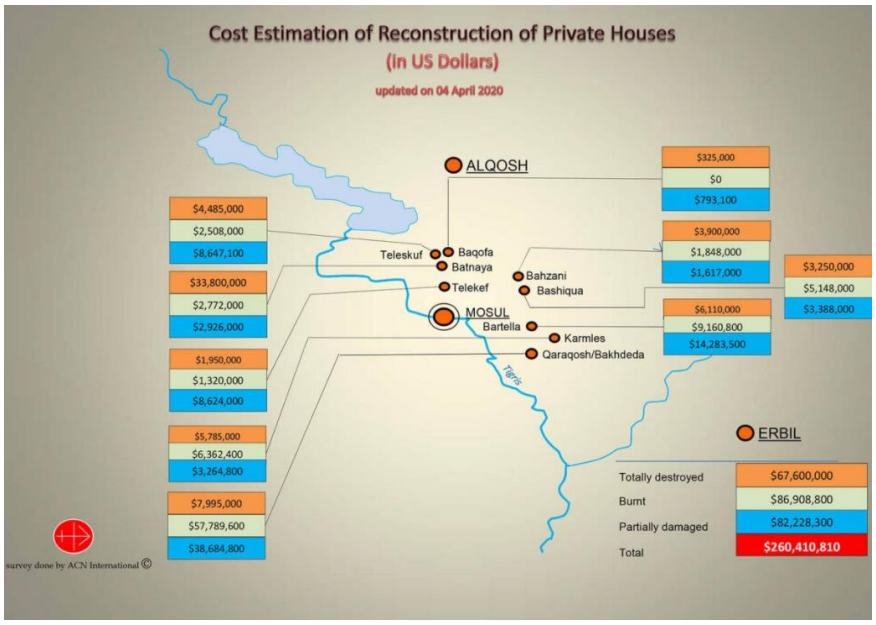

Figure 4: Cost estimation of reconstruction of private houses [23]

Besides private homes, many public and church buildings have also been severely damaged. Between 2004 and 2014 1,107 Christians were killed.

[23] Ibid.

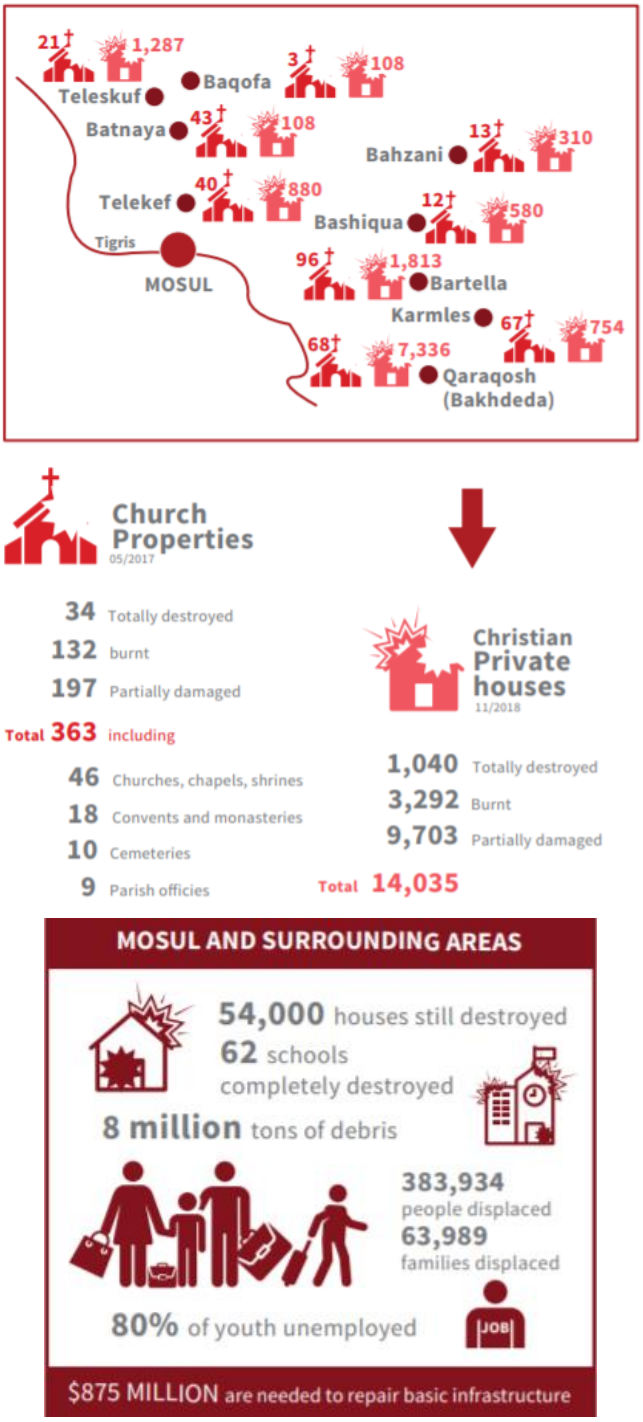

Figure 5: Destruction in the Nineveh Plains [24]

[24] Source: LOZANO op. cit. p. 17, 22.

In co-operation with ACN, the Hungarian Government is also taking part in the reconstructions and will do its utmost to ensure that aid reaches the victims of humanitarian disasters quickly and effectively. This new approach, based on personal contact with local communities, makes the distribution of aid more effective. The "Hungary Helps Program" is unique because there is no other country in the world that has spoken out so frequently at the governmental level against the persecution of Christians and religious discrimination. But the support is still not enough. In addition to the climate of fear and insecurity, the main obstacles because Christian refugees do not return to their homeland are the exclusion of Christians from economic life, since most of the small businesses that were their main source of income have gone bankrupt and the existing jobs are filled primarily by Muslims. For this reason, the main focus of the Hungary Helps Program in Iraq, after the completion of renovations, is to revitalise the economy and create new jobs, primarily for people belonging to the most severely persecuted groups.[25]

Summary

The most important is the rebuilding of not only buildings but communities because if people can return to their rebuilt or renovated cities, churches, and schools, they become stronger, they can create new jobs, which will make their livelihoods sustainable, and lay the foundations of economic development. Nearly half of the Christian families have already returned to their homeland. The provision of further assistance can limit migration towards Europe and the developed world. Nevertheless, the situation is still unclear, and it will take a while for the people who suffered a lot, to regain their confidence and be optimistic about their futures. Hopefully, it is possible to stop the disappearance of Middle Eastern Christians, and their continued presence in their homelands will contribute to the security of the Euro–Mediterranean region, which will also have a positive impact on global security.

Bibliography:

- ACN International: Aid to the Church in Need: Iraq in 2019. www.acninternational.org/regional-activity/middle-east/iraq/ (downloaded 27 december 2020)
- CSICSMANN, László: A kurd államiság esélyei a Közel-Keleten a geopolitikai rivalizálás tükrében; Regio, 2018/1. pp. 24-51. www.regio.tk.mta.hu/index.php/regio/article/view/201/pdf_181 (downloaded 26 December 2020)
- FISCHL, Vilmos: Islamic Civilization and its influence on the World Today; National Security Review, Budapest, 2018/1. pp. 4-17. https://www.knbsz.gov.hu/hu/letoltes/szsz/2018_1_NSR.pdf (downloaded 02 March 2021)

[25] SZILÁGYI-KISS op. cit. p. 331.

- GAZDAG, Ferenc – REMEK, Éva: A biztonsági tanulmányok alapjai; Budapest, Dialóg Campus Kiadó, 2018.
- HARAI, Dénes: The cult of violence and the protection of civilization. Social issues and sociological implications of the fight against terrorism; (Manuscriptinternal use) Zrínyi Miklós Nemzetvédelmi Egyetem; 2008.
- KALÓ, József: Violent Acts against Christians in 2018; In: KALÓ, József – UJHÁZI, Lóránd (eds.): Budapest Report on Christian Persecution 2018; Budapest, Dialóg Campus Kiadó, 2018. pp. 33-48.
- KÓRÉ, András: The Security Situations of Christians in Iraq and Syria in 2018. In: KALÓ, József – UJHÁZI, Lóránd (eds.): Budapest Report on Christian Persecution 2018; Budapest, Dialóg Campus Kiadó, 2018. pp. 65-74.
- LOZANO, Maria ed. (2021): The Christions of Iraq, Resource: Aid to the Church in Need; www.acninternational.org (downloaded 27 December 2020)
- MICHTA, Andrew A.: Watchful Waiting on European Security; 2017. www.carnegieeurope.eu/strategiceurope/66609 (downloaded 28 April 2020)
- Nineveh Reconstruction Committee; https://www.nrciraq.org/nineveh-reconstruction-committee/iraq-in-2019/ (downloaded 04 March 2021)
- NRC Iraq: Iraqi Christian Foundation: Brief Summary on Iraqi Christians, 2019. http://iraqichristianfoundation.org/ (downloaded 04 March 2021)
- NRC Iraq: Reconstruction Committee, www.nrciraq.org/nineveh-plains-destruction-images/ (downloaded 20 december 2020)
- RESPERGER, István: Biztonsági kihívások, kockázatok, fenyegetések és ezek hatása Magyarországra 2030-ig; Felderítő Szemle, 2013/3.
- SZILÁGYI-KISS, Hajnalka: Irakban Magyarország segít; In: UJHÁZI, Lóránd et. al. (eds.): Budapest-jelentés a kereszténytüldözésről; 2020. pp. 321-334.
- UJHÁZI, Lóránd: A keresztények biztonsági helyzete Irakban, „korszakváltás" a vatikáni diplomáciában; Szakmai Szemle, 2015/3. pp. 54-72.
- WAGNER, Péter – SZALAI, Máté (eds.): A többség-kisebbség dinamika szerepe a közel-keleti konfliktusokban; 2019. www.kki.hu/wp-content/uploads/2019/07/0726_kki_mena_tanulmanykotet_fin.pdf (downloaded 02 March 2021)

Legal references

- Act CXX of 2018 on the "Hungary Helps Program". Published on 20 December 2018.
- Government Decree 244/2017. (VIII. 28.) on the Hungary Helps Program.
- Government Resolution 1162/2017. (III. 27.) on supporting Christians suffering from persecution in the Middle East region.

TIBOR SZILVÁGYI PHD.

MILITARY UNMANNED AERIAL SYSTEMS AND THE NEW PARADIGM OF THE WARFARE

Abstract

Unmanned and remotely piloted vehicles (commonly referred to as drones) are typical representatives of our current digital and robotic age. The collaboration between people and machines often becomes remote and indirect due to several specific communication networks. The aviation science should increasingly lean on unmanned aerial vehicles (UAVs) since they enhance the sensing capabilities of their manned counterparts and usually save human nerves and lives. The main task of the remotely piloted aircrafts is to carry payloads to the application scene where they accomplish their monotonous or dangerous mission. Military UAVs take part in combat, combat support and combat service support activities and provide usually a cost-effective and sustainable solution for special operations. They are creating a good platform for innovative applications, environment-friendly alternative or hybrid propulsions, modern communication, artificial intelligence, cyber-attack or cyber-security and network-based command and control. With their disruptive features military UAVs are able to change the paradigm of the warfare in the medium term or at least in the long run. This publication is going to describe and forecast the unmanned aerial vehicles' expected effects on the necessarily changing paradigm of the warfare.

Keywords: unmanned aerial vehicle (UAV) and unmanned aerial system (UAS), remotely piloted aircraft system (RPAS), military application, internet, cyber, artificial intelligence, cost-effectiveness, environment-friendliness, sustainability, paradigm, warfare

1. Introduction

The ancient Roman aphorism declares: "If you want peace, prepare for war." (*"Si vis pacem, para bellum.")*. The foresight and preventive thinking have helped peoples to avoid a plenty of uncertainties and tragedies for centuries. This is the timeless essence of the art of military strategy and warfare. In order to counter or avoid any military assault, attack or offensive against us, our ISTAR (Intelligence, Surveillance, Target Acquisition and Surveillance) forces should get to know the foe's will, capabilities and warfare method. Every military activity begins with intelligence and continues with analysing and evaluating the information flow. Thanks to the quick development of the electronics, informatics and robotics nowadays it seems to be evident that machines, software and robots step by step substitute people and they are able to make 4D (dull, dirty, dangerous and dear)[1] tasks automatically. In the future

[1] MARR, Bernard: The 4 Ds of Robotization: Dull, Dirty, Dangerous and Dear; https://www.forbes.com/sites/bernardmarr/2017/10/16/the-4-ds-of-robotization-dull-dirty-dangerous-and-dear/?sh=43eeef363e0d (downloaded: 20 February 2021)

software defined solutions should be dominant against hardware since a constant development process needs a quick and essential reprogramming (a new firmware) that would be much more difficult, costly and time-consuming in case of a hardware change than modifying the software.

Manned vehicles are still more widespread than unmanned ones but the tendency is pointing inevitably in the unmanned direction. It seems that soldiers are not replaceable but, in the future, we should imagine that military machines will be able to make decisions with the help of their humanlike features and capabilities. Researches on Artificial Intelligence (AI)[2] and its subsets, Machine Learning (ML)[3] and Deep Learning (DL)[4] are aiming to make machines able to have and use cognitive capabilities.

The current digitalisation and spreading software defined solutions will demand a completely new military way of thinking and warfare concept that will be much more electronic in the future. In this new digital environment remotely piloted or controlled vehicles and weapons get more and more sophisticated role since a human being (the soldier) remains the highest value who should be protected at all costs. The SARS-CoV-2 virus and the COVID-19 pandemic have accelerated the digital change and the expansion of the robotics in all over the world and this phenomenon will create new amendments in the military science and aeronautics, too.

Information Technology (IT) has reached an unbelievable dimension and has provided a special offer that basically modifies our artificial environment. The internet using has become extremely common and this medium has opened the whole world for us offering a nearly unlimited knowledge source and new communication opportunities. The so-called disruptive technologies[5] fundamentally amend our earlier habits and practice. With remotely piloted aircraft systems (RPAS) we are able to substitute manned helicopters and airplanes in several cases.[6] Smart application of disruptive technologies in the future will be a basic requirement of a successful military mission or battle as well.

---

2 Artificial intelligence (AI): The ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. COPELAND, B. J.: Artificial intelligence; https://www.britannica.com/technology/artificial-intelligence (downloaded 28 February 2021)

3 Machine learning (ML): In AI it is a discipline concerned with the implementation of computer software that can learn autonomously. HOSCH, William L.: Machine learning; https://www.britannica.com/technology/machine-learning (downloaded 28 February 2021)

4 Deep learning (DL): It is an AI function that imitates the workings of the human brain in processing data and creating patterns for use in decision making. DL is a subset of ML. HARGRAVE, Marshall: What Is Deep Learning? https://www.investopedia.com/terms/d/deep-learning.asp (downloaded 28 February 2021)

5 Disruptive technology is an innovation that sweeps away the systems or habits it replaces because it has attributes that are recognizably superior. SMITH, Tim: What Is Disruptive Technology? https://www.investopedia.com/terms/d/disruptive-technology.asp (downloaded 28 February 2021)

6 MARTIN, Guy: Drones as a Disruptive Technology; https://defense.info/partners-corner/2018/11/drones-as-a-disruptive-technology/ (downloaded 20 February 2021)

Renewable energy consume is getting more and more popularity since using them we might be able to slow down – or probably once even stop – the overuse of the Earth's energy resources. The growing ecological footprint has caused irreversible damages in our nature and on our Planet so the scientifically developed countries and relevant international organisations have decided to achieve a so-called sustainable economic development. This objective should be taken into consideration in other fields, for example in the military, too. The use of the remotely piloted aircrafts is a good example since these aerial vehicles many times offer a much more economical solution than its manned versions do.

Modern Armed Forces have to take into consideration the current phenomena in IT and robotics sector. Usually, military technology is overtaking the civil one but nowadays – on the contrary to the practice in the 20th century – in several cases fresh civilian inventions, modern applications and forward-looking methodologies appear in military adaptations only later on. This is the reason why the innovation in the military science should deal with AI, ML, DL and Autonomous Machines (AM)[7] concepts usable in weapon systems and armed vehicles.

Sometimes the most modern, sophisticated and enhanced weaponry system fail in an asymmetrical warfare[8] situation, so traditional and modern weapons still should be kept in parallel usage. In this hybrid application autonomous weapons and unmanned vehicles are gaining more places in the new concept of a modern warfare. Old methods should be used in new forms.

2. New approach to the unmanned aerial vehicles' application

Drone technology is evolving at a very fast pace and it has an increasing potential to compete successfully with more traditional alternatives in a number of sectors. These include research, observation and monitoring, nature conservation, agriculture, emergency response for humanitarian action and civil protection, leisure, competitive sports, tourism and cultural heritage, cinema and photography.[9]

UAVs' application options have a truly wide range. The hobby, the commercial and the state-owned (public service) use is basically different from each other. Probably the commercial UAV is the most versatile and most dangerous since it has the most interactions with common people, customers and outsiders. Hobby UAVs have a low price, a small size and limited capabilities so these are less but even dangerous in comparison with the commercial one. The state-owned UAVs (military,

---

7 Autonomous Machine (AM): A machine that operates on its own and is not tethered to a control system either wired or wireless; https://www.pcmag.com/encyclopedia/term/autonomous-machine (downloaded 12 March 2021)

8 Asymmetrical warfare: The military capabilities of belligerent powers are not simply unequal but are so significantly different that they cannot make the same sorts of attacks on each other. https://www.britannica.com/topic/asymmetrical-warfare (downloaded 03 March 2021)

9 European Environment Agency: Delivery drones and the environment; https://www.eea.europa.eu/publications/delivery-drones-and-the-environment p. 2. (Downloaded 03 March 2021)

police, law enforcement, disaster management, custom etc.) are the safest since these up-to-date aerial vehicles are guided and controlled by selected and trained professionals. Today Unmanned Aerial Systems (UASs) are rapidly becoming a part of our everyday life. They are increasing in numbers and complexity that is shown in statistical data as well. According to the Federal Aviation Administration (FAA) 868 804 (372 157 commercial and 496 647 recreational) drones were registered and 218 847 remote pilots were certified in the United States until 22nd of March 2021.[10]

UAVs are applied in the airspace that is limited and shared with other participants of the air traffic that is controlled by a designated organisation (in Hungary by the HungaroControl) and supervised by the aviation authority. HungaroControl is responsible for the Unmanned Traffic Management in Hungary as well that is available through the mydronespace application.[11] The airspace surveillance (air defence) belongs to the military tasks.

Similar to the airspace using of the frequency spectrum (electromagnetic wave range) is limited, too. In Hungary the National Media and Infocommunications Authority is responsible for the determination of the use of different frequency bands, issuing radio licences as well as the territorial and time limit of their application. The control of a UAV is usually secured by a radio frequency (RF) data link that provides a safe connection between the operator's ground control station and the UAV. If a frequency band was not a subject to authorisation (for example in case of ISM[12] radio bands), customers would be allowed to use them with a limited performance radio.

After a long preparation period the regulation of the use of UAVs in the European Union was revealed in the spring of 2019. The *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems*[13] and the *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft*[14] unambiguously restrict the use of commercial and hobby drones on the territory of the EU. It proves that the EU is interested much more in safety and security[15] than in the possible promising industrial and economic impacts expected from many UAV applications. Studies have demonstrated that unmanned aircrafts with a take-off mass of 250 g or more would

---

10 UAS by the Numbers; https://www.faa.gov/uas/resources/by_the_numbers/ (downloaded 25 February 2021)

11 Mydronespace by HungaroControl; https://mydronespace.hu/ (downloaded 28 March 2021)

12 This is a radio spectrum that is reserved internationally for Industrial, Scientific and Medical (ISM) purposes.

13 Document 32019R0945; https://eur-lex.europa.eu/eli/reg_del/2019/945/oj (downloaded 25 February 2021)

14 Document 32019R0947; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0947 (downloaded 25 February 2021)

15 In the aviation science safety and security are different expressions. The main disparity between safety and security is that their threats are coming from different sources. Safety stands for accident avoidance, and security for crime prevention. What's the difference between safety and security? https://www.tuev-nord.de/explore/en/explains/whats-the-difference-between-safety-and-security/ (downloaded 26 February 2021)

present risks to security and therefore UAS operators of such unmanned aircrafts should be required to register themselves and the UAV.[16]

According to the EASA (European Union Aviation Safety Agency) report "EU Regulations 2019/947 and 2019/945 set the framework for the safe operation of drones in European skies (EU and EASA Member States). They adopt a risk-based approach, and as such, do not distinguish between leisure or commercial activities. They take into account the weight and specifications of the drone and the operation it is intended to undertake. EU Regulation 2019/947, which is fully applicable from 30th December 2020, caters for most types of operation and their levels of risk. It defines three categories of operations: open, specific and certified. The open category addresses operations in the lower risk bracket, where safety is ensured provided the drone operator complies with the relevant requirements for its intended operation. This category is subdivided into three further subcategories called A1, A2 and A3. The specific category covers riskier operations, where safety is ensured by the drone operator obtaining an operational authorisation from the national competent authority before starting the operation. In order to get the authorisation, the drone operator is required to conduct a safety risk assessment. In the certified category, the safety risk is so high that certification of the drone operator and the aircraft is required to ensure safety, as well as the licensing of the remote pilot(s). The management of traffic for drones will be ensured through the U-space. It creates and harmonises the necessary conditions for manned and unmanned aircraft to operate safely in the U-space airspace, so as to prevent collisions between aircrafts and to mitigate the air and ground risks."[17]

UAVs in the open category are classified according to their weight in the EU Regulation 2019/945: C0 (under 250 g MTOM[18], in Hungary under 120 g), C1 (under 900 g), C2 (under 4 kg), C3 and C4 (under 25 kg).[19] In the specific category UAVs might be heavier than 25 kg, fly above 120 m from the closest point of the surface of the Earth and be operated Beyond Visual Line of Sight (BVLOS). Certified category UAVs should have among others airworthiness licence and so they are allowed to fly over assemblies of people, to transport people and to carry dangerous goods that may result in high risk for third parties in case of an accident.[20]

Concerning the UAV applications three aspects should be in harmony with each other, namely: legal, technical and safety/security requirements. The EU Regulations 2019/945 and 2019/947 that generally deal with UAVs and their missions provide a

---

16 COMMISSION IMPLEMENTING REGULATION (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (14) and (15); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0947&from=EN (downloaded 28 February 2021)

17 EASA: Civil drones (Unmanned aircraft); https://www.easa.europa.eu/domains/civil-drones-rpas (downloaded 28 February 2021)

18 MTOM: maximum take-off mass

19 COMMISSION DELEGATED REGULATION (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (Annex Part 1-5.); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN (downloaded 28 February 2021)

20 COMMISSION IMPLEMENTING REGULATION (EU) 2019/947 op. cit.

detailed determination concerning the legal frames, the technical provisions and the safety/security aspects. The registration of the operator and the UAV, the UAV liability insurance, the operators' training and their exam as well as the notification of the requested airspace all together create a good base for a legal and safe/secure UAV operation. The EU's UAV regulations provide a general framework for the integration of the remotely piloted aircrafts into the whole air traffic system. The same objective is set by the European Defence Agency (EDA) i.e., the integration of military RPAS in non-segregated airspace in the context of the Single European Sky (SES).[21]

According to the EUROCONTROL's[22] statement "UAS operations are becoming more frequent and these new airspace users need to be integrated into the European airspace not just for military purposes, but also for civil, commercial and leisure use. EUROCONTROL and its partners want to ensure that European busy skies are safe and accessible to all and they are working hard to ensure that manned and unmanned aircraft can operate together in a safe and efficient manner. The overall Air Traffic Management (ATM) system will need to handle low-level urban drone operations, high-flying military remotely piloted aircraft systems and the traditional mix of airlines, military, business and private jets. Most military UAS operations in Europe are currently restricted to segregated airspace or they are flown at very high flight levels, or alternatively over the sea. EUROCONTROL and its partners have developed specifications for the harmonisation of air traffic control procedures for military RPAS flying in peacetime as Operational Air Traffic, both within and outside controlled airspace."[23]

The use of UAVs is a dangerous and risky mission, especially in a case of a rogue intention. An unintentionally or intentional loss or fly away of a UAV might cause not only material damages but serious moral (psychological) injuries as well. Everybody should respect others fundamental rights and privacy. Misuse of UAVs is not allowed since it might violate the personality rights by taking photos or making videos from others' private sphere or properties. The complete UAV law and its proper regulations are inevitably important in order to avoid injuries, accidents and tragedies in the air traffic and on the ground.

3. Unmanned aerial and space carriers

UAVs are mainly remotely piloted and autonomous aerial carriers, which transport their payloads to the application scene. The payload is a device that is not taking part in the control or movement of the UAV but this is the most important tool for accomplishing the mission of the flight activity. Payloads are multifarious and probably the appliances that operate with (send or receive) electromagnetic waves

---

21 RPAS and RPAS Air Traffic Integration (RPAS ATI); https://eda.europa.eu/what-we-do/all-activities/activities-search/remotely-piloted-aircraft-systems---rpas (downloaded: 17 March 2021)

22 EUROCONTROL (European Organisation for the Safety of Air Navigation) is a pan-European, civil-military organisation dedicated to supporting European aviation. https://www.eurocontrol.int/about-us (downloaded 28 February 2021)

23 EUROCONTROL: Unmanned aircraft systems; https://www.eurocontrol.int/unmanned-aircraft-systems (downloaded 28 February 2021)

(radars, LIDAR[24], multispectral sensors, cameras etc.) are the most widespread and applied ones on the board of an ISTAR UAV. Even a communication installation might be a payload if it was not supporting the own data link. In this case the UAV carries a radio relay or repeater station in order to extend the telecommunication range. In military use it is more and more general that a UAV carries weapons or explosive devices in order to protect itself or attack the enemy. These UAVs are more intelligent than the self-guided rockets or missiles since these remotely piloted aircrafts safely come back to their operators after finishing their mission. In the future we will see plenty of new applications among others the logistic UAVs that will be able to transport resupply, weapons, life support equipment and medicine or troops (soldiers) at the end.

Thanks to its special structure and function, usually there are no persons on the board of the UAV. However, we have to get used to the fact that in the future passengers will sit in UAVs' cabin in order to be quickly transported to a certain short-distance terminal. We are dynamically approaching to the time when UAVs will carry people without a pilot on the board. The Chinese EHang Autonomous Aerial Vehicle (AAV) is only one of the numerous examples. The eco-friendly and intelligent EHang AAV provides low-altitude, short-and-medium-haul transportation solution for the future. Its main features are: maximal payload is 220 kg; range with maximal payload is 35 km and maximum speed is 130 km/h.[25] Remotely controlled or/and self-guided fellow vehicles are functioning mostly in test phase on the surface (self-guided cars, trucks, trains) and under the surface (self-guided tube, metro) but they are really promising. The Hungarian ZalaZone test track in Zalaegerszeg is worth mentioning that provides validation test opportunities for autonomous and electric vehicles.[26]

Figure 1: Chinese eVTOL-maker EHang Files for $100M Nasdaq IPO[27]

[24] LIDAR: Light detecting and ranging. It is a method for measuring distances by illuminating the target with laser light and measuring the distance between the sensor and the aimed item.

[25] EHang AAV (Autonomous Aerial Vehicle); https://www.ehang.com/ehangaav (downloaded 12 March 2021)

[26] Zala Zone; https://zalazone.hu/introduction/ (downloaded 28 March 2021)

[27] Source: https://www.aviationtoday.com/2019/11/04/chinese-evtol-maker-ehang-files-100m-nasdaq-ipo/ (downloaded 17 March 2021)

A bit expanding the topic of this paper I would like to mention satellites that are quite close to UAVs concerning their special tasks. Both (UAVs and satellites) can cooperate and work together in a common mission where the airspace and the outer space are connected. Satellites are (similarly to the UAVs) remotely controlled payload carriers (but flying in an excursive environment) that move according to the mission's requirements and transport the payload to the right place. Satellites with their carriers (missiles, space planes or spaceships) fly through the airspace to their mission's application territory. In the future even UAVs might help satellites in reaching their orbit (workplace).

RAVN-X UAV is a rocket-launching drone designed to send small satellites to orbit. Aerospace start-up Aevum unveiled the first flight-ready model in December 2020. After flight testing the system's first mission is planned in 2021 for the U.S. Space Force. The UAV takes off from a regular runway, climbs high in the atmosphere, and releases a small rocket that continues spaceward and unleashes satellites weighing between 100 and 500 kilograms. The system is autonomous and requires none of the costly infrastructure.[28]

Nowadays the use of satellite supported remote sensing, telecommunication and navigation systems are inevitably important for a successful military operation. The new warfare's success is depending on them, too. The LEO (Low Earth Orbit) satellite automatic remote sensing is able to predict and foresee terrestrial changes and risks. The GEO[29] and GSO[30] satellite telecommunications are ready to bridge huge distances that are directly not bridgeable on Earth or in the air space since their enormous signal loss or missing line of sight. The MEO (Medium Earth Orbit) satellites are mainly responsible for Global Navigation Satellite System (GNSS) positioning tasks. There are four independent global positioning systems and two additional regional solutions. The global systems are: the American Global Positioning System (GPS), the EU's Galileo, the Russian GLONASS and the Chinese BeiDou (earlier known as Compass). The regional systems are: QZSS (Japan) and IRNSS–NAVIC (India).[31] They provide real time positioning data for navigation on the Earth and in the airspace.

The outer space provides a plenty of new satellite service opportunities that are important in our everyday life and for military (defence) purposes, too. In May 2019 Elon Musk's SpaceX Company launched to plant tens of thousands of LEO miniature Starlink satellites, a so-called "megaconstellation" that will bring internet coverage to the entire Planet in the coming years.[32]

---

28 Rocket-launching drone ready to take satellites into orbit; https://www.sciencemag.org/news/2020/12/rocket-launching-drone-ready-take-satellites-orbit (downloaded 28 February 2021)

29 GEO: Geostationary Orbit. Object in GEO matches the Earth's rotation and it orbits only the Earth's equator.

30 GSO: Geosynchronous Orbit. Object in GSO has an orbital speed that matches the Earth's rotation, yielding a consistent position over a single longitude.

31 CHOUDHARY, Mahashreveta: What are various GNSS systems? Geospatial World; 20 Nov 2019; https://www.geospatialworld.net/blogs/what-are-the-various-gnss-systems/ (downloaded 19 March 2021)

32 SpaceX's Starlink satellite megaconstellation launches in photos; https://www.space.com/spacex-starlink-satellite-megaconstellation-launch-photos.html (downloaded 28 February 2021)

Remotely piloted aircrafts can find their role in satellite communication as repeaters or relays for radio systems in an obstacle's shadow (where line of sight does not exist) as well. Thanks to its fast development, telecommunication has made possible for decades that tactical and strategic commanders get more and more real information about the battlefield. Conventional wars are extremely fluid, especially when time counts the most. Air strikes at strategic targets require battle situation assessments in minutes or hours. With the presence of precision munitions, reliable information has become essential to plan and order air strikes. Turning the data into information and getting the information widely distributed to the troops in the field is absolutely necessary. Information gathered by different tools should be protected otherwise the whole integrated information system and its capability would be unveiled.[33] It is an eternal dilemma, what the maximal piece of information is that might be disseminated about a UAV supported mission in order to avoid the disclosure of its information resources, electronic inputs and new military capabilities.

Summarising this chapter, with their special features satellites are mainly applicable for long-time strategic military missions and static observation while UAVs are mostly suitable for supporting short-time and dynamic military operations.

