MILITARY NATIONAL SECURITY SERVICE

Issue 2/2023

NATIONAL SECURITY REVIEW

BUDAPEST

Scientific Periodical of the
Military National Security Service

Responsible Publisher:

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

Postal Address

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

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

website:
https://hhk.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-szolgalat-tudomanyos-kiadvanyai

HU ISSN 2063-2908

TABLE OF CONTENTS

THEORY OF NATIONAL SECURITY

GEOPOLITICS

INFORMATION AND COMMUNICATION SECURITY

BOOK REVIEW

ÁRON TARKÓ[1]

A COMPARISON OF THE HUNGARIAN, SLOVAK AND CZECH NATIONAL SECURITY SERVICES FROM 1989 TO THE PRESENT

Abstract

As a result of the changes taking place in the previous decades, specific rules and legislations concerning national security organizations have been established, in the form of national security laws and orders.

Regarding Central Europe, one may get a clear picture of this change by examining the evolution of the Czech, Hungarian, and Slovakian national security services, between 1989 and 2020. After the regime change, the socialist regime transformed into a democratic system. My aim is to examine through the presentation of national security structures, the kind of changes these service branches undergone in Hungary, Slovakia, and the Czech Republic. The regime change had a huge effect on the secret intelligence services of these countries. There are major similarities and smaller differences in the structures and operations of these services, among the above-mentioned countries.

The disintegration of Czechoslovakia and the regime change had major effects on politics, government, economics, and national security organizations as well.

In Hungary and Czechoslovakia, the democratic political transformations and political changes took place in such a manner that influenced national security service structures and operations as well; thus, the state security/secret intelligence systems transformed into national security organizations. National security organizations were under government control, their operations were regulated by open legislations and internal instructions. In their study, András Börcsök and Csaba Vida[2] divided national security organizations into two different groups: military and civil ones. Currently, the Slovak and the Czech national security system contains three organizations, while the Hungarian system includes five of them, they all can be classified as either military or civil organizations.[3] The most important task of each organization (whether they are military or civil) is to protect the given state's independence and constitutional order, to which legislators provide the organizations with specific task systems.[4]

Keywords**:** change of political systems, communist secret services, national security services low, legal regulations, organisational structure

[1] ORCID: 0000-0003-3636-9128

[2] BÖRCSÖK, András – VIDA, Csaba: A nemzetbiztonsági szolgálatok rendszere (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására) Nemzetbiztonsági Szemle, 2014/1. p. 76. ISSN 2064-3756

[3] BÉRES János (Ed.): Külföldi Nemzetbiztonsági Szolgálatok. Zrínyi Kiadó, Budapest, 2018. pp. 52-54. ISBN 978 963 12 9548 1

[4] DOBÁK, Imre: Nemzetbiztonsági szolgálatok – Betekintés a visegrádi országok (V4) nemzetbiztonsági rendszereibe. Hadtudományi Szemle, 2015/4. pp. 113-130. ISSN 2060-0437 (downloaded 13 February 2020)

The Effects of the Regime Change on the Organizational Structure

In Hungary, during the regime change, the state security services were operating under a structure that had been stable for decades. The structure was created by the Central Committee and Political Committee of the Hungarian Socialist Workers Party in 1962. Its regulations remained untouched for the next two and a half decades. The unified state security civil organization became the "third main directorate" of the Ministry of Interior. The military state security service operated under the rule of the general staff.

In Hungary, for civil intelligence purposes, the Ministry of the Interior Main Directorate III/1 was responsible for the secret foreign civil intelligence, the Directorate III/2 for civil counterintelligence, the Directorate III/3 for internal political counter-intelligence, the Directorate III/4 for military counter-intelligence and the Directorate III/5 for technical intelligence and technical support for the operations of the other 4 Directorates.[5] This structure remained unchanged until 1989. The ministerial orders contained detailed instructions. In this period, the laws regulating national security were missing.[6] After the revolution in 1956, the 1956. XXXV. Law granted the foundation of the Directorate II (political investigation department). The counterintelligence also became one of the tasks of the Directorate II.

In Czechoslovakia, the operations of the state security services were regulated by the State Security Service Law, during the same period.[7] From 1947, conducting counterintelligence and military intelligence were also added to the task list of the services.[8] This was granted in the Law 286/1948. The Group II was responsible for providing the organizations with the necessary operative technical tools.[9] The structure of the Czech services is similar to the structure of the Hungarian ones.

Examination of Organizational Structures after the Regime Change from 1989 to 2020 in Hungary

The legislator divided the national security services into civil and military organizations after the regime change.[10] The legislature declared that the major role of the national security organizations was to protect the sovereignty and constitutional order of the Republic of Hungary.

[5] RAJOS, Sándor – SZABÓ, Károly Az állandó változás korai. In: CS. FEHÉR, Katalin (Ed.): A magyar Katonai elhárítás. Metropolis Media Group Kft., Budapest, 2018. pp. 99-101. ISBN 978-615-5628-66-5

[6] Ibid. pp. 100-101.

[7] Štátna Bezpečnosť és Státní Bezpečnost, STB

[8] Státní bezpečnost (STB) – Štátna Bezpečnosť és Státní Bezpečnost (StB) http://www.totalita.cz/stb/stb.php/ (downloaded 01 May 2020)

[9] BODA, József – REGÉNYI, Kund (Eds.): A hírszerzés története az ókortól napjainkig. Dialóg Campus Kiadó, Budapest, 2019. p. 153. ISBN 978-615-5945-97-7

[10] KOBOLKA, István (Ed.): Nemzetbiztonsági alapismeretek. Nemzeti Közszolgálati és Tankönyv Kiadó Zrt Budapest, 2013. p. 25. ISBN 9786155344329

The Hungarian civil intelligence services operated in two institutions: Information Office and National Security Office.[11] The Information Office is regulated by the Law X/1990[12] and the decree 26/1990 (II.14) on the regulations[13] of national security services. Yet, legal regulations on national security services did not come into force. Law CXXV. which focused on constitutional scope as well[14] and is still in force today, was only implemented in 1996. In the case of secret intelligence operations, the administration of forces, tools and methods happened through internal authorization regulations and anything related to this, was top secret. The Security Services gathered open and secret information as well abroad.

The information was obtained by human intelligence, by technical sources and open-source intelligence activities as well as by international cooperation. The Law 40/A. § (2), in the new constitution in 1989 – in accordance with the agreement of the interim governing political body, the "National Round Table" – declared that rules concerning the security of the state and the police must be recorded in legislation. The legislation became long overdue when the "Danube-Gate" scandal erupted in 1990. In the scandal opposition politicians were secretly observed by the Directorate III/3 of the state security service.[15] The law about special secret intelligence tools and methods was accepted by the government in 1990.

Another decree (26/1990. (II. 14.) MT) also came into force about the temporary legislation for national security operations. After the decree came into force, two military and two civil intelligence services were created. The Directorate III/5[16] was responsible for supervising and carrying out operational and technical tasks. Some parts of the Information Office underwent major changes. Until 2010, the Office was supervised by ministers without portfolio, then until 2012 the prime minister supervised it (this right was practiced by the state secretary in charge of the prime minister's office). Between 2014 and 2018, the supervision of civil secret intelligence belonged to the minister in charge of the prime minister's office.[17]

Today, the state secretary for leading the civilian national security services is responsible for – among others – the Information Office.[18] The National Security Service took over also the operations of internal defence. Civil services were established after the Laws 1990 and 26/1990. (II. 14.) MT came into force. The 1995.CXV national security services law was accepted by the parliament in 1995, then in 1996 the National Security Service, which was responsible for providing technical support to secret intelligence operations, was divided from the Information Office. The National Security Office carried out operations within Hungary.

[11] A hírszerzés és az Információs Hivatal története. http://www.mkih.hu/tortenet.html (downloaded 08 January 2021)

[12] 1990. évi X. törvény a különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról.

[13] 26/1990. (II. 14.) MT rendelet a nemzetbiztonsági feladatok ellátásának átmeneti szabályozásáról.

[14] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

[15] Nemzetbiztonsági Szakszolgálat honlapja. https://nbsz.gov.hu/?mid=14

[16] Ibid.

[17] A hírszerzés és az Információs Hivatal története. www.mkih.hu/tortenet.html (downloaded 08 January 2021)

[18] Alkotmányvédelmi Hivatal honlapja. http://ah.gov.hu/

The civil intelligence services went through a lot of changes. Between 1996 and-2002, it belonged to ministers without portfolio; between 2002 and 2007, to the minister in charge of the president's office; between 2007 and 2010 and then, to a minister without portfolio again. Civil intelligence services worked as independent units, between 1996 and 2010. The services carried out their operations inland. In 2010, the responsibility for anti-terror activities was taken over from the services by the Counter Terrorism Centre.[19] In 2010, the Constitutional Protection Office was established.[20] As a result of this, an amendment was made to the law, in order to restructure national security services and redistribute their tasks and operations. The Prime Minister's Office supervises the Constitutional Protection Office.

The office has successfully satisfied its legal obligations in recent years by cooperating with other national and international services (within NATO and the European Union). The National Security Strategy was elaborated in 2020; this act regulates the Constitutional Protection Office's tasks and operations. The act also defines Hungary's national security interests. The act lists the following responsibilities: industrial protection, counterintelligence, protection of the constitution, national security supervision, economic protection and exemption requests. The services gather information inland from human sources. The National Security Special Service has been operating as an independent civil intelligence service, since it was born in 1996.[21] Its independence opened the gate for other civil intelligence services to exist and operate independently from 1996.

After the regime change, the professional-technical background was provided first by the National Security Office, then by the National Security Special Service. Law CXXV/1995[22] about national security services was accepted by the parliament in 1995. The legislation made the National Security Special Service independent from the National Security Office. From January 1st, 2012 after an amendment to the law on national security services, the Military Counterintelligence Office and the Military Intelligence Office were merged under the name "Military National Security Service". The service gathers secret information from various resources. The data acquisition part of the service offers professional services to the agents of law enforcement, who have legal authorization to view data. The service applies operative technical devices in its activity.[23] The most frequent requests for the service are: wiretapping and observation of people.[24]

[19] KASZNÁR, Attila: Egyéb titkos információgyűjtést folytató szervezetek. In: RESPERGER, István (Ed.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 282-283. ISSN 978-615-5845-66-6

[20] SZABÓ, Károly: Az elhárítás. In: RESPERGER, István (Ed.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 183-184. ISSN 978-615-5845-66-6

[21] Nemzetbiztonsági Szakszolgálat honlapja. https://nbsz.gov.hu/?mid=14

[22] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

[23] SOLTI, István: A titkos információgyűjtés, elvei, eszközei és módszerei, alkalmazásának lehetőségei a nemzetbiztonsági munkában. PhD értekezés, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Budapest, 2017. p. 37.

[24] DOBÁK, Imre: A Nemzetbiztonsági Szakszolgálat. In: RESPERGER, István (Ed.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 236-242. ISSN 978-615-5845-66-6

The two military intelligence services – the Military Intelligence Office and the Military Security Office – were established in 1995. The law of national security defines the role and operation of these military services. The Military Intelligence Office was founded in 1990, after the regime change as the successor of the Directorate III/4 of the Ministry of Interior Main Directorate III. The Military Intelligence Office operated as the Intelligence Service of the Hungarian Home Defence Forces. Its main goals included supervising the military staff and civil staff of the Hungarian Army and to protect them against any potential threats. The secret intelligence activities and military intelligence were supervised by the Minister of National Defence. Between 1991 and 1995, the service operated as the Security Office of the Hungarian Army. After this period, it changed its name to the Military Counterintelligence Office of the Hungarian Republic. The service operated in this form December 31st, 2011.

The Military Intelligence Office was established in 1990, upon the foundation of the Hungarian Republic. This service was the 2nd Directorate of the General Staff (VKF-2, in Hungarian) of the Hungarian People's Army.[25] The law of 1995 on national security services regulates the activities of secret intelligence organizations and the Military Intelligence office as well. The Military Intelligence Office carries out operations abroad, while the Military Security Office does counterintelligence activities both inland and abroad. Both services operated from 1990 to 2010.

They were integrated in 2012 and the two services became one. The new service was called the Military National Security Service. This integration was a milestone in the transformation of the Hungarian national security structure. The main goal of military intelligence is to explore and prevent activities that are directed against Hungary, to support political decision making, and support international interests of Hungary. One of the most important tasks of the service is to support the legal operation of the Ministry of Defence and the Hungarian Army and support Hungarian soldiers abroad carrying out secret intelligence activities.[26]

The Road Divides: The Division of the Czechoslovak Secret Intelligence Services

In her PhD thesis, Márta Benedek[27] touches upon the effects of the regime change on the two countries – the Czech Republic and Slovakia – and their secret intelligence services. In Czechoslovakia, in 1989, after the democratic elections, the National Security Board underwent major transformations and its supervision got back to the police. The era of STB ended. The Federal Intelligence Service (Federálna Informacna Sluzba) was established in 1990, by Ján Langos under the supervision of the Home Office.

[25] HAJMA, Lajos: A katonai felderítés és hírszerzés története. Egyetemi jegyzet. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2001.

[26] Katonai Nemzetbiztonsági Szolgálat honlapja. https://www.knbsz.gov.hu/hu/index.html

[27] BENEDEK, Márta: A nemzetbiztonság stratégiai kérdései a XXI. század kül- és biztonságpolitikájában. PhD értekezés. Nemzeti Közszolgálati Egyetem, Budapest, 2016. pp. 132-133

The organization's name changed in 1991 from Federal Intelligence Service, it became Federal Defence and Intelligence Service, so from FIS it became to the FBIS (Federální bezpečnostní informační služba).[28] The Law 244 in 1991, gave permission to the service to use secret intelligence tools – the change in its name refers to this phenomenon as well. The national security department of the FBIS was responsible for maintaining the protection of the state's constitutional order. Between 1989 and 1992, there were two national security services in Czechoslovakia: the civil Czechoslovak Federal Defence and Intelligence Service and the military Czechoslovak Military Intelligence Service. The main tasks of the services were; gathering, evaluating and processing information about four main fields: protecting constitutional order, preventing foreign secret intelligence activities, protection against terrorism and protection of the security and economic interests.[29]

Csaba Vida demonstrates[30] that the division of Czechoslovakia -officially Czech and Slovak Republic - was far from being unexpected. The two republics were held together by dictatorial tools, even before the regime change. The democratic transformations could no longer prevent the sovereignty attempts of the Slovaks, so the Slovak parliament declared its independence in 1992. The division took place in a peaceful way, although there were huge political debates about the distribution of state wealth. The two independent countries were less important from a national security's point of view than the one federal Czechoslovakia. In the case of national security, assets were distributed according to a pre-calculated ratio between the two countries. After that, citizens and members of the armed forces could decide which country they want to serve based on their nationality. So the national security staff of the new countries originates from the formerly common national security organizations.

The Czech Republic

It can be stated that the Czech civil and military national security services were built of the former members of the armed forces of the old Czechoslovakia that lived in the Czech Republic. As a result of the transformation, two civil and two military intelligence services were established. The National Security Board (Bezpecnostni Rada Stát – BRS) was formed by law 110/1998, act 9 by the Czech government. The BRS was responsible for the coordination between these services and for national security matters.[31] The Czech national security system was supervised not only by the government, but by the Home Office as well. The president could get information from all four secret intelligence services. In 1993, the Security Information Office (Bezpecnostni Informacni Sluzba – BIS) was set up.

[28] Ibid. pp. 133-134

[29] POKORNY, Ladislav: Zákon o FBIS - první zákonná úprava zpravodajských služeb v Československu. In: „Skúsenosti s fungovaním spravodajských služieb v postkomunistických krajinách". Zborník ABSD 2013.

[30] VIDA, Csaba: Szlovákia államiságának kialakulása és annak katonai vonatkozásai, valamint a szlovák haderőreform folyamata II. Felderítő Szemle, 2008/4, pp. 43-83. ISSN 1588-242X

[31] č. 110/1998 Stb., o bezpečnosti ceské republiky. https://www.vlada.cz/cz/pracovni-a-poradni-organy-vlady/brs/brs-uvod-3851/ (downloaded 22 May 2020)

The necessity of the establishment of a new national security system stemmed from the formation of the independent, sovereign Czech Republic. The BIS had a national jurisdiction. It gathers information inland by concentrating its strength and applying various methods, in order to protect the country's constitution and economic interests. It is supervised by the government and the parliament. It carries out activities like open source data collection. It applies networks, observations and wire-tapping to carry out its operations.[32] The BIS is an armed organization; however, it does not have criminal jurisdiction. It cooperates with the police, the foreign secret intelligence services and other law enforcement organizations.

The Foreign Relations and Information Office (Úřad pro zahraniční styky a informace – ÚZSI) is the Czech Republic's civil intelligence service. It has nationwide jurisdiction. The ÚZSI is supervised by the Home Office, but its tasks are carried out under government control and its legal supervision is carried out by the Foreign Affairs Board. The Office was established in 1993, by the law 153/1994.[33] Its major tasks are the following: provide the various organizations of the state with information that serves the country's strategic economic interests and help repel challenges, like international terrorism and asymmetric security threats.[34] The ÚZSI cooperates with Czech and foreign security services and the police. The secret intelligence activities and the forces, tools and the methods of the ÚZSI are granted by the president of the Supreme Court.

Slovakia

The Military Secret Intelligence Service (Vojenské Zpravodajství – VZ) and the Military Defense Intelligence (Vojenským Obranným Zpravodajstvím – VOZ) were established in 1994, by the law 153/2014, in the freshly independent Slovakia. The two services cooperated until 2005, when the VOZ was integrated into the VZ. The legal predecessor was established in 1992 under the name of Military Intelligence.[35] The VZ carries out secret intelligence activities both inland and abroad. Its work and information request is granted by the government.[36]

It is supervised by the government and the parliament.[37] The service applies various intelligence methods during its activity, these are the following: HUMINT,[38] SIGINT,[39] OSINT.[40] The VZ can use other secret intelligence methods as well. While applying secret intelligence methods, agents of the VZ are authorised to use intelligence techniques and recruit agensts.

[32] Bezpečnostní informační služby honlapja. www.bis.cz/aktuality/ (downloaded 27 June 2023)

[33] 153 Zákon ze dne 7. července 1994 o zpravodajských službách České republiky.

[34] Kdo jsme – Úřad pro zahraniční styky a informace. www.uzsi.cz/cs/kdo-jsme/ (downloaded 25 May 2020)

[35] Béres (2018) op. cit. pp. 27-31.

[36] Vojenske Zravodajství (VZ): Védelmi Minisztérium

[37] Béres (2018) op. cit. p. 31.

[38] Human Intellingence: emberi erőforrás

[39] Signal Intelligence: jelhírszerzés és rádiós és rádióelektronikai hírszerzés

[40] Open Source Intelligence: nyíltforrású adatszerzés

The service's operational tasks include: analysis, internal security, economic security, information protection and radio technical reconnaissance.[41]

The Slovak national security services were established in 1993, when independent Slovakia was born. In 2001, a new civil intelligence service joined these services, under the name of National Security Office (Národny Bezpecnosty Úrad – NBÚ). The Slovakian Information Service (Slovenská Informacná Služba – SIS) carried out intelligence and counterintelligence activities, both inland and abroad. Its work was directed by the government and supervised by the parliament.[42] The Military Intelligence (Vojenská Spravodajská Služba – VSS) is an intelligence and counterintelligence organization, which carries out activities both inland and abroad. All three services are under government supervision. The SIS's legal predecessor was the Czechoslovak Inland Intelligence Service (Federální bezpečnostní informační služba). The service was established in 1993, under the Law 46/1993. The staff of the service became the staff of its predecessor StB stationed in Slovakia.

The service was established because several scandals and law breaking events happened, after the regime change in Czechoslovakia, on the territory of the later Slovakia: the political elite used the intelligence service for observing its political opponents or starting a smear campaign against them. As a response to these, Slovakia established the SIS, its own secret intelligence service. It carries out intelligence activities both inland and abroad and analyses and assesses the gathered information. Its major activities involve: fighting against organized crime and terrorism, repelling threats endangering the country's security, protecting the constitution, the country's territorial integrity and independence, its economic interests, finding and repelling activities endangering international contracts and agreements and preventing the leakage of information that is important to the country. SIS cooperates with foreign intelligence services, the police and other organizations. The SIS informs the country's president about the gathered data. It is supervised by the National Board, which has 14 members that are elected by the parliament, and its president is always an MP who is in opposition to the governing party.[43] SIS may apply secret intelligence forces, tools and methods during its operations. It informs the police about discovered criminal activities.[44]

The SIS submits an annual report about its activity to the parliament. If the president or the parliament submits a written request to the SIS, it is obliged to write and submit a report on the given topic.[45] Its operations and methods are granted by judges, holding special jurisdiction. It gathers information in the following ways: analysis, technical intelligence, foreign intelligence, inland economic intelligence and inland security intelligence.[46]

[41] BÉRES (2018) op. cit. p. 32.

[42] Slovenska informácna sluzba: Szlovák Információs Szolgálat

[43] 543 Zákon z 13. novembra 1992 o zrušení Federálnej bezpečnostnej informačnej služby.

[44] 543 Zákon z 13. novembra 1992 o zrušení Federálnej bezpečnostnej informačnej služby.

[45] HETESY, Zsolt: Titkos felderítés. PhD értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2011.pp. 68-69.

[46] BÉRES (2018) op. cit. pp. 52-53.

The National Security Analytical Centre (Národné Bezpečnostné Analytické Centrum – NBAC) was established in 2013, as Slovakia's service against terrorism. The NBAC has a countrywide jurisdiction in questions of security threats.[47]

The SIS's main roles include: making comprehensive analyses of security events, based on the signals of state authorities of the Slovak Republic, observing the security situation of Slovakia, providing documents from open sources and about security threats endangering the Slovak Republic.[48] The NBAC carries out its operations in the security area of Slovakia, but it has a cooperation agreement also with the Slovakian national security service, the law enforcement service, the Ministry of European Affairs, the National Security Office, the main headquarters of the Armed Forces of the Slovak Republic and with the assigned representative of the Slovak Republic's Government Office. The NBAC works in international cooperation with the UNOCT (United Nations Office of Counterterrorism) in Madrid, and has a bilateral cooperation agreement with the EU, NATO and the intelligence services of the member states.

The NBÚ[49] is a service that has countrywide jurisdiction and does not carry out classical intelligence activities. Its operations are regulated by two laws on privacy protection: the Laws 241 of 2001[50] and 215 of 2004.[51] The basic tasks of the national security service department are the following: the protection of classified information, supervising classified data and information, executing security supervisions, issuing industrial security permits, protecting and administering foreign information, providing password supervision, issuing electronic signatures, protection of encrypted information, industrial security, protection of technological devices, protecting people and objects, information security and cybersecurity. The NBÚ is supervised by the parliament. The leader of the board that supervises the organisation is elected by the parliament, the members are elected by the parties that are present in the parliament. The members are granted by a parliamentary decree. The leader of the service is granted by the parliament, based on the proposal of the government. The NBÚ is a task-centric service and it executes tasks that are defined by the law. The number of its staff is not public.[52]

The military intelligence services were the following: Military Intelligence Service (VSS) and the Military Defense Service (VOS). Both carried out intelligence operations inland and abroad as well. The Military Intelligence Service was established in 2013 from the fusion of the two above-mentioned organizations. The service – similarly to the Czech example – is supervised by the Minister of Defence and controlled by the parliament, and deals with gathering and analysing information about security issues that affect the Slovak Republic. The service actively cooperates internationally with NATO. The service is regulated by the laws 215/2004 and 166/2004, related to protection against wire-tapping.

[47] Národné bezpečnostné analytické centrum – Nemzetbiztonsági Elemző Centrum

[48] Vznik NBAC. https://www.sis.gov.sk/o-nas/nbac.html letöltés: 2023. 06. 22.

[49] BÉRES (2018) op. cit.pp. 52-53.

[50] 241 Zákon z 30. mája 2001 o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

[51] 215 Zákon z 11. marca 2004 o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov

[52] BÉRES (2018) op. cit. pp. 52-53.

The operational units of the service were outsourced to four offices: Military Defence Office, Military Intelligence Office, Intelligence Technical Security Office and Security Office.[53] Besides the operational offices, operation-support and service units also belong to the organization.

Conclusions

It became evident that the countries analysed in this study show resemblance to each other, in terms of the structure of their civil and military services. Further similarities can be found in the operational units of the Czech, Hungarian and Slovak civil and military services. Every country has civilian and military intelligence services. The given countries have established an integrated intelligence-defence service. It can be noted that while the Czech Republic and Slovakia have three services, Hungary has five (AH, IH, NBSZ, KNBSZ, NIK) of them. Both the Czech and the Hungarian civilian intelligence services have a separate department for inland intelligence, and one for abroad. Building the legal background for the intelligence services also happened in a similar way, in the three countries. The Czech and the Slovak services had some advantage concerning the relevant regulations, as their National Security Law (STB – Štátna Bezpečnosť, Státní Bezpečnost), which came into force in 1948, had already contained the rules regarding intelligence services. Another advantage is that both countries are well-equipped[54] with technological tools for intelligence operations, which makes their work easier and more efficient.

The inland and foreign information gathering of the SIS is effective, the information-flow within the service is good and its operation is effective and satisfactory. The NBÚ has its own security office, which is responsible for protecting security data; it blocks unauthorized persons downloading data. The main task of the Data Protection Office is to handle and store classified information. The Slovakian National Security Office deals only with handling and protecting classified information and does not carry out classical national security activities. As opposed to this, in the other two countries the intelligence services themselves handle classified data along with other intelligence operations.

The national security services of the Czech Republic were regulated by the national security law. In Hungary, gathering information is more difficult. Due to the linguistic differences, communication with the neighbouring countries is much more difficult than in the case of the Czech Republic and Slovakia, which belong to the same language family. The Hungarian intelligence services have undergone constant changes, concerning their structure. In Hungary, there was no law regulating the operations of intelligence services, contrary to Czechoslovakia.

[53] BÉRES (2018) op. cit. pp. 55-56.

[54] Státní bezpečnost (StB). http://www.totalita.cz/stb/stb.php (downloaded 11 May 2020)

Bibliography:

- 26/1990. (II. 14.) MT rendelet a nemzetbiztonsági feladatok ellátásának átmeneti szabályozásáról
- 46 Zákon národnej rady slovenskej republiky z 21. januára 1993 o Slovenskej informačnej službe. www.epi.sk/zz/1993-46 letöltés 2020.11.30.
- 73 Zákon zo 17. februára 1998 o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície. www.zakonypreludi.sk/zz/1998-73 letöltés 2020.11.30.
- 153 Zákon ze dne 7. července 1994 o zpravodajských službách České republiky. www.zakonyprolidi.cz/cs/1994-153 letöltés 2020.11.30.
- 215 Zákon z 11. marca 2004 o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov. www.zakonypreludi.sk/zz/2004-215 letöltés 2020.05.25.
- 241 Zákon z 30. mája 2001 o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov www.zakonypreludi.sk/zz/2001-241 letöltés 2020.05.25.
- 361 Zákon ze dne 23. září 2003 o služebním poměru příslušníků bezpečnostních sborů. www.zakonyprolidi.cz/cs/2003-361 letöltés 2020.11.30.
- 412 Zákon ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. www.zakonyprolidi.cz/cs/2005-412 letöltés 2020.11.30.
- 543 Zákon z 13. novembra 1992 o zrušení Federálnej bezpečnostnej informačnej služby. www.epi.sk/zz/1992-543 letöltés 2020.11.30.
- 1990. évi X. törvény a különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról.
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról
- A hírszerzés és az Információs Hivatal története. www.mkih.hu/tortenet.html letöltés: 2021.01.08.
- Alkotmányvédelmi Hivatal honlapja. http://ah.gov.hu/ letöltés: 2020.05.20.
- BÁLINT László: A Terrorelhárítási Információs és Bűnügyi Elemző Központ. In: Resperger István: A nemzetbiztonsági alapismeretek. Dialóg Campus Kiadó, Budapest, 2016. pp. 129–142. ISBN 978-615-5845-68-0
- BENEDEK Márta: A nemzetbiztonság stratégiai kérdései a XXI. század kül- és biztonságpolitikájában. PhD értekezés. Nemzeti Közszolgálati Egyetem, Budapest, 2016.
- BÉRES János (Szerk.): Külföldi nemzetbiztonsági szolgálatok. Zrínyi Kiadó, Budapest, 2018. ISBN 978 963 12 9548 1
- Bezpečnostní informační služby honlapja. www.bis.cz/aktuality/ letöltés: 2023.06.27.

- BODA József – REGÉNYI Kund (Szerk): A hírszerzés története az ókortól napjainkig. Dialóg Campus Kiadó, Budapest, 2019. ISBN 978-615-5945-97-7
- BÖRCSÖK András – VIDA Csaba: A nemzetbiztonsági szolgálatok rendszere (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására). In: Nemzetbiztonsági Szemle, 2014/1. pp. 63–100. ISSN 2064-3756
- č. 110/1998 Stb., o bezpečnosti ceské republiky. https://www.vlada.cz/cz/pracovni-a-poradni-organy-vlady/brs/brs-uvod-3851/ letöltés: 2020.05.22.
- DOBÁK Imre: A Nemzetbiztonsági Szakszolgálat. In: Resperger István (szerk): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 235–242. ISSN 978-615-5845-66-6
- DOBÁK Imre: Nemzetbiztonsági szolgálatok – Betekintés a visegrádi országok (V4) nemzetbiztonsági rendszereibe. Hadtudományi Szemle, 2018/4. szám p. 113-130. ISSN 2060-0437
- HAJMA Lajos: A katonai felderítés és hírszerzés története. Egyetemi jegyzet. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2001.
- HETESY Zsolt: Titkos felderítés. PhD értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2011.
- Katonai Nemzetbiztonsági Szolgálat honlapja. https://www.knbsz.gov.hu/hu/index.html letöltés: 2020.05.22.
- KASZNÁR Attila: Egyéb titkos információgyűjtést folytató szervezetek. In: Resperger István (szerk): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 281–287. ISSN 978-615-5845-66-6
- Kdo jsme – Úřad pro zahraniční styky a informace. www.uzsi.cz/cs/kdo-jsme/ letöltés: 2020. 05. 25.
- KIS-BENEDEK József: A nemzetbiztonsági szolgálatok nemzetközi együttműködése. In: Resperger István (szerk): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 257–280. ISSN 978-615-5845-66-6
- Kobolka István (szerk.): Nemzetbiztonsági alapismeretek. Nemzeti Közszolgálati és Tankönyv Kiadó Zrt Budapest, 2013.
- NATO tükör, 1999/2.
- Nemzetbiztonsági Szakszolgálat honlapja. https://nbsz.gov.hu/?mid=14 letöltés: 2020.05.20.
- POKORNY, Ladislav: Zákon o FBIS - první zákonná úprava zpravodajských služeb v Československu. In: Skúsenosti s fungovaním spravodajských služieb v postkomunistických krajinách. Zborník ABSD 2013. https://www.absd.sk/skusenosti_s_fungovanim_spravodajskych_sluzieb_v_p letöltés: 2023. 06. 23.