4. Military use of remotely piloted aerial vehicles

In military science one requirement is surely timeless namely the surprise effect of an offensive that can possess a strategic and a technical characteristic as well. In the next couple of years strategists, military commanders and decision makers should prepare for an unrestricted battlespace that spreads from the deep waters till the outer space. New modern battles will be coupled by cyberattacks, using the space-based systems, disinformation campaigns, special operations, espionage, and multitude of kinetic and non-kinetic attacks against troops and critical infrastructure. In order to save human lives, it makes sense to have robots in dangerous areas and remotely controlled C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Surveillance) systems in front of soldiers to enhance the Situational Awareness (SA). The human-machine collaboration will be inevitable in the future warfare and the form of control will move from human control of robots (human decides – known as human in the loop, HITL) to human commands of robots (human orders robots and robots decide the rest until they are stopped – known as human on the loop, HOTL).[34]

UAVs are flying robots controlled and commanded by people. Their main advantage is the stealth capability that can be successfully used during a military attack. The surprise effect can be enhanced by a swarm application when dozens of UAVs assault the target at the same time. UAVs have appeared first as military aerial vehicles that technically dominate the current advanced UAV market with their professional innovation and special tasks thanks to the various payload opportunities. At the beginning military UAVs have been applied as aerial targets for the Air

[33] FRIEDMAN, George and Meredith: The Future of War – Power, Technology and American World Dominance in the Twenty-First Century; First St. Martin's Griffin Edition: March 1998, p. 325. ISBN 0-312-18100-0,

[34] ANTAL, John: Thinking about the Future Battlespace: A Glimpse at 2035; Military Technology Vol. XLIV Issue 3 2020, pp. 6-9. ISSN 0722-3226

Defence Forces. Later on, UAVs have got their dedicated payloads and platforms and they have become Surveillance (later ISTAR), search and rescue (SAR), transport, mapping, striking, as well as cyber and psychological warfare RPASs. All of them are specific and aim oriented in order to have as little redundancy as possible and to carry out their tasks more precise, much longer and more effective. Some of the main military (defence) UAV applications are described in the next pages.

4.1. Target UAVs – Effective training assets for Air Defence Forces

Target UAVs are unique remotely piloted aircrafts that imitate or simulate real, hostile, mainly attacking manned aircrafts for the training of the regular ground-based air defence units and subunits. It is acceptable that the use of UAVs for training purposes during air defence live firing and combat exercises is much safer, more secure, ecological and sustainable than the application of an expensive conventional (manned) aircraft for example with a towed target imitation. The Hungarian Defence Forces ('Homeland Defence Forces') are committed to use homemade target UAVs during air defence training exercises. Firstly, it supports the domestic UAV design and development; secondly it decreases the foreign dependence and exposure. Concerning the target UAVs for the ground-based air defence systems I would like to mention the recoverable METEOR-3MA aerial target (developed, produced and operated by HM EI Zrt.) that is a fixed wing remotely piloted aircraft having gas turbine propulsion and providing a remarkable radar cross section, thermal image, electronic and optical visibility due to its special payloads (Luneberg lens, smoke, flare etc.).[35]

In the United States' Armed Forces unmanned aerial targets represent a different dimension since dozens of the original but retired F-16 fighter jets are converted to QF-16 remote-controlled and unmanned target aircrafts that take off and land with their autopilot and many times survive the missile attacks thanks to the diverted and self-destroyed missile before the impact (hit). QF-16 aerial targets are used for the purpose of testing newly developed weapons and tactics. The QF-16s are replacing the existing QF-4 fleet, and provide a higher capability, a fourth-generation aerial target that is more representative of today's targets and threats. The QF-16 program offers a better training opportunity for fighter jet pilots since they can practice air-to-air battle skills, radar intercepts, tactics and targeting against a strongly manoeuvring opponent that owns all the features of a fourth-generation fighter.[36]

[35] METEOR-3MA target unmanned aerial vehicle; https://www.hmei.hu/en/research-and-development/ (downloaded 28 February 2021)

[36] QF-16 Full-Scale Aerial Target; https://www.boeing.com/defense/support/qf-16/index.page (downloaded 28 February 2021)

Figure 2: First unmanned QF-16 flight takes place[37]

As it is usual in other cases, a UAV becomes target UAV by its payloads. According to the QinetiQ Group Public Limited Company's website the current Banshee unmanned aerial targets might be equipped with radar signal reflectors, active radar homing emulators, passive radars, sense-and-avoid radars, smoke tracking flares and IR (infrared) flares, IR Hot Nose (Forward Infrared Emitter), Acoustic and Radar MDI (Miss Distance Indicator) Scoring varied by plug-in modules and they are suitable for use against surface-to-air and air-to-air weapon systems.[38] Summed up, wraith UAVs might be used as sustainable training assets or effective decoys as well, so they are able to distract the enemy's attention from the real striking forces that will be protected and saved while adversary air defence forces will waste their expensive capabilities and capacities.

4.2. ISTAR UAVs – Extended and tireless "sense organs"

Intelligence (Surveillance) is an ancient profession that has been originally made by people (human intelligence or HUMINT). The appearance of the machines in the 19th century did not superseded people since that time vehicles were not able to work alone. Large troops and huge mechanised forces were fighting their endless battles until the end of the Second World War. In the second half of the 20th century however, the development of the electronics, informatics and robotics has slowly made mass armies less important in operations. Modern weapon systems and methods have demanded a more complex aerial Surveillance system that has gained a special attention in the battle management. The air superiority realised by the expedition forces has made possible that the enemy was supervised and observed from a distant aircraft, quasi hidden in the air. Modern radars, analogical and later digital cameras and several other sensors have facilitated an automatic surveillance and observation

---

37 Source: https://www.af.mil/News/Article-Display/Article/467196/first-unmanned-qf-16-flight-takes-place/ (downloaded 17 March 2021)

38 QINETIQ Banshee NG; https://www.qinetiq.com/en/what-we-do/services-and-products/banshee-ng (downloaded 28 February 2021)

system. Cameras put on an aircraft have been able to do their job without a permanent handling by the operator or the pilot. The appearance of the UAVs has minimised the human role in the observation operation (surveillance, guarding, weather scout or meteorology) since after programming remotely controlled sensors have become able to fulfil their monotonous tasks alone.

In comparison with the manned aircrafts the biggest advantage of the UAVs is that they are always ready, vigilant and independent from human needs, so their flight time depends mainly on their own propulsion and available energy resource capacity. Strategic High Altitude Long Endurance (HALE) UAVs equipped with ISTAR installations are able to spend their operation time in the air for a few days with observing objects, people and vehicles. These UAVs can perform identification of dynamic change in the battlefield or can track the location of a moving object in real time. The location of the object of interest can be communicated to a weapon system to engage to the target or to the field commander to take appropriate action.[39] Besides the COVID-19 pandemic, illegal migration poses a serious security challenge. ISTAR UAVs are able to successfully detect and track migration and trafficking routes and to deter illegal migrants and criminals from their unlawful activities.

4.3. Search and rescue operations – Dual use humanitarian actions

Search and rescue operations might be necessary even in peacetime and not only in wartime or during a military conflict. In case of a natural catastrophe (earthquake, landslide[40], flood, icing, avalanche, biological, chemical and nuclear contamination etc.) or accidents (industrial, traffic, adventure etc.) rescue troops should seek lost and injured people. UAVs are advantageous again since they are persistent and tireless so with the help of their payloads (for instance day and night vision and thermal imager, radar and other sensors) they can support or accomplish the rescue missions. For the time being UAVs are not able to rescue people alone but with their payloads they can find victims and transport life support equipment or medicine to the scene and they might assist before and during the rescue operation with lightning, video streaming and sampling contamination traces. Their highest limitations are probably harsh weather conditions that usually affect the success of the operation but at least do not danger the pilots' life. The small size, cost-effective and reliable remotely piloted aircrafts (for example the Austrian Schiebel's Camcopter S-100) represent a good alternative with their advantageous payload and capability options. In peacetime these are able to operate safely in aerial territories dedicated to special operations, naturally if their mission was coordinated with manned aircrafts' flights as it was completed during the above-mentioned Norwegian rescue operation.

---

39 PANIGRAHI, Narayan – TRIPATHY, Smita: Design Criteria of a UAV for ISTAR and Remote Sensing Applications; https://link.springer.com/article/10.1007/s12524-020-01249-7 (downloaded 27 March 2021)

40 13 people were rescued from the collapsed houses and the rubble in the first few hours after the landslide hit the small village of Ask, Gjerdrum in Eastern Norway on 30 December 2020.
Europe's largest drone operation after deadly landslide in Norway – 420 missions and 200 hours of airtime – Unique collaboration between drones and helicopters during a massive rescue operation; https://www.uasnorway.no/europes-largest-drone-operation-after-deadly-landslide-in-norway-420-missions-and-200-hours-of-airtime/ (downloaded: 03 March 2021)

Figure 3: CAMCOPTER S-100 UAS Selected for UK Coastguard's First SAR Missions[41]

4.4. Transport UAVs – Combat service support aerial carriers

In order to support the troops in the success of a battle, the logistics and military transportations are essentially important. The military missions' security requirements and cost-effectiveness often motivate the decision makers to use UAVs. In peace- and wartime military transport is equally important so UAVs can carry postal items, medicine and blood or supply materials and weapons to a designated area during non-military and military operations, too. We are familiar with some transport UAV rehearsals (Amazon, DHL, Google[42] etc.) that are at the beginning but successful enough to continue the coming tests. It is obvious that a UAV might use the missing pilot's place and its virtual weight capacity. Troop carrier UAVs still do not exist since the trust index in autonomous or self-guided vehicles is low in the Armed Forces. It can be stated that soldiers are not ready to confide their life directly to machines.

4.5. Mapping UAV – Bringing the battlefield to the table

UAVs are excellent aerial transporters that are able to carry radars, optical and IR devices, LIDAR and multispectral sensors in order to perform its monotonous and dull tasks that are easily plannable, programmable, repeatable and accomplishable. If there is a need for a hidden mission the UAV is the best solution for military mapping as well. There are special mapping UAVs that have tailored solutions, a complex camera system and mapping software with Geographical Information System (GIS). Synthetic Aperture Radar (SAR) is especially suitable for mapping and geographical surface modelling of unknown or long ago explored territories or terrains.

---

41 Source: https://www.unmannedsystemstechnology.com/2020/08/camcopter-s-100-uas-selected-for-uk-coastguards-first-sar-missions/ (downloaded 17 March 2021)

42 DHL beats Amazon, Google with first drone deliveries; https://www.geekwire.com/2014/drone-dhl-amazon/ (downloaded 03 March 2021)

Amazon's Prime Air drone project is a perfect example of how several GIS technologies, AI and drones have come together to create the future of mapping UASs. Amazon is bringing together a few key technologies in modern geographic information science and technology: AI, remote sensing and imaging, photogrammetry and robotics. Advancements in image recognition and ML, along with faster and lighter on-board processors have made it more feasible for autonomous drones to navigate in chaotic environments. These new technology advancements have contributed to enabling drones to be used for a more efficient and comprehensive GIS analysis.[43]

Trimble is a leading provider of precise positioning solutions to the UAV industry that offer continuous mobile positioning and high-accuracy orientation for applications such as navigation, guidance and control of unmanned vehicles as well as mapping and survey from UAVs (Trimble UX5). Trimble provides opportunities for standard autonomous positioning, global differential correction services and precise centimetre level RTK (Real-time kinematic) positioning.[44]

4.6. UCAVs – Remote or autonomous destroying machines

Unmanned Combat Aerial Vehicles (UCAVs) and loitering munitions (aka suicide drones) are the most known striking UAVs that carry weapons or explosive devices. The loitering munition is a UAV that flies to a target according to a programmed flight route with the help of its positioning system and – unless it gets another order – hits the target in a kamikaze way without coming back. The whole UAV will be destroyed so its price and other costs should be much lower than the damage caused by the attack for the enemy. In contrast to loitering munitions UCAVs (weaponised drones) return to its station or operator and they can repeat their striker missions a plenty of time. So, these UAVs might be more difficult and expensive since they are reusable and recoverable. This UAV category might be the most dangerous and harmful military application if it gets into the hands of terrorists, criminals or hostile forces.

The potential use of drones in a terrorist incident or attack against a critical infrastructure and soft targets is a growing concern as the availability of drone technology gets more widespread globally. Terrorist groups might use drones in surveillance activities and delivering CBRN[45] or explosive materials in conflict zones.[46]

At this point it is worth mentioning the nEUROn initiative that is a European program for a UCAV technology demonstrator, conducted by Dassault Aviation as prime contractor under the authority of the French Defence Procurement Agency

---

43 Amazon's Drone Project and GIS; February 23, 2021; https://gis.usc.edu/blog/amazons-drone-project-and-gis/ (downloaded 03 March 2021)

44 Positioning and Mapping Solution for UAVs; https://www.trimble.com/gnss-inertial/unmanned.aspx (downloaded 27 March 2021)

45 CBRN: Chemical, Biological, Radiological and Nuclear

46 Drone technology: security threats and benefits for police focus of INTERPOL forum; 30 August 2018; https://www.interpol.int/News-and-Events/News/2018/Drone-technology-security-threats-and-benefits-for-police-focus-of-INTERPOL-forum (downloaded 27 March 2021)

(Direction Générale de l'Armement – DGA). It heralds tomorrow's defence programs, since it collects expertise from across Europe (France, Italy, Sweden, Spain, Greece and Switzerland). The nEUROn project is designed to validate the development of complex technologies representing all mission systems: high-level flight control and stealth, launching real air-to-ground weapons from an internal bay, integration in the C4I (Command, Control, Communications, Computers and Intelligence) environment, innovative industrial collaboration processes and so on.

Figure 4: nEUROn and Rafale M in flight over Charles de Gaulle aircraft carrier[47]

The aim of the nEUROn programme is to demonstrate the maturity and the effectiveness of many technical solutions (aerodynamics, innovative composite structures, internal weapon bay solutions, low observability and high-level algorithms for automated processes), but not to perform military missions. The main goal is to validate technologies around command and control of a UAV that has a similar size to a combat aircraft, with all back-up modes ensuring necessary safety and security.[48]

Strategic UCAVs are not so widespread until now but equipped with weapons of mass destruction (WMD) they might be more dangerous than a ballistic missile due to their secret launch and hidden movement that is hard to detect, counteract or withstand. In the future the global restriction and control of them will be inevitable in order to avoid their proliferation and their intentionally or unintentionally caused damages. The only good news is that this technology needs a high-level scientific development and knowledge that are available only for great nations. However, the attack against the Saudi-Arabian oil refinery gives cause for concern and provides another sad example for an asymmetrical warfare that is one of the most dangerous and dirty methods.

---

47 Source: https://www.dassault-aviation.com/en/defense/neuron/programme-milestones/ (downloaded 05 March 2021)

48 nEUROn https://www.dassault-aviation.com/en/defense/neuron/ (downloaded 05 March 2021)

A tragic UAV-related incident well describes how dangerous a hostile UAV use might be. On 14 September 2019 twenty delta-winged Iranian UASs were flying to the Aramco Abqaiq oil facility and they hit the critical refinery infrastructure, temporarily halving the oil production. The attack on the Saudi oil complex highlights the urgent necessity of a complex, multilayer counter-UAS (C-UAS) defence solution.[49]

4.7. Cyberwarfare with UAVs – Advanced IT solutions on board

In our modern world the software controls the hardware so it has less and less sense destroying the hardware or the infrastructure in all cases. Currently the cyberwarfare[50] (among others cyber-attacks, cybersecurity and cyber-protection) mission is one of the most important military operation forms. With a relatively small investment and costs we might be able to immobilise the enemy's command and control (C2) network, infrastructure and weapon systems from a relatively long distance. In this regard UAVs might get special dedication to jam and disturb the enemy's cyber capabilities. These aerial cyber warriors might take over the control of C2 systems, networks or smart devices and they can misinform the enemy's decision makers, who might mislead their troops and administration that can cause damages for them and – in an ultimate case – it can lead to their defeat as well.

A characteristic cyber incident happened in December 2011 when the American RQ-170 Sentinel military UAV secretly mapped Iranian suspected nuclear sites but at the end it was hacked and forced to the ground by the Iranian military. American officials said that the drone was lost because of a malfunction.[51]

Nowadays Special Operation Forces (SOF) are using more and more cyber solutions in which allegedly Russians are well ahead as it has been proven in battles in Ukraine. Between 2014 and 2016 Russian Special Forces supposedly applied a software that has exploited vulnerabilities in Signalling System Seven (SS7), which is the protocol site that most of the world's mobile telecommunication providers use. As a result of this hacking, Russian operatives were able to identify and track Ukrainian soldiers and put malware on their personal mobile devices. Russians wanted to undermine Ukrainian soldiers' fighting spirit by sending disinformation (injuries and death reports) from their mobile phones to their loved ones. Russian special operation cyber teams reportedly disrupted Ukrainian UAV operations through attacks on their data links, although whether those were cyber-attacks or more conventional electronic warfare (EW) is less clear.[52] The SOF, Cyber and UAVs are

---

49 ANTAL, John: Smashing the Swarm – The Art of Interdicting Unmanned Aerial Systems; Military Technology Vol. XLIV Issue 5 2020, p. 10. ISSN 0722-3226

50 Cyberwarfare or cyberwar is conducted in and from computers and networks connecting them, waged by states or their proxies against other states. Cyberwar is usually waged against government and military networks in order to disrupt, destroy, or deny their use. https://www.britannica.com/topic/cyberwar (downloaded 05 March 2021)

51 Drone Crash in Iran Reveals Secret U.S. Surveillance Effort; The New York Times, Dec 7, 2011; http://www.nytimes.com/2011/12/08/world/middleeast/drone-crash-in-iran-reveals-secret-us-surveillance-bid.html (downloaded 27 March 2021)

52 DONALDSON, Peter: Cyber-enabled SOF – Considering special operations in the round, it is essential not to focus only on Kinetic aspects; Military Technology Vol. XLIII Issue 12 2019, pp. 52-53. ISSN 0722-3226;

firmly connected with each other in order to conduct non-kinetic operations in Grey Zones (between peace and war). It is important to mention as well, that non-kinetic effects are much more acceptable by the international community and indigenous public opinion, than disruptive kinetic demolitions.

4.8. Psychological warfare with UAVs – A new tool for old methods

Despite the more and more automatized and mechanised Armed Forces the raison d'etre (right to exist) of the psychological warfare is unambiguously well-founded and proven. It exists from the ancient times and it is inevitably important in our current age of robots as well. No one military (armed) conflict will be successfully finished without the right decision of human beings so the psychological attempts to influence their behaviour might be expedient. The simple presence of the UAV might be a form of a psychological warfare or psychological operation (PSYOP) since common soldiers are not able to judge the UAVs' capabilities and power. Attacking in swarms, UAVs can show a much bigger military threat than they represent in the reality. Remotely piloted aircrafts might take part in classical mass information broadcasting service and naturally in spreading misinformation, too. They can drop misleading flyers and leaflets above the territory of the enemy or they can transmit electronic propaganda contents. According to the statement of the RAND Corporation research organisation *"Aerospace power will tend to perform best when the desired outcome involves affecting adversary behaviour rather than seizing and holding terrain."*[53]

UAV operators (remote pilots) are far from the physical armed conflicts so we might think that they are in a safe haven but this is not true. Psychologically they are really close to the military operations; take part in destroying objects and killing soldiers or sometimes innocent people. After some years of engagement, they are threatened to easily catch mental illnesses (among others post-traumatic stress disorder – PTSD) and suffer mainly from sniper's syndrome and "moral injury" caused by psychological and emotional harms as a consequence of the moral dissonance between battlespace and normalcy.[54]

5. Why military UAVs might change the paradigm of the warfare?

The main difference between UAVs and manned aircrafts is that UAV operators make decisions on the ground while pilots do it in the air, on the board of an aircraft. These are unambiguously different perspectives. The peripheral view of a pilot directly helps perceive the changes in the battlefield and the person can react quickly and accordingly. However, the operator watches only a video stream (camera picture) and gets the telemetric data. It is enough for simple and safe operations but it is not

---

53 DOUGLAS, Maj – JAQUISH, W.: USAF Uninhabited Air Vehicles for Psychological Operations – Leveraging Technology for PSYOP Beyond 2010; https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/jaquish.pdf (downloaded 27 March 2021)

54 HENSCHKE, Adam: Modern soldiers can kill a target on computer, then head home for dinner – and it's giving them "moral injury"; 28 Sep 2019; https://www.abc.net.au/news/2019-09-29/unmanned-combat-drone-pilots-moral-injury-warfare-dissonance/11554058 (downloaded 28 March 2021)

sufficient in case of a complex air combat. This is the reason why remotely piloted aircrafts are still not able to fight air battles "alone" but this is not far from the new warfare imagination that leans on autonomous and AI solutions.

Modern Armed Forces should follow the new trends of the world economy and global society. Cost-effectiveness, security, environment friendliness, sustainability, dual use, counter-UAS and multi-domain operations are inevitably important factors to be considered. There are some interesting aspects why military UAVs are positively contributing to a modern warfare and why their engagement will be important in the near future, too. The following UAS factors detailed in the next pages should be considered substantially since these will certainly influence the new paradigm of the warfare.

5.1. Cost-effective UAV application

UAVs are getting popular mainly due to the miniaturisation of their payloads. That way we can spare not only the life of the pilot but the training and operational costs, too. The lightweight remotely piloted aircrafts need less energy and are much cheaper than the conventional ones. It is not necessary to prove that the requirements and general costs of a UAV operator are less than the expenses of an experienced real pilot on the board. On average UAV operation is much more cost-effective than the flight of a helicopter or a fighter jet. The following data authentically show the cost differences among the below selected aircraft categories. Accounts to which collections are to be deposited for reimbursements for the use of fixed wing and helicopter aircraft in fiscal year 2019 (USD/hour) concerning the US Department of Defense: F-16D (Fighting Falcon) fighter jet: 8274 USD/hour; UH-60A (Black Hawk) helicopter: 4587 USD/hour; MQ-9A (Reaper) UAV: 557 USD/hour.[55]

The example is not perfect since there are a plenty of differences and tiny similarities but it is visible that UAVs are much more cost-effective than manned aircrafts in several cases. If the same task can be performed by a UAV as well, it is recommended to do so.

5.2. Safety first – Security second

Security is the most basic human value. Usually, its presence is not perceptible but its absence is obvious. Why are UAVs more secure and safe than conventional aircrafts? The reason is that operators do not risk their life in air battles, in other military air activities or during dangerous peacetime missions (for example during CBRN challenges or in bad weather conditions). Safety depends mostly on inside but security on outside factors. It can be stated that human life enjoys priority while materials and technics are replaceable. UAVs always "preserve pilots" since operators control their UAVs mainly from a distance in a shelter. Despite of this advantage military UAV operators are not so respected since their general judgement is really negative among real military pilots and especially by the enemy. Operators might be

[55] Fiscal Year (FY) 2019 Department of Defense (DoD) Fixed Wing and Helicopter Reimbursement Rates; https://comptroller.defense.gov/Portals/45/documents/rates/fy2019/2019_b_c.pdf p. 6., 9. (downloaded 28 March 2021)

in trouble during a mission since they are not in direct contact with the air situation and the fast-changing military activities. They easily can commit mistakes and even crime, namely they have only a narrow picture from the camera and do not have peripheral view that might lead to friendly fire or bombing civilian targets.[56]

UAVs are getting safer since electronics, informatics and robotics have made possible to develop reliable microcontrollers, avionics and software packets. Their redundancy provides a safe technical environment and reliable functioning. UAVs might be immune against attacks since they are less detectable and destroyable. They are relatively safe and secure and this is the main requirement for military aerial vehicles.

5.3. Environment-friendly use

A system is environment-friendly if it is as less harmful to our nature as it is possible. In case of an aircraft, the take-off weight is the most important factor that determines the aerial vehicle's effectiveness. Mitigating the weight of the aircraft we could increase the flight time, and we need less energy for taking off and reaching the operational altitude. Among UAVs the electric propulsion is much more widespread than by manned aircrafts. UAVs offer a good platform for rehearsals with electric and solar-electric propulsion as these aircrafts are able to test the limits of this kind of green solution without the risk of human lives.

Zephyr is the world's leading solar-electric stratospheric UAS under development by Airbus with a wingspan of 25 metres and weight of less than 75 kg. With bringing new See, Sense and Connect capabilities to commercial, institutional and military customers Zephyr relies on solar energy, with secondary batteries charged in daylight to power overnight flight. Thanks to its special propulsion, Zephyr's flights are carbon neutral. Its persistence enables a capability of flying continuously for months at a time, at around 70,000 feet, above weather and conventional air traffic.[57]

---

[56] MACASKILL, Ewen: Two US soldiers killed in friendly-fire drone attack in Afghanistan – American soldiers killed in Helmand province by Predator drone after being mistaken for Taliban fighters by US troops; 11 Apr 2011; https://www.theguardian.com/world/2011/apr/11/us-soldiers-killed-in-drone-attack (downloaded 28 March 2021)

[57] Zephyr – Pioneering the Stratosphere; https://www.airbus.com/defence/uav/zephyr.html#introduction (downloaded 06 March 2021)

Figure 5: Zephyr – Pioneering the Stratosphere[58]

Using fossil energy resources by the huge air traffic – not taking into account the current COVID-19 pandemic's positive influence – is unfortunately polluting our air around the Earth and it increases the glasshouse effect and global warming. If we were able to decrease the amount of the polluting materials released into the air by using electric propulsion, we would make a big step towards the protection of the environment, the biosphere and the biodiversity. Today it is unbelievable that once electric military UAVs will fly and fight against each other, however the world is moving in this direction. Someday most probably electric or alternative (fuel cell) propulsion military aerial vehicles will save the environment but the enemy.

5.4. Sustainability and sustainable air operations

Sustainability is defined in 1987 by the United Nations' Brundtland report as it follows: *"Sustainable development is development that meets the needs of the present without compromising the ability of future generations to meet their own needs."*[59] All in all any activity would worth doing if it had much more utility than costs. UAVs might efficiently contribute to sustainable activities. The EU Aviation Safety Regulation 2018/1139 (EASA Regulation) stresses that drones "must be designed" to minimise noise and emissions "as far as possible". Therefore, reductions in emissions will depend on finding ways to diminish the negative impact of extra warehousing, decrease the size of drones and continuously increase the use of renewable energy sources, such as solar and wind power for drone operation.[60] It is acceptable that

---

58 Source: (https://www.airbus.com/defence/uav/zephyr.html (downloaded 17 March 2021)

59 United Nations Report of the World Commission on Environment and Development – Our Common Future; https://www.are.admin.ch/are/en/home/sustainable-development/international-cooperation/2030agenda/un-_-milestones-in-sustainable-development/1987--brundtland-report.html p. 37. (Downloaded 27 March 2021)

60 European Environment Agency: Delivery drones and the environment; op. cit. p. 4., 6.

electromobility and electric vehicles have good influence on the sustainability so UAVs – that are in many cases electric ones – might support this widely accepted and desired trend, too. Current rehearsals aim to develop effective solutions for storing larger capacity electrical energy and charging it back quickly (solid-state battery). New hybrid propulsions (conventional combined with solar energy) are to be used soon since above the clouds the sunshine is dominant. Hydrogen cells and other innovative solutions are making such new technologies that will obviously strengthen the sustainability, partially thanks to the UAVs. Seeing the beneficial role of UAVs, the question of the Armed Forces' sustainability might be raised and answered as soon as possible, too.

Nowadays the aviation sector supports long-term climate goals. International Air Transport Association (IATA) member airlines and the wider aviation industry are collectively committed to ambitious emissions reduction goals. Instead of seeking for new aircraft propulsion solutions Sustainable Aviation Fuel (SAF)[61] has been identified as one of the key elements in helping to achieve environment protection goals. Sustainability, in the context of SAF, may be broadly defined as conserving an ecological balance by avoiding depletion of natural resources. In 2021 about 100 million litres of SAF will be produced. More than 45 airlines now have experience with SAF and around seven billion litres of SAF are in forward purchase agreements. SAF might reduce emissions up to 80% during its full lifecycle.[62]

In 2010, the 37th Session of the International Civil Aviation Organization (ICAO) Assembly adopted two aspirational goals:

- to improve energy efficiency by 2 per cent per year until 2050, and
- to achieve carbon neutral growth from 2020 onwards.

These goals are to be met with technological innovations, operational improvements, sustainable aviation fuels, and market-based measures. At the 39th Session of the ICAO Assembly in 2016, States adopted a global market-based measure scheme for international aviation in the form of the Carbon Offsetting and Reduction Scheme for International Aviation (CORSIA), to address the increase in total CO_2 emissions from international aviation above the 2020 levels (Assembly Resolution A39-3). The international civil aviation sector (that presently accounts for about 1.3% of the global CO_2 emissions) plays a key role in the global efforts to address climate change.[63]

---

61 Sustainable aviation fuel meets the requirements of a standard aviation fuel while its production is sustainable.

62 Developing Sustainable Aviation Fuel (SAF); https://www.iata.org/en/programs/environment/sustainable-aviation-fuels/ (downloaded 17 March 2021)

63 Introduction to CORSIA; https://www.icao.int/environmental-protection/Documents/EnvironmentalReports/2019/ENVReport2019_pg207-210.pdf (downloaded 17 March 2021)

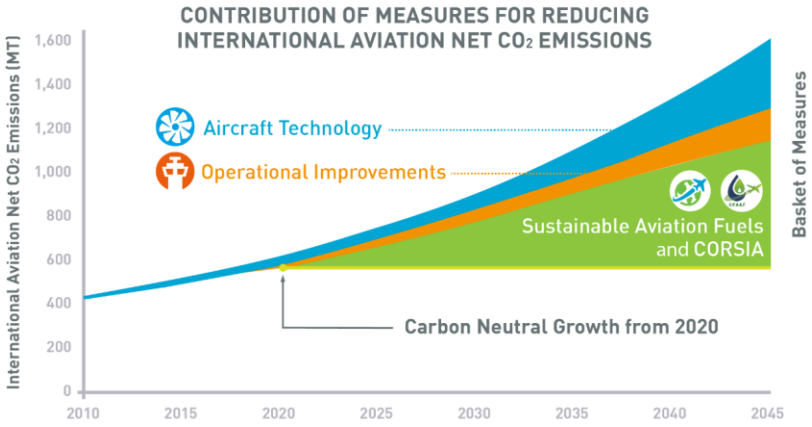

Figure 6: ICAO Global Environmental Trends on CO_2 Emissions and Contribution of Measures for Reducing International Aviation Net CO_2 Emissions[64]

In calendar year 2019, the aviation industry carried more than 4.5 billion passengers, producing roughly 2% of global manmade carbon emissions. Effective action on reducing carbon emissions is essential to ensure the sustainable development of the industry. Companies across this sector are collaborating to reduce emissions through a matrix of measures. These include:

- New Technology (fleet modernisation and the potential future electrification of smaller aircrafts);
- Efficient Operations (lighter on-board materials, fuel saving improvements such as winglets);
- Improved Infrastructure (improved air traffic management, reduced queues on the runway);
- Global Market-Based Measure (CORSIA);
- Sustainable Aviation Fuel (SAF).

IATA believes that the more substantive reductions in net CO_2 from aviation will have to come from sustainable aviation fuels.[65] UAVs might contribute to these efforts by their advantageous application features.

5.5. Dual use opportunity

UAVs are dual use aerial vehicles. They are suitable for military and civilian purposes or for good and hostile goals. The military function is quite complicated since it can be offensive and defensive as well. In addition to this, Armed Forces

[64] Source: (https://www.icao.int/environmental-protection/Documents/EnvironmentalReports/2019/ENVReport2019_pg207-210.pdf (downloaded 17 March 2021)

[65] IATA Fact Sheet 4: Strategic Direction – The Wedge Chart; https://www.iata.org/contentassets/d13875e9ed784f75bac90f000760e998/saf-the-wedge-chart.pdf (downloaded 17 March 2021)

should prepare for the counter measures of hostile UAVs as well. Some years ago, terrorism finally found UAVs as a dirty tool for their hostile activities. In this case rules and laws are not representing any deterrent effect since terrorists and criminals are using drones for their illegal activities. Even commercial UAVs in hands of criminals or terrorists are able to make huge damages with their improvised explosive devices or weapons, so critical infrastructure should be defended by any countermeasure that is available.[66]

Fortunately, the dual use of UAVs has a good side, too. Outer military challenges UAVs are well applicable during natural and industrial catastrophes or accidents. These aerial vehicles might provide support in case of forest fires, floods and earthquakes, so they will not be idle during a peacetime. The UAVs' activity can be utilised by the right meritorious payloads.

5.6. C-UAV versus UCAV

UCAVs are enormously dangerous thanks to their relatively small size, hidden application, low electronic signature and stealth technology. It is worth analysing how to fight against rogue UCAVs that may cause damages in our military troops and equipment. There are several theoretical methods how to counter UCAVs but until now there is no one that is a perfectly reliable tool to realise perfect anti-UAV struggles. The best solution is to use a combined method that consists of observation, Surveillance, detection, identification, jamming, spoofing and destroying of hostile UAVs. The Surveillance should involve visual, audio, radar, thermal imager, multispectral and HUMINT proceedings.

Counter-UAS (C-UAS) technology has been proved several times that it is unable to completely counter the new types of UAV threats. There are C-UAS systems that are effective against hobby drones or against military-class UAVs but there is no one to counter all the different categories. Probably the best solution would be to take a "layered approach", integrating different detection and mitigation systems into a single network, but this is an extremely expensive (sometimes asymmetrical) answer to the problem. The whole countermeasure might be divided into two parts:

- Detection, tracking and identification: radar, radio frequency (RF), electro-optical (EO), infrared (IR), acoustic and combined sensors;
- Interdiction: RF jamming, GNSS jamming, spoofing, dazzling, laser, high power microwave, nets, projectile, collision drone and combined interdiction elements.

These technologies have been miniaturised, integrated and ruggedized, allowing deployment on light (unmanned) vehicles or incorporated into individual soldier's kits. Experts believe that AI, ML and effective lightweight countermeasures will be available soon in order to fight against UCAVs, too. However, drone swarm attacks and other more intelligent UAV technologies (programmed for more autonomy without satellite navigation and RF communication) might highlight new technical

[66] FALK, Thomas O.: How drones have added a new dynamic to conflicts – Drones have become the means of the first choice in modern warfare and are used by state and non-state actors; 20 Feb 2021; https://www.aljazeera.com/news/2021/2/20/how-drones-have-added-a-new-dynamic-to-conflicts (downloaded 28 March 2021)

and operational fallibilities and challenges. C-UAS systems engaged in a complicated EW environment have to cope with RF interference or radar detection shortages. Radar could not always detect UAVs, especially in the loitering phase, where zero Doppler effect causes a detection problem. It is an impossible hard task to identify UAVs as cooperative or non-cooperative drones.[67]

An effective C-UAS should rapidly detect, locate, track, identify and defeat the UAV threat. This task is increasingly difficult since UAVs become smaller, smarter and stealthier. After the detection, countering of the UAV can be carried out by soft- or hard-kill approaches. Soft-kill means for example an EW, a high-power microwave (HPM) device generating an electromagnetic pulse (EMP), or a cyberwarfare system to interdict or control the UAV. Hard-kill means physically destroying of the UAV mainly with kinetic munitions. Combining these methods provides a layered, more effective C-UAS defence.[68] HPM can kill swarms of drones, disabling their electronic circuits, rather than simply jamming the communication frequencies. The using of Non-lethal Weapons (NLWs) is aimed to avoid unnecessary incidental and collateral damages.[69] These new C-UAV methods basically will amend the paradigm of warfare.

5.7. Multi-Domain Operations

Many strategists forecast that the new battlefield in the future will be relocated to the cyberspace. Other experts state that in 20 years the warfare will be hyper-accelerated in some places in the world. Networked smart weapons and munitions are becoming increasingly intelligent since Long Range Precision Fires (LRPF) and Multi-Domain Sensor Networks (MDSN) will dominate the new battlespace. EW, cyberwarfare and MDSNs synchronised and optimised by an AI neural network together with connected weapon systems will create a weaponised Internet of Things (IoT), i.e., an Internet of Weapons (IoW). This super-fast "kill-web" will increase lethality that has two important capabilities: masking and multi-domain convergence. Masking (that can be an active and a passive ability) makes military systems difficult or impossible to identify so it is more than camouflage and stealth. It reduces the electronic signature and renders the system difficult to locate and hard to target with using cognitive EW methods, employing ML and confusing the enemy's targeting system with false readings. Multi-Domain Operations Convergence (MDOC) is becoming a new combined arms doctrine. The US military defines convergence as the rapid and continuous integration of capabilities in all domains. By 2040, MDOC will be MDO Fusion (MDOF) and defined as the rapid and continuous integration and synchronisation of multi-domain capabilities by an AI neural network. Masking is the shield and MDOF will be the sword.[70] This new concept will relatively fast create and continuously provide a kind of superiority and manoeuvrability. UAVs naturally will

---

67 BUTTERWORTH-HAYES, Philip: AI Changes the C-UAS Game; Military Technology Vol. XLIV Issue 5 2020, pp. 13-16. ISSN 0722-3226;

68 ANTAL: Smashing the Swarm – The Art of Interdicting Unmanned Aerial Systems; op. cit.

69 ANNATI, Massimo: Less Lethal Review – Non-Lethal Weapons have an important role in the majority of current operations; Military Technology Vol. XLIII Issue 12 2019, pp. 33-34. ISSN 0722-3226

70 ANTAL, John: Masking, Convergence and Multi-Domain Operations Fusion – An Internet of Weapons on the Battlefield by 2040; Military Technology Vol. XLIV Issue 6 2020, pp. 12-14. ISSN 0722-3226

take part in masking and multi-domain operations with their ISTAR, EW and fire manoeuvre capabilities.

6. Summary

Our world narrows and broadens at the same time since remote controlled machines bring the faraway phenomena closer to us but simultaneously, we realise how many things are unknown for us and it increases our curiosity and desire for further knowledge again. The technological advancement of UAVs is interestingly supported by not only the always increasing and enhancing military requests and requirements but the limitless new ideas of the civilian use. With revealing of new disruptive technologies such opportunities are becoming available that might revolutionise aeronautics and transcend its current limits. The biggest burden of the further development of the manned vehicles is the individual itself, as people have physiological and sensory limitations. All the inventions have the aim to extend the human capacity and capability in order to increase our security and survivability. In this objective military UAVs might get an inevitably important role since saving lives is the highest priority.

The last fifty years' economic development has brought us not only the wellbeing of people in Europe but a huge loss of our natural environment that can be reversed only with enormous efforts. Application of UAVs is only a small but important step towards a desired direction when a military operation will be as short and humane as it is possible. It means that in many cases military tools should act (in harmony with international law) only to make the enemy give up its aggression or attacking intent. Preventive methods and soft-kill solutions might dominate future warfare methods in local armed conflicts and military clashes by using military UAVs.

During the Cold War the so-called security dilemma[71] made the arms race (especially the stockpile of nuclear weapons and weapons of mass destruction) contra-productive and enormously dangerous. Nowadays we face a similar situation with electronics, robotics and cyber. Increased use of expensive IT solutions on military purposes can lead to a tilt of the power balance among opponent parties and this phenomenon either launches a military IT race or encourages the weaker party to take the first step with an asymmetrical military action. This example is particularly perceptible in several conflict areas in North-Africa, in the Middle-East and in Central-Asia, where insurgency troops or terrorist groups commit attacks against critical (military) infrastructures, regular defence and security forces or innocent people. Relatively cheap conventional arms are able to destroy high-value modern weapon systems and networks in order to restore the believed military capability balance. Using AI and ML technologies we can reach an IT dilemma situation (modelled on the security dilemma) much earlier.

[71] The security dilemma means that a state increases its own security – by weapons procurement and developing new military technologies – and it causes military response and reaction from other states that can lead to an exaggerated arm race. An excessive arming can break the balance of power that might lead to an insecure situation, a military conflict or war. Security dilemma (international relations); https://www.britannica.com/topic/security-dilemma (downloaded: 19 February 2021)

UAVs are playing a more and more serious and complex role in the current warfare change. During the planning of the future military missions, UAVs' capabilities ought to take into consideration as well. Several examples and precedents have proved that the military success is increasingly dependent on the use of remotely piloted machines, weapons and vehicles. These have a lot of advantages so they are able to accomplish challenging missions for example search and rescue or liquidation operations against terrorists. UAVs use intelligent and innovative solutions, among others AI and ML techniques. The future is much closer than we think, so we should make the fast technical development smarter, otherwise it becomes contra productive since initial results or the sustainability will be endangered by impatience.

As it is characteristic in other cases of our life, short-term and long-term way of thinking (see sustainability and arms race) are always struggling with each other. This dichotomy seems to be irresolvable. Short-term solutions are deteriorative in the long-term since they do not consider all important factors, mainly the timeline and the consequences. In the short-term, states can primarily base their defence system on the human factor but in the future, they have to change it in favour of automatic, remote controlled, robotic and machine-like solutions. Due to limited human capabilities and senses people are not able to compete with computers (see cyber) and machines (see unmanned solutions) so the "mechanisation and digitalisation" of the Armed Forces is well-founded and inevitable. The password of the new trend should be the sustainability that must be clear and unambiguous. New Armed Forces and multi-domain operations should be relatively "green" as other areas of life do, otherwise the gap between the civilian and military world would be moving apart again as it was happening during the Cold War. The task is to find the harmony among human abilities, machine capacities and cyber capabilities in order to work flawlessly together and to increase the confidence of soldiers in machines, among others in UAVs in order to enhance personal, national and global security.

In favour of finding the right paradigm of the new warfare it is really important to launch scientific research programs on the topic of the sustainability of the Armed Forces and to define Strengths, Weaknesses, Opportunities and Threats (SWOT analysis) of the new digital age warfare concepts concerning the civilian society and the defence sector.

Bibliography:

- Amazon's Drone Project and GIS; February 23, 2021; https://gis.usc.edu/blog/amazons-drone-project-and-gis/ (downloaded 03 March 2021)
- ANNATI, Massimo: Less Lethal Review – Non-Lethal Weapons have an important role in the majority of current operations; Military Technology Vol. XLIII Issue 12 2019, ISSN 0722-3226
- ANTAL, John: Masking, Convergence and Multi-Domain Operations Fusion – An Internet of Weapons on the Battlefield by 2040; Military Technology Vol. XLIV Issue 6 2020, ISSN 0722-3226

- ANTAL, John: Smashing the Swarm – The Art of Interdicting Unmanned Aerial Systems; Military Technology Vol. XLIV Issue 5 2020, ISSN 0722-3226
- ANTAL, John: Thinking about the Future Battlespace: A Glimpse at 2035; Military Technology Vol. XLIV Issue 3 2020, ISSN 0722-3226
- Asymmetrical warfare; https://www.britannica.com/topic/asymmetrical-warfare (downloaded 03 March 2021)
- Autonomous Machine (AM); https://www.pcmag.com/encyclopedia/term/autonomous-machine (downloaded 12 March 2021)
- BUTTERWORTH-HAYES, Philip: AI Changes the C-UAS Game; Military Technology Vol. XLIV Issue 5 2020, ISSN 0722-3226
- CHOUDHARY, Mahashreveta: What are various GNSS systems? Geospatial World; 20 Nov 2019; https://www.geospatialworld.net/blogs/what-are-the-various-gnss-systems/ (downloaded 19 March 2021)
- COMMISSION DELEGATED REGULATION (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (Annex Part 1-5.); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN (downloaded 28 February 2021)
- COMMISSION IMPLEMENTING REGULATION (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Article 6), (14) and (15); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0947&from=EN (downloaded 28 February 2021)
- COPELAND, B. J.: Artificial intelligence; https://www.britannica.com/technology/artificial-intelligence (downloaded 28 February 2021)
- Cyberwarfare; https://www.britannica.com/topic/cyberwar (downloaded 05 March 2021)
- Developing Sustainable Aviation Fuel (SAF); https://www.iata.org/en/programs/environment/sustainable-aviation-fuels/ (downloaded 17 March 2021)
- DHL beats Amazon, Google with first drone deliveries; https://www.geekwire.com/2014/drone-dhl-amazon/ (downloaded 03 March 2021)
- Document 32019R0945; https://eur-lex.europa.eu/eli/reg_del/2019/945/oj (downloaded 25 February 2021)
- Document 32019R0947; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0947 (downloaded 25 February 2021)

- DONALDSON, Peter: Cyber-enabled SOF – Considering special operations in the round, it is essential not to focus only on Kinetic aspects; Military Technology Vol. XLIII Issue 12 2019, ISSN 0722-3226
- DOUGLAS, Maj – JAQUISH, W.: USAF Uninhabited Air Vehicles for Psychological Operations – Leveraging Technology for PSYOP Beyond 2010; https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/jaquish.pdf (downloaded 27 March 2021)
- Drone Crash in Iran Reveals Secret U.S. Surveillance Effort; The New York Times, Dec 7, 2011; http://www.nytimes.com/2011/12/08/world/middleeast/drone-crash-in-iran-reveals-secret-us-surveillance-bid.html (downloaded 27 March 2021)
- Drone technology: security threats and benefits for police focus of INTERPOL forum; 30 August 2018; https://www.interpol.int/News-and-Events/News/2018/Drone-technology-security-threats-and-benefits-for-police-focus-of-INTERPOL-forum (downloaded 27 March 2021)
- EASA: Civil drones (Unmanned aircraft); https://www.easa.europa.eu/domains/civil-drones-rpas (downloaded 28 February 2021)
- EHang AAV (Autonomous Aerial Vehicle); https://www.ehang.com/ehangaav (downloaded 12 March 2021)
- EUROCONTROL (European Organisation for the Safety of Air Navigation); https://www.eurocontrol.int/about-us (downloaded 28 February 2021)
- EUROCONTROL: Unmanned aircraft systems; https://www.eurocontrol.int/unmanned-aircraft-systems (downloaded 28 February 2021)
- European Environment Agency: Delivery drones and the environment; https://www.eea.europa.eu/publications/delivery-drones-and-the-environment (downloaded 03 March 2021)
- FALK, Thomas O.: How drones have added a new dynamic to conflicts – Drones have become the means of the first choice in modern warfare and are used by state and non-state actors; 20 Feb 2021; https://www.aljazeera.com/news/2021/2/20/how-drones-have-added-a-new-dynamic-to-conflicts (downloaded 28 March 2021)
- Fiscal Year (FY) 2019 Department of Defense (DoD) Fixed Wing and Helicopter Reimbursement Rates; https://comptroller.defense.gov/Portals/45/documents/rates/fy2019/2019_b_c.pdf (downloaded 28 March 2021)
- FRIEDMAN, George and Meredith: The Future of War – Power, Technology and American World Dominance in the Twenty-First Century; First St. Martin's Griffin Edition: March 1998, ISBN 0-312-18100-0
- HARGRAVE, Marshall: What Is Deep Learning? https://www.investopedia.com/terms/d/deep-learning.asp (downloaded 28 February 2021)

- HENSCHKE, Adam: Modern soldiers can kill a target on computer, then head home for dinner – and it's giving them "moral injury"; 28 Sep 2019; https://www.abc.net.au/news/2019-09-29/unmanned-combat-drone-pilots-moral-injury-warfare-dissonance/11554058 (downloaded 28 March 2021)
- HOSCH, William L.: Machine learning; https://www.britannica.com/technology/machine-learning (downloaded 28 February 2021)
- https://www.uasnorway.no/europes-largest-drone-operation-after-deadly-landslide-in-norway-420-missions-and-200-hours-of-airtime/ (downloaded 03 March 2021)
- https://www.unmannedsystemstechnology.com/2020/08/camcopter-s-100-uas-selected-for-uk-coastguards-first-sar-missions/ (downloaded 17 March 2021)
- IATA Fact Sheet 4: Strategic Direction – The Wedge Chart; https://www.iata.org/contentassets/d13875e9ed784f75bac90f000760e998/saf-the-wedge-chart.pdf (downloaded 17 March 2021)
- Introduction to CORSIA; https://www.icao.int/environmental-protection/Documents/EnvironmentalReports/2019/ENVReport2019_pg207-210.pdf (downloaded 17 March 2021)
- MACASKILL, Ewen: Two US soldiers killed in friendly-fire drone attack in Afghanistan – American soldiers killed in Helmand province by Predator drone after being mistaken for Taliban fighters by US troops; 11 Apr 2011; https://www.theguardian.com/world/2011/apr/11/us-soldiers-killed-in-drone-attack (downloaded 28 March 2021)
- MARR, Bernard: The 4 Ds of Robotization: Dull, Dirty, Dangerous and Dear; https://www.forbes.com/sites/bernardmarr/2017/10/16/the-4-ds-of-robotization-dull-dirty-dangerous-and-dear/?sh=43eeef363e0d (downloaded: 20 February 2021)
- MARTIN, Guy: Drones as a Disruptive Technology; https://defense.info/partners-corner/2018/11/drones-as-a-disruptive-technology/ (downloaded 20 February 2021)
- METEOR-3MA target unmanned aerial vehicle; https://www.hmei.hu/en/research-and-development/ (downloaded 28 February 2021)
- Mydronespace by HungaroControl; https://mydronespace.hu/ (downloaded 28 March 2021)
- nEUROn https://www.dassault-aviation.com/en/defense/neuron/ (downloaded 05 March 2021)
- PANIGRAHI, Narayan – TRIPATHY, Smita: Design Criteria of a UAV for ISTAR and Remote Sensing Applications; https://link.springer.com/article/10.1007/s12524-020-01249-7 (downloaded 27 March 2021)

- Positioning and Mapping Solution for UAVs; https://www.trimble.com/gnss-inertial/unmanned.aspx (downloaded 27 March 2021)
- QF-16 Full-Scale Aerial Target; https://www.boeing.com/defense/support/qf-16/index.page (downloaded 28 February 2021)
- QINETIQ Banshee NG; https://www.qinetiq.com/en/what-we-do/services-and-products/banshee-ng (downloaded 28 February 2021)
- Rocket-launching drone ready to take satellites into orbit; https://www.sciencemag.org/news/2020/12/rocket-launching-drone-ready-take-satellites-orbit (downloaded 28 February 2021)
- RPAS and RPAS Air Traffic Integration (RPAS ATI); https://eda.europa.eu/what-we-do/all-activities/activities-search/remotely-piloted-aircraft-systems---rpas (downloaded 17 March 2021)
- Security dilemma (international relations); https://www.britannica.com/topic/security-dilemma (downloaded 19 February 2021)
- SMITH, Tim: What Is Disruptive Technology? https://www.investopedia.com/terms/d/disruptive-technology.asp (downloaded 28 February 2021)
- SpaceX's Starlink satellite megaconstellation launches in photos; https://www.space.com/spacex-starlink-satellite-megaconstellation-launch-photos.html (downloaded 28 February 2021)
- UAS by the Numbers; https://www.faa.gov/uas/resources/by_the_numbers/ (downloaded 25 February 2021)
- United Nations Report of the World Commission on Environment and Development – Our Common Future; https://www.are.admin.ch/are/en/home/sustainable-development/international-cooperation/2030agenda/un-_-milestones-in-sustainable-development/1987--brundtland-report.html (downloaded 27 March 2021)
- What's the difference between safety and security? https://www.tuev-nord.de/explore/en/explains/whats-the-difference-between-safety-and-security/ (downloaded 26 February 2021)
- Zala Zone; https://zalazone.hu/introduction/ (downloaded 28 March 2021)
- Zephyr – Pioneering the Stratosphere; https://www.airbus.com/defence/uav/zephyr.html#introduction (downloaded 06 March 2021)

VERONIKA DEÁK

FINDING DIFFERENCES ON CYBER SECURITY BETWEEN PUBLIC AND PRIVATE SECTORS

Abstract

Companies, non-profit organizations, and public services are facing large amounts of cyber-attacks every day. An open discussion where the leaders of these sectors can share their ideas, experiences, suggestions, and future plans to improve the state-of-the-art solutions always plays an important role in the field of cyber security.
Seeking answers for questions about incidents, defense strategies and capabilities, training programmes for employees and financial aspects of investing into cyber defense improvements can help to understand the differences and similarities between the public and private sectors and also allows the leaders to integrate solutions from other areas into their processes.
In this paper, I propose a comparison between the public and private sector from the aspect of cyber-security through interviews with chief executives from both sectors. This includes cyber security training for individuals, the implementation of technological developments, the role of financial and strategic decision-making related to cyber security, and the cyber security tools and measures of individual organizations.

Keywords: interview, cyber security, public service, private sector, security awareness

Introduction

Various info-communication technologies are essential components of our modern society. Thus, these tools and technologies are widely spread. Unfortunately, our everyday tasks depend on such tools even more which can pose several risks. Cyber-attacks are carried out on a daily basis to obtain wide variety of confidential information, targeting both private companies and public services. Hence, it is necessary to increase the defense capabilities of these organizations in order to prevent and effectively react to them. Cyber-attacks can have significant economic, political, national security and social consequences.

The public service can be considered a priority target for cyber attacks, therefore the whole organization - from the smallest element of the system, through large information systems to the people working there - must be prepared to prevent a possible attack or to react to events that have already occurred. A significant part of the attacks targets the unpreparedness and the lack of security awareness of users, which is why the primary goal of the author is to create and continuously improve the

awareness and the cyber defense capabilities of public service employees, which requires a form of training to achieve these goals.

The recognition of the previously mentioned issue led me to specify a cyber security training for the public service, which aims to develop the cyber defense capabilities of people working in the public service in order to improve public service cyber security. However, there are already existing training programs in the context of cyber security, it is important to identify the differences and common part of the cyber security in the public and private sectors.

The purpose of conducting and analyzing the personal interview presented in this study, is to identify differences in the public and private sectors and utilize good practices and people management that are viable options in the private sector but not considered in the public services and vice versa.

In this interview a discussion was held with chief executives in the public and private sector. To examine the cyber security of the public sector, I asked Mr. Lajos Muha, Phd who is the IT security manager of the Hungarian State Treasury. From the private sector, I asked Mr. Csaba Otti, PhD, CEO of Login Autonom Ltd., which is a leading software development company in Hungary.

1.1. Research Method

The present research uses the interview method to perform data collection and then to draw conclusions. The interviews were conducted with verbally structured questions, which were videotaped and audio-recorded.

1.2. Goals and limitations

The purpose of the interview is to answer the following main questions:

- G1. Is there a clearly identifiable difference between the private sector and the public service in terms of cyber security?
- G2. Can a clear priority be specified between the training of individuals and technological developments in the case of the private sector and the public service from financial and professional aspects?
- G3. Is there a cyber defense strategy specific to the private sector or the public service that could possibly be adapted in the other sector?
- G4. In terms of IT infrastructure, can a clear distinction be made between the private sector and the public service?

In order to answer the questions defined here, it is also necessary to identify the limitations that may arise during such an interview so that the research can reflect real results.

- C1. Target persons can only give high-level answers in accordance with the internal policies of their companies or departments, so detailed, specific cases cannot be presented and discussed.
- C2. Target individuals do not have accurate economic numbers during the interview.

- C3. Although the target persons answer the questions to the best of their knowledge and good intentions, in the case of non-factual questions, they only present their own opinions.

Related works

During the preparation of the research, a deeper examination of the relevant international and domestic literature is essential for the implementation of an effective interview, as well as for the analysis of its basic rules and the exploration of the foundations of public and private cyber security.

Basic rules of interviewing

Several scientific studies examine the rules and stages of interviewing[1] in which they explain that the interview can be considered a particularly useful research method, as it helps to get to know and explore through the experiences of the participants, and its advantage is the personal presence and the expansion of the questions asked based on the continuous development of the conversation.[2]

In their article DiCicco-Bloom and Crabtree briefly review the most common qualitative interview methods: structured interviews, semi-structured interviews, and individual in-depth interviews.[3]

Cyber security in the private sector

Private cybersecurity issues have also been examined in several studies along decision-making strategies, training, and international comparisons. Rowe and Gallaher conducted a series of interviews with organizations in different sectors in a case study to explore and understand their investment and execution strategies, particularly the factors that determine the level of cybersecurity they maintain, in their study.[4] According to the awareness can minimize vulnerabilities related to users. This can be achieved through systematic programs.[5] Gordon and co-authors in their Increasing cybersecurity investments in private sector firms study use a

---

1 HORNYACSEK Júlia: A tudományos kutatás elmélete és módszertana; Nemzeti Közszolgálati Egyetem, 2014. pp. 81-85.

2 VALENZUELA, Dapzury – SHRIVASTAVA, Pallavi: Interview as a method for qualitative research; Southern Cross University and the Southern Cross Institute of Action Research (SCIAR), 2002. https://sdhrc.tbzmed.ac.ir/uploads/189/CMS/user/file/3544/conferece/slides/Research2.pdf (downloaded 11 August 2020)

3 DICICCO-BLOOM, Barbara – CRABTREE, Benjamin F.: The qualitative research interview; Medical education, 2006/4. pp. 314-321. https://doi.org/10.1111/j.1365-2929.2006.02418.x (downloaded 11 August 2020)

4 ROWE, Brent R. – GALLAHER, Michael P.: Private sector cyber security investment strategies: An empirical analysis; In: The fifth workshop on the economics of information security (WEIS06). 2006. http://www.infosecon.net/workshop/downloads/2006/pdf/18.pdf (downloaded 11 August 2020)

5 SIPONEN, Mikko T.: A conceptual foundation for organizational information security awareness; Information Management & Computer Security, 2000. pp. 31-41. https://doi.org/10.1108/09685220010371394 (downloaded 11 August 2020)

microeconomic analysis to demonstrate whether government initiatives and legislation can increase cyber security investment by private companies.[6] Hiller and Russell's The challenge and imperative of private sector cybersecurity: An international comparison reviews the various cyber threats and compares approaches to support cybersecurity in the United States and Europe.[7]

Cyber security in the public sector

Cyber security in the public sector, and especially in public administration, has been examined in various EU projects and other studies as a problem of globalization, where the appearance of the Internet has posed challenges to the public service that they have not faced before.
Wirtz et al. examines the attitudes of public sector employees towards cybersecurity and those measures on an empirical basis.[8] Coppolino et al. in How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project state that the appearance of the Internet has opened up new opportunities for public administration. The project aims to increase the awareness, cybersecurity skills and protection of local administrations against digital threats.[9]

Cyber Security: Public Sector Threats and Reactions edited by Andreasson focuses on the convergence of globalization and the online migration of public sector functions and identifies the challenges we need to be aware of.[10]

Preparation process

The interview process consists of the sections shown in Figure 1. They are detailed in the upcoming sections.

---

6 GORDON, Lawrence A., et al.: Increasing cybersecurity investments in private sector firms; Journal of Cybersecurity, 2015/1. pp. 3-17. https://doi.org/10.1093/cybsec/tyv011 (downloaded 11 August 2020)

7 HILLER, Janine S. – RUSSELL, Roberta S.: The challenge and imperative of private sector cybersecurity: An international comparison; Computer Law & Security Review, 2013/3. pp. 236-245. https://doi.org/10.1016/j.clsr.2013.03.003 (downloaded 11 August 2020)

8 WIRTZ, Bernd W. – WEYERER, Jan C.: Cyberterrorism and cyber attacks in the public sector: how public administration copes with digital threats; International Journal of Public Administration, 2017/13. pp. 1085-1100. https://doi.org/10.1080/01900692.2016.1242614 (downloaded 11 August 2020)

9 COPPOLINO, Luigi, et al.: How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project. In: 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE, 2018. pp. 573-578.

10 ANDREASSON, Kim J. (ed.): Cybersecurity: public sector threats and responses; CRC press, 2011.

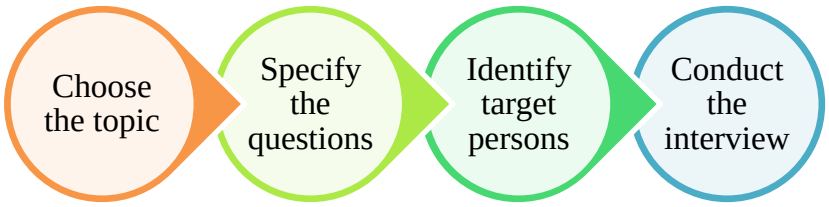

Figure 1. The interview process
(Author's own edition)

1. **Choose the topic:** specifying the topic around the interview will be conducted.
2. **Specify the questions:** elaborating the important questions to cover the previously specified topic during the interview.
3. **Identify target persons:** asking key stakeholders of the topic is important to identify the best takeaways.
4. **Conduct the interview:** organizing and executing the interview.

Rest of the section is organized according to the presented steps.

3.1. Choose the topic

Primarily, the topic is to compare the cyber defense mechanisms of the private sector and the public service to determine whether any difference in the defense strategy of a company and organization can be identified.

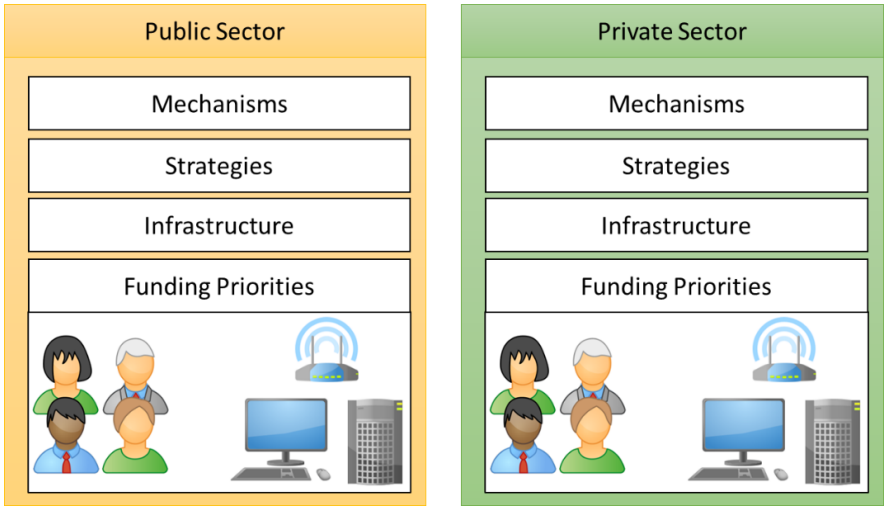

Figure 2: Key properties of the comparison
(Author's own edition)

The key properties of the comparison are visualized on Figure 2. and detailed as follows:

- Mechanisms: according to G1, it is important to understand what the key differences in the mechanisms are when attacks are executed against public/private sectors.
- Strategies: according to G3, it is important to investigate any differences between public and private sectors in the context of strategies that can be applied in the other sector.
- Infrastructure: according to G4, the structure of the IT systems for cyber defense could emphasize different type of cyber attacks connected to public and private sectors.
- Funding priorities: according to G2, it is an interesting question whether the education of employees or the IT infrastructure should be prioritized over the other.

After choosing the topic, the results of previous research on the topic are collected and the rules of interviewing are analyzed.

3.2. Specify the questions

The questions are specified in a way to provide answers to the goals presented Section 1.2. The questions are associated with the goals they are about to provide answers and listed in Figure 3.

Goal	Question
G1	Have you ever faced a cyber security incident? Were you able to prevent or react to events that have already occurred? Has the data CIA been damaged?
G4	What are the main IT infrastructure components of your organization?
G3	What are the key points in your organization usually targeted by cyber-attacks?
G3	What defense strategy is used in your organization?
G2	What cybersecurity training is provided to employees?
G2	Which one do you see more effective in protecting: technology or developing individuals' skills? Why?
G2	From a financial point of view, which one is considered more economical: purchasing advanced technological protection or improving the security awareness of individuals?
G2	What are the cyber defense capabilities needed to perform the day-to-day tasks of employees?
G1, G4	Do you see any difference in cybersecurity risks between the public service and the private sector?

Figure 3: Interview questions by research objectives.
(Author's own edition)

3.3. Identify target persons

The aim is to involve individuals in the interview who effectively represent the interests of the private sector and the public service, and who have the knowledge that is essential for the development and continuous improvement of cyber defense and cyber security. In addition, the selected target persons shall be leaders (e.g., chief executives) in the public service and the private sector. It is important for the interviewees to be involved on a day-to-day basis in developing and making strategic and financial decisions related to cybersecurity.

3.4. Conduct the interview

Following the selection of the competent interviewees, the interview is requested from the interviewees and the appropriate venue is discussed with separately. This is followed by conducting the interview, asking questions. The conversations are recorded in two steps with the permission of the interviewees:

- audio and video recording are created of what was said,
- then the records are converted into a written text.

The responses of the interviewees are sent to them electronically for review, and then, after the approval, I summarize the answers and place them in the present publication.

Interview

Mr. Csaba Otti, PhD (Cs.O.) is the CEO of Login Autonom Ltd. which is a leading software development company in Hungary. The main product of the company is a standalone cloud-based HR software that collects and stores personal data of the employees and provides analysis and reports to the clients from the collected data. The customer base of the company is about 60 organizations from Europe where each organization has hundreds of employees.

Mr. Lajos Muha, PhD (L.M.) is the IT security manager of the Hungarian State Treasury which is responsible for financing, money circulation, clearing of accounts, cash-, deficit- and state debt management, determined data supply as well as management and detailed registration of guarantees and loans extended by the state. From 2004, he is a Certified Information Security Manager (CISM). In 2013, he was one of the main contributors of the Hungarian Information Security Law.