- RAJOS Sándor – SZABÓ Károly: A Belügyminisztérium III/IV. csoportfőnökség időszaka. In: CS. Fehér Katalin (szerk): A magyar Katonai elhárítás története 1918–2018. Metropolis Media Group Kft., Budapest, 2018. pp. 99–162. ISBN 978-615-5628-66-5
- RESPERGER István (szerk): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. ISSN 978-615-5845-66-6
- SOLTI István: A titkos információgyűjtés, elvei, eszközei és módszerei, alkalmazásának lehetőségei a nemzetbiztonsági munkában. PhD értekezés, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Budapest, 2017.
- Státní bezpečnost (StB). http://www.totalita.cz/stb/stb.php (Letöltés ideje: 2020. 05. 11.)
- SZABÓ Károly: Az elhárítás. In: Resperger István (szerk): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 169–208. ISSN 978-615-5845-66-6
- TÓTH Mihály Csaba: A titkos információgyűjtés és a személyiségi jogok. In: Dobák Imre: A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem, Budapest, 2014. pp. 221–236. ISBN 987-615-5305-49-8
- VIDA Csaba: Szlovákia államiságának kialakulása és annak katonai vonatkozásai, valamint a szlovák haderőreform folyamata II. Felderítő Szemle, 2008/4, p. 43-83. ISSN 1588-242X

TAMÁS SOMOGYI[1] – RUDOLF NAGY PHD HABIL[2]

FORMAL BANKING AND FINANCIAL INCLUSION TO WEAKEN HAWALA AND SERVE COUNTER-TERRORISM

Abstract

Terrorism is undoubtedly one of the greatest security challenges of the western world, in the 21st century. One of the central issues of terrorism is how to finance its activities. It has been proved that hawala, the ancient Islamic fund-transfer system is used by terrorist groups to finance their illicit activities. However, previous studies of counter-terrorism have not addressed the question of weakening hawala. The aim of this paper is twofold. First, to examine hawala and the reason for the popularity of legal money-transfer, and second, to identify the ways in which hawala can be weakened or even closed. As it will be explained, offering simple and cheap, Sharia compliant banking services would decrease the number of 'unbanked' households, and eventually make hawala systems unnecessary. For this, the cooperation of the governments and the banking industry is essential.

The outcomes of our investigation may be significant and useful for the scholarly community, the law enforcement agencies and the policymakers.

Keywords**:** counter-terrorism; financing terrorism; hawala; informal fund transfer; banking industry

Introduction

Terrorism is undoubtedly one of the greatest security challenges of the western world in the 21st century. Terrorism has become a widely investigated field, especially after the events on 11 September, 2001.[3] Bonansinga highlights the fact that the 21st century has been characterised by new terrorist threats, including the careful selection of civilian targets and the willingness to use extreme violence, in order to cause mass destruction, with as many casualties as possible.[4] The usage of biological, chemical or radiological weapons might be occur in the future.

[1] ORCID: 0000-0003-1397-697X

[2] ORCID: 0000-0001-5108-9728

[3] PHILLIPS, B. J.: How Did 9/11 Affect Terrorism Research? Examining Articles and Authors, 1970–2019. Terrorism and Political Violence, 2022/2, https://doi.org/10.1080/09546553.2021.1935889 (downloaded 8 September 2023)

[4] BONANSINGA, D.: Counter terrorism in the 21st century and the role of the European Union. Polish Political Science Review, 2015/1, https://doi.org/10.1515/ppsr-2015-0027 (downloaded 8 September 2023)

Among the possible targets are the critical information infrastructure,[5] the healthcare facilities[6] and the food supply chain,[7] just to name a few. As it has been observed, terrorist groups use both expensive modern information technologies[8] and also low-cost methods[9] during their attacks.

Since 11 September, 2001, there is an increased interest in countering terrorist threats. One of the central issues is how to finance the terrorist actions. Among others, the most significant factors in terrorism are found to be the ability to finance the activities.[10] Moreover, paying salaries to terrorist by terrorist groups is not unusual.[11] Therefore, national and international efforts are taken to suppress the financing of terrorism by fighting against its financial infrastructure and the relevant organisations. The banking industry is profoundly regulated; thus, regulations and policies are posing obstacles to financing terrorism. The information infrastructure of the financial sector is considered to be a critical issue;[12] thus, the banking industry and infrastructure are in the focus of law enforcement agencies. Therefore, other channels are looked for by terrorists to transfer money: the informal fund transfer systems. Hawala is an ancient money-transfer method, based on trust, and is in line with the Islamic law in general. However, hawala has been found to meet the objectives of financing terrorism as well. This paper examines hawala, describes the relationship between hawala and financing terrorism, and investigates the factors that make hawala strong. Then attempts to give some recommendations to weaken this informal fund-transfer system and increase financial inclusion and spread the services of the formal banking industry.

[5] Somogyi, T. – Nagy, R.: Cyber threats and security challenges in the Hungarian financial sector. Contemporary Military Challenges, 2022/3, https://doi.org/10.33179/BSV.99.SVI.11.CMC.24.3.1 (downloaded 8 September 2023)

[6] Shaffer, R. – Besenyő, J.: Terrorism against healthcare facilities and workers in Africa: An assessment of attack modes, targets and locations. African Security Review, 2023/1, https://doi.org/10.1080/10246029.2023.2213220 (downloaded 8 September 2023)

[7] Wu, Y. – Nagy, R.: The industrial safety of food processing in light of operational risks reduction aspects. National Security Review, 2022/2, https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_2_NSR.pdf (downloaded 8 September 2023)

[8] Besenyő, J. – Sinkó, G.: The social media use of African terrorist organizations: a comparative study of Al-Qaeda in the Islamic Maghreb, Al-Shabaab and Boko Haram. Insights into regional development, 2021/3, http://doi.org/10.9770/IRD.2021.3.3(4) (downloaded 8 September 2023)

[9] Besenyő, J.: Low-cost attacks, unnoticeable plots? Overview on the economical character of current terrorism. Strategic Impact, 2017/1, https://www.ceeol.com/search/article-detail?id=829355 (downloaded 8 September 2023)

[10] Kumar, A.: Terror Financing in Bangladesh. Strategic Analysis, 2009/6, https://doi.org/10.1080/09700160903255913 (downloaded 8 September 2023)

[11] Farber, S.: Countering the Financing of Terrorists' Salaries. Studies in Conflict & Terrorism, 2023. https://doi.org/10.1080/1057610X.2023.2199471 (downloaded 8 September 2023)

[12] Somogyi, T. – Nagy, R.: The financial infrastructure as a critical infrastructure and it's specialities. National Security Review, 2/2021, https://www.knbsz.gov.hu/hu/letoltes/szsz/2021_2_NSR.pdf#page=213 (downloaded 8 September 2023)

Hawala

According to Iman, hawala has already existed in Asia and the Middle-East a thousand year ago.[13] Zetzsche et al. suggests that hawala can be dated back to the 700‘s.[14] Recent studies have conclusively identified the word hawala with the Arabic term of ‘h-w-l’, which means to transform or to change. According to Mukhtar et al., in the 12th century, when this word and concept had been adopted by the Urdu people, the meaning of ‘trust’ had been added to it.[15] Nevertheless, this kind of informal fund-transfer system has been developed in Middle-Asia and South-Asia as well. The original meaning, to transform, refers to transferring debt, which is an action regulated by the Islamic law, as it has been explained by Schramm and Taube.[16] According to them, the respective legal concept can be found in al-Kasani’s book on Islamic law, written in 1327. If person A owes a debt to person B, who in turn owes a similar or equal sum to person C, then the debt-transfer could be easily done: person B signs over his claim to person C, which is permitted by Islamic law. This compliance may be one of the main reasons why hawala is a popular fund-transfer method among the people of Africa and Asia.

In their study, Ladányi and Kobolka describe hawala as follows.[17] A customer X in country CX wants to send money to customer Y, in country CY. A hawaladar from country CX (HX) receives funds in one currency from X and, in return, gives X a code for authentication purposes. HX then instructs his correspondent in country CY (HY) to deliver an equivalent amount in the local currency to the designated beneficiary CY, who needs to disclose the code to receive the funds. The code was given to CY by CX via phone, email or any kind of communication channel. HX can be remunerated by charging a fee or through using higher exchange rate. The settlement of the liability position of HX vis-à-vis HY that was created by this transaction can be done through imports of goods or reverse fund-transfer. A reverse hawala transaction does not necessarily imply that the settlement of transaction has to involve the same hawaladars; it could involve other hawaladars and be tied to a different transaction. The description of Schramm and Taube (2003) is almost the same. They highlight that this simple way of money-transfer works without any trace: hawaladars do not keep any written record of the transaction. The so-called code can be a verse or a name, something that can be transmitted via regular communication channels.

[13] IMAN, N. Is mobile payment still relevant in the fintech era? Electronic Commerce Research and Applications, 2018/30, https://doi.org/10.1016/j.elerap.2018.05.009 (downloaded 8 September 2023)

[14] ZETZSCHE, D.A. et al.: DLT-based enhancement of cross-border payment efficiency – a legal and regulatory perspective. Law and Financial Markets Review, 2021/1-2, https://doi.org/10.1080/17521440.2022.2065809 (downloaded 8 September 2023)

[15] MUKHTAR, A. et al.: Challenges confronting the ‘One Belt One Road’ initiative: Social networks and cross-cultural adjustment in CPEC projects. International Business Review, 2022/31, https://doi.org/10.1016/j.ibusrev.2021.101902 (downloaded 8 September 2023)

[16] SCHRAMM, M. – TAUBE, M.: Evolution and institutional foundation of the hawala financial system. International Review of Financial Analysis, 2003/12, https://doi.org/10.1016/S1057-5219(03)00032-2 (downloaded 8 September 2023)

[17] LADÁNYI, E. – KOBOLKA, I.: The hawala system. Interdisciplinary management research. 2014/10, https://econpapers.repec.org/RePEc:osi:journl:v:10:y:2014:p:413-420 (downloaded 8 September 2023)

There is a consensus among researchers that this informal fund-transfer system is still operating, particularly in Asia and in Africa. Migrants from these continents tend to use hawala to transfer money to their families. As it has been found, hawala networks provide a much-needed financial service to millions of migrant workers who need a cheap and reliable means of sending money back home.[18] As Chakraborty observes, hawala transactions are the primary ways for Bangladeshi migrant workers to remit their incomes.[19] Most workers from the former Soviet Union's states working in Russia, are found to use hawala to send money home.[20] The case of Somalia has been introduced and investigated by many authors. As Mitra and Sanghi describe, in the 1990s, after the fall of Siad Barre's regime, Somalia plummeted into a fragmented, political crisis characterised by the loss of effective governance.[21] In the absence of effective and recognised central bank, the financial services had been overtaken by an informal fund-transfer system. Leeson and Boettke estimate a 500 million–1 billion USD annually in remittances from Somalis abroad.[22] As Ali and Gersdorf suggest, the hawala was central to the functioning of Somalia's highly developed remittance system, transferring an estimated 1.3 billion–2 billion USD into Somalia each year, in the beginning of 2010's.[23]

Although some may not find hawala illicit by nature, this informal fund-transfer system can be exploited by criminals and terrorists. In the pages that follow, a link will be established between hawala and financing terrorism.

Hawala and terrorism

Fundraising is crucial for terrorism, especially in the case of "expensive" attacks. As Jones and Libicki found, attacking the finances of terrorists has provided effective results, but there are difficulties as hawala exists outside the regulated international financial system.[24]

[18] BALLARD, R.: Hawala: criminal haven or vital financial network? Newsletter of the International Institute of Asian Studies, October, 2006, https://doi.org/10.11588/xarep.00000263 (downloaded 8 September 2023)

[19] CHAKRABORTY, A. Renegotiating Boundaries Exploring the Lives of Undocumented Bangladeshi Women Workers in India. In: JONES – R., FERDOUSH, A. (Eds.): Borders and Mobility in South Asia and Beyond. Amsterdam University Press, 2018. pp. 123-143. https://doi.org/10.2307/j.ctv513ckq.9 (downloaded 8 September 2023)

[20] KAKHKHAROV, J. – AKIMOV, A. – ROHDE, N.: Transaction costs and recorded remittances in the post-Soviet economies: Evidence from a new dataset on bilateral flows. Economic Modelling, 2017/60, http://dx.doi.org/10.1016/j.econmod.2016.09.011 (downloaded 8 September 2023)

[21] MITRA, R. – SANGHI, S.: The small island states in the Indo-Pacific: sovereignty lost?. Asia Pacific Law Review, 2023/2, https://doi.org/10.1080/10192557.2023.2181806 (downloaded 8 September 2023))

[22] LEESON, P.T. – BOETTKE, P.J.: Two-tiered entrepreneurship and economic development. International Review of Law and Economics, 2009/29, https://doi.org/10.1016/j.irle.2009.02.005 (downloaded 8 September 2023)

[23] ALI, D., Gelsdorf, K.: Risk-averse to risk-willing: Learning from the 2011 Somalia cash response. Global food security, 2012/1, http://dx.doi.org/10.1016/j.gfs.2012.07.008 (downloaded 8 September 2023)

[24] JONES, S.G. – LIBICKI, M.C.: How terrorist groups end: lessons for countering al Qa'ida. RAND Corporation, 2008, https://www.jstor.org/stable/10.7249/mg741rc.16 (downloaded 8 September 2023)

Therefore, as Gordon indicated, hawala networks are invaluable for terrorism.[25] As Gatti highlights, the Paris attacks in 2015 provided the first known example of hawala in Europe: the Abaaoud network used it to transfer money to the attackers.[26] Recent studies have confirmed that hawala, as an informal fund-transfer system without written records, is used by terrorist organisations to finance their activities.[27] Hawala is highly probably favoured because of its unrecorded operation and its underground nature, which makes exceptionally difficult for the law enforcement agencies to conduct investigations. The connection between hawala and illegal activities has been supported by many cases from the last decades. The case study of D-Company, reported by Mullins and Wither serves as an example.[28] D-Company was an international crime syndicate, founded in Mumbai in 1976. In the mid-1980s, under the pressure of the Indian authorities it has been re-located to Dubai, where was able to expand its operations, such as smuggling, weapons and drug trafficking, extortion, protection rackets and illegal hawala transfers.

The usage of hawala by terrorist groups has been shown by several studies. Rowland et al. indicate that Al-Qaeda has a vast financial network, including companies and bank accounts, but also relies on hawala to transfer money.[29] Arianti et al. reports a case when the Arakan Rohingya Salvation Army in Myanmar used hawala for the distribution of funds.[30] The Katibat Imam Al-Bukhari group had reportedly received funding from its cells through hawala methods.[31] Fair was able to show that the Khalistan Liberation Force financed itself through criminal activities in India, and receiving money from Sikh diaspora in Canada and the United Kingdom through hawala.[32]

[25] GORDON, S.: Regionalism and Cross-Border Cooperation against Crime and Terrorism in the Asia-Pacific. Security Challenges, 2009/4, https://www.jstor.org/stable/26460070 (downloaded 8 September 2023)

[26] GATTI, A.: Urban terrorist sanctuaries in Europe: the case of Molenbeek. In: PEKTAS, S. – LEMAN, J. (Eds.): Militant jihadism. Leuven University Press, 2019. https://doi.org/10.2307/j.ctvq2vzmt.12 (downloaded 8 September 2023)

[27] REALUYO, C. B.: Following the terrorist money trail. Connections, 2011/2, http://dx.doi.org/10.11610/Connections.10.2.04 (downloaded 8 September 2023); WHITTAKER, J.: The Role of Financial Technologies in US-Based ISIS Terror Plots. Studies in Conflict & Terrorism. 2022. https://doi.org/10.1080/1057610X.2022.2133345 (downloaded 8 September 2023)

[28] MULLINS, S. – WITHER, J. K.: Terrorism and organised crime. Connections, 2016/3, https://doi.org/10.11610/Connections.15.3.06, (downloaded 8 September 2023)

[29] ROWLAND, J., et al.: Whither cyberpower?. International Journal of Critical Infrastructure Protection, 2014/7, http://dx.doi.org/10.1016/j.ijcip.2014.04.001 (downloaded 8 September 2023)

[30] ARIANTI, V. et al.: SOUTHEAST ASIA: Indonesia, Philippines, Malaysia, Myanmar, Thailand, Singapore. Counter Terrorist Trends and Analyses, 2020/1, https://www.jstor.org/stable/26865751 (downloaded 8 September 2023)

[31] SOLIEV, N. – PANTUCCI, R.: CENTRAL ASIA: Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan. Counter Terrorist Trends and Analyses, 2021/1, https://www.jstor.org/stable/26979987 (downloaded 8 September 2023)

[32] FAIR, C.C.: India. Urban Battle Fields of South Asia: Lessons Learned from Sri Lanka, India, and Pakistan, RAND Corporation, 2004, http://www.jstor.org/stable/10.7249/mg210a.11 (downloaded 8 September 2023)

According to Almohamad, the Islamic State heavily uses hawala to evade traceable formal banking transactions. These few examples clearly underpin that terrorist groups do adopt hawala.[33]

But how do they exploit hawala? An insight into their practice is provided by Freeman and Ruehsen, who reports the case of the Times Square bomber Faisal Shahzad.[34] "*In February 2010 Mr. Shahzad's handlers in Pakistan (Tehrik-e-Taliban) arranged for US $4,900 to be sent via an unregistered hawala network operated by two brothers, one of whom, Aftab Ali Khan, was an illegal Pakistani immigrant living in Brookline, Massachusetts. On February 24 or 25th, Mr. Ali Khan met Mr. Shahzad just outside of his Massachusetts apartment to hand over US $4,900 in cash. There was no suggestion in any subsequent investigations that Mr. Ali Khan knew what the money would be used for. He was merely completing an anonymous business transaction.*"[35] (Freeman and Ruehsen, 2013, p. 10.). This example shows how terrorist groups can finance their attacks without written record, through hawala.

Moreover, hawala, as an informal fund-transfer method, also can be used to gain money. Shay reports, that "*Al-Shabaab has managed to generate tens of thousands of pounds in funding through the UK-based Somali population, which is estimated at 250,000. While some British Somalis willingly donate to the terrorist organization, a proportion of the cash legitimately sent back to extended families in the country is syphoned off by the Islamists.*"[36] As Kaunert and Leonard observe, Islamic charities are regularly donated by Muslims, usually in cash through hawala. It is highly probable that some of the donations made to Islamic charities have financed terrorism, without the knowledge of the pious emigrated workers.[37] This view is supported by several studies.[38]

Overall, these studies underpin that hawala is used by terrorist groups, illustrate the role of hawala in financing terrorism and also show those difficulties that the law enforcement agencies are facing. Strong informal fund-transfer systems may help terrorist groups to finance their activities, while the actions that weakens these systems may help counter-terrorism. The factors that make hawala strong and developed have to be understood, in order to plan actions that can weaken the hawala. These factors and possible actions will be discussed in the following part.

[33] ALMOHAMAD, S.: Not a Storm in a Teacup: The Islamic State after the Caliphate. German Institute of Global and Area Studies, 2021, http://www.jstor.org/stable/resrep31795 (downloaded 8 September 2023)

[34] FREEMAN, M. – RUEHSEN, M.: Terrorism Financing Methods: An Overview. Perspectives on Terrorism, 2013/4, http://www.jstor.org/stable/26296981 (downloaded 8 September 2023)

[35] Ibid. p. 30.

[36] SHAY, S.: Al Shabaab from local to regional and global terror threat. Journal of Central and Eastern European African Studies, 2023/3, https://doi.org/10.59569/jceeas.2021.1.3.35 (downloaded 8 September 2023)

[37] KAUNERT, C. – LÉONARD, S.: EU Counterterrorism and the European Neighbourhood Policy: An Appraisal of the Southern Dimension. Terrorism and Political Violence, 2011/2, https://doi.org/10.1080/09546553.2010.538276 (downloaded 8 September 2023)

[38] KAUNERT, C. – LÉONARD op. cit.;
PATEL, I.: Emergence of Institutional Islamophobia: The Case of the Charity Commission of England and Wales. ReOrient, 2017/1, https://doi.org/10.13169/reorient.3.1.0023 (downloaded 8 September 2023)

What makes hawala flourishing?

This study aims to explore the ways in which hawala can be weakened. But first, it is necessary to investigate the factors that makes hawala grow and operate successfully. Why hawala is preferred to formal banking? The research to date has been able to indicate two major factors that are making the informal fund-transfer systems flourish. As it has been explained above, hawala is a fund-transfer system, which is not illicit by nature, however, it can be exploited and used for illicit purposes as well. The illegal side of hawala (e.g., illegal trade or corruption) lies beyond the scope of this study, this research examines the not entirely illegal side of hawala.

The first factor that makes hawala flourish is the absence of the formal banking services. The less of formal, downloadedible and affordable banking, the more of the informal, untraceable and underground banking. As Kosse and Vermeulen note, there are informal fund-transfer organisations "*active in the market, in particular for payments to countries with low levels of financial development. They are often referred to as Hawala or Hundi operators. There is evidence that these systems transfer more than tens of billions of dollars globally.*"[39] This view is supported by de Azevedo, who provides information about the hawala, set up in ISIS's camps, built to accommodate people, mostly ISIS families: "*There are two hawala remittance offices in this part of the camp. [...] Hawala employees within the camp claim they receive dozens of remittances daily and an estimate sum of between 15,000 to 20,000 USD per month.*"[40] The previously mentioned case of Somalia is another important example of how underground banking is flourishing in the absence of formal banking industry.

Iazzolino and Hersi describe the case of a Somalian woman who got loan to start her textile business through hawala.[41] Besenyő mentions the so-called cash bazaar economy: in the absence of downloadedible banking system, many depend on hawala when doing transaction or asking for loan.[42]

The second factor that makes hawala grow is the need for a simple and effective international fund-transfer method. As it has been shown in the previous parts, migrant workers tend to use hawala when sending money home. As migration is growing, so increasing the remittances sent home by migrants.[43]

[39] KOSSE, A. – VERMEULEN, R.: Migrants' Choice of Remittance Channel: Do General Payment Habits Play a Role? World Development, 2014/62, p. 214 http://dx.doi.org/10.1016/j.worlddev.2014.05.002 (downloaded 8 September 2023)

[40] DE AZEVEDO, C. V.: ISIS Resurgence in Al Hawl Camp and Human Smuggling Enterprises in Syria: Crime and Terror Convergence? Perspectives on Terrorism, 2020/4, p. 53. https://www.jstor.org/stable/26927663 (downloaded 8 September 2023)

[41] IAZZOLINO, G. – HERSI, M.: Shelter from the storm: Somali migrant networks in Uganda between international business and regional geopolitics. Journal of Eastern African Studies, 2019/3, https://doi.org/10.1080/17531055.2019.1575513 (downloaded 8 September 2023

[42] BESENYŐ, J.: Barry Buzan's Securitization Theory and the case of Iraqi Kurdish military action against ISIS in 2014. Journal of Security and Sustainability Issues, 2019/3, http://doi.org/10.9770/jssi.2019.8.3(1) (downloaded 8 September 2023)

[43] BESENYŐ, J.: How many faces might migration have? A review of: "Two Faces of European Migration" by Viktor Glied. Journal of Central and Eastern European African Studies, 2023/1-2, https://doi.org/10.59569/jceeas.2021.1.1-2.14 (downloaded 8 September 2023)

Beside remittances, donations are also found to be sent through hawala. Islamic charities may be donated regularly or after a natural disaster or war in the Middle-East, and these donations also can make hawala grow. The principle of *Zakat* in Islam requires to give aids to those in need, therefore Muslims donate at least annually. Those pious Muslims who prefer hawala to donate Islamic charities, contribute to the growing of informal fund-transfer systems.

Together, these findings indicate that hawala, the old money transfer method is flourishing in the absence of downloadedible formal banking industry. Moreover, it is clear that hawala is preferred by people sending remittances or donations to their motherland or region, with which they feel connected. Having investigated some factors that makes hawala strong, the following part attempts to recommend actions that may weaken hawala.

How to weaken hawala?

First of all, it is necessary to briefly describe the banking industry, which is a formal and regulated system. Banks are considered to be the central part of the financial system by playing a key role as they are the intermediaries between savers, borrowers and governments.[44] Should the banking system operate efficiently, savers, investors, borrowers and governments are able to prosper, and aims can be realised. However, the way of modern banking is fragile (banks use deposits to finance loans), meaning that banks would definitely collapse if they could not perform to the satisfaction of their depositors. Moreover, a distressed bank can cause a loss of confidence in the other banks as well. Therefore, the financial sector is rigorously regulated. Central banks have a key role in maintaining the sector’s stability by having regulatory and supervisory responsibilities. It should be mentioned that although there are differences between conventional banking (e.g., banking in the EU) and Islamic banking,[45] the above-mentioned intermediary role is practically the same.

The need for a cheap, simple and effective international money-transfer system has been identified in the previous section. Answering to this need effectively may weaken or even shut down the informal fund-transfer systems, which is undoubtedly help the efforts of counter-terrorism by attacking the channels used for financing terrorism. The above-mentioned examples show that people working abroad regularly send money to their motherland in Africa or in the Middle East. And hawala is used for this purpose, instead of formal banking services. Therefore, it sounds logical that increasing financial inclusion and using formal banking services is a way of weakening informal fund-transfer systems. Therefore, decreasing the number of the so-called 'unbanked’ people and spreading the services of the banking industry should be addressed appropriately. Relevant campaigns could be run by governments and central banks to advertise banking services, in order to increase financial inclusion.

[44] GODDARD, J. – WILSON, J.: Banking. Oxford University Press, 2016. ISBN 978-0-19-968892-0 (downloaded 8 September 2023)

[45] SALMAN, A. – NAWAZ, H.: Islamic financial system and conventional banking: A comparison, Arab Economic and Business Journal, 2018/2, https://doi.org/10.1016/j.aebj.2018.09.003 (downloaded 8 September 2023)

Governments may induce the banks to offer very cheap bank accounts, with free or almost free possibilities of withdrawing cash. Banks should be encouraged to help people to receive relatively small amounts regularly from abroad and make it possible to withdraw it from ATMs or in a branch or at the post office. Taking into consideration that hawaladars pay in cash, easy downloaded to cash may be a key point, especially in the countries or regions, where cashless transactions are not yet widespread. For this purpose, special accounts might be opened, e.g., without fees, if money up to a certain amount arrives to it from abroad in each month. Exchange rates are also have to be set in order to provide cheap solutions to people receiving money from abroad. Withdrawing money from these special bank accounts shall be free of charge to the customers (up to a certain amount of money). The main objective is to provide simple and cheap (or even free) solutions.

Increasing the financial inclusion should be a common goal of the governments and the financial sector. As it has been demonstrated, financial inclusion increases financial stability and reduces inflation in low financial development countries.[46] Thus, governments and banks, policymakers and businessmen should cooperate, in order to make the services of the formal banking industry widely used. No doubt, both formal banking and informal fund-transfer systems are built on trust. A research, examining the link between trust and financial inclusion in Ghana, has found that increasing trust in the banking industry, increases also the usage of banking services and financial inclusion.[47] Thus, trust is essential. A question should be posed here. Can a Muslim person trust in the formal banking institutions? It is clear that banking can be built in line with the Islamic law, as Islamic banks are operating. As Salman and Nawaz report, Islamic banks in Pakistan are oversight by the central bank and a Sharia supervisory board. Thus, the operation – according to divine law of Allah and his last messenger Muhammad – is guaranteed.[48] Moreover, some of the non-Islamic banks in non-Muslim countries offer Sharia compliant products as well. Therefore, Muslim people can be encouraged to use the services of conventional banks (e.g., banks in the EU) and Islamic banks.

Due to the rapid development of ICT, financial services are being digitalised and being available online as well. Harsono considers the digital payment solutions the end of informal money transfer systems, referring to the younger generations that prefer the use of digital services and gadgets, including the everyday transactions.[49] Therefore, young and middle-aged migrant workers probably choose digitalised (Sharia compliant) banking services to send remittances home, if cheap and simple solutions would be available for their family members at home, including downloaded to cash.

[46] OANH, T., et al.: Relationship between financial inclusion, monetary policy and financial stability: An analysis in high financial development and low financial development countries. Heliyon, 2023/6, https://doi.org/10.1016/j.heliyon.2023.e16647 (downloaded 8 September 2023)

[47] KOOMSON, I., et al.: Trust in banks, financial inclusion and the mediating role of borrower discouragement. International Review of Economics and Finance, 2023/88, https://doi.org/10.1016/j.iref.2023.07.090 (downloaded 8 September 2023)

[48] SALMAN, A. – NAWAZ op. cit.

[49] HARSONO, H.: Prioritizing SOF Counter-Threat Financing Efforts in the Digital Domain. The Cyber Defense Review, 2020/3, https://www.jstor.org/stable/26954878 (downloaded 8 September 2023)

All the above indicate that the formal banking industry can be the alternative for informal fund-transfer systems, e.g., hawala. If the people could effectively use the formal payment services of the banking industry to send remittances home or to donate charities, the hawala system would surely be diminished or even it may disappear. In order to reach this goal, first, the banking industry should be incentivised to provide cheap and simple solutions in line with Islamic law. Both conventional and Islamic banks should make these services available. Then, the governments and the banking industry could encourage people to use the simple and cheap, Sharia compliant banking services, instead of hawala that can easily be exploited by terrorist groups. It should be added that in some cases, providing cheap and simple solutions may be a loss-making business for banks. Therefore, the governments and the central banks should find the necessary compensating methods. Fighting against financing terrorism and decreasing the number of unbanked households constitute undoubtedly a common goal; thus, the necessary cooperation should be urged.

Conclusion

The objective of this study was to describe hawala and examine the reason for the popularity of legal money-transfer, and to identify ways in which hawala can be weakened or even closed. As it has been found that the formal banking industry can be the alternative for informal fund-transfer systems, e.g., hawala. If the people could use the formal payment services of the banking industry to send remittances home or to donate charities, the hawala system would surely be diminished or even may disappear. To reach this, first, the banking industry should be encouraged to provide cheap and simple, Sharia compliant services (including withdrawing cash), then the governments and the banking industry should encourage people to use these services, instead of hawala that can easily be exploited by terrorist groups. These steps can decrease the number of unbanked households by spreading the services of the formal banking industry. Financial inclusion increases financial stability and reduces inflation in the less developed countries, which is obviously an objective of the governments.

It should be emphasised that a cooperation is needed between the governments, the central banks and the banking institutions to reach the above-mentioned goals. Fighting against financing terrorism and decreasing the number of unbanked households constitute undoubtedly a common goal of the governments and the banking industry.

Bibliography:

- AKRAM, M., et al.: Misuse of charitable giving to finance violent extremism; a futuristic actions study amidst COVI-19 pandemic. Social Sciences & Humanities Open, 2021/1. https://doi.org/10.1016/j.ssaho.2021.100140 (downloaded 8 September 2023)
- ALI, D., Gelsdorf, K.: Risk-averse to risk-willing: Learning from the 2011 Somalia cash response. Global food security, 2012/1, http://dx.doi.org/10.1016/j.gfs.2012.07.008 (downloaded 8 September 2023)

- ALMOHAMAD, S.: Not a Storm in a Teacup: The Islamic State after the Caliphate. German Institute of Global and Area Studies, 2021, http://www.jstor.org/stable/resrep31795 (downloaded 8 September 2023)
- ARIANTI, V. et al.: SOUTHEAST ASIA: Indonesia, Philippines, Malaysia, Myanmar, Thailand, Singapore. Counter Terrorist Trends and Analyses, 2020/1, https://www.jstor.org/stable/26865751 (downloaded 8 September 2023)
- BALLARD, R.: Hawala: criminal haven or vital financial network? Newsletter of the International Institute of Asian Studies, October, 2006, https://doi.org/10.11588/xarep.00000263 (downloaded 8 September 2023)
- BESENYŐ, J. – SINKÓ, G.: The social media use of African terrorist organizations: a comparative study of Al-Qaeda in the Islamic Maghreb, Al-Shabaab and Boko Haram. Insights into regional development, 2021/3, http://doi.org/10.9770/IRD.2021.3.3(4) (downloaded 8 September 2023)
- BESENYŐ, J.: Barry Buzan's Securitization Theory and the case of Iraqi Kurdish military action against ISIS in 2014. Journal of Security and Sustainability Issues, 2019/3, http://doi.org/10.9770/jssi.2019.8.3(1) (downloaded 8 September 2023)
- BESENYŐ, J.: How many faces might migration have? A review of: "Two Faces of European Migration" by Viktor Glied. Journal of Central and Eastern European African Studies, 2023/1-2, https://doi.org/10.59569/jceeas.2021.1.1-2.14 (downloaded 8 September 2023)
- BESENYŐ, J.: Low-cost attacks, unnoticeable plots? Overview on the economical character of current terrorism. Strategic Impact, 2017/1, https://www.ceeol.com/search/article-detail?id=829355 (downloaded 8 September 2023)
- BONANSINGA, D.: Counter terrorism in the 21st century and the role of the European Union. Polish Political Science Review, 2015/1, https://doi.org/10.1515/ppsr-2015-0027 (downloaded 8 September 2023)
- CHAKRABORTY, A. Renegotiating Boundaries Exploring the Lives of Undocumented Bangladeshi Women Workers in India. In: JONES – R., FERDOUSH, A. (Eds.): Borders and Mobility in South Asia and Beyond. Amsterdam University Press, 2018. pp. 123-143. https://doi.org/10.2307/j.ctv513ckq.9 (downloaded 8 September 2023)
- DE AZEVEDO, C. V.: ISIS Resurgence in Al Hawl Camp and Human Smuggling Enterprises in Syria: Crime and Terror Convergence? Perspectives on Terrorism, 2020/4, https://www.jstor.org/stable/26927663 (downloaded 8 September 2023)
- FAIR, C.C.: India. Urban Battle Fields of South Asia: Lessons Learned from Sri Lanka, India, and Pakistan, RAND Corporation, 2004, http://www.jstor.org/stable/10.7249/mg210a.11 (downloaded 8 September 2023)
- FARBER, S.: Countering the Financing of Terrorists' Salaries. Studies in Conflict & Terrorism, 2023. https://doi.org/10.1080/1057610X.2023.2199471 (downloaded 8 September 2023)

- FREEMAN, M. – RUEHSEN, M.: Terrorism Financing Methods: An Overview. Perspectives on Terrorism, 2013/4, http://www.jstor.org/stable/26296981 (downloaded 8 September 2023)
- GATTI, A.: Urban terrorist sanctuaries in Europe: the case of Molenbeck. In: PEKTAS, S. – LEMAN, J. (Eds.): Militant jihadism. Leuven University Press, 2019. https://doi.org/10.2307/j.ctvq2vzmt.12 (downloaded 8 September 2023)
- GODDARD, J. – WILSON, J.: Banking. Oxford University Press, 2016. ISBN 978-0-19-968892-0 (downloaded 8 September 2023)
- GORDON, S.: Regionalism and Cross-Border Cooperation against Crime and Terrorism in the Asia-Pacific. Security Challenges, 2009/4, https://www.jstor.org/stable/26460070 (downloaded 8 September 2023)
- HARSONO, H.: Prioritizing SOF Counter-Threat Financing Efforts in the Digital Domain. The Cyber Defense Review, 2020/3, https://www.jstor.org/stable/26954878 (downloaded 8 September 2023)
- IAZZOLINO, G. – HERSI, M.: Shelter from the storm: Somali migrant networks in Uganda between international business and regional geopolitics. Journal of Eastern African Studies, 2019/3, https://doi.org/10.1080/17531055.2019.1575513 (downloaded 8 September 2023)
- IMAN, N. Is mobile payment still relevant in the fintech era? Electronic Commerce Research and Applications, 2018/30, https://doi.org/10.1016/j.elerap.2018.05.009 (downloaded 8 September 2023)
- JONES, S.G. – LIBICKI, M.C.: How terrorist groups end: lessons for countering al Qa'ida. RAND Corporation, 2008, https://www.jstor.org/stable/10.7249/mg741rc.16 (downloaded 8 September 2023)
- KAKHKHAROV, J. – AKIMOV, A. – ROHDE, N.: Transaction costs and recorded remittances in the post-Soviet economies: Evidence from a new dataset on bilateral flows. Economic Modelling, 2017/60, http://dx.doi.org/10.1016/j.econmod.2016.09.011 (downloaded 8 September 2023)
- KAUNERT, C. – LÉONARD, S.: EU Counterterrorism and the European Neighbourhood Policy: An Appraisal of the Southern Dimension. Terrorism and Political Violence, 2011/2, https://doi.org/10.1080/09546553.2010.538276 (downloaded 8 September 2023)
- KOOMSON, I., et al.: Trust in banks, financial inclusion and the mediating role of borrower discouragement. International Review of Economics and Finance, 2023/88, https://doi.org/10.1016/j.iref.2023.07.090 (downloaded 8 September 2023)
- KOSSE, A. – VERMEULEN, R.: Migrants' Choice of Remittance Channel: Do General Payment Habits Play a Role? World Development, 2014/62, http://dx.doi.org/10.1016/j.worlddev.2014.05.002 (downloaded 8 September 2023)

- KUMAR, A.: Terror Financing in Bangladesh. Strategic Analysis, 2009/6, https://doi.org/10.1080/09700160903255913 (downloaded 8 September 2023)

- LADÁNYI, E. – KOBOLKA, I.: The hawala system. Interdisciplinary management research. 2014/10, https://econpapers.repec.org/RePEc:osi:journl:v:10:y:2014:p:413-420 (downloaded 8 September 2023)

- LEESON, P.T. – BOETTKE, P.J.: Two-tiered entrepreneurship and economic development. International Review of Law and Economics, 2009/29, https://doi.org/10.1016/j.irle.2009.02.005 (downloaded 8 September 2023)

- MITRA, R. – SANGHI, S.: The small island states in the Indo-Pacific: sovereignty lost?. Asia Pacific Law Review, 2023/2, https://doi.org/10.1080/10192557.2023.2181806 (downloaded 8 September 2023)

- MUKHTAR, A. et al.: Challenges confronting the 'One Belt One Road' initiative: Social networks and cross-cultural adjustment in CPEC projects. International Business Review, 2022/31, https://doi.org/10.1016/j.ibusrev.2021.101902 (downloaded 8 September 2023)

- MULLINS, S. – WITHER, J. K.: Terrorism and organised crime. Connections, 2016/3, https://doi.org/10.11610/Connections.15.3.06, (downloaded 8 September 2023)

- OANH, T., et al.: Relationship between financial inclusion, monetary policy and financial stability: An analysis in high financial development and low financial development countries. Heliyon, 2023/6, https://doi.org/10.1016/j.heliyon.2023.e16647 (downloaded 8 September 2023)

- PATEL, I.: Emergence of Institutional Islamophobia: The Case of the Charity Commission of England and Wales. ReOrient, 2017/1, https://doi.org/10.13169/reorient.3.1.0023 (downloaded 8 September 2023)

- PHILLIPS, B. J.: How Did 9/11 Affect Terrorism Research? Examining Articles and Authors, 1970–2019. Terrorism and Political Violence, 2022/2, https://doi.org/10.1080/09546553.2021.1935889 (downloaded 8 September 2023)

- REALUYO, C. B.: Following the terrorist money trail. Connections, 2011/2, http://dx.doi.org/10.11610/Connections.10.2.04 (downloaded 8 September 2023)

- ROWLAND, J., et al.: Whither cyberpower?. International Journal of Critical Infrastructure Protection, 2014/7, http://dx.doi.org/10.1016/j.ijcip.2014.04.001 (downloaded 8 September 2023)

- SALMAN, A. – NAWAZ, H.: Islamic financial system and conventional banking: A comparison, Arab Economic and Business Journal, 2018/2, https://doi.org/10.1016/j.aebj.2018.09.003 (downloaded 8 September 2023)

- SCHRAMM, M. – TAUBE, M.: Evolution and institutional foundation of the hawala financial system. International Review of Financial Analysis, 2003/12, https://doi.org/10.1016/S1057-5219(03)00032-2 (downloaded 8 September 2023)
- SHAFFER, R. – BESENYŐ, J.: Terrorism against healthcare facilities and workers in Africa: An assessment of attack modes, targets and locations. African Security Review, 2023/1, https://doi.org/10.1080/10246029.2023.2213220 (downloaded 8 September 2023)
- SHAY, S.: Al Shabaab from local to regional and global terror threat. Journal of Central and Eastern European African Studies, 2023/3, https://doi.org/10.59569/jceeas.2021.1.3.35 (downloaded 8 September 2023)
- SOLIEV, N. – PANTUCCI, R.: CENTRAL ASIA: Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan. Counter Terrorist Trends and Analyses, 2021/1, https://www.jstor.org/stable/26979987 (downloaded 8 September 2023)
- SOMOGYI, T. – NAGY, R.: Cyber threats and security challenges in the Hungarian financial sector. Contemporary Military Challenges, 2022/3, https://doi.org/10.33179/BSV.99.SVI.11.CMC.24.3.1 (downloaded 8 September 2023)
- SOMOGYI, T. – NAGY, R.: The financial infrastructure as a critical infrastructure and it's specialities. National Security Review, 2/2021, https://www.knbsz.gov.hu/hu/letoltes/szsz/2021_2_NSR.pdf#page=213 (downloaded 8 September 2023)
- WHITTAKER, J.: The Role of Financial Technologies in US-Based ISIS Terror Plots. Studies in Conflict & Terrorism. 2022. https://doi.org/10.1080/1057610X.2022.2133345 (downloaded 8 September 2023)
- WU, Y. – NAGY, R.: The industrial safety of food processing in light of operational risks reduction aspects. National Security Review, 2022/2, https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_2_NSR.pdf (downloaded 8 September 2023)
- ZETZSCHE, D.A., et al.: DLT-based enhancement of cross-border payment efficiency – a legal and regulatory perspective. Law and Financial Markets Review, 2021/1-2, https://doi.org/10.1080/17521440.2022.2065809 (downloaded 8 September 2023)

MADINA IGIBAYEVA[1]

THE PROBLEM OF UIGHUR SEPARATISM IN THE SHANGHAI COOPERATION ORGANIZATION

Abstract

The SCO constantly deals with the fight against separatism, and developed multilateral mechanism to cope with the problem. From the moment of its formation until now, within the Organization, the Member States have made great strides in reaching consensus on the issue, at regulatory and practical levels. Such documents as the ”Shanghai Convention on Combating Terrorism, Separatism and Extremism” of 2001, the “SCO Charter”, the ”Statement of the Council of Heads of SCO Member States on countering the spread of terrorist, separatist and extremist ideology, including on the Internet” of 2020, etc., ensure the dynamic development of work to combat separatism within the SCO.

“The problem of Uighur separatism” is very complex, multifaceted, multidimensional, and at the same time, a poorly studied issue. The paper reviews the history of the extreme politicization and mythologization of the problem of separatism, including Uighur. It also analyses the ”problem of Uighur separatism” today, which remains, perhaps, one of the key issues in terms of preserving regional security, ensuring positive dynamics in the development of cooperation between China, the Central Asian countries, Russia, Afghanistan, and the adjacent areas. Accordingly, the main solutions to this problem should be to strengthen cooperation between these countries and, first of all, within the framework of the SCO.

Keywords**:** SCO, Central Asia, Xinjiang Uyghur Autonomous Region, separatism, Uighurs.

Introduction

The problem of separatism is one of the main ones for modern international relations. In most multinational states, there are territories that seek independence and sovereignty. The reasons for separatism can be different, ranging from historical and cultural to political reasons. At the same time, when substantiating their actions, the separatists very often refer to the right of peoples to self-determination and free development, which is recorded also in the UN documents. The principle of self-determination was strengthened and received a broader interpretation, with the adoption on December 14, 1960 of the Declaration on the Granting of Independence to Colonial Countries and Peoples (Resolution 1514 (XV) of the UN General Assembly). Article 2 stipulates that all peoples have the right to self-determination, the right to their political status, the right to their economic and socio-cultural development.

[1] ORCID: 0000-0002-7606-4313

But at the same time, Article 6 of the Declaration contains limitations and indicates that any action aimed at attempting partially or completely to violate the territorial integrity of the state is contrary to the basic principles and objectives of the UN Charter.[2]

The principle of self-determination, therefore, does not necessarily imply the creation of an independent State, but it can be implemented in the form of political or cultural autonomy, and does not imply the forcible unilateral separation of a part of the territory, which is the main content of separatism. The Shanghai Convention on Combating Terrorism, Separatism and Extremism defines separatism as *"any act aimed at violating the territorial integrity of a State, including the separation of a part of its territory from it, or the disintegration of a State committed by force, as well as planning and preparing such an act, aiding and abetting its commission and incitement to him."*[3]

The SCO is the first international organization that has been constantly supporting a fight against separatism, and the first multilateral mechanism that has defined separatism. From the moment of its formation until now, within the Organization, the Member States have made great strides in reaching consensus at regulatory and legal levels. Such documents as the "Shanghai Convention on Combating Terrorism, Separatism and Extremism" of 2001, the "SCO Charter", the "Statement of the Council of Heads of the SCO Member States on countering the spread of terrorist, separatist and extremist ideology, including on the Internet" of 2020, etc., ensure the dynamic development of work to combat separatism within the SCO.[4]

Separatism is a serious threat to the integrity of the State. In almost every major country, there are at least 2-3 ethnic groups, on behalf of which, demands are made with more or less intensity to grant for them some measure of independence, up to sovereignty.

L. Snyder[5] defines separatism as an image, activity, principle or practice developed for a complete exit from a centralized political organism. He notes that extremist activists deny autonomy or semi-autonomy only as some half measures and call for secession. The separatists consider themselves liberators, and the authorities of a centralized state regard their activities as treason.

[2] Declaration on the Granting of Independence to Colonial Countries and Peoples (adopted by UN General Assembly Resolution 1514 (XV)), art. 2, art. 6. United Nations. http://www.un.org/ru/documents/decl_conv/declarations/colonial.shtml (downloaded 05 April 2023)

[3] Shanghai Convention on Combating Terrorism, Separatism and Extremism. Official network resources of the President of Russia, http://kremlin.ru/supplement/3405 (downloaded 05 April 2023)

[4] The official page of the SCO. http://chn.sectsco.org

[5] Jack Lewis Snyder is an American political scientist who is the Robert and Renée Belfer Professor of International Relations at Columbia University, specializing in theories of international relations.

If a person is dissatisfied with some aspects of the relations between the center and the periphery that have developed in the state, this in itself does not make him a separatist. On the contrary, the ongoing struggle in the legal field for the establishment of justice in these relations can contribute to strengthening the integrity of the State. Mixing constructive and destructive forms of regional political activity within the same concept, indirectly contributes to the strengthening of the latter and creates an inadequate idea of the scale of their social base.

It should also be noted that skillfully applied autonomization can become a means of resolving interethnic and interregional conflicts, which means the strengthening the integrity of the country and countering separatism. At the same time, the practice shows that separatist intentions can be camouflaged at an early stage, under moderate demands for autonomy. However, the social mimicry inherent in separatism is by no means a reason for confusing it with constructive forms of social activity.

As a rule, separatist movements are formed for reasons of cultural oppression, ethnic violence, denial of rights and other oppression of a certain group of people. Sometimes the occurrence of this phenomenon is associated with the desire to obtain certain expanded rights and powers in the field of self-government. Economy, policy or religion can serve as important factors for such sentiments. For example, these sentiments can prevail, when a certain group of people believes that the dominant majority holds public wealth, pursues discrimination against this group, in terms of political power and religion.

At the same time, SCO members face different levels of separatist threats. On the territory of the People's Republic of China, the actions of separatism are characterized by a long duration and a wide range of areas. Separatist forces in Xinjiang and Tibet, the Hong Kong independence movement, as well as the Taiwan issue have been constantly representing a great concern for Beijing. Russia is also one of the countries under the greatest threat of separatism. Its internal separatist forces are trying to achieve their political aspirations to split the country by carrying out terrorist acts in the country. Other SCO member states also face a potential threat of separatism.

Problem of separatism

”The problem of Uighur (or even broader – ethnic) separatism” is a very complex, multifaceted, multidimensional and, at the same time, a poorly studied issue. Here it is necessary to clearly understand the extreme politicization and mythologization of the problem of separatism, including Uighur. Today, the “problem of Uighur separatism” remains, perhaps, one of the key ones, in terms of preserving regional security, ensuring positive dynamics in the development of cooperation between China, Central Asian countries, Russia, Afghanistan and the adjacent areas. Accordingly, the main solutions to this problem should be to strengthen cooperation between these countries and, first of all, within the framework of the SCO.

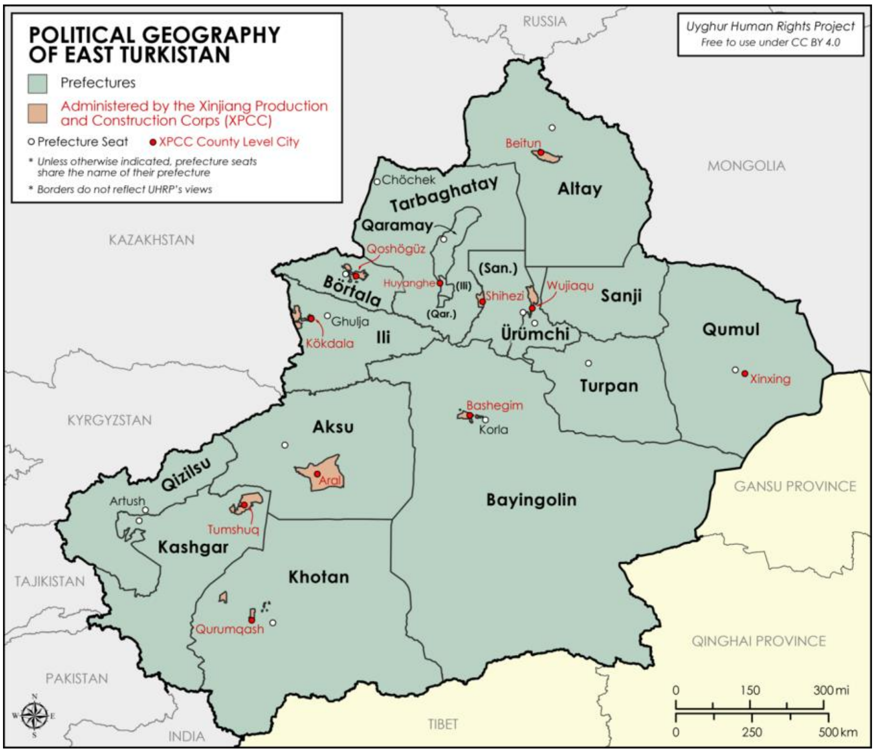


Figure 1: Map of "so-called" East Turkistan[6]

The Uighurs are one of the most ancient peoples inhabiting on the territory of the present day XUAR, and living in large diasporas in a number of countries Central Asia. The first Uyghur state formation is the Uyghur Khaganate, it was founded in the VIII century and existed for about 100 years. In a later period, the Uighurs, still several times, created their own states, which were not distinguished by strong statehood and longevity. In the XVII century, the Uighurs founded another formation called East Turkestan. However, in 1760, under the onslaught of Manchurian-Chinese troops, the Uighurs lost their independence, and the region was finally incorporated into the Chinese Empire and became known as Xinjiang, in Chinese – "new border". Since the annexation of Xinjiang to the Chinese Empire, the indigenous ethnic groups living in this territory, primarily the most numerous – the Uighur, have constantly fought for independence, using both internal resources and external assistance for this.[7]

The first and very large scale uprising in the history of the Uighur struggle for independence occurred a hundred years after the annexation of East Turkestan to the Qing Empire – in the 1860s. Then one of the bloodiest riots in history broke out – the Uighur-Dungan uprising.

[6] Source: https://uhrp.org/report/decolonizing-the-discussion-of-uyghurs-recommendations-for-journalists-and-researchers/ (downloaded 05 May 2023)

[7] Brief history of the Uyghers. https://www.oocities.org/idonkari/Brief%20History%20of%20the%20Uyghers.htm (downloaded 05 May 2023)

As a result of this revolt, the Uighur-Dungan rebels seized most of the Ili Region, but a conflict for power broke out between the two nationalities – the Dungans and the Uighurs, who had once rebelled against Chinese oppression, began to fight among themselves.

Having defeated the Dungans, the Uighurs created several independent associations on the territory of East Turkestan. One of them is the Kulja Sultanate. After 10 years of existence, it was captured by the Russian Empire, which promised to the representatives of the Sultanate not to transfer their lands to China, but acted differently. So the territory of the Kulja Sultan was again subject to China.

In addition to the Kulja Sultanate, in the 1860s, as a result of the Uighur-Dungan uprising, several more associations were formed: the Kuchar Khanate,[8] the Kashgar Khanate[9], the Khotan Islamic State,[10] and the Urumchi Sultanate.[11] They were fragmented and, as a result, were at risk of instant destruction; so the famous Kashgar commander Yakub-bek took responsibility for uniting the fragmented lands and gathered them into a single state, which he called Yettishar. The state of Yettishar existed from 1865 to 1877 and was actively developing: Yakub-bek carried out reforms in all spheres of life and sought to improve the standard of living of his people. It was difficult for the young state to grow and develop independently, so it became involved in political games between China, Russia and England. Yakub-bek tried to cooperate with major powers, in order to achieve diplomatic recognition of the state. However, despite his efforts, no one recognized the state of Yettishar, and in 1877 the Qing Empire defeated it. After thirteen difficult, but independent years of existence of the Uighur state, the power over East Turkestan again passed to China.

First half of the 20th century: Historical background

In the 20th century, the confrontation of the Uyghur people continued, and the level of desperation of the people only increased. Resistance, like a wave, either increased or decreased, but it always remained. In the 1930s, there was another powerful outbreak in the history of the Uyghur struggle for independence. During this period, Xinjiang was under the serious influence of the USSR.

[8] The Uighur Khanate. Time of existence – 1864 AD. In June 1864, the Dungan soldiers of the Kucher garrison rebelled, and the rest of the population, led by Rashidin-khoja, rose up after them. Having liberated four districts – Turfan, Komul (Hami), Aksu and Ush (Ush-Turfan), he established his authority here, creating the Kuchar Khanate.

[9] Then Mogulia, Mamlakat-i-Moguliye, the Yarkend Khanate, Saidiya. The capital is 1514-1596 Yarkand. 1596-1665 Kashgar. Time of existence – 1514-1866. The form of government is the Khanate. Kashgar, East Turkestan is a region stretching from Siberia to Kashmir, from the Pamir Upland to the former border of the Chinese Empire. Since 1877, the Khanate has been part of the Chinese Empire.

[10] The Kingdom of Khotan was an ancient Buddhist Saka kingdom located on the branch of the Silk Road that ran along the southern edge of the Taklamakan Desert in Xinjiang. The ancient capital was originally sited to the west of modern-day Hotan at Yotkan. From the Han dynasty until at least the Tang dynasty it was known in Chinese as Yutian. This largely Buddhist kingdom existed for over a thousand years until it was conquered by the Muslim Kara-Khanid Khanate in 1006, during the Islamization and Turkicization of Xinjiang.

[11] Dungan Sultanate. The capital is Urumqi. Time of existence – 1864-1877.

The Soviet authorities helped China suppress the uprisings and took part in the development of the region. The Soviet Union even adopted a resolution ”on measures to develop the economy of Xinjiang”. During this period, under the leadership of Khoja Niyaz Khazhi and Yulbars Khan, the largest uprising of the Uyghurs took place, during which, they conquered almost 90% of their lands. Thus, an independent Uighur state was created – the First East Turkestan Islamic Republic (Republic of Uyghuristan). The republic introduced a national currency, its own flag, and it was led by the leader of the uprising of the 1930s, Khoja Niyaz Khazhi.[12]

Despite all the efforts of the Uighurs, they, like the last time when they created the state of Yettishar, failed to get recognition of their country's independence from the world community. In such an unrecognized situation, it was extremely difficult for the young republic to coexist alongside the major powers. Having become involved in the game of the USSR and China, the East Turkestan Islamic Republic was defeated by the joint efforts of these countries in 1934. Some of its rulers were killed, some went on the run, and all subsequent uprisings were brutally suppressed. In the early 1940s, the USSR changed its tactics of behavior, due to soured relations with China and took part in the creation of Uighur resistance organizations, after which, in 1944, the Second East Turkestan Republic (East Turkestan Revolutionary Republic) was created, which lasted until 1949, and at the moment became the last independent state in the history of the Uighurs. During the five years of its existence, the republic formed its own army and began to develop, but under pressure from the Soviet authorities, the Second East Turkestan Republic authorities decided to join the PRC in 1949.[13]

After the Communists led by Mao Zedong came to power in China in 1949, Beijing, thanks to Moscow's support, completely restored its lost positions in Xinjiang, and since 1955, this region has acquired the status of the Xinjiang Uygur Autonomous Region of the People's Republic of China. However, the policy subsequently pursued by the Chinese leadership in Xinjiang often provoked protest from ethnic groups living in Xinjiang, primarily Uighurs, which often took the form of armed confrontation with the authorities. Beijing generally managed to keep the situation under control, but the separatist actions caused to the Chinese leadership a quite serious concern.

This concern was also reinforced by the fear of a possible repetition of historical precedents of playing the ”Uighur card” and support for national separatism from the nearest neighbors, including the USSR. In the early 60s, when the cooling of Soviet-Chinese relations came, by the decision of the Central Committee of the CPSU (Communist Party of the Soviet Union), several settlements were created in the eastern regions of Kazakhstan for Uighurs from the XUAR, who were then attracted by the relevant structures to conduct anti-Chinese propaganda.

[12] International Uyghur Foundation for Human Rights and Democracy (IUHRDF). East Turkistan Resume, https://www.iuhrdf.org/cn/east-turkestan-history/ (downloaded 05 May 2023)

[13] DILLON, Michael: A Uighurs’ history of China. The repression in China’s Xinjiang region has deep historical roots. https://www.historytoday.com/archive/behind-times/uighurs’-history-china (downloaded 17 March 2023)

In the second half of the 80s, against the background of the ”perestroika” that began in the Soviet Union and a certain liberalization of the internal political situation in China itself, a noticeable intensification of the activities of Uighur separatists began to be noted in Xinjiang, aimed at secession from the PRC and the proclamation of an independent state of East Turkestan.

According to the latest official Chinese data, the population of the region is about 16 million people, of which the Uighurs make up 7.2 million, and the Chinese 6.4 million. In addition, Kazakhs, Kirgiz’s, Mongols, Tajiks and other peoples also live in the area.[14]

The collapse of the USSR and the emergence of new independent states in Central Asia were a kind of catalyst for another surge of separatist sentiments in the XUAR. The very fact of gaining sovereignty and the creation of national states of ethnically and religiously close peoples of Central Asia had a significant impact on the mood of the local population of Xinjiang, primarily the Uighurs, who perceived the events in the post-Soviet space as a clear example in achieving national independence.

This could not but cause alarm in Beijing, especially given the presence in the Central Asian countries (Kazakhstan, Kyrgyzstan and Uzbekistan) of a fairly large Uighur diaspora, numbering, according to various estimates, from 300 to 500 thousand people. Moreover, in the early 90s, in the conditions of the formation of statehood and the largely objective weakness of the law enforcement structures of the post-Soviet republics of Central Asia, a number of Uighur nationalist organizations became active on the territory of Kazakhstan and Kyrgyzstan, in particular, the International Committee for the Liberation of Turkestan (formerly the National Front of East Turkestan), the Liberation Organization Turkestan, “The United Association of Uighurs”, who began to help their tribesmen in the XUAR, with the aim of recreating the independent state of ”Uighurstan”.[15]

As early as 1992, Xinjiang began to receive ideological literature and financial resources from Saudi Arabia and Turkey through these organizations, whose radical circles helped the supporters of the creation of the Uyghurstan state. After the World Uighur Kurultai, held in Istanbul (Turkey) in December 1992, decided to switch into armed methods of struggle for ”independence”, the transfer of weapons began to the XUAR. A significant part of it came in transit through the territories of the Central Asian republics. There were also attempts to acquire and steal weapons from army warehouses, with the aim of further transfer to Xinjiang.

In addition, fleeing the persecution of the Chinese authorities, the members of separatist groups from XUAR began to hide in Kyrgyzstan and Kazakhstan in the places of residence of the Uyghur diaspora, who tried to conduct anti-Chinese activities, using the capabilities of radical organizations operating in the Central Asian states.

[14] Uighuristan (East Turkestan). http://karty.narod.ru/maps/uygh/uygh.html (downloaded 17 March 2023)

[15] Dosova, B. A.: Kazakhstan and China: Milestones of Bilateral Relations. https://rep.ksu.kz/bitstream/handle/data/7457/Dosova_Kazakhstan_2019.pdf?sequence=1&isAllowed=y (downloaded 22 March 2023)

In particular, since the second half of the 1990s, a noticeable activation of various kinds of extremist organizations and groups began to be noted in Central Asia, primarily the Hizb ut-Tahrir al-Islami party and the so-called Islamic Movement of Uzbekistan (IMU), members of which the Uighurs also became.[16] Through them, these structures established contact with the separatist underground in Xinjiang, which made it possible to organize practical interaction between them. In particular, according to Russian sources, in 1997, a citizen of Saudi Arabia, an Uyghur by nationality, M. Turkistoni, handed over a large sum of money to IMU leader T. Yuldashev to purchase weapons. Half of it, in accordance with the demands of Turkistoni, was transferred to the Uighur separatists in the XUAR.

In 2001, a rather significant event took place, which clearly demonstrated the process of merging the radical circles of Central Asia and Xinjiang. It was announced that instead of the ”Islamic Movement of Uzbekistan”, the ”Islamic Movement of Turkestan” (“Hezbi Islomi Turkiston”) was being formed, which, according to the leader of the so-called IMU T. Yuldashev, was supposed to unite a number of extremist groups of Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan and the People's Republic of China. And although the management of the so-called The IMU tried to give wishful thinking, the very fact of such a propaganda action testified the growing trend of ever closer interaction of radical forces from Central Asia and the Syrian Arab Republic.[17]

At the present stage, as the law enforcement agencies of the Central Asian states declare, the region continues to be the object of the activities of various radical and extremist groups, which, among other things, use Central Asia as a base for carrying out subversive actions against neighboring countries, including China. A clear confirmation of this is the activity of the Hizb ut-Tahrir al-Islami organization, which since the late 90s, has deployed its primary cells in various cities of the XUAR and began to conduct propaganda work with the calls for the establishment of a ”caliphate” in Xinjiang, which, in principle, coincided with the tasks and goals of the most radical Uighur groups.[18]

Geostrategic relations of China and Central Asian countries

The Xinjiang Uygur region of China, having important geostrategic significance, is located at the intersection of hotbeds of instability, having a common border with Afghanistan and Pakistan. In the event of an escalation of a conflict of the XUAR, it will be much more difficult for China to claim not only the place of a world power, but also the position of a leading state in Asia.