Question 1: *Have you ever faced with a cyber security incident? Were you able to prevent or react to events that have already occurred? Has the data CIA been damaged?*

Cs.O.: Yes, we have already faced cyber security incidents. For example, the Production server on which we host our cloud service was unavailable. We are continually correcting issues found in the results of our vulnerability investigations to help prevent future events and respond effectively to events that have already occurred. The principle of confidentiality and integrity has not been violated, however, due to the unavailability of the server, the principle of availability has been violated.

L.M.: We have already faced cyber security incidents, but we are unable to log every potential cyber security incidents that have been prevented by the measures. In the vast majority of incidents, we have been able to deal with them effectively at an early stage. Fortunately, we did not experience any incident with serious results. For example, there have been phishing attacks or receiving malicious code as an attachment to e-mails. In such cases, there were no violations of the CIA principles.

Question 2: *What are the main IT infrastructure components of your organization?*

Cs.O.: The organization has a worksite where the internal data and the equipment of the employees are on a separate network. The internal network includes database servers, application servers, internal data storage, and a firewall through which the Internet can be accessed. The network we use to work includes printers, scanners, mobile devices, and developer computers that connect to the Internet through our internal network. The organization is also affiliated with a cloud provider that hosts cloud-based services related to the company. When working remotely, employees can connect to the internal network through a VPN. Customers, on the other hand, only communicate with the organization's devices via the cloud service.

L.M.: We have a complete infrastructure from firewalls through servers to various workstations. Basically, the National Telecommunications Backbone Network provides access to the Internet as well as connectivity between sites. In special cases, the server, the operating system and the database are also operated by the National Infocommunications Service Company Ltd. and only the application operation is implemented by our organization.

Question 3: *What are the key points in your organization usually targeted by cyber-attacks?*

Cs.O.: Vulnerabilities detected by vulnerability scans on our Cloud infrastructure, as well as phishing through colleagues, such as various phishing messages, can be a key risk to our organization by clicking on malicious code. In addition, it is necessary to mention data leak when, for example, a colleague downloads an Excel spreadsheet from a customer and does not handle customer data as required by our policies.

L.M.: In the past, phishing emails and malwares were attached as email attachments. No targeted attacks have been detected; however, we are constantly monitoring relevant areas using vulnerability scans.

Question 4: *What defense strategy is used in your organization?*

Cs.O.: In the context of administrative protection, we pay special attention to raising the security awareness of our colleagues, such as various awareness training, education and programs. In addition, we have developed a system of policies and regulations which are constantly monitored and, if necessary, amended. We have taken several measures to implement physical protection, such as measures for physical access, protection of offices, premises and facilities, or even protection of equipment. In the context of logical protection, we defend mainly against malwares, observing operational software, logging and monitoring, backups, and access control.

L.M.: Our organization has detailed regulations in all areas related to safety. We have a complex and comprehensive IT security policy. IT security education and exam are mandatory for all employees on an annual basis. The implementation of physical protection is ensured by numerous measures and devices, such as closed objects,

electronic access system, live and mechanical protection, camera systems. In the field of logical protection, we strive to implement closed and comprehensive protection, from firewalls to malware protection to access control.

Question 5: *What cybersecurity training is provided to employees?*

Cs.O.: We provide a general training for all new entrants, followed by additional training in line with emerging safety issues, and as a third element of the training system, our employees receive regular training at specified intervals.

L.M.: We provide mandatory e-learning training for all employees in the organization, which is reviewed and modified as necessary each year. IT security training combined with data protection knowledge (GDPR) is currently being developed, which will enable the necessary data protection and IT security knowledge to be acquired in one training.

Question 6: *Which one do you see more effective in protecting: technology or developing individuals' skills? Why?*

Cs.O.: Both are extremely important and necessary. If people do not understand and are unable to agree on the need for restrictive measures, they will not be able to complement the technological protection. The advantage of the latter is that they operate continuously 24 hours a day and ensure safe operation for us.

L.M.: Both are equally necessary. The skills of individuals need to be developed because technology does not work without well-trained staff. Technology is also needed to complement personal skills. They cannot replace but complement each other, the two together provide effective protection.

Question 7: *From a financial point of view, which one is considered more economical: purchasing advanced technological protection or improving the security awareness of individuals?*

Cs.O.: When training skills of the individuals, not just the cost of the training itself is considered, but the time it takes while they do not work for that company needs to be evaluated as the off-time can even mean a significant loss of revenue. However, at the technology level, a similar amount can be spent. The main task is to identify risks and spend proportionately on training and technology. It is not necessary to insure either page.

L.M.: From a financial and economic point of view, the training of persons can be considered more cost-effective, in fact, staff trained at a relatively low cost can provide effective protection. However, having a personal ability cannot trigger technological protection tools (e.g., firewall, anti-virus). With the help of properly trained staff, costs can be reduced somewhat, but none can trigger the other factor.

Question 8: *What are the cyber defense capabilities needed to perform the day-to-day tasks of employees?*

Cs.O.: The safety awareness mentioned earlier is essential in the performance of day-to-day tasks, in the context of which employees are aware of the risks, the consequences and the regulations. In addition, after acquiring the knowledge, it is crucial that they understand and agree with the various protection tools and measures, as this is the only way to implement them effectively and efficiently in practice.

L.M.: It is extremely important for employees to pay attention to every details. For example, if a suspicious message is received, in which case the employee must

listen and decide how to react to this situation. Either clicking on the attachment, or responding to the email, or notify someone about message that appears suspicious.

Question 9: *Do you see any difference in cybersecurity risks between the public service and the private sector?*

Cs.O.: Depending on the type and profile of the organizations, different risks are present and consequently different measures are required. In the case of critical infrastructure, such as an attack on an energy or water network, problems of a completely different magnitude can be caused, so measures of a completely different magnitude are required. The severity and the factor involved may be different in the public sector, and as a result, the risks and the measures taken to respond to them may also differ.

L.M.: There are some differences, but the private and public sectors are closely related, there are overlaps between these areas. I see the difference primarily in how vital the tasks of a given organization are to the nation.

Conclusions

Based on the answers to the interview questions and the identified limitations, the following results are manifested for the questions specified at the beginning of the research as depicted on Figure 4.:

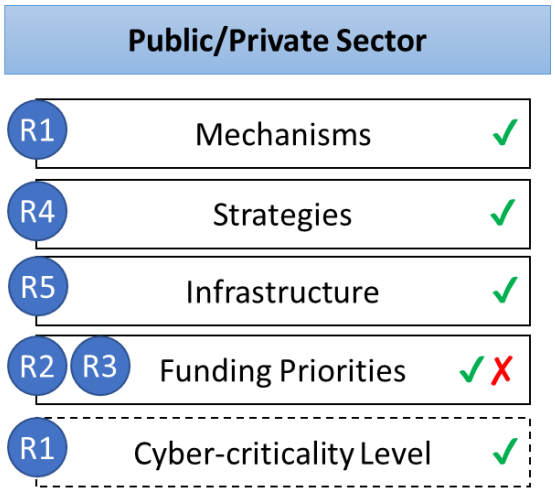

Figure 4: Classification of the conclusions
(Author's own edition)

R1. There is no clear distinction between the private sector and the public service in terms of cyber defense.
Both interviewees stated that although there may be differences between the two sectors mentioned above, there is a huge overlap. It is noteworthy that interviewees tend to see differences in cyber defense according to levels of criticality, but the tasks and defense strategies are the same.

R2. In the private sector and the public service, opinions differ between the training of individuals and technological developments from a financial point of view. While in the public service, clearly greater results can be achieved through further training of employees, in the private sector, reducing production during training can lead to greater economic deficits, so risk analysis is used to determine which aspect can be covered.

R3. No prioritization can be established between the training of individuals and technological developments in the private sector and the public service. Interviewees agreed that technological advances could be ineffective if employees are not trained enough and even the best-trained employees are not able to counter all cyber attacks.

R4. The private sector and the public service use similar cyber defense strategies. Based on the responses of the interviewees, cybersecurity policies, ongoing vulnerability investigations, and the same state-of-the-art approaches are used in both sectors to reinforce cyber security risky surfaces.

R5. In terms of IT infrastructure, the private sector and the public service are similar. Because the interviewees are leaders of organizations with similar criticality, their IT infrastructure have similarities.

To sum up, there are no differences between the public and private sector for the goals G1, G3 and G4. However, the two sectors have other opinions on the goal G2. In addition, both sectors advice the introduction of the cyber-criticality level to separate mechanisms and strategies in organizations on different levels.

Summary and future plans

In this paper, I used a structured interview to investigate whether any distinction can be made between the private sector and the public service in terms of cyber defense in a conversation with a person in a senior position in the public sector and one in a private position. This includes cyber security training for individuals, the implementation of technological developments, the role of financial and strategic decision-making related to cyber security, and the cyber security tools and measures of individual organizations.

The interviewees answered several questions to be able to carry out detailed conclusions in the aforementioned topics. The conclusions will be used during the creation of the public service cyber security training.

As future work, it is important to extend the presented interview to a larger scale of relevant persons working for companies and organizations on different cyber critical level. Additionally, it is requested to develop the public service cyber security training in a way the attendees shall be capable of understanding cyber defense strategies on different cyber critical level.

Bibliography:

- ANDREASSON, Kim J. (ed.): Cybersecurity: public sector threats and responses; CRC press, 2011.
- COPPOLINO, Luigi, et al.: How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project; In: 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE, 2018. pp. 573-578.
- DICICCO-BLOOM, Barbara – CRABTREE, Benjamin F.: The qualitative research interview; Medical education, 2006/4. pp. 314-321. https://doi.org/10.1111/j.1365-2929.2006.02418.x (downloaded 11 August 2020)
- GORDON, Lawrence A., et al.: Increasing cybersecurity investments in private sector firms; Journal of Cybersecurity, 2015/1. pp. 3-17. https://doi.org/10.1093/cybsec/tyv011 (downloaded 11 August 2020)
- HILLER, Janine S. – RUSSELL, Roberta S.: The challenge and imperative of private sector cybersecurity: An international comparison; Computer Law & Security Review, 2013/3. pp. 236-245. https://doi.org/10.1016/j.clsr.2013.03.003 (downloaded 11 August 2020)
- HORNYACSEK Júlia: A tudományos kutatás elmélete és módszertana; Nemzeti Közszolgálati Egyetem, 2014. pp. 81-85.
- ROWE, Brent R. – GALLAHER, Michael P.: Private sector cyber security investment strategies: An empirical analysis; In: The fifth workshop on the economics of information security (WEIS06). 2006. http://www.infosecon.net/workshop/downloads/2006/pdf/18.pdf (downloaded 11 August 2020)
- SIPONEN, Mikko T.: A conceptual foundation for organizational information security awareness; Information Management & Computer Security, 2000. pp. 31-41. https://doi.org/10.1108/09685220010371394 (downloaded 11 August 2020)
- VALENZUELA, Dapzury – SHRIVASTAVA, Pallavi: Interview as a method for qualitative research; Southern Cross University and the Southern Cross Institute of Action Research (SCIAR), 2002. https://sdhrc.tbzmed.ac.ir/uploads/189/CMS/user/file/3544/conferece/slides/Research2.pdf (downloaded 11 August 2020)
- WIRTZ, Bernd W. – WEYERER, Jan C.: Cyberterrorism and cyber attacks in the public sector: how public administration copes with digital threats; International Journal of Public Administration, 2017/13. pp. 1085-1100. https://doi.org/10.1080/01900692.2016.1242614 (downloaded 11 August 2020)

PROF ZOLTÁN RAJNAI PHD – HAYA ALTALEB

RISK ASSESSMENTS METHODS AND CYBER VULNERABILITIES IN SCADA SYSTEMS

Abstract

Modern SCADA systems are based on advanced technology systems, therefore it is profoundly sophisticated SCADA systems are exposed to a large-scale cyber threats range because of the standardization of the hardware components and the communication protocols. Cyber threats to SCADA systems always rising, those are caused by escalating sophistication modernization, continuous real-time operation and distribution, and the multicomponent architecture of the systems. This article mentions the common SCADA vulnerabilities and their assessment methods besides the impact of SCADA vulnerabilities. The authors also discuss some Risk assessment methods of information technology and industrial systems, along with recommendations to ensure more enhancement of SCADA security systems.

Keywords*:* SCADA Vulnerability, Critical infrastructure, SCADA incidents, Security mitigations

1 Introduction

SCADA systems (supervisory control and data acquisition) are considered as master cyber-attack targets based on the extreme impacts on economies, industrial sectors, properties, and human lives. Existing security solutions, like (access controls, firewalls, intrusion detection, online monitoring, intrusion detection and prevention, live forensics analysis, and intrusion response systems) can protect SCADA systems from cyber-attacks such as (SQL injection attacks, denial of service attacks, and spoofing attacks). Still, they are far from ideal protection[1]. The current SCADA market demonstrates that companies continue to see the advantages of their processes being provided by modern SCADA systems. In fact, by 2025, the industry is forecasted to hit US$47.04 billion. Looking at the weaknesses that characterize each year's count gives a general indication of where vulnerabilities can be discovered when it refers to SCADA systems.[2]

Vulnerabilities include unsophisticated bugs including overflows of stacks and buffers and information disclosure. These vulnerabilities let attackers to implement arbitrary code (ACE), remote code execution (RCE), perform a denial of service (DoS), or steal information. The security of the first and second generations of

1 CHEN, Qian – ABDELWAHED, Sherif: Towards Realizing Self-Protecting SCADA Systems; ACM International Conference Proceeding Series, 2014 no. April, pp. 105-108. https://doi.org/10.1145/2602087.2602113 (downloaded 14 December 2020)

2 TrendMicro: One Flaw Too Many: Vulnerabilities in SCADA Systems – Security News – Trend Micro USA; TrendMicro.Com. 2019. https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems (downloaded 14 December 2020)

SCADA systems was ignored because of vendor-proprietary environments. When SCADA systems were first connected to the Internet, cyber attackers exploiting publicly known information security vulnerabilities breached those air-gapped SCADA systems. Most of the vulnerabilities in operating systems, off-the-shelf applications, besides, in IT applications, communication protocols have been patched. Hence, The first step to secure SCADA systems is to alleviate risks of known threats and vulnerabilities by periodically generating and implementing safety control recommendations and alternative solutions.[3,4]

The aim of this paper to review various types of real and prospective SCADA vulnerabilities. Started with a brief literature review following with Vulnerabilities in SCADA Systems and their impacts. Besides, The authors discussed some Risk assessment methods of the information technology and industrial systems, along with recommendations to ensure more enhancement of SCADA security systems.

2. Literature review

In 2004, the document titled "System Protection Profile Industrial Control Systems" has been published via the National Institute of Standards and Technology (NIST); it covers the risks and the objectives of SCADA systems.[5] The US President's Critical Infrastructure Protection Board and the Department of Energy planned the steps an organization must undertake to enhance the security of its SCADA networks in the booklet 21 Steps to Improve Cyber Security of SCADA Networks.[6] According to the Industrial Network Security (Second Edition), in 2015 the author's Eric D. Knapp, Joel Thomas Langill have discussed the consequences of a successful cyber incident on an ICS can be financial loss or physical safety liabilities, with massive effects extending beyond the plant, to the local community, country, and even federal level.[7]

Morgan Henrie in Cyber Security Risk Management in the SCADA Critical Infrastructure Environment report based on his experience in an extensive review of oil and gas (O&G) critical infrastructure, which has presented the project's result in the American Petroleum Institute (API) November Information Technology Security Conferences. Henrie's research output was intended to provide engineering managers with additional information that can be used to make informed decisions on how

---

3 STOUFFER, Keith – PILLITTERI, Victoria – LIGHTMAN, Suzanne – ABRAMS, Marshall – HAHN, Adam: Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2; NIST Special Publication 2015/2. pp. 1-157. https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-82r1 (downloaded 14 December 2020)

4 Ibid.

5 System Protection Profile-Industrial Control Systems Version 1.0. 2004. https://doi.org/10.6028/NIST.IR.7176 (downloaded 14 December 2020)

6 Office of Energy Assurance: 21 Steps to Improve Cyber Security of SCADA Networks; US Department of Energy, 2002. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf (downloaded 14 December 2020)

7 YILMAZ, Ercan Nurcan – GÖNEN, Serkan: Attack Detection/Prevention System against Cyber Attack in Industrial Control Systems; Computers and Security 2018. pp. 94-105. https://doi.org/10.1016/j.cose.2018.04.004 (downloaded 14 December 2020)

organizations should allocate resources to mitigate this expanding risk map.[8] As noted by the Baker Institute Policy Report, SCADA system cybersecurity risks are a recent phenomenon where *"…energy companies…are facing this new risk…,"* and the risk of nature is rapidly evolving.[9]

Vincent Urias, Brian Van Leeuwen, and Bryan Richardson have developed a hybrid tested methodology that can be used to perform cyber-physical security analysis. The method enables building models of both the SCADA system and the physical system. The SCADA system model may include its connectivity to the various business networks and, in cases, its connectivity to the Internet. The physical system model is chosen from different solvers for the physical system under study. On the other side, in hybrid experiments, the SCADA system events and the physical system events are connected in lockstep to create realistic operations.[10] Besides, they created a model of a SCADA system that included modeled Intelligent Electronic Devices (IEDs). It communicates directly to the SCADA Server or the local Remote Terminal.

3. Vulnerabilities in SCADA systems

Cyber-attacks can be conducted within an hour once the computer system security is endangered. Simultaneous attacks from different locations are enabled by the ever-rising power of the Internet. An attack's greatest effect is when an attacker gains access to a SCADA system's supervisory control access and launches control behavior that can cause catastrophic harm. Existing security solutions, like (access controls, firewalls, intrusion detection, online monitoring, intrusion detection and prevention, live forensics analysis, and intrusion response systems) can protect SCADA systems from cyber-attacks such as (SQL injection attacks, denial of service attacks, and spoofing attacks).[11]

A vulnerability is basically "a flaw within a system, application, or service that allows attackers to manipulate security controls and exploit systems in ways never intended by the developer". The systematic method of finding security problems (i.e. vulnerabilities) in a device, network, and communications infrastructure is vulnerability assessment. Organizations use vulnerability assessments to mitigate and manage security issues within their emerging technologies. There are three types of vulnerability evaluation software available today: multipurpose, web application, and specialization. Multipurpose instruments (e.g., Nessus and Qualys) focus on analyzing the vulnerabilities of a wide range of devices, operating systems, and services. Web application scanners, such as Burp Suite, only detect issues within web

---

8 CHEN, Qian – ABERCROMBIE, Robert K. – SHELDON, Frederick T: Risk Assessment For Industrial Control Systems Quantifying Availability Using Mean Failure Cost (MFC); Journal of Artificial Intelligence and Soft Computing Research 2015/3. pp. 205-220. https://doi.org/10.1515/jaiscr-2015-0029 (downloaded 14 December 2020

9 CORT, Pia – ROLLS, Simon: Vet P Olicy R Eport D Enmark 2008; 2008/53 pp. 1-16.

10 URIAS, Vincent – VAN LEEUWEN, Brian – RICHARDSON, Bryan: Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed; Sandia National Laboratories, Albuquerque, USA, 2013. pp. 1-8.

11 TrendMicro 2019. op. cit.

technologies. Specialized tools can only find problems within certain technologies (e.g. MyQL). Among different choices, experts have referred to Nessus as *"one of the most comprehensive and widely deployed."*[12]

Risk Level	CVSS Ranges	Example Vulnerabilities
Critical	10.0	Remote Code Execution, Default Credentials, Buffer Overflows, Unsupported Operating System Versions
High	7.0 – 9.9	Malformed Packet Injection, Privilege Escalation, Redirect Denial of Service, Password Hash Disclosure
Medium	4.0 – 6.9	Remote Information Disclosure, Command Injection, Cryptographic Protocol, File Access and Web Directory Traversal
Low	0.1 – 3.9	Unencrypted Communications, Browsable Web Directory, Internal Information Disclosure.
Informational	0.0	Software Version Disclosure, Protocol Detection, Operating System Identification, Device Type

Figure 1: Risk levels and examples for vulnerabilities[13]

The connectivity of corporate networks usually secured by firewalls; Figure 1 shows the control center Cybernet environment. The network of control centers is linked to other corporate networks and networks of substations and power plants maintained by information technology staff. Control center networks are known to be highly protected and thus unlikely to be directly infiltrated. The focus of[14] study is on the intrusion into the control of center networks by other networks, such as those at substations or power plants.

[12] HARRELL, Christopher R. – PATTON, Mark – CHEN, Hsinchun – SAMTANI, Sagar: Vulnerability Assessment, Remediation, and Automated Reporting: Case Studies of Higher Education Institutions. 2018 IEEE International Conference on Intelligence and Security Informatics, ISI 2018. https://doi.org/10.1109/ISI.2018.8587380 (downloaded 14 December 2020)

[13] Ibid.

[14] TEN, Chee Wooi – LIU, Chen Ching – MANIMARAN, Govindarasu: Vulnerability Assessment of Cybersecurity for SCADA Systems; IEEE Transactions on Power Systems, 2008/4. pp. 1836-1846. https://doi.org/10.1109/TPWRS.2008.2002298 (downloaded 14 December 2020)

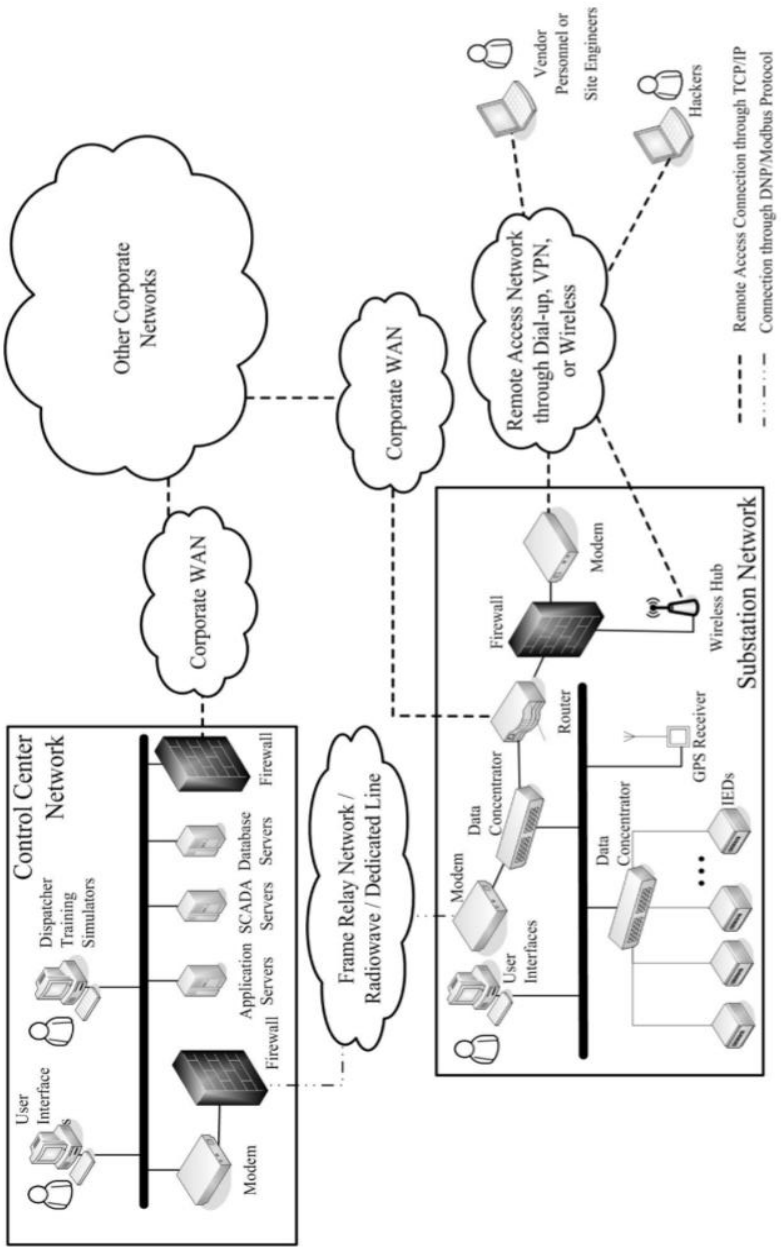

Figure 2: Cyber network environment of a control center[15]

The convenient availability of Internet infrastructure and web search capabilities provide hackers with a systematic footprint to define the security posture of an organization. There are increasingly advanced techniques for intrusion that include:[16]

---

15 Ibid.

16 MCCLURE, Stuart – SCAMBRAY, Joel – KURTZ, George: Hacking Exposed: Network Security Secrets & Solutions; Third Edition; McGraw-Hill Education, 2001.

1. War dialing: When the main telephone number prefix has been established, the corresponding numbers can be executed in scripts to detect potential contact.
2. Scanning: To decide the service ports on the computer that are either operating or in listening state for link to possible access points, it scans the destination IP addresses.
3. Traffic sniffing-The network analyzer is used within a network to catch packets traversing.
4. Password cracking-A program that attempts to guess a password repeatedly in order to obtain entry to a network (unauthorized).

4. The impact of SCADA Systems vulnerabilities

Previous attacks on industrial facilities have illustrated the impact of attacks targeting SCADA systems. The Stuxnet worm in 2010 was the first cyber-weapon Stuxnet was Realized to generate focused damage to mechanical infrastructure that takes advantage of cyber vulnerability, and it attacked industrial installations via SCADA vulnerabilities. Besides, Stuxnet reveals that a cyber-attack against an OT infrastructure can be carried out and that such an attack is feasible. Attacks can cause kinetic consequences.[17] In 2014 Irongate was one of the first malware found after Stuxnet explicitly designed it for the OT system. Analysis study shows that in a simulation setting, IRON GATE invokes ICS attack concepts first seen in Stuxnet. Since malware is restricted to the Industrial Control Systems (ICS) body and supervisory control and data acquisition (SCADA), we exchange information with the wider community.[18] In 2016, power outages were triggered in Ukraine by the malware known as Industroyer. The latest one is Triton attacked industrial security systems in 2017 in Saudi Arabia, which triggered SIS systems (Safety Instrumental System) to cause an operational shutdown. This attack brought to light two issues prevalent in the connected world of today: a need to prevent malware from taking control of significant operations and the potential of hackers to exploit third-party operators such as cloud hosting services administrators or OS and malware introduction driver vendors.[19]

---

https://pastefs.com/resource/download/15855/0/6e7bb1267d3319938554784e1664ad75/Hacking+Exposed+_+Network+Security+Secrets+And+Solutions%2C+3Rd+Edition+%28Partiel%29+-+Osborne+-+2001.pdf (downloaded 14 December 2020)

17 SETOLA, Roberto – FARAMONDI, Luca – SALZANO, Ernesto – COZZANI, Valerio: REFIRE-Reference Implementation of Interoperable Indoor Location & Communication Systems for First Responders View Project Safety in Process Engineering View Project An Overview of Cyber Attack to Industrial Control System; CHEMICAL ENGINEERING TRANSACTIONS, 2019. Vol. 77. https://doi.org/10.3303/CET1977152 (downloaded 14 December 2020)

18 HOMAN, Josh – MCBRIDE, Sean – CALDWELL, Rob: Irongate Ics Malware: Nothing To See Here Masking Malicious Activity on Scada Systems; 2016. https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html (downloaded 14 December 2020)

19 Trusted Cyber Physical Systems Looks to Protect Your Critical Infrastructure from Modern Threats in the World of IoT | Windows Experience Blog; n.d. https://blogs.windows.com/windowsexperience/2018/04/24/trusted-cyber-physical-systems-looks-to-protect-your-critical-infrastructure-from-modern-threats-in-the-world-of-iot/ (downloaded 14 December 2020)

These attacks follow various techniques and instruments, but they all appear as proof of concept, i.e. as tests to verify the methodologies and to demonstrate the ability of these attack groups. There is no proof that such attacks have been carried out by the same group or by a related group, but as shown schematically in Figure 3, they appear as phases of a single strategy.[20]

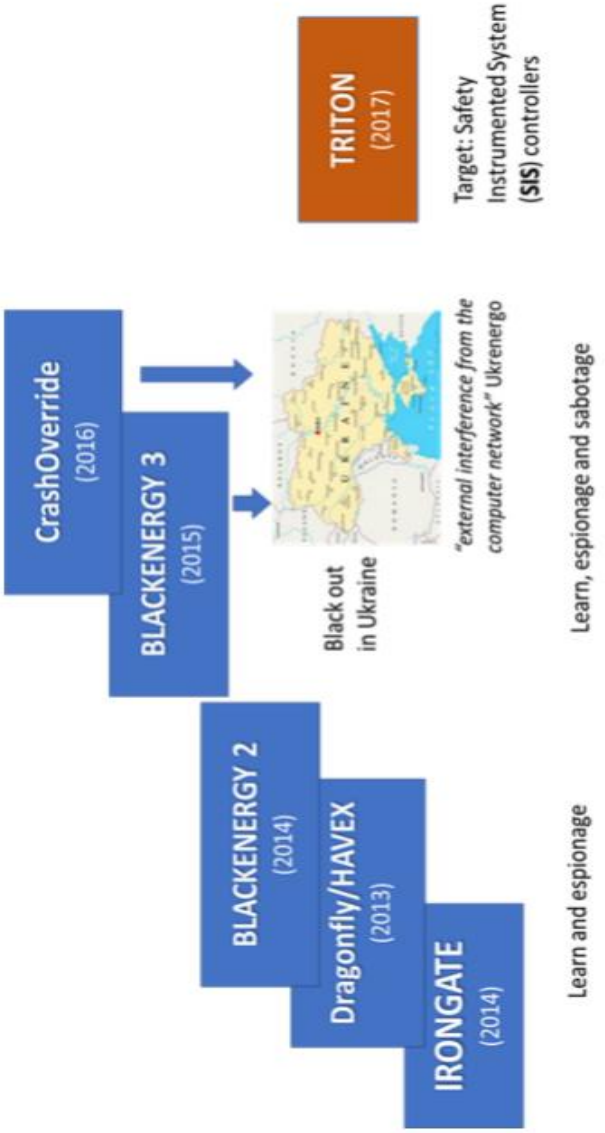

Figure 3: Evolution of cyber-attacks against Operational Technology after Stuxnet[21]

[20] SETOLA et. al. 2019. op. cit.
[21] Ibid.

5. SCADA systems Risk assessment methods

SCADA systems Risk assessment aims to evaluate the system components in terms of their vulnerability to an assault and their relevance to the system's efficient operation. As well as, the danger they pose and their likelihood. The risk assessment leads the engineers and managers of SCADA systems to enhance and develop adequate security policies and the design of the security system and rational allocation of often scarce resources. It shall also facilitate communication between business, security, and SCADA experts.[22,23]

Risk described as the following:[24]

$$R= \{si, pi, xi\}, i=1, 2, N \quad (1)$$

Where

- R: Risk
- {}: must be interpreted as a "set of"
- s: A scenario (undesirable event) description
- p: The probability of a scenario
- x: The measure of consequences or damage caused by a scenario
- N: The number of possible scenarios that may cause damage to a system

the formula for calculating cybersecurity risks in SCADA systems risk when we applied to quantify is accepted as follows:[25]

$$R= t \; v \; xtv \quad (2)$$

Where

- *t:* Threat
- *v:* Vulnerability
- *Xtv*: the consequences of the threat successfully exploiting the vulnerability

There is a range of general IT risk assessment methodologies that can be modified to be used in the industry.

---

22 HENRIE, Morgan: Cyber Security Risk Management in the Scada Critical Infrastructure Environment; EMJ - Engineering Management Journal 2013/2. pp. 38-45. https://doi.org/10.1080/10429247.2013.11431973 (downloaded 14 December 2020)

23 CHERDANTSEVA, Yulia – BURNAP, Pete – BLYTH, Andrew – EDEN, Peter – JONES, Kevin – SOULSBY, Hugh – STODDART, Kristan: A Review of Cyber Security Risk Assessment Methods for SCADA Systems; Computers and Security, Elsevier Ltd. 2016. https://doi.org/10.1016/j.cose.2015.09.009 (downloaded 14 December 2020)

24 KAPLAN', Stanley – GARRICK, B. John: On The Quantitative Definition of Risk; Risk Analysis. 1981/1.

25 HENRIE (2013) op. cit.

5.1 Central Computer and Telecommunications Agency Risk Analysis and Management Method (CRAMM)

CRAMM is an inclusive tool for identifying security and contingency requirements, and justifying expenditure on specific countermeasures especially of an IT operation.[26]

The advantages of CRAMM are:[27]

- A structured approach to risk analysis and management, based on well-established methods;
- Assistance in contingency planning, BS7799 certification, and audits;
- Promotion of security awareness and acceptance;
- Possibility of full reviews and rapid reviews (also allowing high-level reviews that support policy statements);
- Regularly updated extensive hierarchical countermeasure database, covering also nontechnical areas;
- Relative prioritization of countermeasures, including effectiveness criteria and implementation costs;
- Consistency resulting from similar solutions for similar risk profiles.