[16] Chinese Internet Information Center. http://www.china.com.cn/index.shtml (downloaded 19 April 2023)

[17] SAFRONOVA, E.: Problems of Central Asian integration in the context of the SCO. In: SAFRONOVA, E. –TIKHONOV O. (Eds.): China in world and regional politics: History and modernity: Collection of articles. 2003. pp. 69-96. (in Russian)

[18] PEYROUSE, Sebastien: In the face of separatism, the European Union, Central Asia and the Uighur question. EU-Central Asia monitoring (EUCAM). https://eucentralasia.eu/facing-the-challenges-of-separatism-the-eu-central-asia-and-the-uyghur-issue-ru/ (downloaded 11 April 2023)

It will also deal a serious blow to the economy of Xinjiang, as well as significantly complicate the alignment of the PRC–Islamic world axis, and allied relations with Pakistan and Iran, as well as the republics of Central Asia, will be jeopardized.

Of the tense zones in this region, due to their proximity to Xinjiang, the following zones can be distinguished:

1 Fergana, divided between Uzbekistan, Kyrgyzstan and Tajikistan;
2 Afghanistan;
3 Northern Pakistan;
4 Kashmir;
5 Baluchistan, divided between Afghanistan, Iran and Pakistan;
6 Tibet.[19]

All these regions and conflicts are interconnected to some extent. So, for example, Tajikistan comes into contact with Afghanistan and Ferghana, and through its Kyrgyz part and the Pamirs with Xinjiang. In most of these states, the struggle for social justice goes under the banner of Islamic fundamentalism, sometimes extremism. The Ferghana Valley is also of particular interest and concern, in view of the fact that this territory has been and continues to be a kind of trigger mechanism for Uighur movements, mainly in the west and south of Xinjiang. As a proof of this, one can recall the sad events of 1871-1881, when a major anti-Chinese uprising took place in Xinjiang, as a result of which, the Muslim state of Yakub-bek, a native of the Ferghana Valley, was formed. Although it was possible to suppress the center of Islamic resistance during that period; nevertheless, this was achieved with great difficulty.[20]

It should also be noted here that, due to the close proximity to Afghanistan, the stability of both the Fergana Valley itself and the Central Asian states in general is seriously threatened by the presence of the Islamic State group in Afghanistan. Given that Afghanistan is a kind of bridge for the transfer of terrorists to Central Asia, as well as the fact that a large number of citizens of these states have joined the IS terrorist group in Syria and Iraq, it can be assumed that the peoples of these countries, for example, in the Fergana Valley, are adjacent to the ranks of Islamic State terrorists.

In the early 60s, when the cooling of Soviet-Chinese relations came, by the decision of the Central Committee of the CPSU, several settlements were created in the eastern regions of Kazakhstan for Uighurs from the XUAR, who were then attracted by the relevant structures to conduct anti-Chinese propaganda. In the second half of the 80s, against the background of the "perestroika" that began in the Soviet Union and a certain liberalization of the internal political situation in China itself, a noticeable intensification of the activities of Uighur separatists began to be noted in

[19] Ibid.

[20] POCHEKAEV, R. Y.: Russian and British travelers about the administrative and legal transformations of Yakub-bek in East Turkestan (1860-1870s). https://cyberleninka.ru/article/n/rossiyskie-i-britanskie-puteshestvenniki-ob-administrativnyh-i-pravovyh-preobrazovaniyah-yakub-beka-v-vostochnom-turkestane-1860-1870-e/viewer (downloaded 31 May 2023)

Xinjiang, aimed at secession from the PRC and the proclamation of an independent state of East Turkestan.[21]

In parallel with the beginning of the development of interstate relations with the Central Asian states, the theses on the prohibition of the activities of Uighur separatist organizations on the territory of the Central Asian republics were constantly voiced by Chinese officials during negotiations at various levels and then included in the documents, regulating bilateral relations. Thanks to the undertaken political and diplomatic efforts, Beijing managed to enlist the official support of the Central Asian countries in the need to combat Uighur separatism.

Kazakhstan, due to the presence on the territory of the republic of the largest Uighur diaspora and various kinds of Uighur nationalist organizations, which became more active in the early 90s, has become China's main counterpart in terms of countering Uighur separatism. It is not a coincidence that in the spring of 1993, the Ministry of Foreign Affairs of the People's Republic of China, in its official protest note, accused Kazakhstan of *"avoiding taking measures to neutralize the activities of Uighur separatists in the republic, seeking to recreate the statehood of East Turkestan"*. Already in 1995, the activities of Uighur nationalist organizations in Kazakhstan were officially banned. The Prosecutor General's Office of Kazakhstan, having checked and established the illegality of the activities of the "United National Revolutionary Front of East Turkestan" and the "Organization for the Liberation of Uygurstan" and their central bodies – the newspapers "Voice of East Turkestan" and "Uygurstan", issued an order for the immediate termination of their activities. The Kazakh authorities also began to expel from the country those Chinese Uighurs who lived in the republic without official permission. In addition, at the request of China, the law enforcement agencies of Kazakhstan began to detain and deport participants of the separatist movement to China, under various pretexts, leaving the XUAR. For example, in 2000, the Kazakh special services established a safe house in Almaty, where Uighur militants from Xinjiang were hiding for some time, who, during their detention, offered armed resistance and three of them were killed.[22]

The instability of the military-political situation in Afghanistan began to have an increasingly negative impact on the Central Asian region and Xinjiang, since the late 90s of the XX century. And in this regard, the issue of Islamic radicalism and extremism, as well as international terrorism, has become particularly relevant.[23]

Similar actions have been taken in Kyrgyzstan since the mid-90s. In 1996, Uighur activists tried to register the "Party for the Liberation of East Turkestan", but the Ministry of Justice of Kyrgyzstan refused to do so, on the grounds that national legislation prohibits the legalization of parties aiming to isolate the territories of a

[21] KAMALOV, A. K. – YUSUPOV R. K.: Oral history of migration from China to Kazakhstan during the "Cultural Revolution" (1966-1976). https://docs.yandex.ru/docs/view?tm=1691705728&tld=ru&lang=ru&name=11.pdf&text=в%20восточных%20районах%20Казахстана-philosophy-vestnik.ksu.kz%2Fapart%2F2022-107-3D0 (downloaded 31 May 2023)

[22] The Uighur issue is a bargaining chip of Kazakh-Chinese relations. https://neweurasia.info/archive/book/AIBOL3.htm (downloaded 28 May 2023)

[23] WALLACE, T.: China and the Regional Counter-Terrorism Structure: An Organizational Analysis. Asian Security, 2014/3, pp. 627-645

neighboring state. In Kyrgyzstan, a ban was also imposed on the holding of mass actions by representatives of the Uighur community aimed at supporting separatists in the XUAR. As a result of the actions of the Kyrgyz authorities, the most active supporters of the idea of creating an independent state in Xinjiang from among the Uighurs living in Kyrgyzstan were forced to go underground. However, they did not curtail their activities, and with the support of their tribesmen from the XUAR, they increasingly began to use terror tactics. In particular, on May 1, 1998, a minibus was blown up in Osh, as a result of which two people were killed and 12 wounded. Later on, Kyrgyz law enforcement agencies arrested five people in this case, three of whom were Uighurs from the XUAR, who had been trained in camps in Afghanistan. In 2000, the chairman of the cultural and educational society of the Uighurs of Kyrgyzstan "Ittipak" ("Unity") was killed in Bishkek for refusing to donate money to the needs of the separatist movement in Xinjiang. In 2002, the consul of the Chinese Embassy in Kyrgyzstan and a businessman from XUAR were killed by Uighur militants. In 2003, a bus with Chinese shuttles was shot down, as a result of which 19 citizens of the PRC were killed.[24]

From the early 1990s to the mid-2010s, its militants staged a thousand terrorist attacks. Bus bombings, poisoning of water with pesticides and the largest attack of 2009 in Urumqi caused almost two hundred dead. At the same time, if at the beginning such things happened only inside the XUAR, then later, the terrorist attacks went beyond it. A jeep hit a crowd of people in Beijing near Tiananmen in 2013, an attack on the Kunming railway station (Yunnan Province) in March 2014 and on the Guangzhou railway station (Guangdong Province) a year later; all these tragedies made it evident that terrorism in the country has not been broken.

This forced the Chinese authorities to strengthen not only the security measures throughout the region, but also to redouble the ideological struggle against the "forces of three evils" – terrorism, extremism and separatism. Thus, re-education centers appeared in the XUAR.[25]

According to XUAR government spokesman Xu Guixian, such centers were mainly aimed at young people, "infected with extremist ideology". And they decided to re-educate them, based on improving the level of their education and professional training: for six months, young people were trained in the Chinese language, knowledge of the laws of the People's Republic of China and taught new professions.[26]

However, in the West, there was an instant conviction that national minorities were condemned to forced labor in such camps, which later grew into accusations of torture of men and sterilization of Muslim women.

[24] Ibid.

[25] Narynbaev A. I. – Ploskih V. M.: Uighurs of Kyrgyzstan. Dedicated to the twentieth anniversary of the Assembly of the People of Kyrgyzstan and twenty-fifth anniversary of "Ittipak" Uighurs Association. https://docs.yandex.ru/docs/view?tm=1691706276&tld=ru&lang=ru&name=2017%3Akniga_ujgury_new.pdf&text=общества%20уйгуров%20Кыргызстана%20«Иттипак»&url=https%3A%2F%2Fwww.hks.re%2Fwiki%2F_media (downloaded 09 August 2023)

[26] Izvestia learned about China's policy towards the Uyghurs. https://pledgetimes.com/izvestia-learned-about-chinas-policy-towards-the-uyghurs/ (downloaded 09 August 2023)

And since 2018, the narrative of a million interned Uighurs has begun to set the tone for all Western news stories concerning the XUAR.

Over time, accusations of Beijing's violation of human rights in Xinjiang became the reason for the introduction of personal sanctions by the United States against a number of officials of the XUAR, and restrictions on the import of goods produced in Xinjiang, mainly related to the cotton industry, which is harvested here over 5 million tons per year.[27]

The problem of the activities of Uighur separatists in Uzbekistan was practically not identified, since the situation was generally under the control of law enforcement agencies, and the local Uighur community (about 40 thousand people) tried to stand aside from any anti-Chinese actions. The Uzbek authorities, adhering to their obligations, tried to prevent the appearance of members of Uighur separatist organizations on the territory of the republic. A clear example of such activity is the case that received media coverage, with the detention by the Uzbek special services in March 2006 and the subsequent extradition to China of a native of Kashgar, who arrived from Canada, and in the mid-90s was convicted in absentia in China for participating in the Uighur separatist movement.[28]

If we talk about external factors influencing the development of separatism in the XUAR, we must not forget that ethnic conflicts, incited with active support from the outside, played their fatal role in the collapse of more than one state. Here we are talking mainly about the United States. Separatism has become one of the levers of the United States in the fight against the main geopolitical rival at the moment – China. And the object of the close attention of the United States is the Xinjiang People's Republic of China. Xinjiang has an important geostrategic position, it is not for nothing that the interests of Russia, Great Britain, Germany, Japan, China and the United States have already intersected here in turn.

But today it is the United States that has both an interest in destabilizing the PRC, and real institutional and material opportunities to confront the PRC, on the issue of the formation of an independent Xinjiang. In the future, it is likely that the Uighur issue may be used by the Americans in their game with the Central Asian states, in order to obtain concessions from China on various issues.

The United States actively sponsors the ”World Uighur Congress” through the US National Endowment for Democracy and the American Association of Uighurs, headed by Rebiya Kadeer.[29]

[27] New US sanctions are hitting China's light industry, but it is unknown whether the Uighurs are being helped. https://mediazona.ca/article/2022/07/20/ussanctions?ysclid=ll5r6zo86r710364708 (downloaded 09 June 2023)

[28] Stolpovsky O. – Paramonov V.: "The problem of Uighur separatism" in Sino-Central Asian relations: or about the need to set new tasks for the SCO. https://uighur.narod.ru/articles/shos_uyghur_problems3.html?ysclid=ll5rd2rzmq835684292 (downloaded: 09. June 2023)

[29] Rebiya Kadeer is an ethnic Uighur, businesswoman and political activist. Born in the city of Altay of China, Kadeer became a millionaire in the 1980s through her real estate holdings

It is important to note that the US National Donor Fund supported the ”color revolutions” and their attempts in Georgia, Serbia, Ukraine and Iran.

The annual amount of payments to the World Uighur Congress is $ 215 thousand. Since 2016, the National Endowment for Democracy (NED), the United States provided the separatist organization “World Uighur Congress” with the total amount of 1 million 284 thousand dollars.[30] Many high-ranking officials of the United States openly support the activities of the terrorist organization ”East Turkestan”, aggressively seeking to split the PRC. But this is only the official amount. It is obvious that in reality the funding of the Uighur movement is much greater. This is evidenced by the excessively active activity of the organization: meetings in different parts of the world with a large number of delegates, establishing organization in many countries, releasing numerous propaganda literature, videos, etc.

In 2005, the United States obtained from the PRC the extradition of the Uighur dissident R. Kadyr and created her image as the ”mother of the entire Uighur people”, advocating for the rights of the Uighur people. R. Kadeer in 2004, became a laureate of the Norwegian International Human Rights Foundation ”Rafta”, in the field of human rights protection; and in 2006j the Swedish parliamentarian A. Enochson proposed her candidacy for The Nobel Peace Prize, which caused sharp criticism from the official authorities of the People's Republic of China.

Thus, Xinjiang, being an extremely important geostrategic region of the People's Republic of China both economically and politically, is of particular importance to China. The PRC has to strictly control the problematic regions, located in direct proximity to it, so that their conflict potential does not transfer to the XUAR; and take decisive and extremely responsible steps in its foreign policy in a region, that is not directly adjacent to Xinjiang, but directly affects not only the XUAR, but also the political and economic weight of China in the world. In the event of the loss of the XUAR, it will be much more difficult for China to claim not only the place of a world power, but also the position of a leading state in Asia. The separation of the region will certainly deal a serious blow to the Chinese economy. Also, the loss of Xinjiang will significantly complicate the alignment of the axis of the PRC - the Islamic world; allied relations with Pakistan and Iran, as well as the republics of Central Asia, will be put at risk.

and ownership of a multinational conglomerate. Kadeer held various positions in China's parliament and other political institutions before being arrested in 1999 for, according to Chinese state media, sending confidential internal reference reports to her husband, who worked in the United States as a pro-Xinjiang independence broadcaster. After she fled to the United States in 2005 on compassionate release, Kadeer assumed leadership positions in overseas Uyghur organizations such as the World Uyghur Congress.

[30] Ajit Singh: Inside the US-Backed World Uyghur Congress. https://consortiumnews.com/2020/03/09/inside-the-us-backed-world-uyghur-congress/ (downloaded 29 April 2023)

The fight against separatism within the SCO

After the collapse of the Soviet Union, the Chinese authorities were forced to take a number of preventive measures in order to prevent possible support of Uighur separatist groups in the XUAR from outside. To this end, in the early 90s, China strengthened the border protection regime with the Central Asian states and tightened entry into its territory. The number of border guards and posts were increased, and on the routes of movement of “shuttles”, which with the collapse of the USSR began to visit the XUAR masse, the special services of the PRC established tight control.

China's closest cooperation on this issue has been established with Kazakhstan, Kyrgyzstan and Uzbekistan, where significant Uighur diasporas live.

Kazakhstan has become China's main partner in the fight against Uighur separatism.

The first document concerning the Uighur problem was the Joint Declaration of the Republic of Kazakhstan and the People's Republic of China (September 1995) “On the further development and deepening of friendly relations”, in which, in particular, the parties agreed in the field of political relations to oppose any kind of national separatism, not allowing any separatist activities directed against the other Side on their territory, by any organizations and forces; proceeding from mutual respect for the path of development chosen by the people of each of the Parties, taking into account the specific conditions of their country, to conduct mutual acquaintance with the policy and practice of ongoing reforms.[31]

In the ”Joint Declaration of the Republic of Kazakhstan and the People's Republic of China”, the Uighur problem within the SCO (Kazakhstan and China, 1990s – early 2000s), this issue was again touched upon: the parties, confirming that they oppose national separatism in any form, and will not allow the implementation on their territory any separatist activity directed against the other side’s territory by any organizations and forces.

In September 2004, in accordance with the law “On Combating Terrorism”, the National Security Committee of Kazakhstan submitted to the Prosecutor General's Office a list of a number of organizations, among which, along with the Kurdish People's Congress and the Islamic Movement of Uzbekistan, included an Uighur separatist group – the Islamic Party of East Turkestan, whose activities, according to the NSC, is aimed at undermining the existing constitutional order and inciting ethnic hatred. In turn, the Prosecutor General's Office of Kazakhstan sent a submission about these organizations to the Supreme Court, which recognized these international organizations as terrorist ones and banned their activities on the territory of the republic.[32]

[31] Embassy of the People's Republic of China in the Republic of Kazakhstan. https://www.fmprc.gov.cn/rus/wjdt/ (downloaded 29 April 2023)

[32] Ibid.

In 1996, at the initiative of China and with the consent of Russia, the Shanghai Five Agreement appeared, in which the Uighur issue was openly put up for discussion, on which the common position of the participants was fixed.

Since that period, Chinese special services have intensified their fight against Uighur political organizations and their leaders. In addition to the slogan of fighting crime, which is used throughout China, the concept of "fighting national separatism", as well as "fighting Islamic fundamentalism" is used against Uighurs. Since April 1996, during the first 100-day campaign against crime, the Chinese authorities arrested about 20,000 people; 115 people were shot without trial, about 100 mosques and religious schools were closed, more than half a million national printed publications were seized from the population and burned.[33]

In order to combat Uighur separatism, China has made efforts not only in the field of bilateral relations, but also on a multilateral basis. In 1996, at the initiative of China, within the framework of the Shanghai Five, the "Uighur question" was put up for discussion, on which a common position was developed and documented. Already within the framework of the Shanghai Cooperation Organization formed in 2001 by China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan; the Shanghai Convention on Combating Terrorism, Extremism and Separatism was signed, which provided for even closer cooperation between the Central Asian states, China and Russia. Subsequently, the SCO member states have repeatedly confirmed the rejection of any manifestations of national separatism and the consistency of their approaches to countering separatist activities on their territories.[34]

In accordance with the subparagraph "b" of paragraph 1 of the Shanghai Convention on Combating Terrorism, Separatism and Extremism of June 15, 2001; for the purposes of this agreement, the term "separatism" means *"any act aimed at violating the territorial integrity of a State, including the separation of a part of its territory from it, or the disintegration of the State committed by force, as well as the planning and preparation of such an act, aiding and abetting its commission, and being prosecuted, in accordance with the national legislation of the Parties."*[35]

In August 2008, at the next SCO summit in Dushanbe, the Organization's member states had to solve a difficult task for themselves – to develop a common position on the events in South Ossetia and Abkhazia, in which Russia was directly involved. The restraint in official assessments on the part of the Central Asian states and the special position of the Chinese delegation on this issue is a direct consequence of how painful the "problem of national separatism", primarily the Uighur one, is for China.

[33] People's Republic of China: At least 1000 people executed in "strike hard" campaign against crime. https://www.amnesty.org/en/documents/asa17/072/1996/en/ (downloaded 29 January 2023)

[34] The Uighur problem within the SCO. https://web.archive.org/web/20071217021251/http://www.analitika.org/?topic=cis_uygurs (downloaded 29 April 2023)

[35] Regional Anti-Terrorist Structure of Shanghai Cooperation Organization official page. https://ecrats.org/ru/documents/regulatory_legal_acts/

China has fully established control over the Xinjiang Uygur Autonomous Region, relying on its modern power. It considered necessary to establish good relations with Russia, since Russia, like the former Soviet Union, using the national liberation movement of the Uighurs, could create a situation threatening the PRC in the XUAR. Certain cooperation is also possible with Western countries, primarily with the United States. This is due to the fact that the Uighurs profess the Islamic religion, and religious elements in their national liberation movement put them next to Islamic radicalism, and thereby can spoil relations between the Uighurs and the Western world. In this regard, Russia and China share a common opinion.

It is also necessary to take into account the low standard of living in China (and especially in the Xinjiang People's Republic of China), the problem of poverty and the demographic problem coexist in China. One of the ways to relieve tension inside China is the migration of the Chinese population, the ”Chinese threat” for the Republic of Kazakhstan and the Russian Federation. In addition to the possibility of resettlement and solving the problem of lack of space, the Central Asian states represent an excellent market for Chinese goods, which is successfully exploited by the Chinese entrepreneurs. However, this kind of problem is carefully hushed up at the official level, almost all independent news agencies of the Republic of Kazakhstan speak about the indownloadedibility of data.

Throughout Xinjiang, which accounts for one-sixth of the entire territory of the People's Republic of China, as part of efforts to improve living standards in recent years, the number of railway routes has been significantly expanded, including the construction of tracks through the desert, and the 25th airport has already been opened.

The active involvement of the autonomous region in the Belt and Road project, as well as the rapid development of infrastructure for mass tourism, also gave new economic opportunities to residents. Before the Covid pandemic, about 213 million guests, both Chinese and foreign, visited the XUAR, and their number has already exceeded 100 million for the incomplete current year.[36]

As a result, the gross regional product of Xinjiang has been growing in recent years. According to the statistical office of the XUAR, in the first six months of 2023, this figure increased by 5.1%, reaching 854.2 billion yuan.[37]

One of the conditions for ensuring stability in the XUAR region is its successful economic development. Given the complexity of the situation, China has decided to develop Xinjiang not only on its own, but also with the involvement of international forces. In July 2000, during the summit of the Shanghai Five of the heads of two states (China and Kazakhstan), an agreement was reached on the involvement of the countries bordering the People's Republic of China in economic development projects of the western territories of China.[38]

[36] Du Dengwen: Our countries are aimed at expanding cooperation. https://agro.kg/ru/news/24907/?ysclid=ll6zv6kv86515028944 (downloaded 10 July 2023) Online information portal “Tien Shan”. http://russian.ts.cn (downloaded 10 July 2023)

[37] Xinjiang Uygur Autonomous Region. https://www.wikiwand.com/ru/Синьцзян-Уйгурский_автономный_район (downloaded 10 August 2023)

[38] Socio-political website about the activities of the Shanghai Cooperation Organization. http://infoshos.ru

The PRC solves a number of issues with this: the presence of foreign capital will contribute to the stabilization of the situation in the XUAR, but these capitals will be so insignificant that they will not be able to pose a threat to the influence of the center in the region.

For China, the SCO example is unprecedented in the entire political history: before joining the SCO, China did not enter into a political alliance with any state in the world. The solution of border issues with neighboring states took only seven years, and the created organization gradually began to solve other tasks. It has become possible to use the mechanisms of the organization's functioning to combat terrorism, national separatism and extremism (the so-called ”three evils”). China has begun to participate in the global anti-terrorist movement, although previously it preferred to resolve such issues unilaterally or bilaterally. The fact of joint military exercises in the adjacent territories of Kazakhstan and China, as well as joint Kyrgyz-Chinese exercises within the SCO since October 2002, is also unprecedented. Thus, China is creating a multilateral mechanism for influencing the situation in the region in the military sphere. The SCO Regional Anti-terrorist structure (SCO RATS) has been created, in which the Chinese military are present.[39]

Thus, among the priority areas of cooperation within the framework of the Shanghai Cooperation Organization, we can note the joint solution of the problem of Uighur separatism, religious extremism, terrorism; by creating conditions for the successful development of bilateral economic relations with the prospect of economic integration; increasing the authority of the organization and the participating states at the regional and international level.

Despite the declared autonomy of the region, there is no local government here. The Chinese authorities are pursuing a policy of settling Xinjiang by the Chinese. The teaching of the Uighur language and history is difficult, and the implementation of Uighur customs is hindered.

Uighur separatism is a time bomb in the Central Asian region, threatening not only China, but the entire region. The separatist movement in East Turkestan consists of a number of small, marginal Islamist groups, morally supported by Turkey. Military support may be provided by Islamists from the territory of Kashmir, occupied by Pakistan. Support for Pakistan, if any, is heavily conspiratorial.

In general, it can be stated with a sufficient degree of confidence that as a result of the active steps taken by the SCO in the Central Asian direction, a policy – agreed between the PRC and the Central Asian countries regarding the “problem of Uighur separatism” – has been adopted and is currently being implemented.

Conclusion

Finally, I want to refer to an interview: *“there are about 2,000 mosques in the United States, about 1,750 in the United Kingdom, and the number is 24,400 in China's Xinjiang, which means one mosque for every 530 Muslims.*

[39] Regional Anti-Terrorist Structure of Shanghai Cooperation Organization official page. op. cit.

There are more than twice as many mosques in Xinjiang as in the United States, Britain, Germany and France combined.”[40] The Id Kah Mosque in the center of the old city is not only the largest of them, but also the largest in all of China. On the days of important Muslim holidays, it is able to accommodate thousands of believers. The sermons here are always in Arabic, the language of the Koran.[41]

The indisputable advantage remains with the language of the whole of China and with regard to the younger generation of residents of Xinjiang. Education in schools throughout the autonomous region has been conducted in Chinese for several years. The PRC has a unified education system and textbooks, which are the same for all students. This, among other things, aims to create a sense of unity of the Chinese nation.

The PRC authorities have always placed the main stake in the fight against terrorism and separatism not only on security, but also on a significant increase in the standard of living of the local population. So, in order to knock the ground out from under the feet of propagandists of the ideas of “East Turkestan”, and significantly reduce the number of its supporters, the authorities carried out a large-scale renovation of houses at the expense of the budget, affecting about 50 thousand households. Shabby mud-brick, two-story buildings without sewerage and running water, in the historical center of the city, have turned into modern earthquake-resistant houses with all amenities, without losing the traditional Uighur specifics.

And the residents of Jiashi County near Kashgar, finally got clean water. Back in the 1990s, local residents took it from a nearby pond, and the first rare taps in houses appeared in the 2000s, but even then, the water entered them untreated, which led to a number of health problems.

In 2019, the authorities built a giant storage facility for meltwater from the mountains, built a purification station and a pipeline with a length of about 200 km, with 21 substations for water transmission. This project, which cost 1.7 billion yuan, covered the needs of 470 thousand people.[42]

In general, it can be stated with a sufficient degree of confidence that, as a result of the active steps taken by Beijing in the Central Asian direction, a policy – agreed between the PRC and the Central Asian countries regarding the “problem of Uighur separatism” – has been adopted and is currently being implemented. However, it is also obvious that it seems fundamentally wrong to consider this “problem” in such a narrow perspective, because at the present stage, both China itself and the Central Asian states found themselves in difficult socio-economic conditions.

[40] Freedom of religious belief. http://us.china-embassy.gov.cn/eng/zt_120777/dmxj/wjbxinjiang1/zongjiao/202106/t20210625_9039443.htm (downloaded 20 August 2023)

[41] Id Kah Mosque-Kashgar’ Religious Center & the Largest Mosque in Xinjiang and China. https://www.chinadiscovery.com/xinjiang/kashgar/id-kah-mosque.html (downloaded 20 August 2023)

[42] Yin, Cao: Water project slakes thirsts and raises incomes. https://www.chinadailyhk.com/article/148024#Water-project-slakes-thirsts-and-raises-incomes (downloaded 10 August 2023)

A reduction in foreign trade and a decline in industrial production, an increase in the number of unemployed are far from an incomplete list of possible negative consequences.

In the absence of a coordinated socio-economic policy within the SCO, and a clear plan to overcome the crisis by joint efforts, these consequences can undoubtedly contribute to the formation of favorable ground for the activation of radical forces, including separatist ones. Beijing and the countries of the region are well aware of the continuing severity of the ”problem of Uighur separatism”, especially since in recent years it has been ”going on” in increasingly close tandem with the problems of religious extremism, political Islam and instability in Afghanistan.

Therefore, it is obvious that if we do not look at this set of problems in a broader and strategic context, their long-term solution will be unlikely. Such a prospect does not meet the national security interests of either China, the Central Asian states, or Russia, which in the foreseeable future should predetermine their closer and more trusting interaction on problems and problematic moments in the spheres of politics, economy and security, capable of destabilizing any of the national segments of the SCO geopolitical space. Firstly, this interaction should put at the forefront the task of strengthening the analytical potential of the SCO: the creation of research mechanisms and projects constantly operating within the Organization, analytical and analytical-predictive support of decisions taken. Secondly, the tasks of stabilizing Afghanistan and ensuring the socio-economic development of the SCO, it seems, should come to the forefront of the Organization's activities. In this context, the idea of creating a large-scale SCO program – for the integrated development of the internal territories of Eurasia (Central Asia, the XUAR, Siberia, Afghanistan), which have similar geo-economic conditions and, accordingly, require similar and common approaches to solving the problems existing here –, deserves special attention. One of the first steps in this direction should be the creation of water-energy and innovation-industrial integration schemes within the SCO. It is in these conditions - the conditions of the development of regional integration, that the severity of the issue of Uighur (and ethnic separatism in general) can be significantly reduced. Thirdly, a separate task should be to establish closer coordination with the SCO observer countries, the nature of whose participation in solving the Organization's key problems will be the main indicator of their real readiness for full membership in this structure. Of course, such tasks require fundamental reform of the SCO, the development of a new strategy and ideology for the development of the Organization.

The new threats to international security require the improvement of methods of combating them and the adoption of adequate and timely measures. The 2017 Convention, signed during the Astana summit, preserves the continuity of previous acts and is aimed at improving the mechanism for countering extremism, separatism and terrorism in the SCO space, develops the provisions of the SCO Development Strategy until 2025, echoes the main themes and problems solved by the UN global counter-terrorism strategy.

The SCO does not support the use of military means to solve problems, and also follows the principle of non-interference in the internal affairs of other countries. And the issue of the split is mainly considered as an internal matter of sovereign countries.

So, within the framework of the SCO, it is difficult to reveal the map of deep and comprehensive cooperation in the fight against separatism. In addition, when powerful separatist organizations seize power through war, or violate the territorial integrity of a country through the use of force, their behavior belongs to the traditional category of security. It can be said that the SCO cannot solve such a problem of separatism with a military connotation.

Thus, the SCO has achieved legal and conceptual results in the process of solving the problem of regional separatism. The disadvantage of the interaction of all SCO member states in resolving the issue of separatism is the asymmetric requirements for separatist confrontation between members, and a lot of contradictions between reality and the principles of the SCO in the course of practice.