The disadvantages are:[28]

- the need for qualified and experienced practitioners to use the tool,
- Full reviews, which may last long with too much hard-copy output (which may be decreased by keeping the analysis at a required minimum).

5.2 Information security risk analysis method ISRAM

ISRAM is designed for analyzing the risks at complex information systems by enabling the participation of administrators and staff. The purpose of ISRAM is to determine the risk of information security problems. In order to achieve this objective, ISRAM shall use a public opinion on the matter. The public opinion shall be obtained by conducting a survey. The survey consists of questions and answers related to the issue of information security. Managers, directors, technical and common users of the systems are the target candidates for answering the questions of the survey. The objective of the survey is to understand the impact of the information security problem on the system or organization,[29] Figure 4 shows the basic flow diagram of ISRAM.

---

26 YAZAR, Zeki: A Qualitative Risk Analysis and Management Tool-CRAMM, 2002.

27 Ibid.

28 Ibid.

29 KARABACAK, Bilge – SOGUKPINAR, Ibrahim: ISRAM: Information Security Risk Analysis Method; Computers and Security, 2005/2. pp. 147-159. https://doi.org/10.1016/j.cose.2004.07.004 (downloaded 14 December 2020)

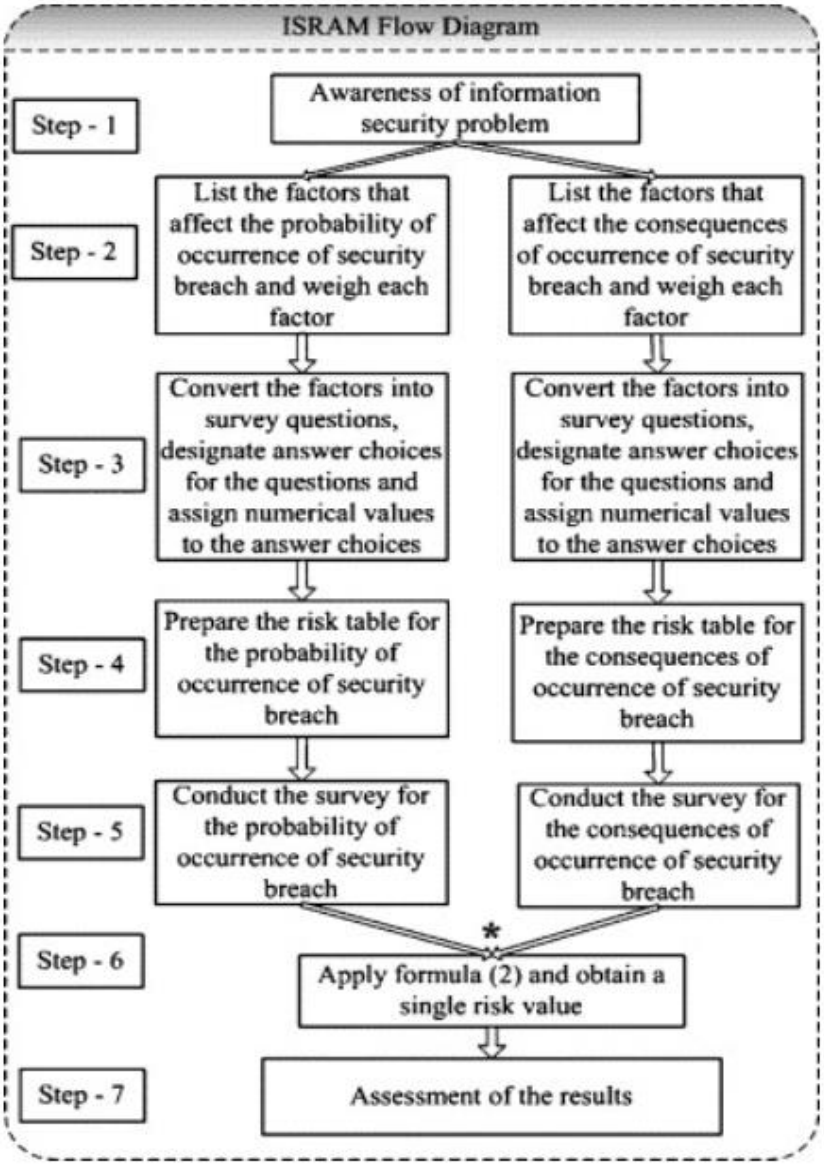

***Figure 4: The** Basic flow diagram of ISRAM*

5.3 Operationally Critical Threat and Vulnerability Evaluation (OCTAVE)

OCTAVE is self-coordinated, implying that individuals from an association accept accountability for setting the association's security system. The strategy uses individuals' information on their association's security-related practices and cycles to catch the present status of security practice inside the association. Dangers to the most basic resources are utilized to focus on territories of progress and set the security

technique for the association. Figure 5 shows the relationship between these activities. Note that risk management activities explain a plan-do-check-act cycle.[30]

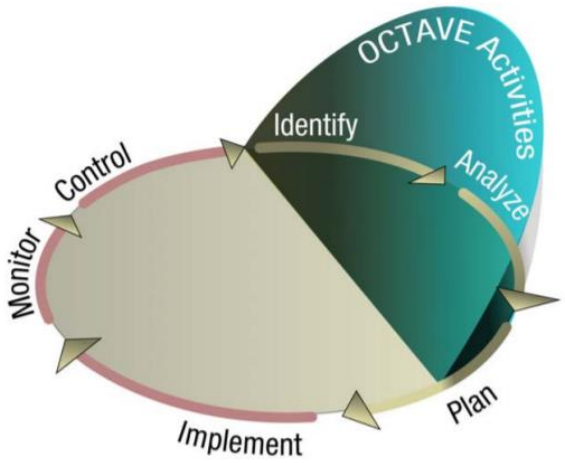

Figure 5: Risk Management Activities[31]

By utilizing the OCTAVE approach, an association settles on data assurance choices dependent on dangers to the classification, trustworthiness, and accessibility of basic data-related resources. All parts of danger (resources, dangers, weaknesses, and hierarchical effect) are calculated into dynamic, empowering an association to coordinate a training based assurance procedure to its security risks.

6. Conclusion and recommendations

Depending on the specific characteristics of a SCADA system, it is slightly or extra susceptible to such an assault. The architecture of SCADA systems has evolved, alongside with computer technology, over the recent years and current designs, although more functional and flexible, may also be more vulnerable. Furthermore, it is significant to understand that an attack on such a system can be an internal source just as easily as an external source. This article overviews SCADA system vulnerabilities and their assessment methods besides the impact of SCADA vulnerabilities. The authors also discuss some Risk assessment methods of information technology and industrial systems, along with recommendations to ensure more enhancement of SCADA security systems.

Some recommendations to enhance systems security; Establish periodic ICS/SCADA security training and awareness campaigns within the organization, promote increased collaboration amongst policy decision-makers, manufacturers, and operators, Define guidelines for the establishment of reliable and appropriate

[30] ALBERTS, Christopher – DOROFEE, Audrey – STEVENS, James: Introduction to the OCTAVE ® Approach, 2003.

[31] Ibid.

cybersecurity insurance requirements. Define network communication technologies and architecture with interoperability in mind and consider security as a significant concept during the design phase of ICS/SCADA systems, Identify and found roles and instructions of people operating in ICS/SCADA systems.

Bibliography:

- ALBERTS, Christopher – DOROFEE, Audrey – STEVENS, James: Introduction to the OCTAVE ® Approach, 2003.
- CHEN, Qian – ABDELWAHED, Sherif: Towards Realizing Self-Protecting SCADA Systems; ACM International Conference Proceeding Series, 2014 no. April, pp. 105-108. https://doi.org/10.1145/2602087.2602113 (downloaded 14 December 2020)
- CHEN, Qian – ABERCROMBIE, Robert K. – SHELDON, Frederick T: Risk Assessment For Industrial Control Systems Quantifying Availability Using Mean Failure Cost (MFC); Journal of Artificial Intelligence and Soft Computing Research 2015/3. pp. 205-220. https://doi.org/10.1515/jaiscr-2015-0029 (downloaded 14 December 2020)
- CHERDANTSEVA, Yulia – BURNAP, Pete – BLYTH, Andrew – EDEN, Peter – JONES, Kevin – SOULSBY, Hugh – STODDART, Kristan: A Review of Cyber Security Risk Assessment Methods for SCADA Systems; Computers and Security, Elsevier Ltd. 2016. https://doi.org/10.1016/j.cose.2015.09.009 (downloaded 14 December 2020)
- CORT, Pia – ROLLS, Simon: Vet P Olicy R Eport D Enmark 2008; 2008/53 pp. 1-16.
- HARRELL, Christopher R. – PATTON, Mark – CHEN, Hsinchun – SAMTANI, Sagar: Vulnerability Assessment, Remediation, and Automated Reporting: Case Studies of Higher Education Institutions. 2018 IEEE International Conference on Intelligence and Security Informatics, ISI 2018. https://doi.org/10.1109/ISI.2018.8587380 (downloaded 14 December 2020)
- HENRIE, Morgan: Cyber Security Risk Management in the Scada Critical Infrastructure Environment; EMJ - Engineering Management Journal 2013/2. pp. 38-45. https://doi.org/10.1080/10429247.2013.11431973 (downloaded 14 December 2020)
- HOMAN, Josh – MCBRIDE, Sean – CALDWELL, Rob: Irongate Ics Malware: Nothing To See Here Masking Malicious Activity on Scada Systems; 2016. https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html (downloaded 14 December 2020)
- KAPLAN', Stanley – GARRICK, B. John: On The Quantitative Definition of Risk; Risk Analysis. 1981/1.
- KARABACAK, Bilge – SOGUKPINAR, Ibrahim: ISRAM: Information Security Risk Analysis Method; Computers and Security, 2005/2. pp. 147-159. https://doi.org/10.1016/j.cose.2004.07.004 (downloaded 14 December 2020)

- MCCLURE, Stuart – SCAMBRAY, Joel – KURTZ, George: Hacking Exposed: Network Security Secrets & Solutions; Third Edition; McGraw-Hill Education, 2001. https://pastefs.com/resource/download/15855/0/6e7bb1267d3319938554784e1664ad75/Hacking+Exposed+_+Network+Security+Secrets+And+Solutions%2C+3Rd+Edition+%28Partiel%29+-+Osborne+-+2001.pdf (downloaded 14 December 2020)
- Office of Energy Assurance: 21 Steps to Improve Cyber Security of SCADA Networks; US Department of Energy, 2002. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf (downloaded 14 December 2020)
- SETOLA, Roberto – FARAMONDI, Luca – SALZANO, Ernesto – COZZANI, Valerio: REFIRE-Reference Implementation of Interoperable Indoor Location & Communication Systems for First Responders View Project Safety in Process Engineering View Project An Overview of Cyber Attack to Industrial Control System; CHEMICAL ENGINEERING TRANSACTIONS, 2019. Vol. 77. https://doi.org/10.3303/CET1977152 (downloaded 14 December 2020)
- STOUFFER, Keith – FALCO, Joe – SCARFONE, Karen: GUIDE to Industrial Control Systems (ICS) Security; The Stuxnet Computer Worm and Industrial Control System Security, 2011. pp. 11-158
- STOUFFER, Keith – PILLITTERI, Victoria – LIGHTMAN, Suzanne – ABRAMS, Marshall – HAHN, Adam: Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2; NIST Special Publication 2015/2. pp. 1-157. https://doi.org/http://dx.doi.org/10.6028/NIST.SP.800-82r1 (downloaded 14 December 2020)
- System Protection Profile-Industrial Control Systems Version 1.0. 2004. https://doi.org/10.6028/NIST.IR.7176 (downloaded 14 December 2020)
- TEN, Chee Wooi – LIU, Chen Ching – MANIMARAN, Govindarasu: Vulnerability Assessment of Cybersecurity for SCADA Systems; IEEE Transactions on Power Systems, 2008/4. pp. 1836-1846. https://doi.org/10.1109/TPWRS.2008.2002298 (downloaded 14 December 2020)
- TrendMicro: One Flaw Too Many: Vulnerabilities in SCADA Systems – Security News –Trend Micro USA; TrendMicro.Com. 2019. https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems (downloaded 14 December 2020)
- Trusted Cyber Physical Systems Looks to Protect Your Critical Infrastructure from Modern Threats in the World of IoT | Windows Experience Blog; n.d. https://blogs.windows.com/windowsexperience/2018/04/24/trusted-cyber-physical-systems-looks-to-protect-your-critical-infrastructure-from-modern-threats-in-the-world-of-iot/ (downloaded 14 December 2020)
- URIAS, Vincent – VAN LEEUWEN, Brian – RICHARDSON, Bryan: Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed; Sandia National Laboratories, Albuquerque, USA, 2013. pp. 1-8.

- YAZAR, Zeki: A Qualitative Risk Analysis and Management Tool-CRAMM, 2002.
- YILMAZ, Ercan Nurcan – GÖNEN, Serkan: Attack Detection/Prevention System against Cyber Attack in Industrial Control Systems; Computers and Security 2018. pp. 94-105. https://doi.org/10.1016/j.cose.2018.04.004 (downloaded 14 December 2020)

AGNES KEMENDI[1]

E-COMMERCE SAFETY AND SECURITY IN THE INDUSTRY 4.0 ERA[2]

Abstract

The spread of information and communication technologies (ICTs) has led to new innovative business models and have rearranged the traditional business channels. The research was conducted in the field of e-commerce with the aim to capture the e-commerce electronic-commerce (e-commerce) business model with an eye on meeting the business needs during COVID-19 pandemic and on the protection of critical infrastructure in the European Union. The research focused on the safety and security concerns and the associated business risks and consequently to highlight the necessity for adequate risk management processes in e-commerce context.

***Keywords*:** e-commerce, ICT, risk, security, critical infrastructure, COVID impact

Introduction

E-commerce has become an everyday term. The business concept of e-commerce is by now integrated part of the day-to-day business. Corporate stakeholders and end users are also regular part of the business cycle. ICTs are drivers of world economic growth.[3] Innovations related to ICTs have opened the era of e-commerce.[4] In the Industry 4.0. era, the role of digital technology is fundamental. The unexpected event of the COVID-19 pandemic has proven impact on the preferred business channels and contributed to an increased use of e-commerce. The volume and impact of potential security threats point to the need for adequate protection measures for the critical infrastructures (CIs). The dynamic spread of e-commerce and information communication technology have brought, however, new risks and safety and security concerns.

The purpose of the research is to provide an understanding behind the e-commerce business model, describe its linkage to critical infrastructures, to observe its role during COVID 19 pandemic and to identify the related safety and security

1 https://orcid.org/0000-0002-6452-8563

2 Though the research aims to provide a comprehensive view on the subject matter of e-commerce, this cannot be considered as exhaustive and closed. The subject matter changes and evolves over time which justifies the need for future research on this matter. Further research in the future could establish the development of the e-commerce business model and identify the state of art risk management methods to manage the business risks.

3 JORGENSON, D. W. – VU, K. M.: The ICT revolution, world economic growth, and policy issues; Telecommun. Pol., 40 (2016), pp. 383-397.

4 HO, SC. – KAUFFMAN, R.J. – LIANG, TP: Internet-based selling technology and e-commerce growth: a hybrid growth theory approach with cross-model inference; Inf Technol Manag 2011/12. pp. 409-429. https://doi.org/10.1007/s10799-010-0078-x (downloaded 14 December 2020)

concerns. Research questions have been asked: What is the business need behind conducting business with the use of information and communication technology (ICT)? Which factors affect the latest trends? What is the concept of e-commerce? Are there any particular risks associated with the e-commerce business model? The paper focuses on e-commerce and is based on the hypotheses that the e-commerce business model has clearly defined business need and the spread of e-commerce poses new risks, safety and security concerns.

Identification of business need behind e-commerce

In the digital world there is a sound shift from the traditional business channels. The business channels are deeply affected by the means of ICT. With the development of ICTs and their sound footprint on the economy, the habits of consumers have changed as well. The availability of information, services and comparison tools supports informed consumer decisions. The role of physical shopping facilities has changed. In the information economy consumers seek new ways to find the desired goods and services that can be sourced locally or even globally. The role of logistics has evolved to support the underlying processes. The traditional product – and service delivery has fundamentally changed.

Enterprises find that the visibility on the internet is important. Eurostat statistics confirm that e-sales has been stable over recent years in the EU, both the percentage of enterprises that had e-sales and the enterprise turnover generated from e-sales have increased.[5]. According to the Eurostat statistics, web sales – the sales transactions happen via websites or apps – is dominant in all EU countries.[6] The percentage of individuals aged 16 to 74 using the internet for ordering goods or services – within the last 12 months before the survey – to buy or order for private use between 2009 and 2019 shows an increase in the EU 28 countries from 36% to 63%.[7]

During the COVID 19 pandemic digital platforms have provided solutions for many problems (social connection, e-commerce, access to information, online schooling, home office etc.) People tried to switch to online platforms and bought the goods/essentials online adhering to the safety standards.[8] The COVID 19 pandemic clearly has shown its impact on e-commerce.

---

5 see: E-sales and turnover from e-sales, EU-28, 2008 to 2018, source: Eurostat: E-commerce statistics, Statistics explained; (2019). https://ec.europa.eu/eurostat/statistics-explained/pdfscache/14386.pdf (downloaded 14 December 2020)

6 Ibid.

7 Eurostat. 2020. https://ec.europa.eu/eurostat/tgm/graph.do?tab=graph&plugin=1&pcode=tin00096&language=en&toolbox=data (downloaded 14 December 2020)

8 GALHOTRA, B. – DEWAN, A.: Impact of COVID-19 on digital platforms and change in E-commerce shopping trends; 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 861-866, https://doi.org/10.1109/I-SMAC49090.2020.9243379 (downloaded 14 December 2020)

The spread of coronavirus has accelerated the development of e-commerce.[9] WTO report notes the increased use of e-commerce as a result of lockdowns and social distancing measures. Induced by the COVID 19 pandemic, the increase in online consumption is now foreseen as an important trend that will be typical or characteristic of the world economy from now on for some time. At the same time in this online environment the competitive pressure remains. Website accessibility, customer satisfaction, trust and loyalty are of key importance.[10]

The e-commerce business model has become more significant as a result of the COVID 19 pandemic. The pandemic has contributed to the enlargement of the e-commerce business model. Covid 19 had an impact on consumer behaviour. Both B2C and B2B sales have increased. Numerous brick-and-mortar businesses have reallocated their resources to focus on e-commerce. Online shopping has become a preferred way of shopping. This was in particular evident in B2C online sales of medical supplies, household essentials and food products whereby end users obtained the products and services of critical infrastructure sectors. On the other hand, there have been disruptions in supply and demand such as delivery delays, cancellation of orders, unreasonable prices, product safety concerns, cybersecurity concerns, and the need for increased bandwidth. Manufacturing as well as international transport and logistics have been affected by the measures introduced to prevent the spread of the virus.[11] Economic sectors and countries are exposed to a disruption of China's exports of intermediate inputs.[12] The COVID 19 pandemic has clearly demonstrated the need for proper ICTs and the need for digital technologies which should come hand-in-hand with adequate cybersecurity measures.[13]

Critical infrastructures have two-fold "functions" in the context of e-commerce: ICTs are critical infrastructures sectors and are backbones of e-commerce; some key e-commerce products and services are critical infrastructures. The COVID 19 pandemic has demonstrated the role of these sectors. *"Critical sectors are not the same for each country, they depend on the national risk assessment results and on the*

---

9 SUSHKO, O. – PLASTININ, A: E-trading: Current Status and Development Prospects; In: MURGUL V. – PUKHKAL V. (Eds.): International Scientific Conference Energy Management of Municipal Facilities and Sustainable Energy Technologies EMMFT 2019. Advances in Intelligent Systems and Computing, 2021. vol 1258. Springer, Cham. https://doi.org/10.1007/978-3-030-57450-5_67 (downloaded 24 January 2021)

10 PAȘTIU, C. A. – ONCIOIU, I. – GÂRDAN, D. A. – MAICAN, S. Ștefania – GÂRDAN, I. P. – MUNTEAN, A. C.: The Perspective of E-Business Sustainability and Website Accessibility of Online Stores; Sustainability, 2020/22. p. 9780. https://doi.org/10.3390/su12229780 (downloaded 14 December 2020)

11 World Trade Organization: E-commerce, trade and the COVID-19 pandemic Information note; https://www.wto.org/english/tratop_e/covid19_e/ecommerce_report_e.pdf (downloaded 14 December 2020)

12 United Nations Conference on Trade and Development (UNCTAD): Global Trade Impact of Coronavirus (COVID-19) Epidemic. 2020. https://unctad.org/en/PublicationsLibrary/ditcinf2020d1.pdf (downloaded 14 December 2020)

13 DIGITALEUROPE: How DIGITALEUROPE members are supporting efforts to tackle COVID-19; 2020. https://www.digitaleurope.org/resources/how-digitaleurope-members-are-supporting-efforts-to-tackle-COVID-19/ (downloaded 14 December 2020)

impact any disruption would have in the vital services to the society."[14] When determining a country's critical infrastructures, the study should cover both the interdependence and intradependence of the infrastructures.[15] The stability of a particular infrastructure significantly depends on the safety of its information system.[16]

The European Directive on crtical infrastructures defines 'critical infrastructure' as follows: *„an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."*[17] Green Paper on the European programme for critical infrastructure protection (Annex 2) provides indicative list of critical infrastructure sectors and products or service.[18] These sectors are closely linked to the e-commerce business context and are affected by the pandemic. For example, as a result of COVID 19 food security related concerns have increased.[19] The provision of food and safeguarding food safety and security in the Food sector is a critical infratructure element. There was also a shift towards e-commerce to obtain products of the Food sector which has affected the entire food value chain. The COVID 19 pandemic affected the trust in water supply (CI); water quality has become a focus area for the public as well. Health sector (CI), medical and hospital care, medicines, vaccines have key role in combating the virus. The pandemic have shown its effect on Financial sector, payment services. During the COVID 19 pandemic the most of the people have used digital wallets to transfer money but few people are still reluctant to do so.[20] The role of Information and communication technology sector, the internet, the protection of information and network systems has been proved to be vital during the pandemic. ICTs have supported the basic fields of life during the COVID-19 pandemic. The role of ICT sector has increased as a result of the COVID-19 pandemic. ICT is a critical infrastructure sector. These technologies are behind the critical infrastructures and provide support for governments and hospitals.[21] ICTs are fundamental in the spread of e-commerce. The main sectors affected by the consumers' needs with regards to

---

14 European Union Agency for Cybersecurity (ENISA): Critical Information Infrastructures Protection approaches in EU, Final Document; 2015. https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf (downloaded 14 December 2020)

15 MUHA, L.: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme; 2015. ISBN 978-963-12-4434-2

16 Ibid.

17 EURLEX (2008): COUNCIL DIRECTIVE; 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114 (downloaded 14 December 2020)

18 EURLEX (2005): Green Paper on a European programme for critical infrastructure protection; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576 (downloaded 14 December 2020)

19 THILMANY, D. – CANALES, E. – LOW, S. A. – BOYS, K.: Local Food Supply Chain Dynamics and Resilience during COVID-19; Applied Economics Perspectives and Policy, 2020/1. https://doi.org/10.1002/aepp.13121 (downloaded 14 December 2020)

20 GALHOTRA, B. – DEWAN (2020) op. cit.

21 DIGITALEUROPE, 2020. op. cit.

online sales COVID-19 pandemic are more or less the same like food, health, water, ICT.

E-commerce business model

E-commerce in a nutshell is about commodity exchange using the digital surface of the internet. The web surface provides unique opportunities for the market participants and rearranges the business platforms using digital capabilities. One undeniable benefit of e-commerce is the transparency. The business participants are easy to reach and the market conditions are close to what is called perfect market conditions. There is a strong price competition amongst traders offering similar products. The available market for the buyers is wider than ever before: cross-border merchandisers even from overseas participate in the competition. Consumers can better select suppliers that meet their needs but the related information costs have to be paid.

E-commerce facilitates electronic trading with the use of technologies such as electronic data interchange (EDI) and electronic funds transfer (EFT) which were introduced in the late 1970s. Commercial brochures – such as purchase orders or invoices – can be sent electronically using technologies. Since 1990, e-commerce is linked to Enterprise Resource Planning as well as to data search and storage. By now the use of e-commerce services has become widespread, its range covers not only ordering ordinary goods and services but also ordering digital content for immediate consumption and services that make other forms of e-commerce possible.[22]

The shell model of the Net Economy by Kollmann[23] differentiates e-shop (e-commerce; Selling), e-procurement (Buying), and e-marketplace (Commerce) under e-business. These terms are subject to overlap. Other definitions like the Eurostat database, however, cover both e-shop (e-commerce) and e-procurement categories under e-commerce. It makes sense to separate the sales and the purchase side of the commercial deal, however, from the point of view of the transaction itself a purchase for company A from company B is a sale for company B. This justifies to cover both under the same category since this represents the two sides of the same transaction. E-Shops allow for electronic sales of products and services by a company using digital networks and support and conclude operative and strategic tasks for the area of sales.[24]

E-commerce and e-entrepreneurship may appear as synonyms but are in fact not identical. *„E-entrepreneurship refers to establishing a new company with an innovative business idea within the Net Economy, which, using an electronic platform in data networks, offers its products and/or services based upon a purely electronic*

---

22 DELITHEOU, V.: E-entrepreneurship Using Innovation Leads to the Development. Management Studies, 2014/8. pp. 500-508. https://doi.org/10.17265/2328-2185/2014.08.002 (downloaded 14 December 2020)

23 see "The shell model of the net economy". KOLLMANN, T.: What is e-entrepreneurship? – fundamentals of company founding in the net economy; International Journal of Technology Management, 2006/4. pp. 322-340. https://doi.org/10.1504/IJTM.2006.009247 (downloaded 14 December 2020)

24 Ibid.

creation of value. Essential is the fact that this value offer was only made possible through the development of information technology."[25]

E-commerce is the sale or purchase of goods or services through electronic transactions conducted via the internet or other online communication networks. The order is placed via computer networks but the payment and the delivery of goods or service are not necessarily conducted by electronic means. The operation of e-commerce happens via websites or apps through online ordering, reservation or booking, e.g., shopping cart *or* via exchange of electronic messages, EDI-type messages. EDI-type refers to Electronic Data Interchange; this type of e-commerce refers to structured transmission of data or documents between enterprises by electronic means which makes automatic processing possible using for instance EDI or XML format. Noted that orders via manually typed e-mails are excluded.[26]

E-commerce is a subset of e-business. E-business is a wider concept that covers also e-advertising, e-marketing, etc.[27] E-business refers to the integrated support of intracompany processes and related communication while e-commerce relates basically to placing the relationships between companies and consumers to electronic platforms such as online shopping.[28] *"Business and technology and the society itself have fundamental roles. There are „three major driving forces behind e-commerce: business development and strategy, technological innovations, and social controversies and impacts."*[29] The use and spread of e-commerce and information and communication technologies (ICTs) may naturally affect some job descriptions, however, the increase in ICT/e-commerce activities appears to be rather neutral to employment and has not led to decrease in jobs.[30]

The development of ICTs and the emerging role of technology and of digitalization forecast the increasing role of the digitalization of business channels and their increasing role next to the traditional business channels. E-commerce is closely connected to business strategy and e.g. many small and middle size enterprises (SMEs) are ready to change their strategies to adapt to the changes of the business environment.[31] Potential benefits of e-commerce for these enterprises: e-commerce helps to extend their market reach, increased sales, improved external communication,

---

25 Ibid.

26 Eurostat Glossary; https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:E-commerce (downloaded 14 December 2020)

27 SKITSKO, V. I.: E-logistics and M-logistics in Information Economy; LogForum (Scientific Journal of Logistics), 2016/1. pp. 7-16. https://doi.org/10.17270/J.LOG.2016.1.1 (downloaded 14 December 2020)

28 CHIKÁN A.: Vállalatgazdaságtan; Akadémiai Kiadó, 2020. https://doi.org/10.1556/9789634545897. (downloaded 14 December 2020)

29 LAUDON, K. C. – TRAVER, C. G.: E-commerce; Business, Technology, Society, Pearson, 2016. p. 908.

30 BIAGI, F. – FALK, M.: The impact of ICT and e-commerce on employment in Europe; Journal of Policy Modeling, 2017/1. pp. 1-18, ISSN 0161-8938, https://doi.org/10.1016/j.jpolmod.2016.12.004 (downloaded 14 December 2020)

31 ALZAHRANI, J.: The impact of e-commerce adoption on business strategy in Saudi Arabian small and medium enterprises (SMEs), Review of Economics and Political Science, 2018/3.

company image, speed of data processing, and employee productivity.[32] The foreseeable benefits of e-commerce business model underpin that this is worth to focus on them.

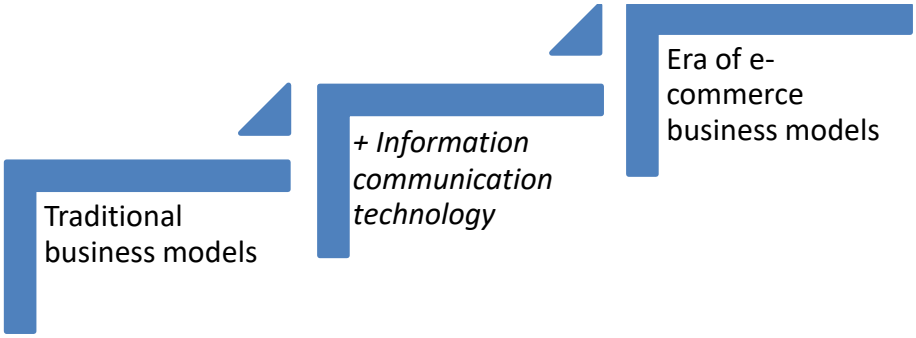

Figure 1: The advancement of business models (simplified depiction)
(Author's own edition)

Business models describe how a company structures and manages its activities.[33] Internet-based (e-business and e-commerce) information systems has laid new foundations for the corporate management as a whole.[34] The fundamental business models have been transformed by ICTs. The new business models that get use of information and communication technologies have lifted the traditional business models to new levels. Figure 2: The advancement of business models is an simplified figure and meant to represent and highlight the role of ICTs behind the spread of e-commerce. The figure disregard other factors and is a simplified depiction and shows that the ICTs are key drivers behind the innovative changes of the business models. Innovation – both the radical and the differential – is a fundamental tool for adapting to changes.[35] Business model innovation is of key importance, is, however, difficult to achieve. In order to innovate business models, ideas and technologies, companies need to develop the capability required for that. Organizational processes must change as well; internal leaders need to manage this and at the same time the corporate culture need to embrace the changes and develop an effectual attitude.[36] E-business has its impact in forms of new business models, transforms the decision-making and authority system of companies; reduces the transaction costs of the whole economy; transforms the cost structure; fills corporate functions with new content (e.g. transformation of marketing function or the possibility of personalized mass production; changes the functioning of coordination mechanisms, creates

---

32 RAHAYU, R. – DAY, J.: E-commerce adoption by SMEs in developing countries: evidence from Indonesia; Eurasian Bus Rev 2017/7. pp. 25-41. https://doi.org/10.1007/s40821-016-0044-6 (downloaded 14 December 2020)

33 CHIKÁN (2020) op. cit.

34 Ibid.

35 Ibid.

36 CHESBROUGH, H.: Business Model Innovation: Opportunities and Barriers; Long Range Planning, 2010/2-3. pp. 354-363, ISSN 0024-6301, https://doi.org/10.1016/j.lrp.2009.07.010 (downloaded 14 December 2020)

opportunities for instantaneous adaptation, for example in electronic marketplaces; etc.[37]

E-commerce can be categorized by consumer segments. Types of e-commerce are e.g. Business-to-Consumer (B2C) E-commerce; Business-to-Business (B2B) E-commerce; Consumer-to-Consumer (C2C) E-commerce; Mobile E-commerce (M-commerce); Social E-commerce; Local E-commerce.[38] This categorization shows the main backbones of e-commerce and grab its main forms.