***Bibliography*:**

- Ajit Singh: Inside the US-Backed World Uyghur Congress. https://consortiumnews.com/2020/03/09/inside-the-us-backed-world-uyghur-congress/ (downloaded 29 April 2023)
- Brief history of the Uyghers. https://www.oocities.org/idonkari/Brief%20History%20of%20the%20Uyghers.htm (downloaded 05 May 2023)
- Chinese Internet Information Center. http://www.china.com.cn/index.shtml (downloaded 19 April 2023)
- Declaration on the Granting of Independence to Colonial Countries and Peoples (adopted by UN General Assembly Resolution 1514 (XV)), art. 2, art. 6. United Nations. http://www.un.org/ru/documents/decl_conv/declarations/colonial.shtml (downloaded 05 April 2023)
- DILLON, Michael: A Uighurs' history of China. The repression in China's Xinjiang region has deep historical roots. https://www.historytoday.com/archive/behind-times/uighurs'-history-china (downloaded 17 March 2023)
- DOSOVA, B. A.: Kazakhstan and China: Milestones of Bilateral Relations. https://rep.ksu.kz/bitstream/handle/data/7457/Dosova_Kazakhstan_2019.pdf?sequence=1&isAllowed=y (downloaded 22 March 2023)
- Du Dengwen: Our countries are aimed at expanding cooperation. https://agro.kg/ru/news/24907/?ysclid=ll6zv6kv86515028944 (downloaded 10 July 2023)
- Embassy of the People's Republic of China in the Republic of Kazakhstan. https://www.fmprc.gov.cn/rus/wjdt/ (downloaded 29 April 2023)
- Freedom of religious belief. http://us.china-embassy.gov.cn/eng/zt_120777/dmxj/wjbxinjiang1/zongjiao/202106/t20210625_9039443.htm (downloaded 20 August 2023)

- Id Kah Mosque-Kashgar' Religious Center & the Largest Mosque in Xinjiang and China. https://www.chinadiscovery.com/xinjiang/kashgar/id-kah-mosque.html (downloaded 20 August 2023)
- International Uyghur Foundation for Human Rights and Democracy (IUHRDF). East Turkistan Resume, https://www.iuhrdf.org/cn/east-turkestan-history/ (downloaded 05 May 2023)
- Izvestia learned about China's policy towards the Uyghurs. https://pledgetimes.com/izvestia-learned-about-chinas-policy-towards-the-uyghurs/ (downloaded 09 August 2023)
- KAMALOV, A. K. – YUSUPOV R. K.: Oral history of migration from China to Kazakhstan during the "Cultural Revolution" (1966-1976). https://docs.yandex.ru/docs/view?tm=1691705728&tld=ru&lang=ru&name=11.pdf&text=в%20восточных%20районах%20Казахстана-philosophy-vestnik.ksu.kz%2Fapart%2F2022-107-3D0 (downloaded 31 May 2023)
- NARYNBAEV A. I. – PLOSKIH V. M.: Uighurs of Kyrgyzstan. Dedicated to the twentieth anniversary of the Assembly of the People of Kyrgyzstan and twenty-fifth anniversary of "Ittipak" Uighurs Association. https://docs.yandex.ru/docs/view?tm=1691706276&tld=ru&lang=ru&name=2017%3Akniga_ujgury_new.pdf&text=общества%20уйгуров%20Кыргызстана%20«Иттипак»&url=https%3A%2F%2Fwww.hks.re%2Fwiki%2F_media (downloaded 09 August 2023)
- New US sanctions are hitting China's light industry, but it is unknown whether the Uighurs are being helped. https://mediazona.ca/article/2022/07/20/ussanctions?ysclid=ll5r6zo86r710364708 (downloaded 09 June 2023)
- Online information portal "Tien Shan". http://russian.ts.cn (downloaded 10 July 2023)
- People's Republic of China: At least 1000 people executed in "strike hard" campaign against crime. https://www.amnesty.org/en/documents/asa17/072/1996/en/ (downloaded 29 January 2023)
- PEYROUSE, Sebastien: In the face of separatism, the European Union, Central Asia and the Uighur question. EU-Central Asia monitoring (EUCAM). https://eucentralasia.eu/facing-the-challenges-of-separatism-the-eu-central-asia-and-the-uyghur-issue-ru/ (downloaded 11 April 2023)
- POCHEKAEV, R. Y.: Russian and British travelers about the administrative and legal transformations of Yakub-bek in East Turkestan (1860-1870s). https://cyberleninka.ru/article/n/rossiyskie-i-britanskie-puteshestvenniki-ob-administrativnyh-i-pravovyh-preobrazovaniyah-yakub-beka-v-vostochnom-turkestane-1860-1870-e/viewer (downloaded 31 May 2023)
- Regional Anti-Terrorist Structure of Shanghai Cooperation Organization official page. https://ecrats.org/ru/documents/regulatory_legal_acts/

- SAFRONOVA, E.: Problems of Central Asian integration in the context of the SCO. In: SAFRONOVA, E. –TIKHONOV O. (Eds.): China in world and regional politics: History and modernity: Collection of articles. 2003. pp. 69-96. (in Russian)
- Shanghai Convention on Combating Terrorism, Separatism and Extremism. Official network resources of the President of Russia, http://kremlin.ru/supplement/3405 (downloaded 05 April 2023)
- Socio-political website about the activities of the Shanghai Cooperation Organization. http://infoshos.ru
- STOLPOVSKY O. – PARAMONOV V.: ”The problem of Uighur separatism” in Sino-Central Asian relations: or about the need to set new tasks for the SCO. https://uighur.narod.ru/articles/shos_uyghur_problems3.html?ysclid=ll5rd2rzmq835684292 (downloaded: 09. June 2023)
- The official page of the SCO. http://chn.sectsco.org
- The Uighur issue is a bargaining chip of Kazakh-Chinese relations. https://neweurasia.info/archive/book/AIBOL3.htm (downloaded 28 May 2023)
- The Uighur problem within the SCO. https://web.archive.org/web/20071217021251/http://www.analitika.org/?topic=cis_uygurs (downloaded 29 April 2023)
- Uighuristan (East Turkestan). http://karty.narod.ru/maps/uygh/uygh.html (downloaded 17 March 2023)
- WALLACE, T.: China and the Regional Counter-Terrorism Structure: An Organizational Analysis. Asian Security, 2014/3, pp. 627-645
- Xinjiang Uygur Autonomous Region. https://www.wikiwand.com/ru/Синьцзян-Уйгурский_автономный_район (downloaded 10 August 2023)
- YIN, Cao: Water project slakes thirsts and raises incomes. https://www.chinadailyhk.com/article/148024#Water-project-slakes-thirsts-and-raises-incomes (downloaded 10 August 2023)

TIBOR SZILVÁGYI PHD

NEW OPPORTUNITIES AND OLD CHALLENGES OF THE EUROPEAN DEFENCE INDUSTRY

Abstract

Europe's security situation is mainly determined by external factors, causing unpredictable security threats. The European defence industry plays an indispensable role in distracting and solving many emerging security challenges. Despite the plenty endeavours, the continental defence industry is still a fragmented one; however, it has got a new impetus for reconsidering and joining its diverse activities, in order to diminish the impact of the Russian invasion of Ukraine. There are many lessons to be learned from this military conflict for the defence industry, enjoying potential opportunities and facing old challenges that need to be overcome by new approaches to the original problems. The EU and NATO are interested in a much more unified and cooperative European defence industry, which can respond with proper tools and methods, to the current and future security challenges. The comprehensive SWOT analysis on the European defence industry helps to understand the current position of this special sector and its possible perspective. As a conclusion, this article explains why the European defence industry might play a balancing and regulating role in the society and the economy of a country.

***Keywords*:** security situation, threat and challenge, European defence system and industry, Russian-Ukrainian armed conflict, UAS, artificial intelligence, internet of things, asymmetric warfare, military technology, EU, NATO, SWOT analysis

Introduction

The security situation in Europe is changing continuously and unpredictably. In the last 15 years, citizens of the European Union (EU) experienced a challenging period of time that was characterised firstly by the global financial crisis, then by the illegal migration flow and the COVID-19 pandemic, as well as by the recent the Russian–Ukrainian armed conflict and its consequences. All of them have made it necessary to take new security, political or economic measures by the governments of EU countries, in order to avoid much more serious political, economic and social damages.

It is indisputable that military clashes in Southern and Eastern Ukraine have resulted in a changing European defence policy and new strategic concepts in several European countries. The EU is committed to protect its common interests and democratic values, which have been achieved for decades. One of them is the sovereignty and territorial integrity of states. which is an internationally accepted basic value.[1]

[1] Repertory of Practice of United Nations Organs – Charter of the United Nations, Chapter I – Purposes and Principles, Article 2(1)–(5); https://legal.un.org/repertory/art2.shtml (downloaded 10 October 2023)

Regarding this principle, the EU leadership has decided to support Ukrainian homeland defence activities with political, financial and military tools. Since the Ukrainian demand for old and new military technology has increased, in order to fight successfully against Russian regular and paramilitary troops, the American and also the European defence companies have enhanced their marketing, production, sales and aid activities towards the Ukrainian state and its defence forces. Until 31st of July 2023 Ukraine's supporters had provided approximately 100 billion USD in military assistance to Ukraine, since Russia's invasion in February 2022. This includes heavy conventional weapons such as tanks, armoured vehicles, artillery systems and unmanned combat aerial vehicles, in addition to small arms and light weapons.[2] Additionally, some of the East-Central European (former socialist) EU countries have also provided their old and obsolete Soviet military technology for Ukraine. Tanks from Poland, air defence system from Slovakia and armoured trucks from Slovenia are meant to boost Ukraine's resistance and keep the armed conflict far from the EU member states. The transactions, many of which are unpublicized, have added a new dynamic to an already volatile military procurement activity in Europe, which clashes with the bloc's plans for developing collectively the weapons.[3] Western political and defence interests seem to have met and they are moving forward together until their energy runs out.

The Ukrainian battlefield has become a test venue for the Western military technology that faces plenty of opportunities and threats in armed clashes. In this special military operation, as it is the case with the Russian–Ukrainian conflict, there are many irregular activities and unexpected consequences, where even an up-to-date military technology can fail or be misused. This can especially happen when operators are not trained properly. That is the reason why this terrain is so important and dangerous at the same time for the newly developed precision weapons. This controversial situation has advantages and disadvantages for the European defence industry, which is lagging behind the American military technological qualitative capabilities and the Chinese or Russian quantitative abilities.

Besides the ascent of the European defence industry, there are many old challenges that have to be faced, in the short and long term as well. The defence industry is an unambiguously raw material demanding sector, where especially strategic and critical raw materials are needed, which are available (downloadedible) mainly in China and Russia at the moment. The defence industry in the EU is almost 100% reliant on imports for most of its heavy and light rare earth elements (REE) and platinum-group metals (PGMs) needs. The EU's dependence on foreign supplies continues to represent a high-security risk for the EU countries' economy and national defence that can deteriorate or threaten their resilience.

[2] Security Council Report. Ukraine: Meeting under the "Threats to International Peace and Security" Agenda Item. https://www.securitycouncilreport.org/whatsinblue/2023/10/ukraine-meeting-under-the-threats-to-international-peace-and-security-agenda-item-4.php (downloaded 12 October 2023)

[3] Ukraine weapon switcheroos are flushing Soviet arms out of Europe. https://www.defensenews.com/global/europe/2022/04/28/ukraine-weapon-switcheroos-are-flushing-soviet-arms-out-of-europe/ (downloaded 06 October 2023)

This situation is expected to remain a worrying factor in the 2020s.[4] This creates a serious dependency of the EU and European NATO-countries on non-friendly states, which is a serious disadvantage for the European defence industry.

The emerging new security challenges always boost military production activity, but usually it lasts only for a short period of time. If the domestic demands decrease, owners (mainly states) start to give up parts of the defence production or industry. However, this is a huge mistake and misjudgement. The defence industry should be kept up not only in economic rise, but during a recession time as well. It should work differently from other economic sectors, not only according to the principle of supply and demand of the military technology. This should be a long-term enterprise, with conservative features and stubborn players, who need commitment and enthusiasm for properly functioning. Especially the states are obliged to run the defence industry and control its stakeholders, since this sector is the most controversial, indispensable and neglected, sensitive and harsh, expensive and fragile, well profitable and attractive for corruption.

Changing security policy situation in Europe

In political and economic sense, Europe is mainly characterised by the European Union (EU) that has about 448.4 million inhabitants and covers over 4 million square kilometres.[5] The EU is a relatively small, but significant player in the international political and economic scene, in comparison to the United States of America (USA), China and Russia. However, the EU would like to take part actively in the global political, economic, social, technological, environmental and legal (PESTEL) processes, in order to commit to a more liveable Globe having more than eight billion inhabitants. Besides the global challenges, the EU should face its own security problems, which are not unambiguously solvable for the 27 member states. The EU would like to act successfully, under its Common Security and Defence Policy (CSDP), in several civilian and military missions in Europe (EUFOR ALTHEA in Bosnia and Herzegovina, EULEX KOSOVO in Kosovo, EUAM Ukraine, EUMAM Ukraine, EUPM Moldova) and on the international stage (EUAM Iraq, EUAM RCA in the Central African Republic, EUBAM Libya, EUBAM Rafah, EUCAP Sahel Mali, EUCAP Sahel Niger, EUCAP Somalia, EUM Armenia, EUMM Georgia, EUMPM Niger, EUNAVFOR MED IRINI, EUNAVFOR Somalia, EUPOL COPPS/Palestinian Territories, EU RACC Sahel, EUTM Mali, EUTM Mozambique, EUTM RCA in the Central African Republic, EUTM Somalia)[6] as well, but it is not easy to be always determined and unified in defending its global and continental interests.

[4] NITSCHKE, Stefan: Dependence of Strategic and Critical Raw Materials May Soon Replace Today's Dependence on Oil, Says the European Commission – What Lessons are to be Learned? Military Technology, 2023/2, pp. 16-19, ISSN 0722-3226

[5] Facts and figures on life in the European Union; https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/life-eu_en (downloaded 06 September 2023)

[6] European Union – External Action, Missions and Operations – Working for stable world and a safer Europe, Ongoing missions and operations; https://www.eeas.europa.eu/eeas/missions-and-operations_en#9620 (downloaded 10 September 2023)

The biggest difficulty is the different approach of the member states towards external security challenges. This is the reason why the EU had not and has not been able to represent a common standpoint concerning the financial crisis in 2008–2009, the peak of the illegal migration in 2015, the COVID-19 in 2020–2021 and the Russian–Ukrainian armed conflict in Southern and Eastern Ukraine from February 2022.

Even though the EU is coping with its own difficulties, this entity remains attractive for non-EU countries' companies and citizens as well. The reason for this is the relatively high economic and social development standard in its member states that provides reliable economic environment and job opportunities for their natives and immigrants. It is not a surprise that nowadays the EU is facing a shortage of workforce in several business and commercial segments, due to the growing demand for production, services and consumption. This situation can be sustained only with the support of a smart security and defence policy, aimed at protecting peace. Stability needs modern military technology that is produced by defence industry companies. The current European security situation (armed conflict in certain parts of Ukraine and its consequences) is a good basis for the ascent of the defence industry production in Europe that has been valued less than the American, the Chinese or the Russian one.

The security architecture of a European state can be determined with a good predictable security chain. Usually, the geopolitical situation of a country determines its security conditions, which derive from many security challenges that demand special defence forces and capabilities, which usually need a good-functioning national defence industry as well. A relatively rich country has plenty of values to lose, so it should have its own capability for self-defence. Inside of an alliance like the EU or NATO, member states can expect a protective umbrella from the partner's but neutral countries can rely only on themselves. The defence industry's purpose is twofold. It deters the enemy and protects its own physical and intangible values. Usually the defence capability (armed forces and defence industry together) is controversial, since military activities and products cost a huge amount of money; however, it probably will never be used in a real war. Reserving reliable defence capabilities is moreover a great advantage, because it means that there is a certain level of resilience capability.

Where is the place of the European defence industry?

The European defence industry contains the EU's and non-EU-states' defence industry. In a wider extent, it contains even the Russian defence industry or a part of it as well, but in an ideological context, at the moment it is not the case. Great EU-members have famous defence industry companies that are able to compete with the American, the Chinese and the Russian ones. However, their fame and capacity are not enough to build an impressive European defence industry conglomerate.

Every year Defence News, a global website and magazine, publishes the top 100 defence industry companies, from all over the world.[7]

[7] Top 100 Defense Companies; https://people.defensenews.com/top-100/ (downloaded 10 September 2023)

In this list for 2023, European companies (altogether 30 from 100) are unfortunately a bit underrepresented. Companies from France, the United Kingdom, Germany and Turkey are dominating the European list, but Leonardo and Fincantieri S.p.A. from Italy have more annual defence revenue as four German and four Turkish companies altogether.

No.	This Year's Rank	Company	Country	Defence Revenue (in million USD)
1.	7	BAE Systems	United Kingdom	25,238.85
2.	11	Leonardo	Italy	12,866.12
3.	12	Airbus	Netherlands/France	12,022.44
4.	14	Thales	France	9,644.49
5.	19	Rheinmetall AG	Germany	5,060.70
6.	20	Dassault Aviation	France	5,034.01
7.	24	Naval Group	France	4,586.45
8.	28	Safran	France	4,214.33
9.	33	Saab AB	Sweden	3,707.69
10.	36	KNDS	Netherlands	3,342.00
11.	47	Aselsan A.S.	Turkey	2,250.39
12.	48	Fincantieri S.p.A.	Italy	1,998.43
13.	49	QinetiQ Plc	United Kingdom	1,905.56
14.	50	Serco	United Kingdom	1,857.57
15.	51	Hensoldt AG	Germany	1,798.46
16.	58	Turkish Aerospace Industries	Turkey	1,483.70
17.	59	Melrose Industries	United Kingdom	1,438.32
18.	61	Kongsberg Gruppen	Norway	1,387.84
19.	62	Polish Armaments Group	Poland	1,302.60
20.	65	Ukroboronprom	Ukraine	1,284.65
21.	66	Eaton	Ireland	1,245.12
22.	69	Navantia	Spain	1,112.48
23.	80	Roketsan	Turkey	873.35
24.	83	Diehl Group	Germany	780.75
25.	85	Indra	Spain	697.47
26.	90	Nammo	Norway	598.96
27.	91	Patria	Finland	594.63
28.	93	MTU Aero Engines AG	Germany	522.58
29.	95	SES S.A.	Luxembourg	512.04
30.	100	Askeri Fabrika ve Tersane Isletme A.S.	Turkey	177.94

Figure 1: European defence companies from Top 100 for 2023[8]

[8] Ibid.

The European defence industry is not a unified and compact system. It is a simple composition individual national or company level defence industry components. Some synergies are under development year by year, but they are not sufficient, due to the different approaches of European countries to the security challenges and their solutions. The USA, China and Russia have a much more homogenous and compact defence industry, thanks to their common values and interests. Europe and its countries are diverse, therefore the ideas and the imaginations about the European defence system and industry are also different. However, it is clear that a more unified and coherent European defence industry is needed as soon as possible, in order to preserve and enhance the competitiveness at international level. EU and NATO member states and their defence companies should focus more and more on cooperation with each other and create a high level compatibility and interoperability. Probably this way might help Europe to cope with external security challenges and threats.

The Defence Industry Europe (DIE) professional internet website deals with defence industry questions and news in Europe and worldwide. It reports about modernization of European armed forces, defence industry, new defence technologies, development of the defence business, companies operating in that industry and political events with relevance to the defence sector. Its mission is to offer to the defence professionals, the decision-makers, the politicians, the journalists and the general public reliable information on the European defence industry. According to the statement of the DIE, a strong, integrated, innovative and efficient European defence industry could contribute to a more effective cooperation between Europe and all partner countries in all over the world. It usually promotes the initiatives undertaken by individual European countries, the EU and the other international organisations to pursue common armament programmes and work together on future technologies, ensuring full interoperability and compatibility of the equipment and weapons, used by the armed forces of the European countries.[9]

The European defence industry is partially characterised by the EU's and NATO's initiatives and programmes, so it is relevant to mention some military procurement and production supporting initiatives of these multinational organisations.

The EU's European Defence Agency (EDA) was established under a Joint Action of the Council of Ministers on 12 July 2004, in order "to support the Member States and the Council in their effort to improve European defence capabilities, in the field of crisis management and to sustain the European Security and Defence Policy, as it stands now and develops in the future". EDA currently has three main missions:

- supporting the development of defence capabilities and military cooperation among the EU member states;
- stimulating defence Research and Technology (R&T) and strengthening the European defence industry;
- acting as a military interface to EU policies.[10]

[9] Defence Industry Europe; https://defence-industry.eu/about-us/ (downloaded 06 October 2023)

[10] European Defence Agency – Who we are; https://eda.europa.eu/who-we-are (downloaded 12 October 2023)

EDA supports its 27 member states in improving their defence capabilities through European cooperation and with engaging in collaborative defence projects. The Agency has become a kind of hub for a promising European defence teamwork, uploaded with expertise and networks and for allowing an easy downloaded to the whole spectrum of defence capabilities. Member states are able to decide on a case-by-case basis whether to participate in certain projects or not. Their choice depends on their needs and interests. EDA plays an important support and implementation role in all the EU defence initiatives. Special tools are designed to raise the EU's ambition level, through the Capability Development Plan (CDP), Coordinated Annual Review on Defence (CARD), Permanent Structured Cooperation (PESCO) and European Defence Fund (EDF).[11]

PESCO is one of the key EU defence initiatives. It provides a framework for EU member states to develop defence capabilities, coordinate investments, enhance operational readiness, interoperability and resilience of their armed forces, and to collaborate in projects. The 11 new PESCO projects adopted in May 2023 aim to help in increasing the coherence of the European capability landscape and to deliver operational benefits for European armed forces. Projects range from the development of new military capabilities to the identification of future needs in areas such as future military rotorcrafts, air-launched missiles, communication infrastructure and joint training for defence airlift.

The 11 new projects are the followings:

- European Defence Airlift – Training Academy (EDA–TA);
- Integrated Unmanned Ground Systems 2 (iUGS 2);
- Counter Battery Sensors (CoBaS);
- Anti-Torpedo Torpedo (ATT);
- Critical Seabed Infrastructure Protection (CSIP);
- Future Short-Range Air to Air Missile (FSRM);
- Next Generation Medium Helicopter (NGMH);
- Integrated Multi-Layer Air and Missile Defence System (IMLAMD);
- Arctic Command & Control Effector and Sensor System (DOWNLOADED);
- Robust Communication Infrastructure and Networks (ROCOMIN);
- ROLE 2F.

Three of them are critical defence capabilities. The CoBaS project aims at developing a common concept for a next generation counter-battery capability for EU armed forces, and facilitating future common procurement for counter-artillery. The CSIP project would like to increase the EU's operational efficiency in the protection of critical maritime infrastructure by making the best use of the current, and the developing future underwater assets. The Next Generation Medium Helicopter (NGMH) project has an aim to create a dedicated forum that will address operational needs, both on the upgrade of existing fleets and on the European Next Generation Rotorcraft.

[11] European Defence Agency – What we do; https://eda.europa.eu/what-we-do (downloaded 12 October 2023)

Currently 26 states are participating in PESCO, the EU 27 members, with the exemption of Malta. There are 22 common members in the EU and NATO, and all of them are also taking part in PESCO. Now 68 PESCO projects are in progress, among them 21 have already reached the execution phase and it can be expected that 26 more will achieve this stage until 2025.[12]

Besides the EU, NATO is also interested in defence development. In this case, European NATO member states are able to benefit from a huge defence capability and capacity led by the USA. NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) programme provides deep tech[13] and dual-use innovators, with the downloaded to NATO resources including grant funding, acceleration services, and pathways to adapt their solutions for defence and security needs. It tries to unite the best innovators across the Alliance to ensure the protection of one billion citizens in member states. DIANA's aim is to bring start-ups, together with operational end users, scientists and system integrators, in order to advance compelling deep tech with dual-use solutions for the Alliance.

Companies joined DIANA accelerator programme gain downloaded to:

- grants to support technology development and demonstration;
- 10+ accelerators across the Alliance, with more planned over the coming years;
- 90+ test centres (with more planned) across the Alliance where entrepreneurs can de-risk, demonstrate and validate their proposed dual-use technological solutions;
- mentoring from scientists, engineers, industry partners, end users, and government procurement experts;
- an investor network for trusted third-party funding;
- opportunities to demonstrate technology in operational environments;
- pathways to market within the NATO enterprise and 31 Allied markets.

[12] 11 new PESCO projects focus on critical defence capabilities and interoperability, 23 May 2023; https://eda.europa.eu/news-and-events/news/2023/05/23/11-new-pesco-projects-to-focus-on-critical-defence-capabilities-and-interoperability (downloaded 12 October 2023)
EU defence cooperation: Council welcomes Denmark into PESCO and launches the 5th wave of new PESCO projects, 23 May 2023; https://www.consilium.europa.eu/en/press/press-releases/2023/05/23/eu-defence-cooperation-council-welcomes-denmark-into-pesco-and-launches-the-5th-wave-of-new-pesco-projects/#new_tab (downloaded 12 October 2023)

[13] According to the European Institute of Innovation and Technology (EIT), Europe's largest innovation ecosystem, deep tech is a key to tackling the most pressing global challenges such as climate change, sustainable energy or health. EIT mentions fifteen deep tech areas that may change as technologies and markets alter over time: Advanced Computing / Quantum Computing; Advanced Manufacturing; Advanced Materials; Aerospace, Automotive and Remote Sensing; Artificial Intelligence and Machine Learning, including Big Data; Biotechnology and Life Sciences; Communications and Networks, including 5G; Cybersecurity and Data Protection; Electronics and Photonics; Internet of Things, W3C, Semantic Web; Robotics; Semiconductors (microchips); Sustainable Energy and Clean Technologies; Virtual Reality, Augmented Reality, Metaverse; Web 3.0, including Blockchain, Distributed Ledgers, NFTs. See: What is deep tech? https://www.eitdeeptechtalent.eu/the-initiative/what-is-deep-tech/ (downloaded 12 October 2023)

Allied nations are working together with the private sector to adopt and integrate new technologies and create standards. Among other technology areas, DIANA is focusing on big data, artificial intelligence (AI), autonomy, quantum, biotechnologies and human enhancement, energy and propulsion, novel materials and advanced manufacturing, hypersonic and space solutions, especially where they are dual-use (civilian and defence) and deep tech in nature, and where they can be used to solve challenging defence and security problems.[14]

Lessons learned for the European defence industry from the Russian–Ukrainian armed conflict

The Russian–Ukrainian armed conflict is neither a conventional nor a modern form of warfare. It is a mixture that should not be an example, since it is not driven by rationale in many aspects. There are huge casualties and damages, but the participants are not coming closer to their goals. Even though the conflict is irrational, there are many lessons that can be drawn from the political, military and economic activities, which usually go hand in hand with each other. This work does not aim to evaluate and assess the military activities of the Russian–Ukrainian conflict, but it would like to highlight some aspects that the European defence industry should take into consideration, in order to avoid surprisingly emerging security challenges or to use good business opportunities evolving from security needs.

The European defence system was nearly dormant when the Russian–Ukrainian conflict began in 2014 and in 2022 as well. Only some European countries were aware of the importance of building their own defence production capability. It is an axiom that peace and security are the greatest values for a person, a country, an alliance or for the whole world. These values should be treated, protected and be restored in case of an uncertainty or crises. In this case, defence industry plays an inevitable role in deterring the potential enemy or defending the own properties. An indigenous defence industry might decrease the vulnerability and might increase the resilience of a country. States that do not have their own defence industry capabilities should procure foreign military technology that generally is not available in the requested quality and quantity, during crisis situations. This is the reason why prevention and timely preparation for several security challenges are the most important aspects of a smart and prudent defence policy.

Especially a state located along the border of an alliance or between civilisations should take into consideration that security is a fragile value, which is usually not secured by others, but mainly with the country’s own armed or police forces and security services. Neutral or non-allied states are in a more difficult situation, because these countries usually are not supported by others. Probably this is the reason why these countries regularly have to keep up a relatively up-to-date and independent defence industry and a continuous military technology production. This version is an expensive one, but much better than waiting for the support of others.

[14] NATO – Defence Innovation Accelerator for the North Atlantic (DIANA). https://www.diana.nato.int/ (downloaded 12 October 2023)

The European defence system has been generally unprepared for the Russian–Ukrainian armed conflict. The EU has decided relatively fast that it imposes sanctions on Russia and supports Ukrainian self-defence. After the COVID-19 – which has caused enormous social and economic damages – at first sight, this was a counterproductive decision. The EU has been partially dependent on the Russian energy resources and the country was one of the main trade partners of the EU before February 2022. After Russia's invasion of Ukraine, the EU has imposed a number of import and export restrictions on several products. The value of exports to Russia fell by 61% between February 2022 and June 2023, while imports from Russia fell by 84% in this period.[15] The conflict has revealed that EU countries do not have enough obsolete military technology and equipment for supporting Ukraine and that the former Soviet (Russian) military technology – used and still in service in the EU's former socialist countries – are in a bad condition, because there is no OEM (original equipment manufacturer) support from Russia. Interestingly, this phenomenon also poses an opportunity, since these countries now have got the chance to get rid of their obsolete Soviet technology forever. Serviceable, outdated Russian military technology and their spare parts have been welcomed in Ukraine, so it is the cheapest way to remove them from the own military inventory.

Electronic warfare (EW) is gaining more and more its raison d'être. It means that nowadays, a military operation can be successful only with strong EW. Electronic devices are faster than soldiers and these are much more efficient and more punctual than human sensory systems. This is the reason why an up-to-date EW system is a huge advantage against a general one. EW might reduce casualties and can spare civilians' lives, when it is applied smartly. Joint operations might be controlled only with electronic devices and solutions, which are supplemented more and more with artificial intelligence (AI) and internet of things (IoT). EW is a decisive factor in a military operation, so its development is a crucial question in the planning of the armed forces and their activities. The conflict in Ukraine has so-far proved the importance of highly mobile tactical medium and long-range radar systems to guide short and medium range air-defence units, and protecting major cities from the Russian air, cruise missile and kamikaze drone strikes. Less mobile surveillance radars are much more vulnerable to the enemy's anti-radiation missiles.[16] The European defence industry should take into account the importance of an independent EW device production capability.

Heavy losses in Ukraine are partially the consequence of the lack of air superiority by either Russia or Ukraine. This results in slow, protracted and bloody ground operations. The USA and NATO consider air dominance as a precondition for ground manoeuvres, in order to conduct the mission without a risk of a devastating adversary air attack. Air Power should be developed and modernised, since it remains the cornerstone of the US' and NATO's strength.

[15] Eurostat – EU Trade with Russia – latest developments; https://ec.europa.eu/eurostat/statistics-explained/index.php?title=EU_trade_with_Russia_-_latest_developments&stable=0&redirect=no#Latest_developments (downloaded 14 October 2023)

[16] TAGHVAEE, Babak: Long-range Land-based Early Warning Radars – Lessons from Ukraine. Developments for the Future. Military Technology, 2023/3, pp 28-32, ISSN 0722-3226

The US Next Generation Air Dominance (NGAD) and the European Future Combat Air System (SCAF/FCAS) and Global Combat Air Programme (GCAP) developments aim to maintain an effective Air Power that will not fail in an emergency situation. New fighters will be produced in small numbers while autonomous aircraft will be able to create a sufficient mass to counter the overwhelming quantitative superiority of the adversary, like China or Russia.[17] The European defence industry should keep an eye on the development of methods and technology for securing air superiority in the EU and NATO member countries.

Nowadays Unmanned Aerial Vehicles (UAVs) play an inevitable role in current armed conflicts, as it has been the case in the Russian–Ukrainian military clashes. Modern warfare is not imaginable without Unmanned Aerial Systems (UAS). These remotely piloted aircraft systems (RPAS) support the land forces with information from the air or kill and destroy the enemy unpredictably. These UAVs are less detectable than piloted aircraft, because they are smaller in size and have a scarcely visible radar cross section (RCS). This makes them capable to conduct stealth missions against the enemy as well. The Russian–Ukrainian armed conflict is probably the first occasion when flying (loitering) munitions (kamikaze drones) have been used massively (thousands of them) in direct battles. Combat UAVs equipped with weapons, rockets or missiles have been applied several times by the Allied Forces and NATO in the Middle East, Central Asia and in the Western Balkans, but kamikaze drones have not been used there in such large amount. I am not certain that these flying munitions are operated wisely at the moment, but they are undoubtedly effective in some cases. I believe that in the future, kamikaze drones should be integrated much more into sophisticated weapon systems, and this process is visible by the endeavours of many Western military technology manufacturers who plan to deploy UAVs together with tanks and armoured personnel carriers, in order to increase the level of self-defence capability. Rheinmetall and UVision are promoting different armoured vehicles armed with a couple of launchers for Hero munitions, for example Boxer, KF-41 Lynx and KF-51 Panther.[18] So these kamikaze UAVs will be important and useful parts of the striking and defending forces, in future combats and military operations.

It is also an axiom that a weapon does not work without ammunition. Therefore, munition production is a crucial precondition for a successful use of weapon systems. A shortage of ammunition might cause serious difficulties during a military mission or action. This might be even the weakest point in the supply chain that can also decide about the result of the military activities. A defence system without a proper munition production is not effective and it is usually vulnerable. Munition is needed in peace time as well when troops should be trained and exercised with special shooting tasks. In some cases, simulators might substitute life firing exercises, but simulation is not an equal solution. An armed conflict needs a huge amount of ammunition. This is the reason why EU in March 2023 decided to supply Ukraine with vital ammunition for the short, medium and longer term and replenish national stockpiles.

[17] BARONE, Marco Giulio: Foreword – Preparing for Future Air Warfare. Military Technology, Special Supplement 2023, The Future of Air Power; 2023/4, pp. 4-5, ISSN 0722-3226

[18] ANNATI, Massimo: Doctrinal Developments and Market Perspective in Loitering Munitions. Military Technology, 2023/5, pp. 62-65, ISSN 0722-3226

The first track aims to dedicate 1 billion EUR to countries able to either donate ammo immediately from their own stocks or pending orders.[19] The volume depends on the production line, which in turn, depends on the raw materials. The lesson learned is that an own and efficient ammunition production is a must if you want to avoid empty cartridge clips and magazines in need, in an emergency situation.

Logistics is very important not only in our civilian life, but for the military operations as well. The military supply system is traditionally older than any current logistical task. In the ancient times military troops were the first groups that were supplied with food, animals (for example horses), weapons and other equipment. Later on, they needed ammunition, accommodation and transport vehicles as well. Warfare is modernising in every decade and logistics remain an important factor. You might have enough weapons and ammunition, but these are to be transported to the scene in a fast and secure way. A broken supply chain might easily cause difficulties for the troops and the military operation, as it happened with Russian troops in Ukraine, especially in the first half of 2022.[20]

A military conflict involves not only the armed forces but the heartland as well. The latter one is responsible for the supplies: energy, human resources, vehicles, military technology, weapons, ammunition, transportation and so on. In this case critical infrastructural systems or essential subsystems play an enormously important role, in order to secure the supply chain for the population and soldiers. Therefore, the protection of critical infrastructure is a vital task in the sense of a stable hinterland of a military operation.[21] The enemy is often conducting proxy or asymmetric warfare that endangers our troops and our critical infrastructure (power plants, water and electric systems, defence and food industry or transportation routes) as well.

In the current conflict, old and new military technology is used simultaneously. Moreover, civilian tools or so called improvised devices are usually applied even for military purposes. Due to this, asymmetric warfare might cause enormous damages with relatively cheap and easily available tools. New ideas might give tips for surprise-causing military solutions or methods. Precision guided missiles and advanced weapon systems often are failing against a simply armed and individually acting enemy.

The above mentioned modern military technology is worth nothing without well-trained and good-equipped personnel (operators) and proper military employment or proceeding rules. Motivation and will are also important factors concerning the success of the military operation. Sometimes psychological warfare might influence the behaviour of the enemy in favour of our aims.

[19] TANI, Caterina: Boosting Ammunition Supplies – A Big Step for Ukraine and a Bigger One for Europe? Military Technology, 2023/3, pp. 10-15, ISSN 0722-3226

[20] Russian Logistics and Sustainment Failures in the Ukraine Conflict. Status as of January 1, 2023, https://www.rand.org/pubs/research_reports/RRA2033-1.html (downloaded 14 October 2023)

[21] Ukraine to build a critical infrastructure protection system in line with the world's best practices and EU law. https://cip.gov.ua/en/news/ukrayina-pochinaye-buduvati-sistemu-zakhistu-kritichnoyi-infrastrukturi-vidpovidno-do-naikrashikh-svitovikh-praktik-ta-chinnikh-vimog-yevropeiskogo-zakonodavstva (downloaded 14 October 2023)

Warfare is a complex method that should be treated as a whole system in which all the elements should be in harmony with each other. The indigenous defence industry should take into account dual-use production and products that are useful in peace and wartime as well. Civilian UAS modified for military use is probably one of the best examples how a commercial product can serve military operations.[22] The military conflict in Ukraine has shown that many civilian products might be used for military purposes as well. But to tell the truth, it should have happened only, since Ukrainian defence industry has not been prepared for such a security challenge, and it has not been able to support self-defence activities with proper weapon and equipment production either.

In order to avoid a plenty of risks, an up-to-date defence industry should prepare for the above mentioned challenges to secure survivability and resilience of the own headquarters, forces and troops. The European defence industry should learn the necessary lessons, but it should not take exaggerated actions either. The own defence system (armed forces and military technology) should prepare mainly against a potential enemy's military ambitions and capabilities, since it is not able to prepare for all possible security challenges. There should be theoretical priorities, feasible defence aims and sustainable military system, in order to avoid underestimated or exaggerated reactions.

Opportunities for the European defence industry

The European defence industry has a chance to redefine itself and start a new era with a smarter planning, manufacturing and distributing policy. In my opinion, the key word is cooperation. The security of Europe – and especially of the EU – is based on collaboration. Cooperative security means a common way of thinking and a joint activity that is easier to realise if there are common values, which should be protected.

There are many initiatives in the EU and in NATO that support the cooperation among national defence systems or companies. Instead of national, only multinational projects are supported by the EDA and DIANA programs. Current inventions are knowledge-intensive, and there is no one company that possesses all the necessary learnings and experiences. One country is not able to cope with all the security challenges; thus, in an alliance the capabilities and responsibilities are shared smartly among the member states. It has rationale since it helps to avoid obsolete technical parallelisms and exaggerated financial expenses.

Purpose-designed solutions might help avoid redundancy. Military technology should be precise and target-oriented, otherwise it would not be able to fulfil its tasks and it might endanger the life of the own soldiers, pilots, operators or other personnel.

[22] How Ukrainians modify civilian drones for military use; https://www.economist.com/science-and-technology/2023/05/08/how-ukrainians-modify-civilian-drones-for-military-use?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18151738051&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gclid=EAIaIQobChMIzqigstD4gQMVdIpoCR2AQQccEAMYASAAEgIME_D_BwE&gclsrc=aw.ds (downloaded 14 October 2023)

Multi-functionality is not a good solution in the case of weapons or military equipment if we need an effective and successful operation tool. The defence industry focuses more and more on systems that with their complexity provide tailored and autonomous solutions for the armed forces.

Defence industry should be in harmony with the defence system of a state. Every country has the right to decide: keeping up a functional defence industry or maintaining good relationship with neighbours, in order to avoid unpredictable external security challenges. Indigenous defence industry supports military and police forces, state authorities and security services, and it positively contributes to gross national product (GNP) and foreign trade. The independence from foreign vendors is a huge advantage in crisis situations, especially if a country had its own raw material resources. The EU would like to strengthen the competitiveness of defence industry and stimulate the defence internal market and its stakeholders. The European Defence Fund 2023 Work Programme will provide 1.2 billion EUR for defence RD&I, through its annual calls for proposals.[23]

It is unambiguous that the EU should open its defence industry market (in the sense of trade and cooperation) for non-EU members as well, since the European security challenges are a common concern. It means that Europe should be united, in order to give adequate answers for external security challenges. The question is only: Where is the border of Europe? In the East, it seems to be between Ukraine and Russia actually. Ukraine would like to join the European sphere, while Russia is moving away from it.

The European defence industry has a chance to compete with other players thanks to the current trends that always need less and less hardware and more and more software, that is, a big advantage regarding the raw material shortage in Europe. Added-value comes from knowledge and not from expensive rare materials. Embedded software plays a much more important role than the hardware that is the case for example concerning the software defined radios (SDR). Some of the most important tools of current warfare are UAV systems for surveillance and for fighting. The operation safety and security of a UAV depends on its SDR, so an UAS is as good as its communication system.[24]

Rising military expenditures in Europe are forecasting a certain ascent of the defence industry production, since a great part of the defence budget will land in procurement that is booming nowadays. According to the data of the SIPRI Yearbook 2023, global military expenditure rose for the eighth consecutive year, and in 2022, it reached an estimated 2,240 billion USD, the highest level ever recorded by SIPRI. Despite the 3.7% year-on-year increase in spending, world military expenditure as a share of world gross domestic product (GDP) remained at 2.2%, because the global economy also grew in 2022. Governments around the world spent an average of 6.2% of their budgets on the military or 282 USD per person.

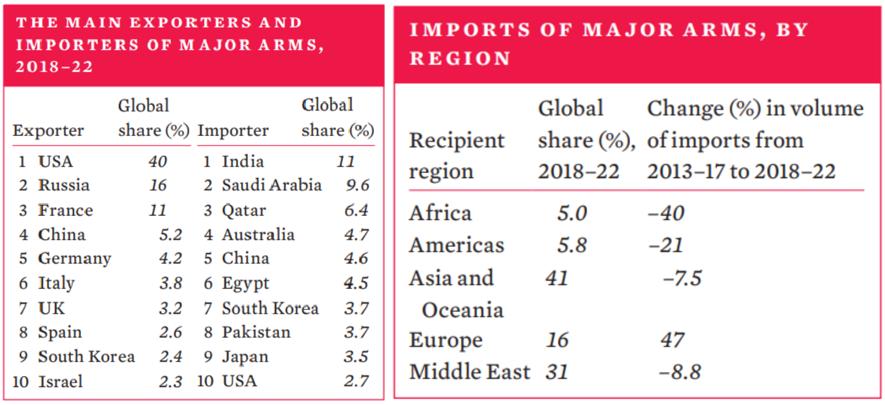
[23] The EU Defence industry. https://defence-industry-space.ec.europa.eu/eu-defence-industry_en (downloaded 14 October 2023)

[24] Per Vices: Software Defined Radios and Military UAS – Preventing jamming, providing secure communications and maintaining high-throughput data capture. Military Technology, 2023/4, pp. 74-75, ISSN 0722-3226

Europe spent about 480 billion USD for military purposes, which were 21% of the total world military spending in 2022.

The armed conflict in Southern and Eastern Ukraine had a major effect on both global and regional military expenditure in 2022. In Europe it grew by 13% between 2021 and 2022, with most Central and Western European countries responding to the Russian invasion of Ukraine with significant increases in military spending. Military aid for Ukraine was another reason of the increase in military expenditure in Central and Western Europe and North America. Many countries in these sub-regions either sent financial military aid to Ukraine or spent more to replenish decreasing stockpiles, after sending military equipment. Ukraine's own military spending rose more than sevenfold, amounting to over one third of the country's economy. Despite economic sanctions from Western countries, Russian military spending also increased by 9.2%.[25] Rising military expenditures provide new demands for the European defence industry.

The arms sales of the 100 largest arms producing and military service companies (the SIPRI Top 100) totalled to 592 billion USD in 2021 (the most recent year for which data is available), 1.9% higher than in 2020 and this trend is continuing upward, since at least 2015. This growth came despite the continuing effects of the COVID-19 pandemic, as a consequence of the disruption in supply chains, labour shortages and a lack of semiconductors. In 2022, the USA continued to dominate the ranking with 40 companies with total arms sales of 299 billion USD.[26]



THE MAIN EXPORTERS AND IMPORTERS OF MAJOR ARMS, 2018–22

	Exporter	Global share (%)		Importer	Global share (%)
1	USA	*40*	1	India	*11*
2	Russia	*16*	2	Saudi Arabia	*9.6*
3	France	*11*	3	Qatar	*6.4*
4	China	*5.2*	4	Australia	*4.7*
5	Germany	*4.2*	5	China	*4.6*
6	Italy	*3.8*	6	Egypt	*4.5*
7	UK	*3.2*	7	South Korea	*3.7*
8	Spain	*2.6*	8	Pakistan	*3.7*
9	South Korea	*2.4*	9	Japan	*3.5*
10	Israel	*2.3*	10	USA	*2.7*

IMPORTS OF MAJOR ARMS, BY REGION

Recipient region	Global share (%), 2018–22	Change (%) in volume of imports from 2013–17 to 2018–22
Africa	*5.0*	*−40*
Americas	*5.8*	*−21*
Asia and Oceania	*41*	*−7.5*
Europe	*16*	*47*
Middle East	*31*	*−8.8*

Figure 2: The main exporters and importers of major arms, 2018–22 and Imports of major arms, by region[27]

[25] SIPRI Yearbook 2023: Armaments, Disarmament and International Security (Summary). Oxford University Press, 2023, pp. 10. ISBN 978–0–19–889072–0 https://www.sipri.org/sites/default/files/2023-06/yb23_summary_en_1.pdf, (downloaded 12 September 2023)

[26] Ibid. p. 11

[27] Source: Ibid. p. 11.

SIPRI has identified 63 states as exporters of major arms in 2018–2022, but most of them are minor companies. The 25 largest suppliers accounted for 98% of the total volume of exports, and the five of them – the United States, Russia, France, China and Germany – in this period, accounted for 76% (see the chart above) of the total volume of exports. Europe's import of major arms is 16% (see the chart above) in global share that is an acceptable figure.[28] Good news for the European defence industry that France, Germany, Italy and the United Kingdom are in the list of ten largest exporters of major arms (see the chart below), in all over the world.

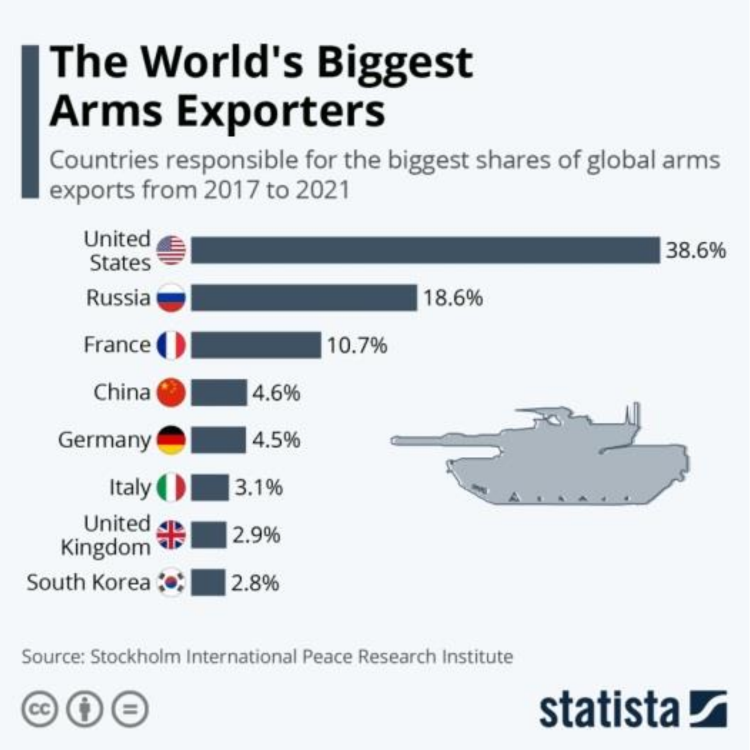


Figure 3: The World's Biggest Arms Exporters[29]

While SIPRI data on arms transfers does not represent their financial value, many arms-exporting states publish figures on the financial value of their arms exports. Based on this data, SIPRI estimates that the total value of the global arms trade was at least 127 billion USD in 2021 (the most recent year for which financial data is available), compared with 95 billion USD (in constant 2021 US dollars) in 2012. The total value of the arms trade in 2021 was about 0.5% of the total value of global international trade in 2021.[30] The global arms trade increased nearly 34% in 10 years, between 2012 and 2021.

[28] Ibid. p 12

[29] Source: https://www.statista.com/chart/18417/global-weapons-exports/ (downloaded 12 October 2023)

[30] Ibid. p 13

All the above mentioned sales, procurement and arms trade processes provide new opportunities for the European defence industry, and contribute to a more prosperous business activity.

Remaining challenges for the European defence industry

The defence industry is a raw material-intensive sector, especially because of the electronics. Unfortunately, Europe is not rich in raw materials, exclusively in REE. The biggest owners of rare raw materials are Russia and China, but they are nowadays not partners of the EU and NATO countries. Europe, as a densely populated continent, has a slight chance for finding REE deposits, but there is a tiny opportunity as well. For most of the strategic and critical raw materials – listed by the European Commission – there is no mining production in the EU. According to some sources, Sweden (and Scandinavia in general) can be a future raw material source for Europe until 2030, since there are huge unexplored but promising mining territories.[31] Reliable and unhindered downloaded to certain raw materials is a growing concern for the EU. In order to highlight this challenge, the European Commission has created a list of critical raw materials (CRMs), which is subject to a regular review and update.[32]

The defence industry uses energy, chemicals and heavy metal in a huge amount for its production activity. In the case of improper neutralisation processes or missing filters, the factories emit harmful substances polluting the air and our drinking water resources. In the future, sustainability will be a real demand in the defence industry as well, so this sector should find solutions for this challenge as soon as it is possible. The Strategic Compass, the EU's military strategy, also stated that armed forces and operations must participate in the green transition. In the future, member states' armed forces need to reduce their fossil fuel dependency, without compromising their operational effectiveness.[33]

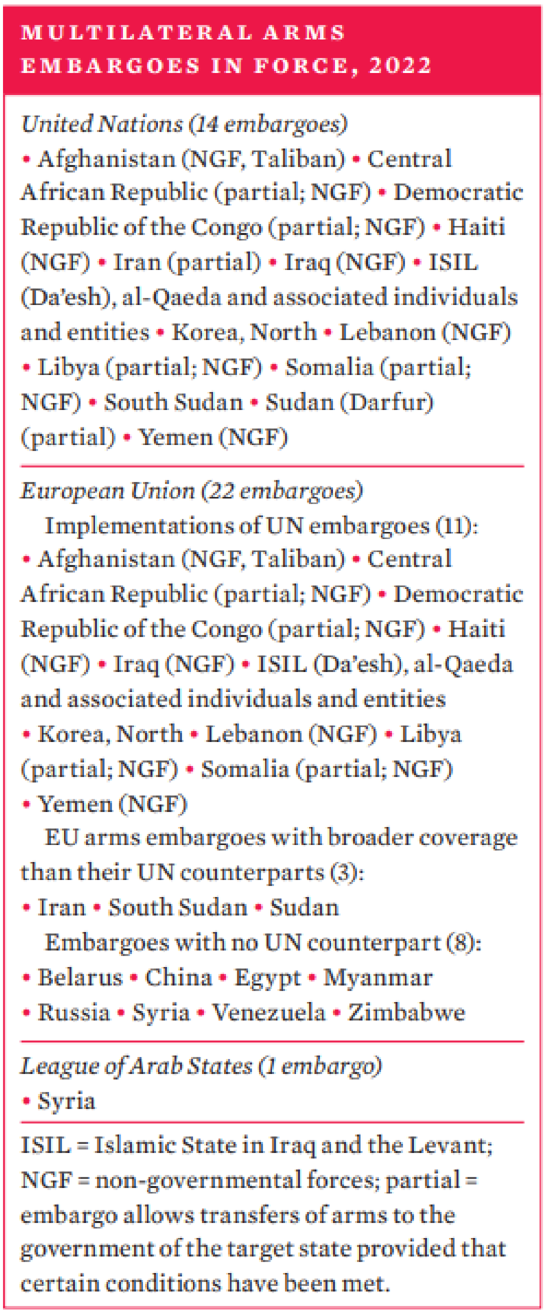
Weapon and ammunition trade is not only a commercial, but a political question as well. Thanks to several prohibitions, sanctions and embargos, defence industry companies are working in limitations and frames. They should keep the international and national rules and regulations, in order to continue their legal activity and profit-making job. Even inside of an alliance might happen that two members are not willing to cooperate with each other (for example Greece and Turkey in some cases inside NATO), since they have different security interests, goals or simply disputes. Sanctions against Russia have advantages and disadvantages as well. Russian raw materials and energy resources are not available and that is a negative effect. However, where Russians are disqualified from the military business, the European defence industry might ground or enhance its production and sales successfully.

[31] NITSCHKE op. cit. pp. 18-19

[32] Critical raw materials; https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials_en (downloaded 06 September 2023)

[33] EU and industry look for balance in greener defence plans; https://www.euractiv.com/section/defence-and-security/news/eu-and-industry-look-for-balance-in-greener-defence-plans/ (downloaded 14 October 2023)

In 2022, 14 United Nations embargoes, 22 European Union (EU) embargoes and one League of Arab States embargo were in force.



MULTILATERAL ARMS EMBARGOES IN FORCE, 2022

United Nations (14 embargoes)
• Afghanistan (NGF, Taliban) • Central African Republic (partial; NGF) • Democratic Republic of the Congo (partial; NGF) • Haiti (NGF) • Iran (partial) • Iraq (NGF) • ISIL (Da'esh), al-Qaeda and associated individuals and entities • Korea, North • Lebanon (NGF) • Libya (partial; NGF) • Somalia (partial; NGF) • South Sudan • Sudan (Darfur) (partial) • Yemen (NGF)

European Union (22 embargoes)
Implementations of UN embargoes (11):
• Afghanistan (NGF, Taliban) • Central African Republic (partial; NGF) • Democratic Republic of the Congo (partial; NGF) • Haiti (NGF) • Iraq (NGF) • ISIL (Da'esh), al-Qaeda and associated individuals and entities • Korea, North • Lebanon (NGF) • Libya (partial; NGF) • Somalia (partial; NGF) • Yemen (NGF)
EU arms embargoes with broader coverage than their UN counterparts (3):
• Iran • South Sudan • Sudan
Embargoes with no UN counterpart (8):
• Belarus • China • Egypt • Myanmar • Russia • Syria • Venezuela • Zimbabwe

League of Arab States (1 embargo)
• Syria

ISIL = Islamic State in Iraq and the Levant; NGF = non-governmental forces; partial = embargo allows transfers of arms to the government of the target state provided that certain conditions have been met.

Figure 4: Multilateral arms embargoes in force, 2022[34]

[34] SIPRI Yearbook 2023 Armaments op. cit. p. 20.

The level of international consensus around decisions to lift or extend UN arms embargoes deteriorated in 2022, with disagreements between, on the one hand, China, Russia and several like-minded African states, and mainly Western powers on the other. Together with the United States and 10 like-minded states, the EU put in place a set of security-focused trade restrictions on Russia and Belarus – implemented via member states' domestic export control systems – that were the most significant and wide-ranging ever imposed on a major industrialized state in the post-cold war period. The restrictions clearly disrupted the flow of parts and components to Russia's defence industry, but there were indications that Russia was able to acquire many of these items indirectly, which makes the effectiveness of these measures questionable.[35] Especially in 2022, the armed conflict in Ukraine caused difficulties for the European defence industry, due to the temporary or permanent loss of steel and component production.

The increased geopolitical tensions – posed by Russia's invasion of Ukraine in 2022 – significantly affected the work of the four multilateral export control regimes; the Australia Group (on chemical and biological weapons), the Missile Technology Control Regime (MTCR), the Nuclear Suppliers Group (NSG), and the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies (WA), but the nature and extent of the disruption varied. Despite these difficulties, the regimes exchanged experiences and good practices, adopted minor changes in their control lists and continued their technical work.[36] It can be stated that sanctions might deteriorate good relations, economic and military cooperation, and they are harming the mutual confidence building endeavours as well.

It is not questionable that defence industry companies from different countries are able to cooperate with each other only when they have commonly accepted standards. EDSTAR is the European Defence STAndards Reference system containing references to "Best-Practice" Standards (BPS), in support of programme organisations. EDSTAR has been established by the EDA, in 2011. As a means to consolidate the highly fragmented defence market in Europe, EDSTAR aims at optimising efficiency and interoperability of standards application for defence and security products and services. In order to implement standardisation as critical enabler, EDSTAR targets the stakeholders (such as EDA participating Member States, European Commission, European Union Military Staff, European and International Standardisation Organisations, Industry including Small and Medium Enterprises and associations, R&T and Academia), supporting the European defence capability development.

The military cooperation inside NATO without a standardisation would be impossible. To carry out multinational operations, countries need to share a common set of standards – rules or guidelines that ensure mutual understanding and practical functionality – covering everything from ammunition sizes to rail gauges to the words that troops use to communicate with each other. Standardization helps the forces of NATO Allies and partners to achieve interoperability, allowing for more efficient use of resources and enhancing the Alliance's operational effectiveness.

[35] Ibid.

[36] Ibid. pp. 22-23

A Standardization Agreement (STANAG) is a NATO standardization document, which defines the agreement of member countries to implement a standard. NATO Allies have agreed hundreds of STANAGs, over the years, covering a huge range of technical specifications for equipment and common practices. Some examples include equipment and procedures for air-to-air refuelling; common sizes, safety rules and tests to make ammunition interchangeable; specifications to make national communications systems compatible; and formats to facilitate sharing intelligence and other information.[37]

Standardization is not an easy task, since these regulations should be implemented in legal documents, processes and operations. This procedure takes long time and costs a huge amount of money; thus, it is a great challenge for the European defence industry as well.

SWOT analysis of the European defence industry

The next SWOT analysis evaluates the present situation of the European defence industry, and forecasts its opportunities and challenges in the future.

Strengths:

- *Increasing demand for military technology:* The continuous uncertain security situation in Europe and in its neighbourhood has increased the demand for defence acts and military technology, in order to protect stability and peace inside the continent.
- *Strong Research and Technology background:* The EU (through EDA) and NATO (by DIANA programme) provide downloaded to funds and research programs aiming at finding up-to-date solutions for defence technological challenges.
- *Academic and engineering knowledge and experience in the defence industry:* Research institutes of universities are cooperating with start-ups, scientists, production companies and service providers, in order to implement the latest technology and methods in the defence system.
- *Cooperation with American companies:* European defence industry firms are traditionally good collaborators of American partners.
- *Good preferences:* Famous European defence companies have reached reputation in the international defence market as well.

Weaknesses:

- *Shortage in raw materials:* The defence industry is a raw material-intensive sector, so it needs downloaded to ores and special elements, but these are unfortunately not available in a needed amount in Europe.
- *Emission of harmful substances:* The defence industry is energy, chemicals and heavy metal-demanding sector, which without proper filters or neutralisation processes, emits harmful, water and air polluter substances.

[37] NATO – Standardization. https://www.nato.int/cps/en/natohq/topics_69269.htm (downloaded 12 September 2023)

- *Limited capacity:* Mainly relatively small defence companies represent the European defence industry and these are not prepared for mass production.
- *Lack of unity:* Usually individual European defence companies are cooperating with each other according to simple business interests.
- *Political fragmentation:* Political cooperation among countries usually determines the relationship of different national defence industry companies.

Opportunities:

- *Increasing defence spending:* European states spend more and more financial resources for defence purposes, so the orders towards defence industry companies are growing.
- *Dual use products:* In peacetime these products save the defence industry (manufacturing dual use goods), since during this time, there is no need for huge amount of military technology.
- *Cooperative programs:* Multinational organisations (mainly the EU and NATO) provide transnational defence industry cooperation through projects and funds.
- *Demand for modernisation of the armed forces and its military technology:* New security challenges expect new military capabilities, supported by modern military technology.
- *Disruptive technologies, artificial intelligence (AI), Internet of Things (IoT), software defined appliances:* New methods are aiming to spare materials, persons or time, and to make the operations more successful, the missions faster accomplished and the battlefield more human in legal term.
- *Balancing role in economic terms:* During an economic prosperity, defence industry works on enhancing stability with its production activity (defence value creation), while during a recession period, it deterrents counter-stability movements, criminal activities or external threats (defence value protection).

Threats:

- *Uncertain supply chain in raw materials:* European defence industry is dependent on non-friendly states' (for example Russia and China) raw material supplies.
- *Increasing proliferation, corruption and illegal arms trade:* Since demand is always higher and higher for weapons and armaments in unstable regions in all over the world; thus, official defence industry companies are not able to keep the arms trade in a legal frame and so illegal players take over proliferation roles.
- *Dirty competition in the global weapons market:* Arms smuggling has a negative effect on a legal defence industry because this phenomenon spoils the pure competition.
- *Asymmetric warfare:* This kind of military phenomenon (tool or method) might deteriorate or eliminate expensive high precision weapons and systems with small technical investment.

- *Espionage:* Adversary firms are interested in gaining information and taking over technological advantage – in a certain segment – to maximise the profit and control the manufacturing and sales activity.

Conclusions

The Russian–Ukrainian armed conflict has provided many lessons for the European armed forces and for the European defence industry as well. Recent military clashes in Ukraine prove that every country should develop its own defence forces, according to the potential (mainly the closest) enemy's military capabilities and technology. This theoretical and practical hostile power should be stopped with deterrence or must be defeated with real weaponry. The most complicated question in this case is: How can a country afford well-equipped and well-trained armed forces without a harmful economic overload, while also taking into consideration economic sustainability aspects as well?

The European defence industry should be reviewed from time to time, in order to define its new paths. However, it is not an easy task to determine such a long term activity that would like to avoid dead-end streets. After every security or technological milestone, the defence industry should be taken under scrutiny, and should be revised. Smart forecasting of new trends in armament, military technology and arms sales would be a huge advantage. The changing security situation and the appearance of a new, disruptive technology expect cutting-edge solutions inside the defence industry. While military operation-cycle consists of reconnaissance, surveillance, identification, tactical action and interception, the defence industry consists of demand, design, production and supply. These two lanes should run parallel and in harmony with each other.

The defence industry is a special sector. It starts up very slowly and moves also adagio, but can be demolished in a very short time. This fact sends a message that defence industry should be always valued and re-evaluated. During an economic boom, defence companies should be entrusted with larger orders to produce protecting and deterring tools, namely weapons against potential threats. During an economic recession defence firms should be kept and maintained in good condition, in order to be able to respond to highly possible security challenges, emerging more often in this period of time. In conclusion, defence industry should be run continuously and in long term to avoid the loss of expertise (human potential) and technology, supplied with such documentation and infrastructure that are hard to substitute.

Every state would like to have a stable society and a promising economic prosperity, in order to avoid most of the internal security challenges. In this endeavour, defence system and its subsystem, the defence industry – besides its original mission – might play an important social and economic, balancing role. In peacetime, a good-functioning defence industry employs well-trained and educated workforce, contributing – with civil or dual-use products – to the increasing industrial production and economic growth of the country. During an economic crisis or a security emergency, a well-functioning defence industry keeps its workers and contributes – with its dual-use or military products – to economic stability and social security.

All in all, defence industry is an important sector inside the national defence system, with a complex mission, including political, economic, social, environmental and legal activities.