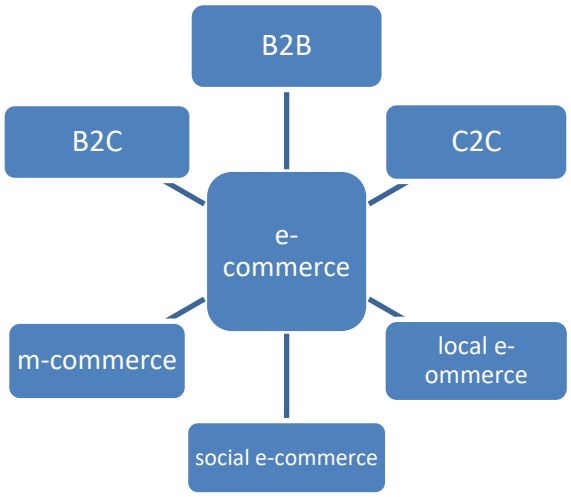

Figure 2: E-commerce types[39]

B2C means pursuing retail business. B2B refers to the trade systems between companies. B2B is the fastest growing form of electronic commerce. C2C creates link between two end users, most probably between two natural persons using electronic market places.[40] Commercial end users are deeply affected by B2C model whereby the daily life has changed. As a result of technological developments and environmental changes including the effects of COVID-19 pandemic everyday people started to meet their needs using e-commerce; e-commerce has become part of day-to-day life, people from each age group have started to catch up on new technologies. M-commerce means doing business and providing services over portable, wireless devices.[41] Social e-commerce gets use of social network sites such as Facebook to conduct business transactions. Social commerce strategy can be developed either through adding social features to the e-commerce platform of the company or through

---

37 CHIKÁN (2020) op. cit.
38 LAUDON – TRAVER 2016.) op. cit.
39 Source: Compiled by author based on LAUDON – TRAVER 2016.) op. cit.
40 CHIKÁN (2020) op. cit.
41 SENN, J. A.: The emergence of m-commerce; Computer, 2000/12. pp. 148-150, https://doi.org/10.1109/2.889097 (downloaded 14 December 2020)

adding commerce features to their social network platform.[42] Local e-commerce means that retailers with physical store (offline) sell online.[43] B2C. B2B, and C2C categorizations are the most typical types of commerce.

The implementation of e-commerce is project and carries risk. The project requires sound project management, careful planning with risk management, adequate realization and monitoring. There is an optimal level of functionalities worth to invest in. Certain functionalities are essential while all the rest can be classified as „accessory". The essential set of functionalities can be grouped round Order processing, Advertising and featured items, Product analysis and Traditional payment. Order processing cover information on order status and delivery details. With respect to the payment methods the necessary functionalities are limited to cash at pickup payment and money transfer payment (traditional payment methods) while credit card payment is not marked as essential. This may relate to the distrust in online payment methods (perceived by the Portuguese focus group of the research). Focusing on the core needs of the consumers promote cost effective way of online commercial presence.[44] The basic needs required for penetrating the e-commerce market as a supplier of goods or services is quite straightforward and open up new way for launching a business. Traditional payment methods are just appropriate to start e-commerce. This is inclusive; suppliers can select the offered payment method according to their cost-benefit assessment. From the customers' perspective their genuine need is to apply their own risk assessment and select the transaction details like payment following their preferences. Due to the conditions during the pandemic the people may generally tend to prefer the electronic payment methods (contactless payments).

The fast growth of e-commerce in Europe has provided basis for the development of related sectors such as e-payment or delivery services. The volume of cash free transactions and goods delivery services have risen in the recent years significantly. There is competition between payment technologies in the payment market. The card payments have the greatest share in the field of e-commerce market where some participants have monopolized role such as American Express, MasterCard, Visa brand cards. Non-bank players such as PayPal, BitCoin, Google Wallet, Facebook are offering payment services as well on the international market; banks have to watch out for them as competitive market players. The courier, express and parcel (CEP) business shows integration and globalization of processes with respect to e-commerce; the international segment is highly concentrated and is

---

42 HUANG, Z. – BENYOUCEF, M.: From e-commerce to social commerce: A close look at design features; Electronic Commerce Research and Applications, 2013/4. pp. 246-259. https://doi.org/10.1016/j.elerap.2012.12.003 (downloaded 14 December 2020)

43 YU, L.: E-Commerce Models, Players, and Its Future; Encyclopedia of Information Science and Technology, Fourth Edition, 2018. https://doi.org/ 10.4018/978-1-5225-2255-3.ch238 (downloaded 14 December 2020)

44 FERREIRA, A. – ANTUNES, F.: Commercial Websites: A Focus on the Essential. In Lee (Eds.): Encyclopedia of E-commerce Development, implementation and Management, IGI Global. 2016/3. https://doi.org/10.4018/978-1-4666-9787-4.ch030 (downloaded 14 December 2020)

organized almost round four major players: the German DHL, the Dutch TNT, the American UPS and FedEx.[45]

Operating a business in the network economy may also accelerate to focus on core competencies in the market and underpin the need for clear strategic objectives. Innovations stimulate e-entrepreneurship. Customers play an important role in creating innovations. Implementation of e-entrepreneurship processes are the interest of companies; these processes strengthen their market position. Implementing e-entrepreneurship activities calls for special knowledge compared to traditional entrepreneurial activities; this affects market entry, electronic products and electronic services, employees, marketing and advertising, transactions, payments, distribution, relationships with customers, cooperation with suppliers and networking. E-entrepreneurship embraces changes; changes are actively looked for and are addressed with swift reaction.[46] The e-commerce business model gives more insight to the enterprises' operation as a result of the online presence and enterprises need to be prepared for this. Organizations need to focus on consistent quality delivery throughout the organization.[47]

The network economy has created new conditions and opportunities for the entrepreneurs that is evident in its sound and growing footprint; its impact is shown in new and innovative business models. ICTs are the engines of these transformational changes. The investment in new technologies can excel the expected results, the changes, however, require adequate project – and change management which includes proper risk management processes.

E-commerce associated risks

Digital transformation intensifies digital security risk in critical infrastructure and essential services across sectors.[48] Digital security risk should be accessed and reduced to an acceptable level; it cannot be eliminated but is manageable.[49] The use of ICTs, the Internet, and IoT (Internet of things) are all the ingredients of this life changing transformation as a result of the spread of e-commerce.

---

45 TSYGANOV, S. – APALKOVA, V.: Digital Economy: A New Paradigm of Global Information Society; Ekonomické Rozhl'ady/Ecomomic Review, 2016/3. pp. 295-311. https://www.euba.sk/en/science-and-research/economic-review (downloaded 14 December 2020)

46 JELONEK, D.: The Role of Open Innovations in the Development of e-Entrepreneurship; Procedia Computer Science, International Conference on Communication, Management and Information Technology, ICCMIT, 2015. pp. 65, 1013-1022. https://doi.org/10.1016/j.procs.2015.09.058 (downloaded 14 December 2020)

47 TATE, M. – JOHNSTONE, D: ICT, Multichannels and the Changing Line of Visibility: An Empirical Study; E-Service Journal, 2011/2. pp. 66-98. doi:10.2979/eservicej.7.2.66 (downloaded 14 December 2020)

48 OECD: Digital security and resilience in critical infrastructure and essential services; OECD Digital Economy Papers, 2019. No. 281, OECD Publishing, Paris, https://doi.org/10.1787/a7097901-en (downloaded 14 December 2020)

49 Ibid.

Both the trader and customer face risks in e-commerce context. The COVID-19 pandemic has accelerated already existing risks and threats and have led to new ones as well.

There are new money laundering and terrorist financing threats and vulnerabilities arising from the COVID-19 crisis[50] E-commerce risks including COVID-19 related financial crime risks require adequate risk management.

E-commerce associated risks, such as:

"Credibility risks" – risks related to the risk of trust between the trading parties and to trustworthiness:

- product unseen at the time of the purchase;
- sometimes misleading or inadequate product descriptions;
- risk of existence of the supplier's legal entity, (esp. relevant for private customers who does not conduct due diligence on counterparties);
- delivery issues;
- privacy concerns;
- customer complaints;
- credit risk – risk that the counterparty is unable or unwilling to pay;
- fraud committed by insiders or customers;
- product scams, and insider trading in relation to COVID-19;[51]
- increased likelihood of various medical scams targeting innocent victims;[52]
- money laundering and terrorist financing threats and vulnerabilities;
- increased fraud due to COVID-19 pandemic: Counterfeiting including essential goods such as medical supplies and medicines, advertising and trafficking in counterfeit medicine;[53]
- etc.

System-, information-, and cyber security related risks:

- increased systems' exposure in e-commerce context;
- cyber security risks and threats - risks to the availability and trustworthiness of independent networked services on both corporate and national security levels, thereof critical infrastructure assets are at particular risk;[54]
- malicious or fraudulent cybercrimes;
- threats of maliciously modifying web e-commerce applications or rendering them unavailable to legitimate customers;

---

50 *„The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global antimoney laundering (AML) and counter-terrorist financing (CFT) standard."* Financial Action Task Force (FATF): COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses, FATF, Paris, France, 2020. https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf (downloaded 14 December 2020)

51 Ibid.

52 Ibid.

53 Ibid.

54 PARN, E. A. – EDWARDS, D.: Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence; Engineering, Construction and Architectural Management, 2019/2. pp. 245-266. https://doi.org/10.1108/ECAM-03-2018-0101 (downloaded 14 December 2020)

- network security risks, network attacks;
- threats posed by employees to information security;
- social engineering and phishing attacks;
- sharp rise in social engineering attacks due to COVID-19 pandemic: Cyber-crime: email and SMS phishing attacks, Business email compromise scams, Ransomware attacks;[55]
- threats that concern private data;
- data integrity risks;
- criminals and terrorists may try to find gaps and weaknesses in national anti-money laundering and counter terrorist financing (AML/CTF) systems while resources are focused elsewhere; etc.[56]

The author differentiates e-commerce associated risk in two major groups: "Credibility risk"– related to the risk of trust and trustworthiness between the trading parties; and System-, information- and cyber security related risks. Risks were accelerated financial crime risks related to the COVID-19 pandemic.

The first risk group "Credibility risks" – risks related to the risk of trust between the trading parties and to trustworthiness – focuses on the genuine nature of risks associated to online transactions. Trustworthiness of the trading partner is main ingredient of a mutually successful business relationship. Risks associated to the trustworthiness of the business partners and customers are present throughout the entire business relationship. Risk levels correlate to the level of trustworthiness of the other party. The role of trust is fundamental element in business relationships and this relates to the robustness of control environment. In online trading context due to the digital surface of the transactions there are particular risks associated to a transaction. Customers' face the risks that: the product is unseen at the time of the purchase and consumers have to rely on the descriptions indicated on the online platform that might be sometimes misleading or inadequate. The received goods might not meet the consumers' needs since the product differs from the anticipated product. There can be issues with the delivery. The mandatory return of product price of an online purchase may mitigate the risk, this has, however, usually some administrative costs, and requires time and effort to have the return accomplished which is sometimes not worthwhile. There is risk regarding the existence of the legal entity from whom the product is purchased, especially relevant for private customers, end users which client segment naturally does not conduct due diligence of the counterparties. E-shops are popular among customers in the digital era, however, customers are also interested in privacy concerns; consumers are well aware of leaving digital traces on the internet. Research based on data collected by means of printed questionnaire (n=431) found that as for purchase refusal due to the requirement of providing too much personal data in the e-shops, there is no difference between men and women when shopping online. Research result uncovered that the majority of respondents have ever refused the purchase.[57]

---

55 FATF (2020) op. cit.

56 FATF (2020) op. cit.

57 MARTISKOVA, P. – SVEC, R.: Digital Era and Consumer Behavior on the Internet; In: ASHMARINA, S. – VOCHOZKA, M. – MANTULENKO, V. (Eds.): Digital Age: Chances, Challenges and Future. ISCDTE 2019. Lecture Notes in Networks and Systems, 84.

At the same time the traders run risks. The credit risk for traders known in traditional business transactions is naturally part of an online transaction. There is elevated risk level of an online transactions. Traders and retailers have to handle customer complaints, if any. On EU level the so called Online Dispute Resolution (ODR) provide solution for dispute management to make online transactions safer and fairer.[58] This stresses the rights of customers when shopping for consumers and the protection of their online reputation for traders. All online retailers and traders in EU, Iceland, Liechtenstein and Norway are obliged to share an easily accessible link to the ODR platform from their website and provide their email address for the ODR platform.[59] Both parties run risks during the transactions, traders can complain against customers as well if they reside in Belgium, Germany, Luxemburg or Poland.[60]

There is risk that insiders and/or customers commit fraud and misconduct. Money laundering and terrorist financing threats and vulnerabilities are of significant importance. Due to the pandemic situation the "credibility risk" has even increased. Counterfeiting essential goods, product and medical scams have spread which misconduct targeted innocent victims.

Both parties – traders and customers – have to achieve the comfort level appropriate for their "risk appetite". The wide scale of options in the electronic trading options facilitates the arrangements and the realization of business deals at ease. For traders the role of counterparty due diligence is even more important as a result of pandemic due to the pandemic-related risks. In e-commerce context customers have greater exposure to risks and threats. Consumers have to be prepared and be cautious against threats to prevent that they became victims of criminals. Risk management, adequate preparation and pre-cautiousness are inevitable for safety and security of a business transaction.

The second risk group – System-, information-, and cyber security related risks – gathers the risks associated with the online trading platforms, the risks related mainly to the systems and to the cyberspace. In the digital era the enterprises face new challenges. The role of infrastructure is key in the digital economy. E-commerce intensifies the systems' exposure through making business services available via the internet or other networks and by integrating with back-office systems like ERP softwares. The use of Web services, multitiered applications, distributed databases, security zones and other technologies make e-commerce complex.[61]

Malicious behaviour recognition in the context of e-commerce, handling cyber risk, threats that concern private data are essential. Threats ranging from maliciously

---

Springer. https://doi.org/10.1007/978-3-030-27015-5_12 (downloaded 14 December 2020)

58 (European Commission, n.d.).

59 Article 14 of the Regulation (EU) No 524/2013.

60 European Commission: An official website of the European Union; Daily News; 2020/6. https://ec.europa.eu/commission/presscorner/detail/en/mex_20_1063 (downloaded 14 December 2020)

61 Reducing e-commerce risks; Work Study, 2002/7. https://doi.org/10.1108/ws.2002.07951gaf.003 (downloaded 14 December 2020)

modifying web e-commerce applications or rendering them unavailable to legitimate customers are amongst the risks to be addressed.[62]

Cyber-security is a key focus area of information security. Cyber threats pose risks to the availability and trustworthiness of independent networked services on both corporate and national security levels, thereof critical infrastructure assets are at particular risk.[63] Cyber-attacks have serious impact on critical infrastructures and services and ensuring the robustness of ICT capabilities against these attacks is a key objective.[64] The ICT security assessment of critical infrastructures is a key problem.[65] Industrial control systems (ICS) are a new major target of cyber criminals.[66] The study of Hurst et al. finds that with damaged or destroyed critical infrastructure components modern society cannot function. The impact of a critical infrastructure failure has four dimensions: (i) safety (the loss of life, serious personal injury or damage to the environment); (ii) mission (the inability of an infrastructure to provide vital services); (iii) business (significant economic losses); and (iv) security (the loss, damage or destruction of physical, cyber or human assets).[67] The impact is very serious. Adequate cybersecurity should ensure the protection of critical infrastructure as well. This is an objective on the agenda of the European Union, on 15.06.2020 the European Commission has announced to grant €38 million for protection of critical infrastructure against cyber and physical threats and making cities smarter and safer, through Horizon 2020, the EU's research and innovation programme.[68] ENSURESEC project is a sociotechnical solution for safeguarding the Digital Single Market's e-commerce operations against cyber and physical threats.[69]

As a subset of cyber security, the area of network security and the management of network attacks are of key importance in the organizations' information security agenda. Network safety is an essential part of safety where security gateways, firewalls, virus protection, the so-called API security are key to a company's security system. The safety of industrial control systems is of crucial importance for large

---

62 European Commission: Cordis: Horizon 2020; End-to-end Security of the Digital Single Market's E-commerce and Delivery Service Ecosystem, 2020. https://cordis.europa.eu/project/id/883242 (downloaded 14 December 2020)

63 PARN – EDWARDS (2019) op. cit.

64 European Union Agency for Cybersecurity (ENISA): Critical Infrastructures and Services; 2020. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services (downloaded 14 December 2020)

65 FOVINO, I. N. – MASERA, M.: Methodology for Experimental ICT Industrial and Critical Infrastructure Security Tests. In: ORTIZ-ARROYO, D. – LARSEN, H. L. – ZENG, D. D. – HICKS, D. – WAGNER, G. (Eds.): Intelligence and Security Informatics; EuroIsI 2008. Lecture Notes in Computer Science, 5376. Springer. https://doi.org/10.1007/978-3-540-89900-6_28 (downloaded 14 December 2020)

66 LEITA, C.: Challenges in Critical Infrastructure Security; In: SADRE, R. – NOVOTNÝ, J. – ČELEDA, P. – WALDBURGER, M. – STILLER, B. (Eds.): Dependable Networks and Services; AIMS 2012. Lecture Notes in Computer Science, 7279. Springer https://doi.org/10.1007/978-3-642-30633-4_1 (downloaded 14 December 2020)

67 HURST, W. – MERABTI, M. – FERGUS, P.: A Survey of Critical Infrastructure Security; In: BUTTS, J. – SHENOI, S. (Eds.): Critical Infrastructure Protection VIII. ICCIP 2014. IFIP Advances in Information and Communication Technology; 2014. p. 441. Springer. https://doi.org/10.1007/978-3-662-45355-1_9 (downloaded 14 December 2020)

68 European Commission (2020) op. cit.

69 European Commission, Cordis (2020) op. cit.

market companies and for strategically important companies (critical infrastructure). In an industrial environment, a network attack carries significant risk of malfunction of operation, complete operation failure, personal injury and/or environmental damage. Different attacks, extortion viruses, malicious codes articulate the need for adequate system of protection ensuring a proper level of border protection.[70]

The integrity and security of data are of critical importance in e-commerce context.[71]

There are threats posed by employees to information security. Human factors are inherent part of the organizational processes. Systems are operated by human beings. *„Security is like a chain. It is as strong as its weakest link. Security depends on people more than on technology. Employees are far greater threat to information security than outsiders"*[72] User behaviours pose risks intentionally or even unintentionally. Social engineering attacks use social skills to acquire and jeopardize information about an organization or its computer system.[73] Phishing is a subset of social engineering. Phishing attacks use email or malicious websites to ask personal information by posing as a trustworthy organization.[74] Social engineering has significantly increased with ICT technologies.[75] Moreover, there have been sharp rise in social engineering attacks due to COVID-19 pandemic. These attacks get use of links to fraudulent websites or malicious attachments to obtain personal information, for instance in form of email and SMS phishing attacks, business email compromise scams, or ransomware attacks.[76] Hospitals and medical institutions are at the forefront of ransomware attacks, for instance malicious websites or mobile applications appear to share COVID-19-related information, insert ransomware to the computer or mobile devices to obtain and lock access to victims' devices until they receive payment. Criminals and terrorists may try to find gaps and weaknesses in national anti-money laundering and counter terrorist financing (AML/CTF) systems while resources are focused elsewhere.[77] The entire e-commerce order to cash business transaction shall withstand the risks effectively and efficiently.

The internet-based business environment is full of security challenges. The enterprise's defence system fulfils an important role. The components of the internal control system – control environment, risk management, control activities, monitoring

---

70 MICHELBERGER, P. – KEMENDI, Á.: DATA, INFORMATION AND IT SECURITY – SOFTWARE SUPPORT FOR SECURITY ACTIVITIES; Problems of Management in the 21st Century, 2020/2. pp. 108-124. http://www.scientiasocialis.lt/pmc/files/pdf/108-124.Michelberger_Vol.15-2_pmc.pdf (downloaded 14 December 2020)

71 DELITHEOU (2014) op. cit.

72 Technical Department of ENISA Section Risk Management ENISA: Risk Management – Principles and Inventories for Risk Management / Risk Assessment methods and tools, 2006.

73 Cybersecurity& Infrastructure Security Agency (CISA): Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks, 2020. https://us-cert.cisa.gov/ncas/tips/ST04-014 (downloaded 14 December 2020)

74 Ibid.

75 ENISA (n.d.). What is "Social Engineering"? https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering (downloaded 14 December 2020)

76 FATF (2020) op. cit.

77 Ibid.

activities and the information and communication levels[78] – are in support of the enterprise safety and security. Risk analysis - and management processes mean value for an organization. *„If you want enterprise security, prepare for risk management"*[79] The control system of an enterprise shall be designed and operated to be strong and resilient enough to handle the risks. The defence system of an enterprise shall be robust to stand the increased volume of risks and threats as a result of the COVID-19 pandemic. The control network shall ensure the optimal level of safety and security.

The risk management framework is complex, and its pillars are deeply embedded to the organization and encompasses the organization as a network. To combat challenges of the digital economy and handle the risks and threats effectively and efficiently, organization shall handle both the system- and information security and the human-factor related risks and threats as well. Risk management procedures are required to identify, analyse the risks and provide the necessary risk response.

Cyber secure e-commerce is a strategic objective that is even more important in light of the COVID-19 pandemic. ENISA's recommendations in support of this strategic objectives from helicopter view are: 1. securing the website for customers (https connections, two-factor authentication where possible, test the security of the website); 2. protection of assets (protecting information like any other business asset, including storage, processing and transmission of information); 3. ensuring secure storage of passwords of client accounts; 4. compliance with data protection requirements (legal framework); 5. monitor and prevent incidents (security incident response plan and relevant measures).[80]

„Security is "simply" a matter of identifying and understanding potential threats and implementing measures to remove or reduce them." Risk depends on threats which increase with exposure to people or other systems; vulnerabilities which increase with complexity; and business impact which increase with the business value of the system and the length of time the system is compromised during an attack. E-commerce has had a big impact on all the factors of risk. These risk factors have to be reduced in order to reduce the overall risk related to e-commerce.[81]

System and ICT driven solutions are desired on the one hand and the human factor-related potential issues are necessary to be handled at the same time on the other hand. The mindset of risk cautiousness and control awareness in the organization are fundamental building blocks of an organization in the era of industry 4.0. This should be part of an ongoing corporate learning procedure and should be accompanied by appropriate trainings to early detection of risks and threats and to successful prevention of attacks. In the digital economy the role of human factors is of crucial

---

78 ANDERSON, R. J. – FRIGO, M. L.: Creating and Protecting Value, Understanding and implementing Enterprise Risk Management; commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2020.

79 MICHELBERGER, P.: Risk Management for Business Trust; In Management, Enterprise and Benchmarking in the 21st Century, Óbuda University, Budapest, Hungary, 2014. pp. 401-413.

80 European Union Agency for Cybersecurity (ENISA): INFOGRAPHIC – Cyber Secure eCommerce; 2020. https://www.enisa.europa.eu/topics/wfh-covid19 (downloaded 14 December 2020)

81 Reducing e-commerce risks (2002) op. cit.

importance to manage the risks. The threat of humans to information protection can be minimized by ideal or strong information security culture.[82] Trainings and ongoing awareness raising can help to reduce the likelihood that employees unintentionally provide information for criminals. Strong ethical foundation, adherence to high ethical standards and employees' commitment are key pillars of the control network that is able to withstand the risks and threats and able to reduce the likelihood of malicious insider behaviour.

The volume and importance of e-commerce relationships have increased. The development of processes in this direction raises safety issues in parallel with the technological developments, and also pointing out the need for appropriate risk management processes, including continuous monitoring. The challenges generated by online spaces require ongoing risk management and adequate responses to incidents. Risks cannot be ignored, risk management is essential as the safe operation of a company can become compromised. The context of e-commerce clearly highlights the necessity of proper risk management processes. Proper risk management contributes to the protection of enterprises and of their assets. E-commerce deeply relies on ICT technology, therefore ICT safety principles and tools available to manage ICT risk are core part of the risk management processes.

Conclusions

In correlation with the expansion of online spaces, it is worth examining the reorganization of business relationships. In the digital world there is a sound shift from the traditional business channels to the business channels „impregnated" by the means of information and communication technology. The E-commerce footprint has become significant. The business model contribute to transparency and to strong price competition. The fast growth of e-commerce in Europe serves as basis for the development of related sectors such as delivery and payment services. Some key e-commerce products and services are critical infrastructures. ICTs belong to critical infrastructures sectors and are building blocks of e-commerce. The COVID-19 pandemic has created new conditions on the market due to the lockdowns and social distancing measures; consumers have naturally started to prefer contactless options for ordering goods & services. This change has provided unique opportunities for the spread of e-commerce for enterprises who were ready to take the challenge with the necessary resources. Considering health and safety concerns the possibility of contactless shopping could gain market and attract consumers who were otherwise unlikely to use online platforms or online payment methods. The sudden event of the COVID-19 pandemic has accelerated the changes as well as the risks and has started an unexpected learning curve, opened new opportunities for businesses, and on the other hand made the operation of traditional business models much harder or even made it impossible for them to operate.

The business model of e-commerce is closely connected to continual improvement, carries, however, new risks and has significant exposure to cyber risk.

---

[82] VEIGA, Da A. – ASTAKHOVA, L. V. – BOTHA, A. – HERSELMAN, M.: Defining organisational information security culture—Perspectives from academia and industry; Computers & Security, 2020. p. 92. https://doi.org/10.1016/j.cose.2020.101713 (downloaded 14 December 2020)

In this widely digitalized environment the volume and impact of security threats are very significant that requires sound protective actions. Proper risk management processes are essential in the context of e-commerce. Safety and security measures should come hand in hand with the development of ICT technology. ICT safety and security have become a must have objective on enterprises' agenda that top management need to focus on. Protection of critical infrastructure and adequate risk management framework have fundamental roles in the defence system.

The research has identified the features of the e-commerce business model. Furthermore, the research has provided an overview of the identified risks, safety and security concerns with respect to the business model for business stakeholders to focus on. The paper has answered the research questions posed and described the need behind the e-commerce business model that get use of ICTs and revealed the role of COVID-19 pandemic and of the critical infrastructures. The paper introduced the concept of e-commerce and the particular risks associated with the e-commerce business model. The paper has confirmed the concept set that the e-commerce business model has clearly defined business need and this is natural part of everyday - and corporate life. The volume of e-commerce transactions confirm that the business need behind e-commerce is well founded and shows an increasing volume. The COVID-19 pandemic has accelerated the need for e-commerce, highlighted the weak points of the system and the elevated to the risk exposure. E-commerce gets use of information and communication technologies which comes hand-in-hand with risks, safety and security concerns linked to the new way of business.

Bibliography:

- ALZAHRANI, J.: The impact of e-commerce adoption on business strategy in Saudi Arabian small and medium enterprises (SMEs), Review of Economics and Political Science, 2018/3.
- ANDERSON, R. J. – FRIGO, M. L.: Creating and Protecting Value, Understanding and implementing Enterprise Risk Management; commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2020.
- BIAGI, F. – FALK, M.: The impact of ICT and e-commerce on employment in Europe; Journal of Policy Modeling, 2017/1. pp. 1-18, ISSN 0161-8938, https://doi.org/10.1016/j.jpolmod.2016.12.004 (downloaded 14 December 2020)
- CHESBROUGH, H.: Business Model Innovation: Opportunities and Barriers; Long Range Planning, 2010/2-3. pp. 354-363, ISSN 0024-6301, https://doi.org/10.1016/j.lrp.2009.07.010 (downloaded 14 December 2020)
- CHIKÁN A.: Vállalatgazdaságtan; Akadémiai Kiadó, 2020. https://doi.org/10.1556/9789634545897. (downloaded 14 December 2020)
- Cybersecurity& Infrastructure Security Agency (CISA): Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks, 2020. https://us-cert.cisa.gov/ncas/tips/ST04-014 (downloaded 14 December 2020)

- DELITHEOU, V.: E-entrepreneurship Using Innovation Leads to the Development. Management Studies, 2014/8. pp. 500-508. https://doi.org/10.17265/2328-2185/2014.08.002 (downloaded 14 December 2020)
- DIGITALEUROPE: How DIGITALEUROPE members are supporting efforts to tackle COVID-19; 2020. https://www.digitaleurope.org/resources/how-digitaleurope-members-are-supporting-efforts-to-tackle-COVID-19/ (downloaded 14 December 2020)
- ENISA (n.d.). What is "Social Engineering"? https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering (downloaded 14 December 2020)
- EURLEX (2005): Green Paper on a European programme for critical infrastructure protection; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576 (downloaded 14 December 2020)
- EURLEX (2008): COUNCIL DIRECTIVE; 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114 (downloaded 14 December 2020)
- EURLEX (2016): Protecting critical infrastructure; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0013 (downloaded 14 December 2020)
- European Commission. (n.d.): Online Dispute Resolution; https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home2.show&lng=EN (downloaded 14 December 2020)
- European Commission: An official website of the European Union; Daily News; 2020/6. https://ec.europa.eu/commission/presscorner/detail/en/mex_20_1063 (downloaded 14 December 2020)
- European Commission: Cordis: Horizon 2020; End-to-end Security of the Digital Single Market's E-commerce and Delivery Service Ecosystem, 2020. https://cordis.europa.eu/project/id/883242 (downloaded 14 December 2020)
- European Union Agency for Cybersecurity (ENISA): Critical Information Infrastructures Protection approaches in EU, Final Document; 2015. https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf (downloaded 14 December 2020)
- European Union Agency for Cybersecurity (ENISA): Critical Infrastructures and Services; 2020. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services (downloaded 14 December 2020)
- European Union Agency for Cybersecurity (ENISA): INFOGRAPHIC – Cyber Secure eCommerce; 2020. https://www.enisa.europa.eu/topics/wfh-covid19 (downloaded 14 December 2020)

- Eurostat Glossary; https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:E-commerce (downloaded 14 December 2020)
- Eurostat. 2020. https://ec.europa.eu/eurostat/tgm/graph.do?tab=graph&plugin=1&pcode=tin00096&language=en&toolbox=data (downloaded 14 December 2020)
- Eurostat: E-commerce statistics, Statistics explained; (2019). https://ec.europa.eu/eurostat/statistics-explained/pdfscache/14386.pdf (downloaded 14 December 2020)
- FERREIRA, A. – ANTUNES, F.: Commercial Websites: A Focus on the Essential. In Lee (Eds.): Encyclopedia of E-commerce Development, implementation and Management, IGI Global. 2016/3. https://doi.org/10.4018/978-1-4666-9787-4.ch030 (downloaded 14 December 2020)
- Financial Action Task Force (FATF): COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses, FATF, Paris, France, 2020. https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf (downloaded 14 December 2020)
- FOVINO, I. N. – MASERA, M.: Methodology for Experimental ICT Industrial and Critical Infrastructure Security Tests. In: ORTIZ-ARROYO, D. – LARSEN, H. L. – ZENG, D. D. – HICKS, D. – WAGNER, G. (Eds.): Intelligence and Security Informatics; EuroIsI 2008. Lecture Notes in Computer Science, 5376. Springer. https://doi.org/10.1007/978-3-540-89900-6_28 (downloaded 14 December 2020)
- GALHOTRA, B. – DEWAN, A.: Impact of COVID-19 on digital platforms and change in E-commerce shopping trends; 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 861-866, https://doi.org/10.1109/I-SMAC49090.2020.9243379 (downloaded 14 December 2020)
- HO, SC. – KAUFFMAN, R.J. – LIANG, TP: Internet-based selling technology and e-commerce growth: a hybrid growth theory approach with cross-model inference; Inf Technol Manag 2011/12. pp. 409-429. https://doi.org/10.1007/s10799-010-0078-x (downloaded 14 December 2020)
- HUANG, Z. – BENYOUCEF, M.: From e-commerce to social commerce: A close look at design features; Electronic Commerce Research and Applications, 2013/4. pp. 246-259. https://doi.org/10.1016/j.elerap.2012.12.003 (downloaded 14 December 2020)
- HURST, W. – MERABTI, M. – FERGUS, P.: A Survey of Critical Infrastructure Security; In: BUTTS, J. – SHENOI, S. (Eds.): Critical Infrastructure Protection VIII. ICCIP 2014. IFIP Advances in Information and Communication Technology; 2014. p. 441. Springer. https://doi.org/10.1007/978-3-662-45355-1_9 (downloaded 14 December 2020)