Bibliography:

- 11 new PESCO projects focus on critical defence capabilities and interoperability, 23 May 2023; https://eda.europa.eu/news-and-events/news/2023/05/23/11-new-pesco-projects-to-focus-on-critical-defence-capabilities-and-interoperability (downloaded 12 October 2023)
- ANNATI, Massimo: Doctrinal Developments and Market Perspective in Loitering Munitions. Military Technology, 2023/5, pp. 62-65, ISSN 0722-3226
- BARONE, Marco Giulio: Foreword – Preparing for Future Air Warfare. Military Technology, Special Supplement 2023, The Future of Air Power; 2023/4, pp. 4-5, ISSN 0722-32260
- Critical raw materials; https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials_en (downloaded 06 September 2023)
- Defence Industry Europe; https://defence-industry.eu/about-us/ (downloaded 06 October 2023)
- EU and industry look for balance in greener defence plans; https://www.euractiv.com/section/defence-and-security/news/eu-and-industry-look-for-balance-in-greener-defence-plans/ (downloaded 14 October 2023)
- EU defence cooperation: Council welcomes Denmark into PESCO and launches the 5th wave of new PESCO projects, 23 May 2023; https://www.consilium.europa.eu/en/press/press-releases/2023/05/23/eu-defence-cooperation-council-welcomes-denmark-into-pesco-and-launches-the-5th-wave-of-new-pesco-projects/#new_tab (downloaded 12 October 2023)
- European Defence Agency – What we do; https://eda.europa.eu/what-we-do (downloaded 12 October 2023)
- European Defence Agency – Who we are; https://eda.europa.eu/who-we-are (downloaded 12 October 2023)
- European Union – External Action, Missions and Operations – Working for stable and a safer Europe, Ongoing missions and operations; https://www.eeas.europa.eu/eeas/missions-and-operations_en#9620 (downloaded 10 September 2023)
- Eurostat – EU Trade with Russia – latest developments; https://ec.europa.eu/eurostat/statistics-explained/index.php?title=EU_trade_with_Russia_-_latest_developments&stable=0&redirect=no#Latest_developments (downloaded 14 October 2023)

- Facts and figures on life in the European Union; https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/life-eu_en (downloaded 06 September 2023)
- How Ukrainians modify civilian drones for military use; https://www.economist.com/science-and-technology/2023/05/08/how-ukrainians-modify-civilian-drones-for-military-use?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18151738051&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gclid=EAIaIQobChMIzqigstD4gQMVdIpoCR2AQQccEAMYASAAEgIME_D_BwE&gclsrc=aw.ds (downloaded 14 October 2023)
- NATO – Defence Innovation Accelerator for the North Atlantic (DIANA). https://www.diana.nato.int/ (downloaded 12 October 2023)
- NATO – Standardization. https://www.nato.int/cps/en/natohq/topics_69269.htm (downloaded 12 September 2023)
- NITSCHKE, Stefan: Dependence of Strategic and Critical Raw Materials May Soon Replace Today's Dependence on Oil, Says the European Commission – What Lessons are to be Learned? Military Technology, 2023/2, pp. 16-19, ISSN 0722-3226
- Per Vices: Software Defined Radios and Military UAS – Preventing jamming, providing secure communications and maintaining high-throughput data capture. Military Technology, 2023/4, pp. 74-75, ISSN 0722-3226
- Repertory of Practice of United Nations Organs – Charter of the United Nations, Chapter I – Purposes and Principles, Article 2(1)–(5). https://legal.un.org/repertory/art2.shtml (downloaded 10 October 2023)
- Russian Logistics and Sustainment Failures in the Ukraine Conflict. Status as of January 1, 2023, https://www.rand.org/pubs/research_reports/RRA2033-1.html (downloaded 14 October 2023)
- Security Council Report. Ukraine: Meeting under the "Threats to International Peace and Security" Agenda Item. https://www.securitycouncilreport.org/whatsinblue/2023/10/ukraine-meeting-under-the-threats-to-international-peace-and-security-agenda-item-4.php (downloaded 12 October 2023)
- SIPRI Yearbook 2023: Armaments, Disarmament and International Security (Summary). Oxford University Press, 2023, pp. 10-23, ISBN 978–0–19–889072–0 https://www.sipri.org/sites/default/files/2023-06/yb23_summary_en_1.pdf (downloaded 12 September 2023)
- TAGHVAEE, Babak: Long-range Land-based Early Warning Radars – Lessons from Ukraine. Developments for the Future. Military Technology, 2023/3, pp 28-32, ISSN 0722-3226
- TANI, Caterina: Boosting Ammunition Supplies – A Big Step for Ukraine and a Bigger One for Europe? Military Technology, 2023/3, pp. 10-15, ISSN 0722-3226

- The EU Defence industry. https://defence-industry-space.ec.europa.eu/eu-defence-industry_en (downloaded 14 October 2023)
- Top 100 Defense Companies. https://people.defensenews.com/top-100/ (downloaded 10 September 2023)
- Ukraine to build a critical infrastructure protection system in line with the world’s best practices and EU law. https://cip.gov.ua/en/news/ukrayina-pochinaye-buduvati-sistemu-zakhistu-kritichnoyi-infrastrukturi-vidpovidno-do-naikrashikh-svitovikh-praktik-ta-chinnikh-vimog-yevropeiskogo-zakonodavstva (downloaded 14 October 2023)
- Ukraine weapon switcheroos are flushing Soviet arms out of Europe. https://www.defensenews.com/global/europe/2022/04/28/ukraine-weapon-switcheroos-are-flushing-soviet-arms-out-of-europe/ (downloaded 06 October 2023)
- What is deep tech? https://www.eitdeeptechtalent.eu/the-initiative/what-is-deep-tech/ (downloaded 12 October 2023)

WU YUE[1] – TIBOR BABOS[2] – KATALIN TAKÁCS-GYÖRGY PHD[3]

THE IMPORTANCE OF AGRICULTURE, IN THE LIGHT OF GLOBAL SECURITY CHANGES AND TRENDS

Abstract

Agriculture and food are the most important parts of any nation and country. Most research focuses on the issues of sustainable development in agriculture, but there is a lack of overview regarding the future possible risks and threats-trend in agriculture. In order to reveal future agricultural risks and threats, we have to think forward and assess any potential factors. The aim of this research is to identify the risks and threats-trend in agriculture and food, in the light of global security changes and trends. We used secondary research review and analysis as a research methodology, the theory of value chain, and the background of global security changes, from the book; "The five central pillars of European security" in 2007. In the end, we have found that most of the agricultural risks and threats-trend originates from global security changes and trends. Therefore, we highlighted that both individual and public sectors should handle and emphasize agriculture as an important part of global security. The value of this research is to construct a framework of reference for a continuous study on the essential and urgent topics of agriculture and food security, as well as on the sustainable agriculture and food production.

Keywords: agricultural risks; food security; sustainable agriculture, five central pillars of the Europeans security, climate change, digital methods in agriculture, national and global security

1. Introduction

As agriculture is where the crop is cultivated and animals bred, agriculture is one of the most important sectors for any nation. Under the global security changes and trends,[4,5] agriculture has been and will be obviously exposed to various threats and risks (climate change, biodiversity loss, natural risks and disasters, health security, aging farmers, energy supply, infrastructure security, limited resources, increasing food demand, due to increasing population, market fluctuations, etc.). The safety and security of a country or a region, as well as the risks – stemming from globalization, international and local policy background – and the requirements for sustainable development also are influencing the agriculture.[6.]

[1] ORCID: 0000-0003-0349-5654

[2] ORCID: 0000-0001-7459-8349

[3] ORCID: 0000-0002-9129-7481

[4] BABOS, T.: The five central pillars of European security. NATO Public Diplomacy Division – Strategic and Defense Research Center – NATO School, 2007.

[5] BABOS, T.: A biztonság globális és európai összefüggései. Hadtudomány, 2019/4, pp. 16-29

[6] BALL, M.: Digital Farming: Driving productivity and a more sustainable way of farming. www.euractiv.com, October 08, 2019. https://www.euractiv.com/section/agriculture-

Agriculture has changed human life from a nomadic to permanent settlements lifestyle, since 12,000 years ago[7] (Figure 1). A stable food supply is guaranteed when animals and crops can be farmed and meet the demands.[8] The evolution of Agriculture 1.0 started in early 1900s.[9] Thanks to the industrial revolution, agriculture experienced its 2.0 era, in the late 20th century. The Agriculture 3.0 revolution, called also as a precision agriculture, happened, due to the rapid development of intelligent applications in the 1980s, such as sensors, robotics, satellite imagery, and field mapping.[10] Therefore, crop quality and profitability could improve, and some sustainable agricultural problems can potentially be solved. Agriculture 4.0, or the smart agriculture or digital agriculture, has been the product of developing digital technologies and improving precision agriculture, since the 2010s, such as IoT, big data, cloud computing, AI, 5G, etc.[11]

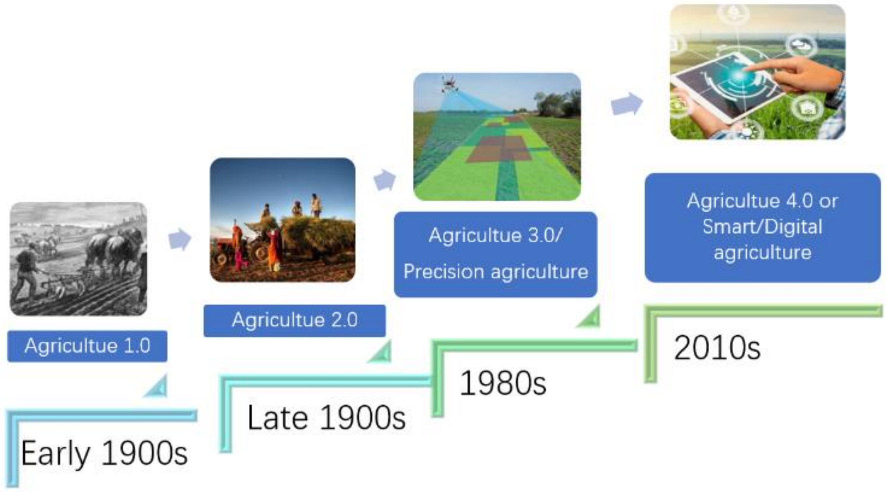

Agricultue 1.0
Agricultue 2.0
Agricultue 3.0/ Precision agriculture
Agricultue 4.0 or Smart/Digital agriculture
Early 1900s
Late 1900s
1980s
2010s

Figure 1: Timeline of agricultural development stages[12]

food/video/digital-farming-driving-productivity-and-a-more-sustainable-way-of-farming/ (downloaded 26 October 2022)

[7] The Development of Agriculture. https://education.nationalgeographic.org/resource/development-agriculture (downloaded 13 March 2023)

[8] RASMUSSEN, Wayne D. et al.: Origins of agriculture – The Americas. Britannica, Jul. 29, 2022. https://www.britannica.com/topic/agriculture (downloaded 13 March 2023)

[9] GAGLIARDI, G. – COSMA, A. I. M. – MARASCO, F.: A Decision Support System for Sustainable Agriculture: The Case Study of Coconut Oil Extraction Process. Agronomy, 2022/1, doi: 10.3390/agronomy12010177 (downloaded 16 March 2023)

[10] Precision Agriculture Technology, Benefits & Application. 20 April 2022. https://eos.com/blog/precision-agriculture/ (downloaded 13 March 2023)

[11] KOVÁCS, Imre – HUSTI, István: The role of digitalization in the agricultural 4.0 – how to connect the industry 4.0 to agriculture? Hungarian Agricultural Engineering, no. 2018/33 pp. 38-42, 2018, doi: 10.17676/HAE.2018.33.38 (downloaded 16 March 2023)

[12] Source: own construction based on BABOS (2007) op. cit., BABOS (2019) op. cit., BALL (2019) op. cit., The Development of Agriculture op. cit., RASMUSSEN (2022) op. cit.

2. Methodology

Nevertheless, agriculture and food are important for both individuals and a nation. In this research, we aimed at highlighting the importance of agriculture from the viewpoint of global security changes and trends. Hence, the review is based on secondary research[13] and content analysis.[14] The literature resources of our research are from reliable and prestigious journals, official international organizations' reports and databases (FAO, the UN, etc.), etc. Besides, the theory of value chain from Michael E. Porter's[15] helped us to have a well-structured view of agriculture and food threats and risks, across the food value chain. Michael E. Porter's value chain theory describes the full chain and activities, from where a product or service comes. Value chain theory has five main activities and four supporting activities (Table 2).

Main or primary activities	Supporting activities
inbound logistics	technology development
operations	procurement
outbound logistics	immutable infrastructure
marketing and sales	human resources
services	-

Table 2: Main activities and supporting activities in value chain theory[16]

3. Results

3.1. Future production and demand

Agricultural products provide food, which is one of the three primary elements for human existence; food, water and air. Agriculture and food production will face the challenge related to its amount and quality. As the increasing population will be 8.6 billion in 2030, 9.8 billion in 2050, and 11.2 billion in 2100 estimated,[17] the middle class is also increasing, which means that the requirements for food will become more and more complicated.[18] So far, due to the loss of pollinators, global crop production at risk can be up to 577 billion dollars.[19]

[13] Garza-Reyes, J. A.: Green lean and the need for Six Sigma. International Journal of Lean Six Sigma, 2015/3, pp. 226-248, doi: 10.1108/IJLSS-04-2014-0010 (downloaded 16 March 2023)

[14] Stemler, Steve: An overview of content analysis. Practical Assessment, Research, and Evaluation, 2001/7. doi: 10.7275/Z6FM-2E34 (downloaded 16 March 2023)

[15] Chai, Wesley: What is a value chain and why is it important? SearchCIO, Feb. 2021. https://www.techtarget.com/searchcio/definition/value-chain (downloaded 29 November 2022)

[16] Source: Own construction based on Kovács – Husti (2018) op. cit.

[17] World population projected to reach 9.8 billion in 2050, and 11.2 billion in 2100. United Nations, https://www.un.org/en/desa/world-population-projected-reach-98-billion-2050-and-112-billion-2100 (downloaded 26 October 2022)

[18] Challenges for modern agriculture. Syngenta, https://www.syngenta.com/en/innovation-agriculture/challenges-modern-agriculture (downloaded 26 October 2022)

[19] UNEP: Facts about the nature crisis. UNEP–UN Environment Programme, Jul. 07, 2022. http://www.unep.org/facts-about-nature-crisis (downloaded 11 March 2023)

And 33 percent of croplands are used to grow livestock feed.[20] If it is possible to produce cultured (lab-grown) and plant-based meats to reduce the production pressure, and if consumers can accept it, are the questions left for agriculture and food. According to the latest statistics from FAO on 03/03/2023, global cereal production and stocks are forecasted to decline, and the utilization seems unchanged, from the last year.[21] (Figure 2) By 2050, it is estimated that 70% more food should be available. The dilemma; how to improve agriculture and food production – while at the same time taking care of the environment and obtaining sustainability – will reshape the current agricultural methods.

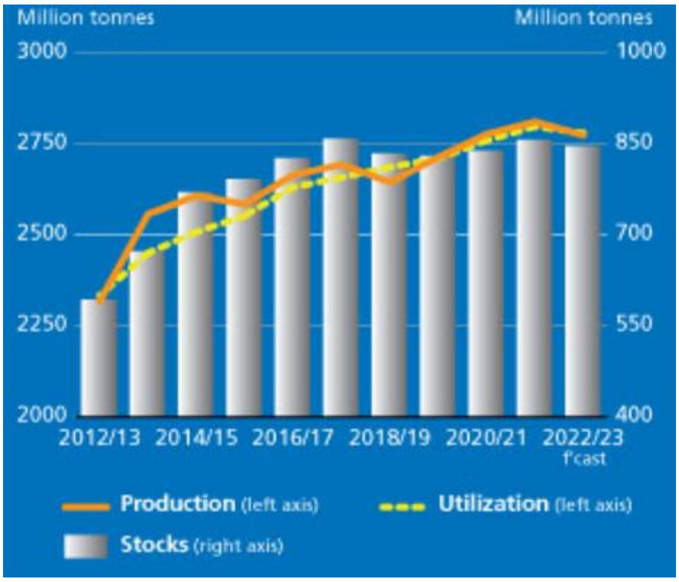


Figure 2: Global cereal production, utilization, and stocks[22]

3.2. Climate change or extreme weather

As discussed above, environmental security has been threatening the human living for decades. Environmental security issues threaten the agriculture, but the agriculture is also a major cause of global environmental degradation. Just three aspects of agriculture (land clearing, crop production, and fertilization) account for one quarter of the GHG emissions.[23]

[20] Livestock and Landscapes. FAO, https://www.fao.org/3/ar591e/ar591e.pdf (downloaded 11 March 2023)

[21] FAO Cereal Supply and Demand Brief – World Food Situation – Food and Agriculture Organization of the United Nations. 03 March 2023. https://www.fao.org/worldfoodsituation/csdb/en/ (downloaded 13 March 2023)

[22] Source: FAO: Word Food Situation – FAO Cereal Supply and Demand Brief. https://www.fao.org/worldfoodsituation/fao-cereal-supply-and-demand-brief/en (downloaded 11 March 2023)

[23] UNEP: Facts about the nature crisis. op. cit.

The agriculture affects biodiversity through habitat replacement: local species' richness declines and some important functional species can disappear, such as pollinators.[24] The management-choice (pesticides, fertilizers, herbicides, and crop type)[25] can also have a harmful impact on the environment.. Coastal habitat loss can also bring floods and hurricanes. Floods, droughts, erratic rainfall patterns, and other extreme weather conditions are the killers of agricultural production. With every 3℃ increase, 50% of the crop yield will be lost.[26,27]

3.3. Limit of resources

Agriculture is highly dependent on resources, including natural resources, human-made and human resources.[28] Especially natural resources are the cornerstone of agriculture, such as water, arable land, energy, etc. However, as mentioned in Chapter 3.1.10, the agriculture altered the earth's face most than any other human activity.[29] Agriculture depends on the earth, but it also has a negative impact on the earth.

So far, the agriculture has rapidly depleted water and land.[30] We have lost nine lakes already, and 90% of the water is disappearing in some lakes. Agricultural water accounts for 70% of the world's freshwater,[31] but availability changes. Some regions face dangerous freshwater paths, and some suffer from drought.[32] Human actions have altered 75% of the earth's land surface and 85% is wetland areas. Agricultural lands account for 12% of the world's land, and 33% of croplands are used to grow livestock feed.[33] In the last 40 years, we have lost 30% of farming land.[34] There will be no available topsoil by 2080 if this decreasing rate maintains.

[24] Challenges for modern agriculture. Syngenta. op. cit.

[25] RAMANKUTTY, N. et al.: Trends in Global Agricultural Land Use: Implications for Environmental Health and Food Security. Annual Review of Plant Biology, 2018 April, pp. 789-815, doi: 10.1146/annurev-arplant-042817-040256 (downloaded 16 March 2023)

[26] Sustainable and Digital Agriculture – United Nations Development Programme. UNDP, https://www.undp.org/sgtechcentre/sustainable-and-digital-agriculture-1 (downloaded 26 October 2022)

[27] AGRIMONTI, C. – LAURO, M. – VISIOLI, G.: Smart agriculture for food quality: facing climate change in the 21st century. Critical Reviews in Food Science and Nutrition, 2021/6, pp. 971-981, doi: 10.1080/10408398.2020.1749555 (downloaded 16 March 2023)

[28] Types of Resources Class 8 Geography. https://www.excellup.com/ClassEight/sseight/reourceseight.aspx (downloaded 10 March 2023)

[29] UNEP: Facts about the nature crisis. op. cit.

[30] Sustainable and Digital Agriculture – United Nations Development Programme op. cit.

[31] Challenges for modern agriculture. op. cit.

[32] RODELL M. et al.: Emerging trends in global freshwater availability. Nature, May 2018, pp. 651-659, doi: 10.1038/s41586-018-0123-1 (downloaded 16 March 2023)

[33] Livestock and Landscapes op. cit.

[34] MAXIMILLIAN, J. – BRUSSEAU, M. L. – GLENN, E. P. – MATTHIAS, A. D.: Pollution and Environmental Perturbations in the Global System. Environmental and Pollution Science, Elsevier, 2019, pp. 457-476. doi: 10.1016/B978-0-12-814719-1.00025-2 (downloaded 16 March 2023)

The improper land use (tillage, land clearing, grazing, and rotation plan) and agricultural management (fertilization, irrigation, and crop choice) cause soil health problems, such as soil erosion and soil degradation[35] (loss of soil fertility and soil biodiversity), destruction of land by natural hazards, unilateral and irreversible built-up area expansion, and so on[36,37]. And 3.2 billion population is affected negatively by land degradation.

3.4. The irresistible trend of digital agriculture and the obstacles

Digitalization is used in agriculture to collect, store, analyze and share data and information with a series of digital tools, such as GPS, big data, sensors, drones, etc.[38]. Digital agriculture can not only increase agricultural productivity (decide crop type based on field condition,[39] but can improve water efficiency, etc.), but also pursue sustainability (protect biodiversity, reduce GHG emission, and keep soil fertility), which make agriculture more resilient to climate change.[40,41]

Undoubtedly, sophisticated and advanced technologies improve agricultural productivity and profits (from the points of seeds treatment, crop protection, crop harvesting, and data analysis). However, the high price threshold stops a lot of small-scale farmers (80% of the developing countries' food supplies) from downloadeding these technologies.[42,43]

[35] RAMANKUTTY op. cit.

[36] BALL op. cit.

[37] XIN, L. – FAN, Y. Z. – TAN, M. H. – JIANG, L. G.: Review of Arable Land-use Problems in Present-day China. AMBIO: A Journal of the Human Environment, 2009/2, pp. 112-115, doi: 10.1579/0044-7447-38.2.112 (downloaded 16 March 2023)

[38] BASSO B. – ANTLE, J.: Digital agriculture to design sustainable agricultural systems. Nature Sustainability, 2020/4, pp. 254-256, doi: 10.1038/s41893-020-0510-0 (downloaded 16 March 2023)

[39] MAFFEZZOLI, F. – ARDOLINO, M. – BACCHETTI, A. – PERONA, M. – RENGA, F.: Agriculture 4.0: A systematic literature review on the paradigm, technologies and benefits. Futures, Sep. 2022, p. 102998, doi: 10.1016/j.futures.2022.102998 (downloaded 16 March 2023)

[40] AGRIMONTI, C. – LAURO, M. – VISIOLI op. cit.

[41] SHAO, L. – GONG, J. – FAN, W. – ZHANG, Z. – ZHANG, M.: Cost Comparison between Digital Management and Traditional Management of Cotton Fields—Evidence from Cotton Fields in Xinjiang, China. Agriculture, 2022/8, p. 1105, doi: 10.3390/agriculture12081105 (downloaded 16 March 2023)

[42] SOMOSI, S. – SZÁMFIRA, G.: Agriculture 4.0 in Hungary: The challenges of 4th Industrial Revolution in Hungarian agriculture within the frameworks of the Common Agricultural Policy. In: UDVARI, B. (Ed.): Proceedings of the 4th Central European PhD Workshop on Technological Change and Development. University of Szeged, Doctoral School in Economics, Szeged, pp. 162-189.

[43] Digital Agricultural Academy of Hungary to take farmers into new age. https://www.freshplaza.com/latin-america/article/9428745/digital-agricultural-academy-of-hungary-to-take-farmers-into-new-age/ (downloaded 04 October 2022)

The aging farmers and young farmers not equipped with digital technology knowledge and the unclear digital agricultural education constitutes also an obstacle to digital agriculture development.[44,45]

3.5. Security Issues in Agriculture 4.0

Agriculture 4.0 is the era surrounded by the internet. It is a lack of research on data security and reliability, scalability, and interoperability in digital agriculture.[46] Cyberattacks are the highest growth rate of crime globally, which bring financial loss and reputation damage[47] for Agriculture 4.0.[48] The most common cyber-attacks experienced by companies are phishing (37%), network instruction (30%), inadvertent disclosure (12%), stolen device records (10%), and system misconfiguration (4%). And the top global fraud types are phishing (40%), rogue mobile apps (28%), Trojan horse (16%), and bran abuse (15%). The volume of cybersecurity incidents by sector is financial services (27%), ICT (18%), manufacturing (13%), retail (9%), and professional services (1%). Unfortunately, all these aspects are permeating the agriculture.

Besides, more and more agricultural machines are equipped with data storage functions, which is good for the data owner. However, the tragedy (for individuals or national security) comes from data abuse or "improper" data ownership. For example, Deere & Company (John Deere) is an American manufacturing company for agricultural machinery and other industrial machinery and equipment targeting North America, Africa, Asia-Pacific, the Middle East, and Europe. As it is written on their official web page, *"We rely on more than 180 years of experience and terabytes of precision data to know them and their businesses better than anyone else. Our easy-to-use technology helps deliver results they see in the field, on the job site, and on the balance sheet."*[49].

[44] SOMA, T. – NUCKCHADY, B.: Communicating the Benefits and Risks of Digital Agriculture Technologies: Perspectives on the Future of Digital Agricultural Education and Training. Frontiers, 2021/6, p. 762201, doi: 10.3389/fcomm.2021.762201 (downloaded 16 March 2023)

[45] TAKÁCSNÉ GYÖRGY, K. et al.: Precision agriculture in Hungary: assessment of perceptions and accounting records of FADN arable farms. Studies in Agricultural Economics, 2018/1, pp. 47-54, doi: 10.7896/j.1717 (downloaded 16 March 2023)

[46] ABBASI, R. – MARTINEZ, P. – AHMAD, R.: The digitization of agricultural industry – a systematic literature review on agriculture 4.0. Smart Agricultural Technology, 2022/2, p. 100042, doi: 10.1016/j.atech.2022.100042 (downloaded 16 March 2023)

[47] CHANG, J.: 10 Cybersecurity Trends for 2022/2023: Latest Predictions You Should Know. Financesonline.com, 08 November 2019. https://financesonline.com/cybersecurity-trends/ (downloaded 14 March 2023)

[48] FERRAG, M. A. – SHU, L. – FRIHA, O. – YANG, X.: Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions. IEEE/CAA Journal of Automatica Sinica, 2022/3, pp. 407-436, doi: 10.1109/JAS.2021.1004344 (downloaded 16 March 2023)

[49] John Deere: About Our Company. https://www.deere.com/en/our-company/ (downloaded 14 March 2023)

The reported John Deere tractor 4240 display hacks indicated the vulnerability of food supply security for a nation in high-tech farming.[50,51]

3.6. Agricultural commodities market fluctuations

Agricultural food price fluctuation is common, but affects food security, farmers, and the vulnerable people.[52,53] When the food price volatility is too high, it can even affect the countries. The reasons for agricultural food price fluctuation are complicated.[54] In the short term, the reasons can be supply and demand, weather, disease outbreaks, war, and natural disasters. In the long term, the reasons to drive food price fluctuations are unstable oil prices, climate change, government subsidies, World Trade Organization Limits on Stockpiles, and increasing meat-demand.

3.7. Food security issue--food loss and waste

The food security crisis has already alerted all over the world. The most common definition of food security includes three pillars: food availability, food downloaded, utilization, and stability.[55] The factors of food insecurity are multi-dimensional. In this subchapter, we mainly highlight the effects of food loss and waste, one of the biggest challenges in the food system (from social, environmental, and economic aspects).[56] Food loss and waste is also food safety, sustainability, and ethics problem.[57]

[50] BUCHANAN, Kallee – MURPHY, Tanya: What the John Deere tractor hack reveals about cyber threats to food supply. ABC News, 23 August 2022, https://www.abc.net.au/news/rural/2022-08-24/tractor-hack-reveals-food-supply-vulnerable/101360062 (downloaded 14 March 2023)

[51] KIRK, Jeremy: Flaws in John Deere Systems Show Agriculture's Cyber Risk. 09 August 2021, https://www.bankinfosecurity.com/flaws-in-john-deere-systems-show-agricultures-cyber-risk-a-17240 (downloaded 14 March 2023)

[52] FAO publications catalogue 2022. FAO, 2022. doi: 10.4060/cc2323en (downloaded 16 March 2023)

[53] CHAUDHRY, Ifra – SULEMAN, Raheel – BHATTI, Adrish – ULLAH, Inam: Review: Food price fluctuations and its influence on global food market. Annals of Social Sciences and Perspecitve, 2021/1, pp. 21-33, doi: 10.52700/assap.v2i1.33 (downloaded 16 March 2023)

[54] AMADEO, Kimberly: Why Food Prices Are Rising, Recent Trends, and 2021 Forecast – 5 Causes of High Food Prices. The Balance, 15 March 2022, https://www.thebalancemoney.com/why-are-food-prices-rising-causes-of-food-price-inflation-3306099 (downloaded 14 March 2023)

[55] FAO: Policy Brief-Food Security. FAO's Agriculture and Development Economics Division (ESA). 2006. https://www.fao.org/fileadmin/templates/faoitaly/documents/pdf/pdf_Food_Security_Cocept_Note.pdf (downloaded 13 March 2023)

[56] GORYŃSKA-GOLDMANN, E. – GAZDECKI, M. – REJMAN, K. – ŁABA, S. – KOBUS-CISOWSKA, J. – SZCZEPAŃSKI, K.: Magnitude, Causes and Scope for Reducing Food Losses in the Baking and Confectionery Industry – A Multi-Method Approach. Agriculture, 2021/10, p. 936, doi: 10.3390/agriculture11100936 (downloaded 16 March 2023)

[57] ŁABA, S. – CACAK-PIETRZAK, G. – ŁABA, R. – SUŁEK, A. – SZCZEPAŃSKI, K.: Food Losses in Consumer Cereal Production in Poland in the Context of Food Security and Environmental Impact. Agriculture, 2022/5, p. 665, doi: 10.3390/agriculture12050665 (downloaded 16 March 2023)

Food loss and waste happen in all the agriculture and food value chains: agricultural production stage (cultivation/breeding and storage), post-harvest processing (processing and distribution), retail and consumption. Some other severe social events can also affect food loss and waste, such as COVID-19[58,59] and the Russia-Ukraine war.[60] The effects of food loss and waste can be found in GHG emissions, waste of energy, waste of water, and lands.[61] It is very important to produce more food and realize sustainability, while utilizing the food resources, and reducing food loss and waste are also important to guarantee sustainable agriculture and food.

The risks and threats in agriculture and food are summarized in Table 3.

Risks and threats in agriculture and food	Reference
Declining production and increasing demand	7,21
Climate change or extreme weather	26
Limit of resources	3,4,19,24,27,31,33,36
Obstacles of the irresistible trend of digital agriculture	43,44,45,46
Security issues in agriculture 4.0	49,51,52
Agricultural commodities market fluctuations	53,54
Food loss and waste	57,58,59,61-68

Table 3: The risks and threats in agriculture and food
(Author's own edition)

3.8. Threats to agriculture and food, but not a trend

Some temporary, but profound global or regional events bring security issues, and so does the agricultural and food security, such as epidemics and conflicts.

[58] Brenna, Ellison – Kalaitzandonakes, Maria: Food Waste and Covid-19: Impacts along the Supply Chain. farmdoc daily, Sep. 2020. https://farmdocdaily.illinois.edu/2020/09/food-waste-and-covid-19-impacts-along-the-supply-chain.html (downloaded 26 October 2022)

[59] FAO: Covid-19 FLW related readings –| Community of Practice on food loss reduction (CoP) – Food and Agriculture Organization of the United Nations – Food Loss Reduction CoP – Food and Agriculture Organization of the United Nations. https://www.fao.org/food-loss-reduction/resources/covid-19-flw-related-readings/en/ (downloaded 08 January 2023)

[60] Nasir, M. A. – Nugroho, A. D. – Lakner, Z.: Impact of the Russian–Ukrainian Conflict on Global Food Crops. Foods, 2022/19, p. 2979, doi: 10.3390/foods11192979 (downloaded 16 March 2023)

[61] How will Russia's invasion of Ukraine affect global food security? International Food Policy Research Institute, 24 February 2022. https://www.ifpri.org/blog/how-will-russias-invasion-ukraine-affect-global-food-security (downloaded 27 May 2022)

In the year 2023, we are paying the consequences of COVID-19, and suffering soaring food prices, due to the ongoing war in world food supply countries. Fortunately, these temporary threats will not be the future agriculture and food trend.