- IIA Position Paper: The three lines of defense in effective risk management and control January; 2013, pp. 1-7. https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf (downloaded 14 December 2020)
- ISO 31000: 2018 Risk Management – Guidelines
- ISO/IEC 31010: 2019 Risk Management – Risk Assessment Techniques
- JELONEK, D.: The Role of Open Innovations in the Development of e-Entrepreneurship; Procedia Computer Science, International Conference on Communication, Management and Information Technology, ICCMIT, 2015. pp. 65, 1013-1022. https://doi.org/10.1016/j.procs.2015.09.058 (downloaded 14 December 2020)
- JORGENSON, D. W. – VU, K. M.: The ICT revolution, world economic growth, and policy issues; Telecommun. Pol., 40 (2016), pp. 383-397.
- KOLLMANN, T.: What is e-entrepreneurship? – fundamentals of company founding in the net economy; International Journal of Technology Management, 2006/4. pp. 322-340. https://doi.org/10.1504/IJTM.2006.009247 (downloaded 14 December 2020)
- LAUDON, K. C. – TRAVER, C. G.: E-commerce; Business, Technology, Society, Pearson, 2016. p. 908.
- LEITA, C.: Challenges in Critical Infrastructure Security; In: SADRE, R. – NOVOTNÝ, J. – ČELEDA, P. – WALDBURGER, M. – STILLER, B. (Eds.): Dependable Networks and Services; AIMS 2012. Lecture Notes in Computer Science, 7279. Springer https://doi.org/10.1007/978-3-642-30633-4_1 (downloaded 14 December 2020)
- MARTISKOVA, P. – SVEC, R.: Digital Era and Consumer Behavior on the Internet; In: ASHMARINA, S. – VOCHOZKA, M. – MANTULENKO, V. (Eds.): Digital Age: Chances, Challenges and Future. ISCDTE 2019. Lecture Notes in Networks and Systems, 84. Springer. https://doi.org/10.1007/978-3-030-27015-5_12 (downloaded 14 December 2020)
- MICHELBERGER, P. – KEMENDI, Á.: DATA, INFORMATION AND IT SECURITY – SOFTWARE SUPPORT FOR SECURITY ACTIVITIES; Problems of Management in the 21st Century, 2020/2. pp. 108-124. http://www.scientiasocialis.lt/pmc/files/pdf/108-124.Michelberger_Vol.15-2_pmc.pdf (downloaded 14 December 2020)
- MICHELBERGER, P.: Risk Management for Business Trust; In Management, Enterprise and Benchmarking in the 21st Century, Óbuda University, Budapest, Hungary, 2014. pp. 401-413.
- MUHA, L.: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme; 2015. ISBN 978-963-12-4434-2
- OECD: Digital security and resilience in critical infrastructure and essential services; OECD Digital Economy Papers, 2019. No. 281, OECD Publishing, Paris, https://doi.org/10.1787/a7097901-en (downloaded 14 December 2020)

- PARN, E. A. – EDWARDS, D.: Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence; Engineering, Construction and Architectural Management, 2019/2. pp. 245-266. https://doi.org/10.1108/ECAM-03-2018-0101 (downloaded 14 December 2020)
- PAȘTIU, C. A. – ONCIOIU, I. – GÂRDAN, D. A. – MAICAN, S. Ștefania – GÂRDAN, I. P. – MUNTEAN, A. C.: The Perspective of E-Business Sustainability and Website Accessibility of Online Stores; Sustainability, 2020/22. p. 9780. https://doi.org/10.3390/su12229780 (downloaded 14 December 2020)
- RAHAYU, R. – DAY, J.: E-commerce adoption by SMEs in developing countries: evidence from Indonesia; Eurasian Bus Rev 2017/7. pp. 25-41. https://doi.org/10.1007/s40821-016-0044-6 (downloaded 14 December 2020)
- Reducing e-commerce risks; Work Study, 2002/7. https://doi.org/10.1108/ws.2002.07951gaf.003 (downloaded 14 December 2020)
- SENN, J. A.: The emergence of m-commerce; Computer, 2000/12. pp. 148-150, https://doi.org/10.1109/2.889097 (downloaded 14 December 2020)
- SKITSKO, V. I.: E-logistics and M-logistics in Information Economy; LogForum (Scientific Journal of Logistics), 2016/1. pp. 7-16. https://doi.org/10.17270/J.LOG.2016.1.1 (downloaded 14 December 2020)
- SUSHKO, O. – PLASTININ, A: E-trading: Current Status and Development Prospects; In: MURGUL V. – PUKHKAL V. (Eds.): International Scientific Conference Energy Management of Municipal Facilities and Sustainable Energy Technologies EMMFT 2019. Advances in Intelligent Systems and Computing, 2021. vol 1258. Springer, Cham. https://doi.org/10.1007/978-3-030-57450-5_67 (downloaded 24 January 2021)
- TATE, M. – JOHNSTONE, D: ICT, Multichannels and the Changing Line of Visibility: An Empirical Study; E-Service Journal, 2011/2. pp. 66-98. doi:10.2979/eservicej.7.2.66 (downloaded 14 December 2020)
- Technical Department of ENISA Section Risk Management ENISA: Risk Management – Principles and Inventories for Risk Management / Risk Assessment methods and tools, 2006.
- THILMANY, D. – CANALES, E. – LOW, S. A. – BOYS, K.: Local Food Supply Chain Dynamics and Resilience during COVID-19; Applied Economics Perspectives and Policy, 2020/1. https://doi.org/10.1002/aepp.13121 (downloaded 14 December 2020)
- TSYGANOV, S. – APALKOVA, V.: Digital Economy: A New Paradigm of Global Information Society; Ekonomické Rozhl'ady/Ecomomic Review, 2016/3. pp. 295-311. https://www.euba.sk/en/science-and-research/economic-review (downloaded 14 December 2020)
- United Nations Conference on Trade and Development (UNCTAD): Global Trade Impact of Coronavirus (COVID-19) Epidemic. 2020. https://unctad.org/en/PublicationsLibrary/ditcinf2020d1.pdf (downloaded 14 December 2020)

- VEIGA, Da A. – ASTAKHOVA, L. V. – BOTHA, A. – HERSELMAN, M.: Defining organisational information security culture—Perspectives from academia and industry; Computers & Security, 2020. p. 92. https://doi.org/10.1016/j.cose.2020.101713 (downloaded 14 December 2020)
- World Trade Organization: E-commerce, trade and the COVID-19 pandemic Information note; https://www.wto.org/english/tratop_e/covid19_e/ecommerce_report_e.pdf (downloaded 14 December 2020)
- YU, L.: E-Commerce Models, Players, and Its Future; Encyclopedia of Information Science and Technology, Fourth Edition, 2018. https://doi.org/10.4018/978-1-5225-2255-3.ch238 (downloaded 14 December 2020)

ATTILA NÉMETH – SÁNDOR MAGYAR PHD.

AN INVESTIGATION OF DATA USED TO SUPPORT CONTACT TRACING TO CURB THE SPREAD OF COVID-19 PANDEMIC FROM THE ASPECT OF POSSIBLE NATIONAL SECURITY APPLICATION (PART 2)

Abstract

The first part of the publication dealt with to determine to what extent the data managed, stored in information systems or accessible by certain transformations can be used to support contact tracing, which state and which data sources can be used to achieve the goal. In this publication, we aim to determine how and to what extent the data managed, stored in the information systems, or accessible through conversion can be used to support contact tracing, which states can use what data sources to achieve the goal. The publication examines the geographic location data collected by application service providers; the data collected by mobile devices in geographic location service provider systems; data processed in video systems located in a public place; card usage data for financial services; data from global observations by drones.

Keywords: COVID-19, mobile applications, data management

As indicated in our previous publication[1], one of the most efficient means of curbing the spread of the COVID-19 epidemic is the isolation of persons taken ill in order to prevent or reduce further infections. Identification of persons who have been in contact with the infected person in the incubation period, and potentially exposed to the infection i.e. contact tracing is a challenging task.

The outbreak and rapid spread, the uncertainty around the disease resulting in a severe syndrome or even death, and the determination of the governments to curb the spread of the epidemic provided a good opportunity for this study.

Unprecedented emergency measures were introduced, and the governments considered, sometimes implemented, the use of techniques that are otherwise used for purposes of national security and criminal prosecution The otherwise un-published capabilities were published by the governments. The capabilities published provide a good opportunity for analysis for purposes of national security.

This study aims to determine how and to what extent the data managed, stored in the information systems, or accessible through conversion can be used to support contact tracing, which states can use what data sources to achieve the goal.

[1] NÉMETH, Attila – MAGYAR, Sándor: An investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible national security application (Part 1); National Security Review, 2020/2. pp. 52-64.

The data on the citizens' movement, location related to the epidemic[2] have been examined and the following data groups have been identified for the examination of the spread of the epidemic, including the identification of persons having been in contact with the infected person. Data that can be elicited from the information systems, suitable for drawing conclusions related to the spread of the virus are the following:

1. Data on the devices linked to, or establishing contact with to the mobile telephone in the vicinity;
2. Data on geographical location, collected by the application providers (user advertisements, social media search engine or data managed by other online content providers);
3. Geolocation data on the mobile phones collected in the systems of the telecommunication service providers;
4. Data managed in video surveillance systems installed in public areas (cameras, drones, robots), perhaps coupled with facial recognition systems.
5. Card usage data from financial service providers.
6. Details of devices connected to the Internet.
7. Electrical energy consumption data.
8. The health data collection of connected medical devices.
9. Data available in relation to health care services.
10. Data from global surveillance conducted with drones or satellites.

The above list typified the services that may provide the government with data on the movement, geolocation and medical records of the citizens, to assess the effect of the measures taken by the government to curb the spread of the virus, and provide clues for further measures.

In the first part of the publication[3] we examined data on devices connected to mobile phones in close proximity, from the viewpoint of their functioning, accessibility of the data managed by them.

In the present publication we aimed at the examination of the usability of the following data:

- Data on geolocation, collected by the application provider (user advertisements, social media, search engine collected by the application provider or data managed by other online content providers);
- Geolocation data of mobile devices collected in the systems of the telecommunications service providers;
- Data managed in video systems installed in public areas (cameras, drones, robots), possibly coupled with facial recognition systems;
- Card usage data in connection with financial services;
- Data from global surveillance conducted with drones.

---

[2] COMITE NATIONAL PILOTE D'ETHIQUE DU NUMERIQUE: Réflexions et points d'Alerte sur les enjeux d'éthique du numérique en Situation de crise sanitaire Aiguo; https://www.ccne-ethique.fr/sites/default/files/publications /bulletin-1-ethique-du-numerique-COVID19-2020-04-07.pdf (downloaded 24 May 2020)

[3] NÉMETH – MAGYAR (2020) op. cit.

In connection with the spread of the COVID-19 disease it has been established that the virus spreads in the air over a distance of 1.5 – 2 meters.[4] In order that the persons potentially exposed to infection can be effectively identified in a novel approach, the data source based on information systems had to be found or created, where data on persons within 2 meters of the source of infection are available and can be obtained, linked to a specific individual.

During their operation, the application service providers work with GPS-based geolocation data and geolocation data linked to WLAN network identifiers to ensure that users receive geographically relevant advertisements, thereby providing user experience, and maximizing profits from advertisements by the way, and also financing their services.

During the outbreak of the epidemic, application providers, Facebook, Google, Apple did not publicly offer governments to use data on their existing users' in managing the pandemic situation, because thy protect their users' rights and according to their statements they always store geolocation data in an anonymized format.

Facebook

One of the co-authors in an earlier publication[5], conducted research on the Facebook mobile application, more specifically on the location data available to the company, where he made the following statement: In addition to the fact that during the use of the application Facebook has access to location data, if the *"background location data" feature is enabled, the application provider has access to the location data of the device if the user is not using the application.*[6] *Thus, the application provider (Facebook in this case) has continuous access to device location data, ultimately user location data when the device is on and connected to the Internet Facebook will also be notified of user activity if the user of a device with Android OS is not logged into Facebook, in such a way that the owner of the application transfers their Google Advertisement ID of the Android OS to Facebook, who then based on the ID can link it to the user.*[7] *This is for their business purposes, more accurately targeted advertisements, information can reach the user."*[8]

So far, Facebook has contributed to dealing with the spread of the COVID -19 epidemic by making credible news available.

---

4 http://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-COVID-19/novel-coronavirus-2019-ncov (downloaded 16 May 2020)

5 NÉMETH, Attila: The importance of info communication tools in connection with the coordination of mass events and mass movements, with special regard to the European Union's Let's Crowd program; Intelligence Review, 2016/3.

6 https://en-hu.facebook.com/help/337244676357509?helpref=faq_content (downloaded: 29 April 2019)

7 https://nki.gov.hu/it-biztonsag/hirek/nem-csak-ugyfeleirol-gyujt-adatok-a-facebook/ (downloaded 16 May 2020)

8 NÉMETH (2016) op. cit.

Google

Google published location data of the citizens of 131 countries, including Hungary, that are managed by the company, in an anonymized form[9] in a format called COVID-19 Community Mobility Report. The report made a list of anonymized data, as *"they may be of use for public health authorities"*.

The report data show how many people visit shops, foodstuff stores, dispensaries, parks plazas, public transport stops, office buildings, that is, where overcrowding occurs, and thereby there is a high risk of the virus spreading. The data are elicited from the Location History of Google applications in the case of users who enabled the Google Location History[10] feature. Resulting from the terms of use, location history is based on GPS, mobile or WLAN network data which are accurate enough to determine when a user is at a dispensary at the moment. The Google mobility report displays the appearance of Google users at a specific location according to pre -defined categories.

Locations identifiable by Google:

Figure 1: Demonstration of frequency of visits between 03 March and 14 April 2021 in Budapest based on Google users' movement data[11]

9 https://www.google.com/COVID19/mobility/ (downloaded 29 April 2021)

10 https://support.google.com/accounts/answer/3118687?visit_id=637252339694495441-3473975026&p=location_history&hl=en&rd=1 (downloaded 29 April 2021)

11 Source: https://www.google.com/COVID19/mobility (downloaded 29 April 2021)

Public transport stations	Mobility trends in locations like public transport hubs, such as subway stations, compared to baseline bus terminals and railway stations
Workplaces	Mobility trends related to workplaces compared to baseline
Residential areas	Mobility trends related to residential areas compared to baseline
Retail shops, leisure activities	Mobility trends in places like restaurants, cafés, shopping centers, fun fairs, museums libraries and movie theaters compared to baseline
Grocery stores, pharmacies	Mobility trends in places like food markets, food stores, farmers' markets, special cuisine shops, drugstores and pharmacies compared to baseline
Public parks	Mobility trends in places like national parks, public baths/beaches, ports, dog parks, squares and community parks

Figure 2: Report the location categories used by Google[12]

It is clearly visible in the Google list that in addition to large open spaces like parks and residential areas, visit statistics of grocery stores and pharmacies can be established, that is, Google can identify a particular visit by the individual user in a particular type of shop with great certainty. In the report, Google was able to tell the various types of shops from one another, and the following figure shows the number of visitors there were in groceries and pharmacies:

Figure 3: Demonstration of frequency of visits between 28 March and 09 May 2021 in groceries and pharmacies in Budapest based on Google users' movement data[13]

[12] Source: https://support.google.com/covid19-mobility/answer/9824897?hl=en&ref_topic=9822927 (downloaded: 16 May 2021)

[13] Source: https://www.google.com/COVID19/mobility (downloaded: 16 May 2021)

The data are anonymized by Google with the help of Google Ads ID[14], which can be found in every smart phone using Android OS, and in the case of smart phones using the IoS operating system, they can be read via an application, the data are generated for the Google account of the device.

Presenting the data in this way allows us to see how accurately the application providers can retrace the movements of the users.

The data managed by the systems clearly provide an opportunity to positively identify users who are/were at the same location at the same time. In law enforcement and in national security, these data can be used very effectively.

Usability of data found in mobile networks

Today, the penetration of mobile phones all over the world is significant with 5.8 billion subscriptions[15], thus the use of data connected to the mobile phone is the most obvious choice. The number of mobile phone subscriptions per 1,000 of population in most countries of the European Union[16] ranges from 997 to 1438, generally speaking there is at least one mobile subscription per each member of the population.

The mobile phone networks – irrespective of their level of technology – must be suitable for managing the location of the end user devices, thus ensuring continuity of seamless service with ever changing geographical locations. According to the operating principles of cellular networks operating principles, due to the structure and technology of a specific network, they can provide varying degrees of accuracy of position data related to mobile phones.
"During the communication and connection of terminal equipment a number of data are generated that are either stored by the system for maintaining the functioning of the network. for billing, or they are just managed in order to provide seamless service."[17] It is important to highlight the fact that data managed by the mobile service providers and data stored in the systems of the service providers that are necessary for historic data analysis show significant differences. The differing data quality (data detail and data quantity) can be attributed to economic reasons. The management and storage of data kept for the above reasons require significant financial expenditure, thus the majority of data is stored for a short period or not at all following the provision of required operation.

Due to the structure of mobile networks, the data linked to positioning provide varying degrees of accuracy. The usability of the data needs to be examined to determine who was identifiably present in the close proximity (within a distance of 2 meters) of the infected person.

---

14 https://support.google.com/analytics/answer/3123662?hl=en_GB (downloaded: 16 May 2021)
15 https://www.gsma.com/mobileeconomy/ (downloaded: 16 May 2020)
16 https://www.ksh.hu/docs/eng/xstadat/xstadat_eves/i_int074b .html (downloaded: 16 May 2020)
17 NÉMETH (2016) op. cit.

The accounting of data that can be elicited from mobile networks via radio technologies, in terms of area size of location:

a. The base station ID (Cell ID) is stored in connection with the call activity of the device. Location from data related to the Cell ID, where the geographical address can be elicited from the service provider's system. In this case the device can be anywhere within the service area of the cell, even 10 km-s from the geographical address assigned to the Cell ID.
b. Location by arc intersection based on delay of the signal of the aerial belonging to the Cell ID received by mobile phone device (Time of Arrival, TOA). With this method a much smaller area can be identified, a polygon of 100-500 meters in size.
c. Location based on time difference detected (TDOA – Time Difference of Arrival). The signal emitted by the mobile device is received by the aerials belonging to different Cell ID-s at different points in time, on this basis the various network elements can calculate the distance between the device and the aerial. In the case of TDOA, it is possible to determine a polygon with a size of 10-100 m.

The location data with the above precision can only be considered during the management of the epidemic if the service provider manages and stores the data. As for Hungary, Act C of 2003 on electronic communications defines the data to be kept that are *"in case of mobile radiotelephone service the service provider network and Cell ID upon commencement of the communication, furthermore data allowing the location of the actual geographical position assigned to the given Cell ID at the time of the provision of the service."*[18] The various countries may have different regulations in place on the types of data that the service provider is obligated to store and the data detail that can be used for managing an epidemic situation.

Most countries have made public the kinds of data in the system of mobile service providers that they use to curb the spread of the COVID-19 epidemic. The reason for informing the public may have been an intent to demonstrate effective management of the epidemic, while at the same time the data protection concerns also had to be addressed. These the publications, press releases were analyzed, which was suitable to draw conclusions, namely to determine what level of data detail in some countries can be elicited from the network using the stored data.
The practices of three countries were presented in detail.

Finland

This is the most widely used practice among the member states of the EU.

The government of Finland entered into a contract[19] with the largest Finnish mobile communication company on making the nationwide mobile phone subscribers' data available in an anonymized form. The data were used to assess the effectiveness of measures taken to prevent the spread of COVID-19 virus. The changes in the mobile phones' location data were analyzed in order to assess the

[18] Paragraph g, Subsection (1), Section 159/A, Act C of 2003

[19] https://yle.fi/uutiset/osasto/news/chancellor_of_justice_probes_use_of_location_data_to_combat_coronavirus_outbreak/11303135 (downloaded 23 April 2020)

efficiency of the measures restricting freedom of movement, from the most infected areas before the restrictions and after them, to see what massive movements could be identified. No specific individual's movement can be traced from these data. Data from mobile service providers were not used to identify persons getting into contact with confirmed infected persons.

Norway

Norway utilized a particular application, typically they requested data to account for Norwegian subscriptions in various countries.

The two largest mobile phone service providers in Norway made anonymized subscriber location data available to the government. Based on these data, the number of subscribers arriving in Norway from foreign countries in the early stage of the epidemic was determined and also the country from which they came. In the initial period of the epidemic, China, Italy and Austria were considered to be highly infected.[20] Many Norwegian citizens spent their holidays far away from their homeland, such as going for a skiing trip in Austria or Italy. The service providers continuously shared with the government the number of Norwegian subscribers connected to foreign networks, including information on the country they stayed in, which may have contributed to the effective management of quarantine measures. They sent information in short text messages to foreign mobile phones roaming in Norway on the regulations pertaining to quarantine and leaving the country.

Israel

In the case of Israel, the level of data detail the government has access to from the mobile phone service providers was rather clearly demonstrated.

On 15 March 2020,[21] the Israeli Government adopted the emergency measures that allowed the Secret Service (the Shin Bet) to track people sick with COVID-19 and persons getting in contact with them. Up until then, the use of this technique was only permitted in combating terrorism, and no official information has been issued yet on the level of data detail that mobile phone service providers are bound to store and make available to the authorized government entities.

According to reports on the news sites, telecommunications service providers are bound by law to store data linked to communication. That is the case in several countries, but there may be differences in the level of detail of the data linked to communication. According to reports, mobile phone service providers are bound by law to store location data of both parties in the communication, namely location data of both parties, performance data of the antenna servicing the mobile phone call, and

[20] https://www.nrk.no/norge/xl/mobildata-viser-hvordan-nordmenn-reiste-hjem-da-koronakrisen-traff-verden-1.14974784 (downloaded 13 April 2020)

[21] https://www.theguardian.com/world/2020/mar/17/israel-to-track-mobile-phones-of-suspected-coronavirus-cases (downloaded 14 April 2020)

performance data of neighboring antennas detecting the mobile phone signal.[22] With this method, very accurate (10-100 m) location possibilities can be achieved retrospectively from mobile networks.

Based on reports, data of such great accuracy are available that the movement of a confirmed COVID-19 infected person can be traced back historically, and identify those persons with whom he is presumed to have met or been in the same place, then warn those persons in short text messages [SMS][23] to be quarantined.[24]

The mainly European states that made use of data obtainable from mobile phone networks to deal with the epidemic situation are:

Austria	Belgium	Bulgaria
Czech Republic	United Kingdom	Finland
France	The Netherlands	Hungary
Germany	Italy	Spain
Sweden	Slovakia	Israel

Figure 4: Use of data found in mobile networks in dealing with the epidemic
(Authors' own edition)

Based on information in the press, the most accurate geolocation data elicited from mobile phone networks can be obtained in Israel. Looking at the utilization of the data from a national security point of view, it can be stated that the movement of mobile phones logged in the Israeli mobile phone networks can be even retrospectively reconstructed with a high degree of accuracy, which offers a serious potential for the support of national security and law enforcement agencies.

The service providers in the countries subject to the EU regulation - EC Directive 2006/24, repealed in the meantime – did not find an opportunity to provide data of sufficient accuracy (distance of 2 meters between two persons) for contact tracing. An analysis of the aggregated geolocation data may, however, facilitate the assessment of the efficiency of the measures on social distancing, it may provide a model of the transmission and infection potential of the virus and may identify possible "hot spots" of the infection. The Norwegian example stands out with the ability to quantify subscribers who are abroad.

Data managed in video systems installed in public areas (cameras, drones, robots), possibly coupled with facial recognition systems

The recordings provided by video systems installed in public areas are suitable for real-time facial recognition to a limited extent. The facial recognition systems,

[22] https://www.al-monitor.com/pulse/originals/2020/03/israel-palestinians-shin-bet-coronavirus-surveillence.html (downloaded 17 April 2020)
[23] https://www.phillyvoice.com/israel-coronavirus-cell-phone-surveillance-text-alerts-COVID-19-exposure/ (downloaded 12 April 2020)
[24] https://www.timesofisrael.com/the-big-brother-surveillance-that-may-put-you-in-quarantine-or-keep-you-out (downloaded 12 April 2020)

when used in community spaces, are typically installed in major public transport hubs, and in securing events. The pre-installed facial recognition systems may be suitable for curbing the spread of the virus, for identifying possible contacts, for tracing the movement of the confirmed infected person, for identifying contacts. Facial recognition systems achieve effective results through the examination of the whole geometry of the face. If a significant part of the face is covered, its efficiency is significantly reduced.

Facial recognition is a regularly used technique in China. Based on information made public, it is clear that China cannot use the high number of facial recognition systems because the faces are covered with masks due of the legal obligation of masking up.[25]

During the efforts aimed at protection from the virus it became apparent that facial recognition systems cannot effectively support the epidemiologic measures on account of people wearing masks until a solution is found to recognize faces covered with masks. This also affects the efficient performance of facial recognition systems used for national security purposes.

The protective measures taken in relation to COVID-19 have pointed out one of the weak spots in facial recognition systems, namely the fact that covering of the face under the line of the eyes prevents recognition. In as much as researchers and developers find a new technology, facial recognition can, more effectively than before, support national security and law enforcement efforts.

United Kingdom	France	

Figure 5: Facial Recognition System data used in dealing with the pandemic
(Authors' own edition)

Card usage data for financial services.

Of the financial transaction data, the bank card usage data can carry relevant information on the location of the card usage, which come with time stamps.

While studying the spread of the epidemic[26], cash money was identified as a potentially infectious medium, therefore members of the public can more actively make use of card based payment services.

While preparing this study, we only found few references to card usage data being used in combating the epidemic. This can also be attributed to the fact that the duration of time spent by a potentially infected person in the vicinity of ATM terminal does not follow from the card usage.

[25] https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay (downloaded 17 April 2020)

[26] https://www.telegraph.co.uk/news/2020/03/02/exclusive-dirty-banknotes-may-spreading-coronavirus-world-health/ (downloaded 17 April 2020)

The following countries utilized card usage data in the course of dealing with the epidemic:

Czech Republic	United Kingdom	

Figure 6: Card User data utilization in the course of dealing with the pandemic
(Authors' own edition)

Data from surveillance operations conducted by drones

Drones were mainly used in the context of the epidemic to verify compliance with the masking and social distancing rules. Mandatory wearing of masks in public areas also affected the use of drones, as the identification of non-compliant persons became more difficult.

The following countries have used drones in dealing with the epidemic:

Austria	Belgium	United Kingdom
France	Greece	Israel
Germany	Italy	Portugal
Spain		

Figure 7: Drones use of epidemic management course
(Authors' own edition)

Summary

All in all, it can be stated that data from information systems, at the level of both the population and of the individual, contribute to combating the disease.

Data from the mobile telephone networks, especially at the collective level, may be useful in being able to study and model the spread of the epidemic, and in being able to identify the focal points of the epidemic. However, the solution used by Israel allows high accuracy location based on mobile networks, a degree of accuracy that can only be achieved by supporting the application providers.

The application providers made data available only in anonymized form, as an indication of trends, but the accuracy of those data may be inferred by the fact that they were able to identify the data related to visiting grocery stores, pharmacies, using stations and means of public transport. In addition to the aggregated data they designed the software environment of contact tracing applications in support of dealing with the epidemic. The use of the data for national security and law enforcement purposes has great potential.

With regard to data managed by video systems installed in public areas and to facial recognition systems, the weak spot of the systems has clearly been exposed by the fact that identification of persons becomes difficult when a major part the face is covered with a mask. By making the wearing of masks mandatory, the efficiency of

the surveillance systems supporting national security and law enforcement agencies has been significantly reduced.

With regard to financial data no information surfaced that the application was affected, however, the number of card usages has increased, because cash (banknotes) may also carry the virus. Therefore, many more data become available to the national security and law enforcement agencies.

With regard to data from surveillance operations conducted with drones, observations on the video systems apply. Drones as new technology, have found no new function with regard to dealing with the epidemic, and no new aspects of their use in connection with national security and law enforcement efforts have emerged.

Bibliography:

- AMBRUS Eve: Artifical intelligence a community media; Hadmérnök (Military Engineer) 2018/3. pp. 353-361.
- BEIDU: How Baidu is bringing AI to the fight against coronavirus; MIT Technology Review, 2020. https://www.technologyreview.com/2020/03/11/905366/how-baidu-is-bringing-ai-to-the-fight- against-coronavirus / (downloaded: 16 May 2020)
- CALVO, R. A. – DETERDING, S. – RYAN, R. M: Health Surveillance During COVID 19- pandemic How to SafeGuard Autonomy and why it matters, https://www.bmj.com/content/bmj/369/bmj.m1373.full.pdf (downloaded: 16 May 2020)
- CHAN, Justin – FOSTER, Dean – GOLLAKOTA, Shyam – HORVITZ, Eric – JAEGER, Joseph – KAKADE, Sham – KOHNO, Tadayoshi – LANGFORD, John – LARSON, Jonathan – SHARMA, Puneet – SINGANAMALLA, Sudheesh – SUNSHINE, Jacob – TESSARO, Stefano: PACT: Privacy Sensitive Protocols and Mechanisms for Mobile Contact Tracing; Cornell University, 2020. https://arxiv.org/pdf/2004.03544.pdf (downloaded 24 May 2020)
- COMITE NATIONAL PILOTE D'ETHIQUE DU NUMERIQUE: Réflexions et points d'Alerte sur les enjeux d'éthique du numérique en Situation de crise sanitaire Aiguo; https://www.ccne-ethique.fr/sites/default/files/publications /bulletin-1-ethique-du-numerique-COVID19-2020-04-07.pdf (downloaded 24 May 2020)
- FERRETTI, Luca– WYMANT, Chris– KENDALL, Michelle– ZHAO, Lele– NURTAY, Anel – ABELER-DÖRNER, Lucie – PARKER, Michael – BONSALL, David – FRASER, Christophe: Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing; https://science.sciencemag.org/content/early/2020/04/09/science.abb6936/tab-pdf (downloaded 13 April 2020)

- LIN, Leesa – HOU, Zhiyuan: Combat COVID-19 with artif icial intelligence and big data; Academic Journal of Travel Medicine, Oxford, https://academic.oup.com/jtm/advance-article/doi/10.1093/jtm/taaa080/5841603?searchresult= 1 (downloaded 16 May 2020)
- NÉMETH, Attila – MAGYAR, Sándor: An investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible national security application (Part 1); National Security Review, 2020/2. pp. 52-64.
- NÉMETH, Attila: The importance of info communication tools in connection with the coordination of mass events and mass movements, with special regard to the European Union's Let's Crowd program; Intelligence Review, 2016/3.
- O'NEILL HOWELL, Patrick – RYAN-MOSLEY, Tate – JOHNSON, Bobbie: A flood of coronavirus apps are tracking us . Now it's time to keep track of them; MIT Technology review https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-COVID-tracing-tracker/ (downloaded 24 May 2020)
- http://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-COVID-19/novel-coronavirus-2019-ncov (downloaded 16 May 2020)
- https://en-hu.facebook.com/help/337244676357509?helpref=faq_content (downloaded: 29 April 2019)
- https://nki.gov.hu/it-biztonsag/hirek/nem-csak-ugyfeleirol-gyujt-adatok-a-facebook/ (downloaded 16 May 2020)
- https://www.google.com/COVID19/mobility/ (downloaded 24 May 2021)
- https://support.google.com/accounts/answer/3118687?visit_id=637252339694495441-3473975026&p=location_history&hl=en&rd=1 (downloaded 24 May 2021)
- https://www.ksh.hu/docs/eng/xstadat/xstadat_eves/i_int074b .html (downloaded: 16 May 2020)
- https://www.gsma.com/mobileeconomy/ (downloaded: 16 May 2020)
- https://support.google.com/analytics/answer/3123662?hl=en_GB (downloaded: 16 May 2020)
- https://www.google.com/COVID19/mobility (downloaded: 24 May 2021)
- https://yle.fi/uutiset/osasto/news/chancellor_of_justice_probes_use_of_location_data_to_combat_coronavirus_outbreak/11303135 (downloaded 23 April 2020)
- https://www.nrk.no/norge/xl/mobildata-viser-hvordan-nordmenn-reiste-hjem-da-koronakrisen-traff-verden-1.14974784 (downloaded 13 April 2020)
- https://www.theguardian.com/world/2020/mar/17/israel-to-track-mobile-phones-of-suspected-coronavirus-cases (downloaded 14 April 2020)
- https://www.al-monitor.com/pulse/originals/2020/03/israel-palestinians-shin-bet-coronavirus-surveillence.html (downloaded 17 April 2020)

- https://www.phillyvoice.com/israel-coronavirus-cell-phone-surveillance-text-alerts-COVID-19-exposure/ (downloaded 12 April 2020)
- https://www.timesofisrael.com/the-big-brother-surveillance-that-may-put-you-in-quarantine-or-keep-you-out (downloaded 12 April 2020)
- https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay (downloaded 17 April 2020)
- https://www.telegraph.co.uk/news/2020/03/02/exclusive-dirty-banknotes-may-spreading-coronavirus-world-health/ (downloaded 17 April 2020)

BÉLA PUSKÁS PHD – BENCE LÁZÁR

CYBER PROTECTION OVERVIEW

Abstract

The explosive development of cyberspace in recent years, the increased role and importance of cyber security and cyber operations have become unquestionable. In addition to international commitments, Hungary's goal is clearly to create a secure and innovative cyberspace that is competitive and meets new technical challenges. It is worth summarizing the major events of the recent period on the part of both our domestic and international associations.

Keywords: security, cyber security, cyber protection, information security

Introduction

Information security is understood to mean the confidentiality, integrity and its protection from threats. The number of information security threats has increased significantly in recent decades. The reason for this is the evolving technology, the soaring rise of informatics, the global spread of the Internet. These phenomena also had a number of negative consequences such as the spread of computer viruses, the entering of espionage into a new dimension, the golden age of hacking activities, etc. It has become a general need to create an information security system that is able to provide adequate protection against all kinds of threats, and thus is able to protect sensitive data and information managed by the organization.

Serious attention should be given to the growing cybersecurity challenges because security problems, such as breakdowns or viruses are capable of causing serious damage. According to a Hungarian survey of Panda Security conducted in 180 countries around the world in 2019, more than 60 percent of the 260 small and large companies that responded have had a successful cyberattack in the previous 12 months.[1]

"Cyberspace is an umbrella term that includes users, devices, software, processes, information, services and systems stored or transmitted that are linked directly or indirectly to a computer network."[2]

"Cyber security" is understood as the continuous and planned use of political, legal, economic, educational and awareness-raising means that ensure an acceptable level of risks in handling existing threats in cyberspace, and also change the

1 https://hirek.pandahungary.hu/panda-security-sajtokozlemeny/ (downloaded 15 June 2020)

2 KOVÁCS, László: Cyber Security and Strategy; Dialóg Campus Publishing House, Budapest, 2018. p. 18

cyberspace into a safe environment to ensure the uninterrupted operation of the social and economic processes.[3]

"Cyber defense" is protection against threats occurring in cyberspace, including the maintenance of own cyberspace capabilities.

"Cyber operation" refers to activities related to the operation of the electronic data management and data management capabilities with cyberspace, including activities, processes for the manipulation or attack in this direction.

Historical overview

At the end of the 20th century, in tandem with the advent and spread of the Internet, threats to computer systems emerged. The first really devastating threat was the Trojan virus that caused the 1982 Soviet gas pipeline to explode,[4] which was built into the monitoring software and overloaded the equipment by changing the pressure control of the pumps and valves in a timed manner, the detonation of which was so powerful that it was even visible from space.

The North Atlantic Treaty Organization (NATO)[5] for the first time faced cyber warfare during the 1999 bombing of Kosovo when military operations began without the UN Security Council authorization, before the starting command was issued, then the Alliance's website became inaccessible. The Serbian hacker group named Black Hand (Crna Ruka) was responsible for the attack.[6]

One of the best-known cyberattacks took place in Estonia in the spring of 2007, when so-called overload (DDoS)[7] attacks were launched against the Estonian state administration that crippled communication lines and websites used by government offices, banks and the media. The country's Internet traffic control centers shut down repeatedly because the data traffic volume increased to more than one thousand times the normal daily volume. Following the attack certain servers involved in the attack were successfully identified, which were presumably operated in the Russian Federation, Russia, however, denied the charges against it.

In July 2009, there was a hacker attack against the South Korean government. In this pre-planned operation, attacks were received from a total of 86 IP addresses, which can be linked to 16 countries. The South Korean intelligence, in light of the current security situation, put the blame for what happened on North Korea, but no signs of North Korea's involvement could be found.

Since then, espionage and attacks against various information systems has become an almost constant threat. Ever more frequent events have increasingly

3 Government Resolution No. 1139/2013. (III. 21.) On the National Cyber Security Strategy of Hungary
4 Logic Bomb
5 North Atlantic Treaty Organisation
6 Source: SZENTGÁLI, Gergely: Development of NATO's cyber defense policy; National and Security 2013/3-4. pp. 76-83.
7 Distributed Denial of Service

contributed to the growing awareness of the seriousness of cyber threats. It is also clear from the cases mentioned above that in most cases it is not possible to identify the perpetrators of the attacks with 100% certainty.

Under Article 5 of the NATO Charter, an attack against a member country is considered an attack on the whole military alliance. With respect to cyberspace, this principle is difficult to implement, as the 2007 cyberattack in Estonia demonstrate that the clarification of the identified perpetrators involved is not unambiguous, and other issues may also emerge such as when an attack can be considered to be directed against military targets and when it can be considered to be directed against a civilian target, etc.[8]

Due to, among other things, the incident in Estonia in the spring of 2007, and the growing number of cyberattacks, the development of protection in the global cyberspace is a priority. To this end, the NATO Cooperative Cyber Defense Center of Excellence (NATO CCD COE) was established on 14 May 2008 in Tallinn, which Hungary joined on 23 June 2010. It is responsible for strengthening the cyber defense capabilities of NATO member countries and their partners, training and research and development.[9]

In 2013, a decision was made on NATO's cyber defense response capability,[10] which is responsible for protecting the computer systems of 51 NATO facilities.[11]

At the 27th NATO Summit in Wales in 2014, NATO adopted an enhanced policy on the subject. *"In the future, a cyberattack will be considered by the Alliance as an act covered by collective defense, which the NAC*[12] *will decide on a case-by-case basis."*[13]

NATO directive

NATO's Cyber Defense Policy (CDP[14]), adopted at the end of 2007, laying down the Alliance's cyber defense principles and common structures and standards, was the first step. This is followed by NATO's Strategic Concept[15] highlights the need to further develop the capabilities to prevent, detect and combat rapidly evolving, increasingly frequent and sophisticated cyber-attacks, and to recover from cyber-attacks.

---

8 The NATO Cyber Defense Manual (Tallinn Manual and Tallinn Manual 2.0) attempts to regulate the legal framework for cyber warfare. https: //www.nato.int/cps/en/natohq/topics_78170.htm, (downloaded 25 June 2020)

9 PUSKÁS, Béla Dr.: The Relationship between Diplomacy and Cyberspace EXPLORATORY REVIEW 2018/3. pp. 39-54.

10 NATO Computer Incident Response Capability, NCIRC

11 Source: http://www.ncirc.nato.int/

12 North Atlantic Council

13 Wales Summit Declaration, paragraph 72

14 NATO Cyber Defense Policy

15 Strategic CoOncept 2010; https://www.nato.int/cps/ic/natohq/topics_82705.htm (downloaded: 28 May 2020)

NATO 's Cyber Defense Concept (CDC)[16] was presented in March 2011, which formed the basis of the NATO CDP - Protecting Networks, adopted at the NATO Defense Ministers' Meeting on 8 June 2011.[17] This policy document was complemented by an action plan, and the NATO CDP Implementation Plan sets out in detail the responsibilities of Allied forces and the cyber defense activities to be carried out. The significance of the former documents is that it has placed cyber defense on a par with the fight against terrorism and crisis management tasks generated by conflicts outside NATO, and has made it a pillar of the chapter on defense and deterrence.

In April 2013, the Alliance published the *"Tallinn Handbook on the Applicability of International Law to Cyber Warfare"* to address the legal aspects of cyberattacks on individual states[18] on how international law applies to cyber conflict and cyber warfare. Continuation of the Tallinn Handbook 2.0.,[19] published in February 2017, supplementing the scope of the previous manual. This is currently the most comprehensive analysis on the subject, providing a single legal framework for dealing with all malicious cyber operations.[20]

Cyberspace, similarly to land, sea and air, was recognized as a new operational area, and cyber operations were recognized as part of hybrid warfare at the NATO Summit in Warsaw in July 2016,[21] on the basis of the Joint Resolution on cyberspace. The emergence of the new theater has an impact on defense and operational planning alike.

As a consequence of the decision, NATO issued the 2017 NATO Capability Goals in August 2016[22] that set before the member states much higher standards than ever before for the 2018-2020 period. These requirements display capacity building in the area of cyber defense at Member State level and the requirement of integrating cyber defense capabilities in military operational planning.

According to NATO's position, the development of cyber defense capability is essentially a national task, so the appropriate level of cyber defense of the Alliance is ensured if the Member States are individually, one by one, able to ensure the adequate level of protecting the systems they use.

International cooperation is of utmost importance in establishing effective defense, based on compatibility between countries at technical, procedural and regulatory levels alike.

---

16 NATO Cyber Defense Concept

17 Defending the Networks – NATO Policy on Cyber Defense 2011.

18 SCHMITT, Michael N.: Tallinn Manual on the International Law Applicable to Cyber Warfare 2013. https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to- cyber-warfare / 50C5BFF166A7FED75B4EA643AC677DAE (downloaded 08 June 2020)

19 Tallinn Manual 2.0.; https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9 (downloaded 08 June 2020)

20 https://ccdcoe.org/research/tallinn-manual/ (downloaded 08 June 2020)

21 NATO Warsaw Summit

22 NATO Capability Target Package

At present, with regard to the Alliance's cyber defense commitments, focused training courses for Member States and the continuous flow of information for them will be given top priority, and NATO will ensure the protection of the Alliance's networks. In addition, a cyberspace operations command has been set up to integrate into military operations, and rapid response teams are being set up.

The Declaration adopted at the NATO Summit in Brussels, 11-12 July 2018,[23] sets out specific proposals and directions for development to address the triad of terrorist, cyber and hybrid threats. The establishment of a Cyberspace Operations Center[24] to be set up before 2023 was announced, with the aim of creating a permanent, comprehensive protection against cyber-attacks, as well as managing specific aspects of cyberspace.[25]

EU directive

In June 2004, the European Council called for a strategy on critical infrastructure protection. As a result, the Commission of the European Communities adopted a Communication on 20 October 2004 entitled *"Critical Infrastructure Protection in the Fight against Terrorism"*.

In 2005, the Council of the European Union passed a decision on attacks against information systems.[26]

On 17 November 2005, the Commission also adopted a Green Paper[27] on a European Program for Critical Infrastructure Protection and decided on the establishment of a warning information network.[28]

The first all-European cyber exercise took place on 4 November 2010. This was made possible in 2009 by the European Commission's Communication on Critical Information Infrastructure Protection entitled *"Protecting Europe from large-scale cyber-attacks and network disruptions: enhancing preparedness, security and resilience"*.[29]

On 19 May 2010, the European Union published a Communication entitled the *"Digital Agenda: A Commission action plan to boost Europe's prosperity"*.[30]

---

23 Brussels Summit Declaration; https://www.nato.int/cps/ic/natohq/official_texts_156624.htm (downloaded 28 May 2020)
24 Cyberspace Operations Center, CyOC
25 NAC Communique Issued by Heads of State & Government, Brussels, 11-12 July 2018
26 Council Framework Decision 2005/222 / JHA
27 COM (2005) 576 final
28 CIWIN, Critical Infrastructure Warning Information Network.
29 COM (2009) 149
30 IP-10-581_EN

The goal of the Digital Agenda was to create a system that could respond in a timely manner to computer attacks. In this context, the aim was to establish a network of CERT-s.[31]

In September 2010, the European Commission announced two new measures to help defend against attacks on Europe's key IT systems. The first action of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA.[32] In addition to repealing the Framework Decision, the aim was to strengthen the fight against cybercrime by bringing Member States' criminal justice systems closer together and encouraging cooperation between authorities. The second measure[33] was a Joint Regulation of the European Parliament and of the Council[34] on the European Network and Information Security Agency (ENISA).[35] The purpose of the regulation is to strengthen, modernize and define ENISA's new five-year mandate. ENISA will help the EU, the EU Member States and businesses to better prevent and address cybersecurity challenges.

Also in 2010, the *"Communication from the EU Commission to the European Parliament and the Council Implementing the EU Internal Security Strategy: Five steps towards a more secure Europe"*[36] set the goal of increasing the security of IT networks.

Objective 3 set out to increase the security of cyberspace, which was to be implemented in several steps.

- Capacity building in the field of law enforcement and justice, with the announcement of the establishment of a Cybercrime Center, which is, inter alia, a point of contact between national CERTs.
- Working with industry to equip and protect citizens. At this point, special attention was paid to the flow of information, easier access to information. The Commission will set up a real-time central database to share resources and best practices between Member States and the industry.
- Improving the ability to respond to cyberattacks. This is to be achieved, inter alia, by linking Member States' national / governmental CERTs. The CERT should work as a network element in a single system.[37]

2013 was a milestone in the construction of the EU's cyber defense, the birth of a document also known as the 'Cyber Defense Act', the European Union's Cyber Security Strategy. Among the main content elements of an open, secure and reliable

---

31 Computer Emergency Response Team (CERT) – (US term: Computer Event Management Center; EU term: CSIRT, Computer Security Incident Response Team)

32 COM (2010) 517

33 COM (2010) 521

34 Regulation (EC) No 460/2004 provides for its establishment for a period of 5 years.

35 ENISA (European Union Agency for Network and Information Security), European Network and Information Security Agency

36 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM/2010/0673) (downloaded 12 December 2020)

37 PUSKÁS, Béla: Changes in IT systems and the legal environment; NEWS = SIGNAL BADGE, 2013/2, pp. 204-214. HU ISSN 2061-9499

cyberspace, military and operational implications of cyber defense appear robustly. The most important thing to say about the principles of cyber security is that it strategically puts the digital space on an equal footing with physical space and the importance of legal regulation, protection and control issues that apply to them.

In 2016, two key documents were adopted in Brussels: the new EU Security Strategy and Directive (EU) 2016/1148 of the European Parliament and of the Council on the security of network and information systems ensuring a uniformly high level throughout the Union (NIS[38] Directive). There is hardly a point in the new global European security strategy that does not mention cyber defense. Four of the five priorities identified in the document are displayed explicitly. Emphasizing as a new element that, in the event of an attack, the Union will assist its Member States in their rapid recovery.[39] The strategy emphasizes that it also protects its values in the digital world and promotes a free and secure global Internet. To ensure this, it delegates a complex set of tasks, covering critical (information) infrastructure, data protection, citizen protection, cyber diplomacy, global cooperation and multilateral digital governance.

The Network and Information Systems Directive provides the legal framework for measures to increase cybersecurity in the EU, and it also serves as practical guidance.[40] It identifies strategic goals for all Member States, obligations such as the development of National Strategy for the security of networks and information systems and the establishment of joint Cooperation Groups. It places great emphasis on education and training programs, the planning of research and development. The directive also includes the strengthening of the EU cybersecurity agency and the introduction of an EU cybersecurity certification scheme.

The NIS Directive is the first Community regulation in the field of information security, which defines rules along geographical lines and mandatory cooperation between different institutions. Its aim is to launch Europe-wide co-operation and to lay the foundations of common terminology and institutions and to deter perpetrators from cyberattacks, and to enable member states to respond immediately. The Directive had to be integrated by the member states in their own legal systems before 9 May 2018, and the deadline for identifying actors providing essential services related to cyber security was 9 November 2018.

Domestic regulation and objectives

Cyber security in Hungary is first mentioned in the National Security Strategy issued in 2012.[41] The document defined the strategic directions in accordance with the then security environment and makes a generalizing mention of the role and place of

[38] Network and Information Systems
[39] Shared Vision Common Action
[40] NIS Toolkit
[41] Government Decree No. 1035/2012. (II. 21.) on the National Security Strategy of Hungary. Hungarian Gazette 2012/19., pp. 1378-1397. http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK12019.pdf (downloaded 28 May 2020)

the Hungarian Defense Forces (HDF) in this area, however, it does not address the protection of cyberspace or cyberspace operational activities.

The importance of cyber security is reflected in more detail in Government Decree No. 1139/2013 on the National Cyber Security Strategy. (III. 21.) and this Government Decree states that Hungary undertakes to perform the tasks related to its responsibility to protect cyberspace.

The basic goal of the 2013 Strategy is to ensure the creation of a free, secure, forward-looking cyberspace by creating the basic pillars of information security, as well as by using and further developing existing tools, organizations and knowledge.

The legal environment created by Act L of 2013 on the Electronic Information Security of State and Local Government Bodies, enacted together with the adoption of the Strategy and amended several times since then, facilitated the establishment and consolidation of state organizations operating in the field of cyber security with regard to state and administrative electronic information systems.

With regard to state and local government organizations covered by the Information Security Act, the National Cyber Defense Institute belonging to the National Security Service is responsible for the management of security incidents.[42]

In 2014, the government adopted the National Info-communication Strategy, which set the goal of developing the Hungarian digital environment on four pillars:

- digital infrastructure,
- digital economy,
- digital state,
- digital skills.

In military terms, the recognition of cyberspace as an area of operation as a new dimension in addition to traditional land and air was the amendment in 2018 to the Defense Act.[43]

In a Government Decree issued in 2018, the Government adopted its strategy for Hungary's security of networks and information systems.

"The Government

1. adopts Hungary's Strategy for the Security of Network and Information Systems (hereinafter: the Strategy);

2. calls on the Minister of the Interior, with the involvement of the ministers concerned, to draw up an action plan for the implementation of the measures referred to in Articles 1 to 56 of the Strategy"[44]

---

42 http://nbsz.hu/?mid=42

43 Act CXIII of 2011 on National Defense and the Hungarian Armed Forces, as well as on measures that can be introduced in the special legal order. Paragraph 22 of Section 80.

44 Government Decree No. 1838/2018. (XII. 28.) on the Strategy for the Security of Network and Information Systems in Hungary

The explosive development of cyberspace in recent years, the increased role and importance of cyber security and cyber operations can be well observed in Hungary's new National Security Strategy issued at the end of April 2020,[45] where we can already find a much larger number of guidelines in this area. The document could make a big difference to cyberspace for the future. The most significant part is the discussion of potential physical responses to cyberattacks, which is the first official government document to state and record all of this. Its purpose is to act as a deterrent from a security and defense policy point of view, and it is also a priority for the area. Statements about offensive cyber capabilities have been avoided in security policy environments in the past, although offensive activities may be necessary to achieve complex protection. Because cyberspace players cannot be identified exactly, we do not know exactly when and from what direction hostile operations may come from.

In terms of proactive self-defense, we can prevent an attack (for example, by attacking the computer systems of a potential attacker) before the attack on our own systems has started.

In addition to international commitments, Hungary's goal is clearly to create a secure and innovative cyberspace that is competitive and meets new technical challenges. It is important to build a secure electronic public administration system and to strengthen social security awareness.

NATO's oft-quoted motto related to the cyber issue is: *"All of Us are Smarter than One of Us"*, which refers to the importance of cooperation between Member States. By all means, the strengthening of technical cooperation is to be emphasized, both domestic and international, especially with the EU, NATO and the Visegrad Countries, with our allies, which covers a variety of research centers, universities and relevant incident management centers, communication based on trust and education, training. The goal is to create a competitive domestic knowledge base.

As cyberattacks show ever increasing complexity and frequency, as well as the damage done by them is more and more significant, it is necessary in all sectors to prepare for attacks, most importantly in the case of government agencies, critical infrastructures and multinational big companies.

In order to provide effective protection, the operation of well-functioning technical units (CSIRTs[46]) to deal with various security incidents and sectoral network security emergency response teams (CERTs[47]) that coordinate them should be ensured.

---

45 Government Decree No. 1163/2020. (VI.21.) on the National Security Strategy of Hungary. Hungarian Gazette, 2020/81., pp. 2101-2119. http://www.kozlonyok.hu/nkonline/index.php?menuindex=0400&pageindex=0400 (downloaded 28 July 2020)

46 CSIRT = Computer Security Incident Response Team

47 CERT = Computer Emergency Response Team

Summary

In summary, it can be stated that cyber defense is undergoing continuous development in both the domestic and international arenas. A strategic-level system of investigative criteria has been developed to help develop the five levels of cyber defense capabilities, namely identification, defense, detection, response, and recovery capabilities.

An increasing number of Allied cyber defense exercises facilitate cooperation and information sharing between countries. Due to the complexity of the global cyberspace, it is inconceivable to address the challenges effectively without international cooperation.

Cyberspace as a new area of operations, as well as the new National Security Strategy sets clear goals and tasks in the area of the military processes. In the course of the development of the HDF, the development of cyberspace operational capabilities, the design of the organizational framework required for the planning, organization and command of cyberspace operations is of utmost importance. In addition to "laboratory" table-top exercises in training centers, it is necessary to be involved in live military operations and to gather the experience gained from them.

Based on the experience of recent years, it can be stated that Hungary treats the challenges created by cyberspace as a priority, it strives to keep abreast with the development of technology, and supports international initiatives and forms of cooperation.

Bibliography:

- 2007 Cyber Attacks Estonia: https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia, (downloaded 28 May 2020)
- Act CXIII of 2011 on National Defense and the Hungarian Armed Forces, as well as on measures that can be introduced in the special legal order
- Brussels Summit Declaration; https://www.nato.int/cps/ic/natohq/official_texts_156624.htm (downloaded 28 May 2020)
- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM/2010/0673) (downloaded 12 December 2020)
- CYBER DEFENSE; https: //www.nato.int/cps/en/natohq/topics_78170.htm, (downloaded 25 June 2020)
- FEKETE-KARYDIS, Klára – LÁZÁR, Bence: Development of cyber defense strategies, cyber defense challenges, current events (2.); Home Defense Review 2019/5.

- FEKETE-KARYDIS, Klára – LÁZÁR, Bence: The cyber military dimensions; Military Review, 2020/3. http://real.mtak.hu/109353/1/Fekete-KarydisKlaraLazarBence.pdf (downloaded 15 June 2020)
- Government Decree No. 1035/2012. (II. 21.) on the National Security Strategy of Hungary. Hungarian Gazette 2012/19., pp. 1378-1397. http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK12019.pdf (downloaded 28 May 2020)
- Government Decree No. 1163/2020. (VI.21.) on the National Security Strategy of Hungary. Hungarian Gazette, 2020/81., pp. 2101-2119. http://www.kozlonyok.hu/nkonline/index.php?menuindex=0400&pageindex=0400 (downloaded 28 July 2020)
- Government Decree No. 1838/2018. (XII. 28.) on the Strategy for the Security of Network and Information Systems in Hungary
- Government Resolution No. 1139/2013. (III. 21.) On the National Cyber Security Strategy of Hungary
- https://ccdcoe.org/research/tallinn-manual/ (downloaded 08 June 2020)
- KOVÁCS, László: Cyber Security and Strategy; Dialóg Campus Publishing House, Budapest, 2018.
- MUHA, Lajos –KRASZNAY, Csaba: Security Management of Electronic Information Systems; https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/7135/Az%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20biztons%C3%A1g%C3%A1nak%20menedzsel%C3%A9sej%C3%B3.pdf?sequence=5&isAllowed=y (downloaded 03 October 2019)
- NATO Warsaw Summit Communiqué 07/08/2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm (downloaded 25 November 2018)
- PUSKÁS, Béla Dr.: The Relationship between Diplomacy and Cyberspace EXPLORATORY REVIEW 2018/3. pp. 39-54.
- PUSKÁS, Béla: Changes in IT systems and the legal environment; NEWS = SIGNAL BADGE, 2013/2, pp. 204-214. HU ISSN 2061-9499
- RENNER, Wolfgang: The Military Role in Cyberspace; Lecture, NIAS'18 Symposium, Mons, Belgium, 16-18 October 2018.
- SCHMITT, Michael N.: Tallinn Manual on the International Law Applicable to Cyber Warfare 2013. https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to- cyber-warfare / 50C5BFF166A7FED75B4EA643AC677DAE (downloaded 08 June 2020)
- SZENES, Zoltán: Forward to the past? NATO After Wales, Foreign Affairs Review, 2014/3.
- SZENTGÁLI, Gergely: Development of NATO's cyber defense policy; National and Security 2013/3-4. pp. 76-83.

- Tallinn Manual 2.0.; https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9 (downloaded 08 June 2020)
- The Original Logic Bomb article: https://rconnon12.wordpress.com/2014/10/26/third/, (downloaded 28 May 2020)

AUTHORS OF THIS ISSUE

- **ÁGNES JOBST** PhD is a Research Associate, Historical Archives of the State Security Services of Hungary, Budapest;
- **ÁGNES KEMENDI** is a PhD student, Doctoral School of Safety and Security Sciences, Óbuda University, Budapest, Hungary;
- **ANDRÁS NOVÁK** is a journalist specialising in security and defence;
- **ATTILA NÉMETH** is a PhD student at the Óbuda University Doctoral School on Safety and Security;
- **BÉLA PUSKÁS** is a Colonel of the Hungarian Armed Forces;
- **BENCE GÖBLYÖS** is an Army Captain of the Hungarian Armed Forces;
- **BENCE LÁZÁR** is a
- **BERK CAN KOZAN** is a PhD student of security studies at the National University of Public Service;
- **FAISAL WARIKAT** is a PhD student of security studies at the National University of Public Service;
- **HAJNALKA SZILÁGYI-KISS** is a PhD student of at the National University of Public Service;
- **HAYA ALTALEB** is a PhD student of the Óbuda University, Doctoral School on Safety and Security Sciences;
- **ISTVÁN BANDI** is a Research Associate, Historical Archives of the State Security Services of Hungary, Budapest
- **NIKOLETT KATALIN BÚS** is a PhD student at the Óbuda University;
- **ÖMER AKYÜZ** is a PhD student at the Kodolanyi Janos University European Union's Global and Regional Common Foreign, Security and Defence Policy;
- **SÁNDOR MAGYAR** is a Colonel of the Hungarian Armed Forces;
- **TIBOR SZILVÁGYI** PhD, is a free-lance security and defence policy analyst;
- **VERONIKA DEÁK** is a PhD student at Military Engineering Doctoral School of University of Public Service,
- **ZOLTÁN RAJNAI** PHD is a Professor at Óbuda University, Doctoral School on Safety and Security Sciences.

CONDITIONS FOR PUBLISHING IN THE NATIONAL SECURITY REVIEW

Requirements to be met by the writings

Ethical requirements:

- the writing has not been published yet elsewhere in its present form;
- it represents the author(s)' exclusive literary property, which is verified by the author(s), through his signing an author's declaration;
- it must be annotated with correct references that can be easily checked up;
- as well as with appropriate bibliographical information (including the literatures referred to, the list of Internet material, together with the date of downloading);
- it can reflect the author(s)' own opinion, which does not need to necessarily coincide with the Service's standpoint.

Content requisites:

- we publish in our reviews – in conformity with their nature – those scholarly writings (studies, essays and articles) that relate to home defense, first of all to military science, national security, intelligence, Surveillance, military security and security policy;
- the writing must be logically worded, easy to survey, coherent, relevant and well-arranged;
- the formulation of the author(s) own concept needs to be clear, his (their) conclusions have to be well-founded, supported by clear arguments and data.

Formal requisites:

- the size of the manuscripts cannot possibly exceed the space of one author's sheet (40,000 characters or 20-21 pages); written by Times New Roman 12 letters, 1.5 spacing; the pictures and graphics prepared in an easy to be processed format (.jpg or .tif), on electronic data carrier (CD), accompanied by a printed hardcopy. All this has to be taken into account when the author(s) sends his (their) writing to our address;
- however, the manuscript can be sent also by Internet to the following E-mail addresses: natsecreview@gmail.com (National Security Review). It is necessary to attach to the manuscript the author(s)' name, rank, position, sphere of activity, permanent address, phone number and Internet address;
- we pay royalty for the accepted and published writings, based on the contract of agency, in harmony with the relevant HDF regulations and according to our available financial resources;
- the Editorial Board has the manuscript revised in every case by the Service's competent, officers (with academic degree) or other experts;

- the Editorial Board preserves the right – taking into consideration the advisers' recommendations – to deny (without justification) the publication of those works that have proved to be ill-qualified to appear. However, it does not send back such writings and does not hold them either;
- everyone is entitled to publish in our periodicals, if the Editorial Board assesses his writing – on the basis of ethical, content and formal requirements – to be suitable for being published in our reviews and on the Internet. The Board holds until the end of the given year those writings that have been accepted, but not published. If the author wishes, we are ready to return his writing to him;
- the author has to enclose in his work an "Abstract/Résumé" maximum in 10-12 lines, in Hungarian and also in English;
- he also has to provide at least 3-5 keywords in Hungarian and English;
- we kindly ask the author to send us also the correct English title of his writing.

Formal requirements of academic communications

Our periodical publishes exclusively such studies that are provided with appropriate references and are prepared on the basis of the MSZ ISO 690 design standard.

The author has to attach to his communication:
- NAME OF THE AUTHOR, (his rank);
- TITLE OF HIS WRITING (in Hungarian and English);
- ABSTRACT/RESUME (in Hungarian and English);
- KEYWORDS (in Hungarian and English);
- AUTHOR'S DECLARATION.

Bibliographical reference

We kindly request the author to apply the usual numbered references, with the method to be found in "the Bibliographical references, (Bibliográfiai hivatkozások) MSZ ISO 690. p. 19-20".

If the author fails to use this method, we send back his writing for re-elaboration.

Citations

If the author has citations within the text, he has to mark them with raised numbers (superscripts) in the order of their appearance, immediately following a passage of research information. At the foot of that same page, a note beginning with the corresponding number identifies the source of information.

First citations

If we have a list of citations (bibliography), the first citation has to comprise at least: the author's name, his full address, the page-numbers of the citation, in such a way to be easily identified in the list of biographical references.

Examples:

1. Jenő KOVÁCS: Roots of the Hungarian Military Science, ideological problems of its development. p. 6.
2. Tibor ÁCS: Military culture in the reform era. p. 34.
3. Lajos BEREK: Basic elements of research work in Military Science. p. 33.
4. www.globalsecurity.org/army/iraq (downloaded: 19 04 2012)

List of biographical references (biography):

We have to fill the list by arranging the authors' name in alphabetical order.

Examples:

1. Tibor ÁCS: Military culture in the reform era. Budapest, 2005, Zrinyi Publishing House. ISBN 963 9276 45 6
2. Lajos BEREK: Basic elements of research work in Military Science. In: Tivadar SZILÁGYI (editor): Excerptions. Budapest, 1944 Zrínyi Miklós Military Academy. pp. 31-50.
3. Jenő KOVÁCS: Roots of the Hungarian Military Science, ideological problems of its development. In: New Defense Review, 2993. 47. vol. no. 6. pp. 1-7, ISSN 1216-7436
4. www.Globalsecurity.org/army/iraq (downloaded: 19 04 2012)

Requirements for pictures, sketches, illustrations, diagrams and other appendixes:

- title of the picture or illustration;
- source of the picture or illustration (or its drafter);
- serial number of the picture or illustration, (e.g. 1. picture);
- if it is possible, a Hungarian legend should be provided when the caption of the picture or illustration is given in a foreign language.

Requirements for abbreviations and foreign terms:

- foreignisms and abbreviations should be explained – at their first appearance – in the footnote, in Hungarian and in the original foreign language;
- e. g. WFP – World Food Program – ENSZ Világélelmezési Programja.

Points of Contact of the MNSS Scientific Board:

Postal address:
Katonai Nemzetbiztonsági Szolgálat Tudományos Tanácsa
1525 Budapest, Pf. 74.

E-mail: natsecreview@gmail.com

Editor in chief: Colonel István Talián
E-mail: talian.istvan@knbsz. gov.hu