3.9. COVID-19

The first cases of COVID-19 happened at the end of 2019[62] and broke out globally at the begging of 2020,[63,64] which seriously interrupted all industrial and agricultural activities.[65,66] Ultimately, huge food loss, waste, and food security issues came with COVID-19. During the pandemic time, the pandemic measurements and effects have challenged agriculture from both supply and demand[67,68] and the agricultural share in the economy.[69] From the point of view of transportation, the influence of COVID-19 on agriculture is a shortage of empty non-refrigerated marine shipping containers, closure of temporary processing plants, and increasing demand for food and grocery delivery. But the agricultural supply chain cost could reduce, due to the lower transportation demand from other sectors.

3.10. War between Russia and Ukraine

The ongoing Russia-Ukraine war between two important world food and fertilizer suppliers and gas suppliers (Russia) broke out in February 2022, and put agriculture and food security closer to the cliff.[70] Black Sea area, the "World's bread basket," including Russia and Ukraine, started to function three decades ago,[71] but now it is the cause of soaring food prices and a food security crisis, due to the Russia-

[62] WHO Timeline: COVID-19. https://www.who.int/news/item/27-04-2020-who-timeline---covid-19 (downloaded March 07, 2023).

[63] FAO: Stop food loss and waste. For the people. For the planet. FAO, 2021. https://www.fao.org/3/cb6236en/cb6236en.pdf (downloaded 13 March 2023)

[64] International Day Food Loss and Waste – Technical Platform on the Measurement and Reduction of Food Loss and Waste – Food and Agriculture Organization of the United Nations. FoodLossWaste, 2022. https://www.fao.org/platform-food-loss-waste/flw-events/international-day-food-loss-and-waste/en (downloaded 11 November 2022)

[65] BRENNA– KALAITZANDONAKES op. cit.

[66] FAO: Covid-19 FLW related readings op. cit.

[67] GRAY, R. S.: Agriculture, transportation, and the COVID-19 crisis. Canadian Journal of Agricultural Economics/Revue canadienne d'agroeconomie, 2020/2, pp. 239-243, doi: 10.1111/cjag.12235 (downloaded 16 March 2023)

[68] ROUBÍK, H. et al.: Current coronavirus crisis and past pandemics – What can happen in post-COVID-19 agriculture? Sustainable Production and Consumption, March 2022, pp. 752-760, doi: 10.1016/j.spc.2022.01.007 (downloaded 16 March 2023)

[69] BECKMAN, J. – COUNTRYMAN, A. M.: The Importance of Agriculture in the Economy: Impacts from COVID-19. American Journal of Agricultural Economics, 2021/5, pp. 1595-1611, doi: 10.1111/ajae.12212 (downloaded 16 March 2023)

[70] NASIR – NUGROHO – LAKNER op. cit.

[71] GHOSH, P. R. – SHARMA, S. B. – HAIGH, Y. T. – EVERS, A. L. B. – HO, G.: An overview of food loss and waste: Why does it matter? Cosmos, 2015/1, pp. 89-103, doi: 10.1142/S0219607715500068 (downloaded 16 March 2023)

Ukraine war.[72,73] And the international sanctions on Russia also influenced heavily on the food export and import and other agricultural materials, such as fertilizer, seeds and pesticides.[74] Other threats to agriculture and food, but not trend agriculture and food, are summarized in.

Other threats to agriculture and food, but not a trend	**Reference**
COVID-19	63,64,74-76
Russia-Ukraine war	65,66,79,81,82

Table 4: Other threats to agriculture and food, but not trend agriculture and food
(Author's own edition)

To understand the risks and trends of agriculture and how important it is in the agriculture and food value chain, and the nexus between global security changes and risks and trends in agriculture, we summarized in Table 5 and Figure 3.

Agriculture and food value chain	**Risks and threats**						
Agriculture production	Future production and demand	Climate change	Limit resources	Digital agriculture obstacles	Digital security issues	Market fluctuation	Food loss and waste
Food processing	Future production and demand		Limit resources	Digital agriculture obstacles	Digital security issues	Market fluctuation	Food loss and waste
Distribution	Future production and demand	Climate change	Limit resources				Food loss and waste
Retail and food service	Future production and demand		Limit resources			Market fluctuation	Food loss and waste
Consumption	Future production and demand					Market fluctuation	Food loss and waste

Table 5: The summary of risks and threats in agriculture in different value chain steps
(Author's own edition)

[72] THUKRAL, N.: World food supplies at risk as Russia withdraws from Black Sea deal. Reuters, 31 October 2022. https://www.reuters.com/world/world-food-supplies-risk-russia-withdraws-black-sea-deal-2022-10-31/ (downloaded 16 March 2023)

[73] Millions more children could face hunger crisis if Black Sea grain deal not renewed. Save the Children International, 08 March 2023. https://www.savethechildren.net/news/millions-more-children-could-face-hunger-crisis-if-black-sea-grain-deal-not-renewed (downloaded 16 March 2023)

[74] The importance of Ukraine and the Russian Federation for global agricultural markets and the risks associated with the current conflict. FAO, March 2022, https://www.fao.org/3/cb9236en/cb9236en.pdf (downloaded 16 March 2023)

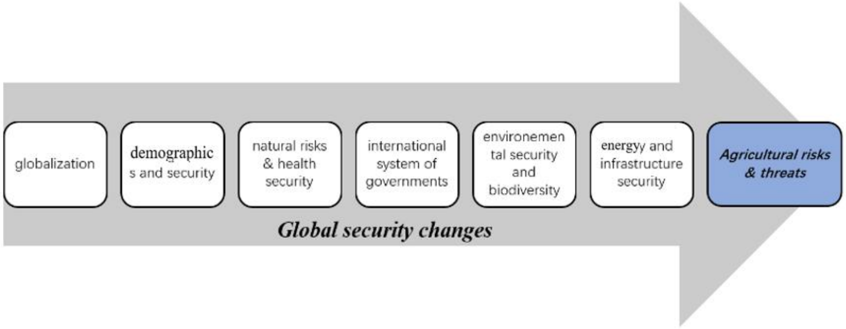

globalization
demographics and security
natural risks & health security
international system of governments
environemental security and biodiversity
energyy and infrastructure security
Agricultural risks & threats
Global security changes

Figure 3: the risks and threats in agriculture and food in the face of global security changes and trends
(Author's own edition)

As mentioned above, we can see the meeting points between global security trends and agricultural threats and risks.

3.11. The interesting positive aspect of global warming on agriculture

The agriculture faces such challenges and risks that can be considered to be as global security changes as well. However, we cannot ignore that there is also something "positive" from the aspect of global security trends in agriculture. For example, global warming makes it possible for the Arctic[75,76,] to be navigable, because the increasing temperature makes the ice melt in the Arctic. Therefore, the logistics or shipment between Asian and European countries is shorter and cheaper, such as China, South Korea, Japan, the UK, Norway, etc.[77,78]. The journey between Norway and South Korea along Russia's northern coast was 19 days, saving 30% more time than traditional travel through the Suez Canal in 2017. In recent decades, the average temperature increased by 2.5°C, and if this rate remains, the navigable time in the Arctic will increase from two months of the year by 2030 to three months of the year by 2040.

[75] TORRENT, Jordi: New Arctic routes: breaking the ice of North Pole shipping. PierNext, 04 April 2019, https://piernext.portdebarcelona.cat/en/logistics/new-arctic-routes-breaking-the-ice-of-north-pole-shipping/ (downloaded 16 March 2023)

[76] LEPAN, Nicolas: The final frontier: how Arctic ice melting is opening up trade opportunities. World Economic Forum, 13 February 2020, https://www.weforum.org/agenda/2020/02/ice-melting-arctic-transport-route-industry/ (downloaded 16 March 2023)

[77] MORIKAWA, Shohei – OGAWA, Tomoyo – KIDA, Kazuhiro – MIYASHITA, Hiroyuki – YASUDA, Shohei –YAMADA, Toru – KATO, Hiroya: How the Northern Sea Route will change the world's major traffic flows. Nikkei Asia, 2021. https://vdata.nikkei.com/en/newsgraphics/northern-sea-route/ (downloaded 16 March 2023)

[78] JAKOBSON, Linda: China prepares for an ice-free arctic. SIPRI Insights on Peace and Security, 2010/2.

4. Discussion

4.1. Implications

As regards the global security regarding agriculture and food security, we found that in the light of the global view, the most agricultural risks and threats trends are related to it, such as globalization, demographics and security, natural risks, and health security (limit of resources[79,80]), international system of governments, environmental security and biodiversity (climate change or extreme weather), energy and infrastructure security. Additionally, the future agricultural production and demand,[81] obstacles to irresistible digital agriculture,[82,83] security issues in agriculture 4.0,[84,85] market fluctuations[86,87,88] and food security issues (food loss and waste)[89,90] are also under agricultural risks and threats trend. The other two points, which are temporary influencing factors in agriculture but not trends, belong to the global security change and trend category, natural risks (COVID-19[91]) and post-cold war security characteristics (Russia-Ukraine war[92,93]). If global warming is continuously increasing, there will be more positive events to have a short supply chain, due to the Arctic ice melting.[94,95,96,97]

4.2. Limitations and directions for future research

We argued that there are two basic points (start point and end point) to realize sustainable agriculture and food development: to produce more food and utilize/optimize agricultural and food products or reduce food loss and waste. Firstly, the way to produce more for future generations is to adopt digital tools, such as robotics, AI, IoT, etc. However, the unclear question is what are the determinant and supporting factors for farmers to perceive and use these digital agricultural tools.

[79] BALL op. cit.

[80] Challenges for modern agriculture. op. cigt.

[81] World population projected to reach 9.8 billion in 2050, and 11.2 billion in 2100. United Nations, https://www.un.org/en/desa/world-population-projected-reach-98-billion-2050-and-112-billion-2100 (downloaded 26 October 2022)

[82] SOMOSI, S. – SZÁMFIRA op. cit.

[83] Digital Agricultural Academy of Hungary to take farmers into new age. op.cit.

[84] ABBASI – MARTINEZ – AHMAD op. cit.

[85] FERRAG – SHU – FRIHA – YANG op. cit.

[86] FAO publications catalogue 2022. op. cit.

[87] CHAUDHRY – SULEMAN – BHATTI – ULLAH op.cit.

[88] AMADEO op. cit.

[89] GORYŃSKA-GOLDMANN – GAZDECKI – REJMAN – ŁABA – KOBUS-CISOWSKA – SZCZEPAŃSKI op. cit.

[90] ŁABA – CACAK-PIETRZAK – ŁABA – SUŁEK – SZCZEPAŃSKI op. cit.

[91] BRENNA – KALAITZANDONAKES op. cit.

[92] NASIR – NUGROHO – LAKNER op. cit.

[93] How will Russia’s invasion of Ukraine affect global food security? op. cit.

[94] TORRENT op. cit.

[95] LEPAN op. cit.

[96] MORIKAWA – OGAWA – KIDA – MIYASHITA – YASUDA –YAMADA – KATO op. cit.

[97] JAKOBSON op. cit.

On the other hand, what is the consumers' reorganizational level of food security, how to reduce food loss and waste, or how to implement the food loss and waste measurements at public and individual level? We suggest that future researchers could use Roger's theory of Diffusion of Innovation[98,99] and the de-growth theory[100,101] to investigate the powers to enter the digitalization era.

5. Conclusion

In our secondary research review, we used content analysis as research methodology, based on the theory of value chain and the suggestions from the book; "The five central pillars of European security", which revealed that global security changes and trends have been increasing since 2007, and they are doing the same more or less in the year of 2023, compared to 2007. And most of the risks and trends in agriculture and food are related to global security changes and trends. For example, the main seven risks and threats trends in the agriculture and in the food value chain are; future production and demand, climate change, limited resources, digital agriculture obstacles, digital issues, market fluctuation, and food loss and waste, which are across all the value chain steps (agriculture production, food processing, distribution, retail and food service and consumption). However, we have not surprisingly concluded that most of the agricultural risks and threats are found from the main global security changes, such as globalization, demographics and security, international systems of government, environmental security and biodiversity, and energy and infrastructure security (described from the viewpoint of global security changes). We appealed to both individual and public sectors to highlight the risks and threats in agriculture, which we prove that they are important from the standpoint of national and global security.

[98] Diffusion of Innovation Theory. https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behavioralchangetheories/behavioralchangetheories4.html (downloaded 17 October 2022)

[99] ROGERS, E.: The diffusion of innovations model. Nato Asi Series D Behavioural And Social Sciences, 1993.

[100] TAKÁCS-GYÖRGY, Katalin – TAKÁCS, István: What makes the society better if agriculture is precision? – by the thoughts of the "de-growth" theory. Towards sustainable agricultural and biosystems engineering, 2017, pp. 47-62

[101] PIPER, K.: Can we save the planet by shrinking the economy? Vox, 03 August 2021, https://www.vox.com/future-perfect/22408556/save-planet-shrink-economy-degrowth (downloaded 28 February 2023)

Bibliography:

- ABBASI, R. – MARTINEZ, P. – AHMAD, R.: The digitization of agricultural industry – a systematic literature review on agriculture 4.0. Smart Agricultural Technology, 2022/2, p. 100042, doi: 10.1016/j.atech.2022.100042 (downloaded 16 March 2023)
- AGRIMONTI, C. – LAURO, M. – VISIOLI, G.: Smart agriculture for food quality: facing climate change in the 21st century. Critical Reviews in Food Science and Nutrition, 2021/6, pp. 971-981, doi: 10.1080/10408398.2020.1749555 (downloaded 16 March 2023)
- AMADEO, Kimberly: Why Food Prices Are Rising, Recent Trends, and 2021 Forecast – 5 Causes of High Food Prices. The Balance, 15 March 2022, https://www.thebalancemoney.com/why-are-food-prices-rising-causes-of-food-price-inflation-3306099 (downloaded 14 March 2023)
- BABOS, T.: A biztonság globális és európai összefüggései. Hadtudomány, 2019/4, pp. 16-29
- BABOS, T.: The five central pillars of European security. NATO Public Diplomacy Division – Strategic and Defense Research Center – NATO School, 2007.
- BALL, M.: Digital Farming: Driving productivity and a more sustainable way of farming. www.euractiv.com, October 08, 2019. https://www.euractiv.com/section/agriculture-food/video/digital-farming-driving-productivity-and-a-more-sustainable-way-of-farming/ (downloaded 26 October 2022)
- BALL, M.: Digital Farming: Driving productivity and a more sustainable way of farming. www.euractiv.com, 08 October 2019, https://www.euractiv.com/section/agriculture-food/video/digital-farming-driving-productivity-and-a-more-sustainable-way-of-farming/ (downloaded 26 October 2022)
- BASSO B. – ANTLE, J.: Digital agriculture to design sustainable agricultural systems. Nature Sustainability, 2020/4, pp. 254-256, doi: 10.1038/s41893-020-0510-0 (downloaded 16 March 2023)
- BECKMAN, J. – COUNTRYMAN, A. M.: The Importance of Agriculture in the Economy: Impacts from COVID-19. American Journal of Agricultural Economics, 2021/5, pp. 1595-1611, doi: 10.1111/ajae.12212 (downloaded 16 March 2023)
- BUCHANAN, Kallee – MURPHY, Tanya: What the John Deere tractor hack reveals about cyber threats to food supply. ABC News, 23 August 2022, https://www.abc.net.au/news/rural/2022-08-24/tractor-hack-reveals-food-supply-vulnerable/101360062 (downloaded 14 March 2023)
- CHAI, Wesley: What is a value chain and why is it important? SearchCIO, Feb. 2021. https://www.techtarget.com/searchcio/definition/value-chain (downloaded 29 November 2022)

- Challenges for modern agriculture, Syngenta, https://www.syngenta.com/en/innovation-agriculture/challenges-modern-agriculture (downloaded 26 October 2022)

- CHANG, J.: 10 Cybersecurity Trends for 2022/2023: Latest Predictions You Should Know. Financesonline.com, 08 November 2019. https://financesonline.com/cybersecurity-trends/ (downloaded 14 March 2023)

- CHAUDHRY, Ifra – SULEMAN, Raheel – BHATTI, Adrish – ULLAH, Inam: Review: Food price fluctuations and its influence on global food market. Annals of Social Sciences and Perspecitve, 2021/1, pp. 21-33, doi: 10.52700/assap.v2i1.33 (downloaded 16 March 2023)

- Diffusion of Innovation Theory. https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behavioralchangetheories/behavioralchangetheories4.html (downloaded 17 October 2022)

- Digital Agricultural Academy of Hungary to take farmers into new age. https://www.freshplaza.com/latin-america/article/9428745/digital-agricultural-academy-of-hungary-to-take-farmers-into-new-age/ (downloaded 04 October 2022)

- Ellison, Brenna – Kalaitzandonakes, Maria: Food Waste and Covid-19: Impacts along the Supply Chain. farmdoc daily, Sep. 2020. https://farmdocdaily.illinois.edu/2020/09/food-waste-and-covid-19-impacts-along-the-supply-chain.html (downloaded 26 October 2022)

- FAO Cereal Supply and Demand Brief – World Food Situation – Food and Agriculture Organization of the United Nations. 03 March 2023. https://www.fao.org/worldfoodsituation/csdb/en/ (downloaded 13 March 2023)

- FAO publications catalogue 2022. FAO, 2022. doi: 10.4060/cc2323en (downloaded 16 March 2023)

- FAO: Covid-19 FLW related readings – Community of Practice on food loss reduction (CoP) – Food and Agriculture Organization of the United Nations – Food Loss Reduction CoP – Food and Agriculture Organization of the United Nations. https://www.fao.org/food-loss-reduction/resources/covid-19-flw-related-readings/en/ (downloaded 08 January 2023)

- FAO: Policy Brief-Food Security. FAO's Agriculture and Development Economics Division (ESA). 2006. https://www.fao.org/fileadmin/templates/faoitaly/documents/pdf/pdf_Food_Security_Cocept_Note.pdf (downloaded 13 March 2023)

- FAO: Stop food loss and waste. For the people. For the planet. FAO, 2021. https://www.fao.org/3/cb6236en/cb6236en.pdf (downloaded 13 March 2023)

- FERRAG, M. A. – SHU, L. – FRIHA, O. – YANG, X.: Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions. IEEE/CAA Journal of Automatica Sinica, 2022/3, pp. 407-436, doi: 10.1109/JAS.2021.1004344 (downloaded 16 March 2023)

- GAGLIARDI, G. – COSMA, A. I. M. – MARASCO, F.: A Decision Support System for Sustainable Agriculture: The Case Study of Coconut Oil Extraction Process. Agronomy, 2022/1, doi: 10.3390/agronomy12010177 (downloaded 16 March 2023)

- GARZA-REYES, J. A.: Green lean and the need for Six Sigma. International Journal of Lean Six Sigma, 2015/3, pp. 226-248, doi: 10.1108/IJLSS-04-2014-0010 (downloaded 16 March 2023)

- GHOSH, P. R. – SHARMA, S. B. – HAIGH, Y. T. – EVERS, A. L. B. – HO, G.: An overview of food loss and waste: Why does it matter? Cosmos, 2015/1, pp. 89-103, doi: 10.1142/S0219607715500068 (downloaded 16 March 2023)

- GORYŃSKA-GOLDMANN, E. – GAZDECKI, M. – REJMAN, K. – ŁABA, S. – KOBUS-CISOWSKA, J. – SZCZEPAŃSKI, K.: Magnitude, Causes and Scope for Reducing Food Losses in the Baking and Confectionery Industry – A Multi-Method Approach. Agriculture, 2021/10, p. 936, doi: 10.3390/agriculture11100936 (downloaded 16 March 2023)

- GRAY, R. S.: Agriculture, transportation, and the COVID-19 crisis. Canadian Journal of Agricultural Economics/Revue canadienne d'agroeconomie, 2020/2, pp. 239-243, doi: 10.1111/cjag.12235 (downloaded 16 March 2023)

- How will Russia's invasion of Ukraine affect global food security? International Food Policy Research Institute, 24 February 2022. https://www.ifpri.org/blog/how-will-russias-invasion-ukraine-affect-global-food-security (downloaded 27 May 2022)

- International Day Food Loss and Waste – Technical Platform on the Measurement and Reduction of Food Loss and Waste – Food and Agriculture Organization of the United Nations. FoodLossWaste, 2022. https://www.fao.org/platform-food-loss-waste/flw-events/international-day-food-loss-and-waste/en (downloaded 11 November 2022)

- JAKOBSON, Linda: China prepares for an ice-free arctic. SIPRI Insights on Peace and Security, 2010/2.

- John Deere: About Our Company. https://www.deere.com/en/our-company/ (downloaded 14 March 2023).

- KIRK, Jeremy: Flaws in John Deere Systems Show Agriculture's Cyber Risk. 09 August 2021, https://www.bankinfosecurity.com/flaws-in-john-deere-systems-show-agricultures-cyber-risk-a-17240 (downloaded 14 March 2023)

- KOVÁCS, Imre – HUSTI, István: The role of digitalization in the agricultural 4.0 – how to connect the industry 4.0 to agriculture? Hungarian Agricultural Engineering, no. 2018/33 pp. 38-42, 2018, doi: 10.17676/HAE.2018.33.38 (downloaded 16 March 2023)

- ŁABA, S. – CACAK-PIETRZAK, G. – ŁABA, R. – SUŁEK, A. – SZCZEPAŃSKI, K.: Food Losses in Consumer Cereal Production in Poland in the Context of Food Security and Environmental Impact. Agriculture, 2022/5, p. 665, doi: 10.3390/agriculture12050665 (downloaded 16 March 2023)

- LEPAN, Nicolas: The final frontier: how Arctic ice melting is opening up trade opportunities. World Economic Forum, 13 February 2020, https://www.weforum.org/agenda/2020/02/ice-melting-arctic-transport-route-industry/ (downloaded 16 March 2023)

- Livestock and Landscapes. FAO, https://www.fao.org/3/ar591e/ar591e.pdf (downloaded 11 March 2023)

- MAFFEZZOLI, F. – ARDOLINO, M. – BACCHETTI, A. – PERONA, M. – RENGA, F.: Agriculture 4.0: A systematic literature review on the paradigm, technologies and benefits. Futures, Sep. 2022, p. 102998, doi: 10.1016/j.futures.2022.102998 (downloaded 16 March 2023)

- MAXIMILLIAN, J. – BRUSSEAU, M. L. – GLENN, E. P. – MATTHIAS, A. D.: Pollution and Environmental Perturbations in the Global System. Environmental and Pollution Science, Elsevier, 2019, pp. 457-476. doi: 10.1016/B978-0-12-814719-1.00025-2 (downloaded 16 March 2023)

- Millions more children could face hunger crisis if Black Sea grain deal not renewed. Save the Children International, 08 March 2023. https://www.savethechildren.net/news/millions-more-children-could-face-hunger-crisis-if-black-sea-grain-deal-not-renewed (downloaded 16 March 2023)

- MORIKAWA, Shohei – OGAWA, Tomoyo – KIDA, Kazuhiro – MIYASHITA, Hiroyuki – YASUDA, Shohei –YAMADA, Toru – KATO, Hiroya: How the Northern Sea Route will change the world's major traffic flows. Nikkei Asia, 2021. https://vdata.nikkei.com/en/newsgraphics/northern-sea-route/ (downloaded 16 March 2023)

- NASIR, M. A. – NUGROHO, A. D. – LAKNER, Z.: Impact of the Russian–Ukrainian Conflict on Global Food Crops. Foods, 2022/19, p. 2979, doi: 10.3390/foods11192979 (downloaded 16 March 2023)

- PIPER, K.: Can we save the planet by shrinking the economy? Vox, 03 August 2021, https://www.vox.com/future-perfect/22408556/save-planet-shrink-economy-degrowth (downloaded 28 February 2023)

- Precision Agriculture Technology, Benefits & Application. 20 April 2022. https://eos.com/blog/precision-agriculture/ (downloaded 13 March 2023)

- RAMANKUTTY, N. et al.: Trends in Global Agricultural Land Use: Implications for Environmental Health and Food Security. Annual Review of Plant Biology, 2018 April, pp. 789-815, doi: 10.1146/annurev-arplant-042817-040256 (downloaded 16 March 2023)

- RASMUSSEN, Wayne D. et al.: Origins of agriculture – The Americas. Britannica, Jul. 29, 2022. https://www.britannica.com/topic/agriculture (downloaded 13 March 2023)

- RODELL M. et al.: Emerging trends in global freshwater availability. Nature, May 2018, pp. 651-659, doi: 10.1038/s41586-018-0123-1 (downloaded 16 March 2023)

- ROGERS, E.: The diffusion of innovations model. Nato Asi Series D Behavioural And Social Sciences, 1993.

- ROUBÍK, H. et al.: Current coronavirus crisis and past pandemics – What can happen in post-COVID-19 agriculture? Sustainable Production and Consumption, March 2022, pp. 752-760, doi: 10.1016/j.spc.2022.01.007 (downloaded 16 March 2023)

- SHAO, L. – GONG, J. – FAN, W. – ZHANG, Z. – ZHANG, M.: Cost Comparison between Digital Management and Traditional Management of Cotton Fields—Evidence from Cotton Fields in Xinjiang, China. Agriculture, 2022/8, p. 1105, doi: 10.3390/agriculture12081105 (downloaded 16 March 2023)

- SOMA, T. – NUCKCHADY, B.: Communicating the Benefits and Risks of Digital Agriculture Technologies: Perspectives on the Future of Digital Agricultural Education and Training. Frontiers, 2021/6, p. 762201, doi: 10.3389/fcomm.2021.762201 (downloaded 16 March 2023)

- SOMOSI, S. – SZÁMFIRA, G.: Agriculture 4.0 in Hungary: The challenges of 4th Industrial Revolution in Hungarian agriculture within the frameworks of the Common Agricultural Policy. In: UDVARI, B. (Ed.): Proceedings of the 4th Central European PhD Workshop on Technological Change and Development. University of Szeged, Doctoral School in Economics, Szeged, pp. 162-189.

- STEMLER, Steve: An overview of content analysis. Practical Assessment, Research, and Evaluation, 2001/7. doi: 10.7275/Z6FM-2E34 (downloaded 16 March 2023)

- Sustainable and Digital Agriculture – United Nations Development Programme. UNDP, https://www.undp.org/sgtechcentre/sustainable-and-digital-agriculture-1 (downloaded 26 October 2022)

- TAKÁCS-GYÖRGY, Katalin – TAKÁCS, István: What makes the society better if agriculture is precision? – by the thoughts of the “de-growth” theory. Towards sustainable agricultural and biosystems engineering, 2017, pp. 47-62,

- TAKÁCSNÉ GYÖRGY, K. et al.: Precision agriculture in Hungary: assessment of perceptions and accounting records of FADN arable farms. Studies in Agricultural Economics, 2018/1, pp. 47-54, doi: 10.7896/j.1717 (downloaded 16 March 2023)

- The Development of Agriculture. https://education.nationalgeographic.org/resource/development-agriculture (downloaded 13 March 2023)

- The importance of Ukraine and the Russian Federation for global agricultural markets and the risks associated with the current conflict. FAO, March 2022, https://www.fao.org/3/cb9236en/cb9236en.pdf (downloaded 16 March 2023)

- THUKRAL, N.: World food supplies at risk as Russia withdraws from Black Sea deal. Reuters, 31 October 2022. https://www.reuters.com/world/world-food-supplies-risk-russia-withdraws-black-sea-deal-2022-10-31/ (downloaded 16 March 2023)

- TORRENT, Jordi: New Arctic routes: breaking the ice of North Pole shipping. PierNext, 04 April 2019, https://piernext.portdebarcelona.cat/en/logistics/new-arctic-routes-breaking-the-ice-of-north-pole-shipping/ (downloaded 16 March 2023)

- Types of Resources Class 8 Geography. https://www.excellup.com/ClassEight/sseight/reourceseight.aspx (downloaded 10 March 2023)

- UNEP: Facts about the nature crisis. UNEP–UN Environment Programme, Jul. 07, 2022. http://www.unep.org/facts-about-nature-crisis (downloaded 11 March 2023)

- WHO Timeline: COVID-19. https://www.who.int/news/item/27-04-2020-who-timeline-covid-19 (downloaded March 07, 2023).

- World population projected to reach 9.8 billion in 2050, and 11.2 billion in 2100. United Nations, https://www.un.org/en/desa/world-population-projected-reach-98-billion-2050-and-112-billion-2100 (downloaded 26 October 2022)

- World population projected to reach 9.8 billion in 2050, and 11.2 billion in 2100. United Nations, https://www.un.org/en/desa/world-population-projected-reach-98-billion-2050-and-112-billion-2100 (downloaded 26 October 2022)

- XIN, L. – FAN, Y. Z. – TAN, M. H. – JIANG, L. G.: Review of Arable Land-use Problems in Present-day China. AMBIO: A Journal of the Human Environment, 2009/2, pp. 112-115, doi: 10.1579/0044-7447-38.2.112 (downloaded 16 March 2023)

ANDRÁS ÁRPÁD NOVÁK[1]

THE CHALLENGES OF THE SAHEL AND HUNGARY'S PRESENCE AND ASSISTANCE IN CHAD

Abstract

The countries in the Sahel region have been facing major security and humanitarian crises for a long time. The region's countries are dealing with several security challenges due to political turmoil, coups, and attempted coups. The article focuses on Chad, one of the most stable countries in the region, and introduces the Hungary Helps program as a way to provide local aid in various forms. The article also discusses the issue of illegal migration to Europe and highlights the importance of stability in the Sahel region.

Keywords: Chad, Sahel, terrorism, migration, Hungary Helps

Introduction

The countries in the Sahel region have been grappling with major security and humanitarian crises for a long time. The region is facing terrorism, climate change, food insecurity, and other issues that have made it difficult to manage without international cooperation and assistance. In this article, we analyze the threat posed to Europe, specifically Hungary, by instability in the Sahel region. We also address how to help people there and ourselves.

The infiltration of terrorism and organized crime through migration is no longer just a theoretical threat to Europe, including Hungary, as developments in Africa have direct effects. The people of Europe are already experiencing the negative consequences of recent events.

In this article, I introduce the Hungary Helps Program for humanitarian aid alongside a military engagement in the Sahel.

Due to the Hungarian military's future involvement and assistance in the country, this article focuses on Chad, which is one of the poorest but most stable countries in the region. It is crucial for the stability of the region that Chad does not get dragged into the political unrest that has become a trend in neighboring countries. Chad is burdened with an influx of refugees from neighboring countries, particularly Sudan. The situation has already turned into a humanitarian crisis. The nation requires international aid to address the issue.

[1] ORCID: 0000-0002-2206-0181

Chad, a former French colony, has maintained close ties with France and is considered its last ally in the Sahel. The two nations collaborate on multiple military operations in the area. The most recent development is the replacement of the French army from Niger to Chad.[2]

Alongside French cooperation, Chad seeks to strengthen and diversify its external relations. As a result of these objectives, in January 2023, it signed a Chad aims to strengthen and diversify external relations. In January 2023, it signed a Memorandum of Understanding with Saudi Arabia to enhance cooperation, and *"[...] mainly the development of cooperation in military training and exercises, logistical support, military medical services, cultural and social activities, and awareness in combating terrorism."*[3]

The Wagner Group, a Russian mercenary organization, has expanded rapidly in Africa's Sahel region. According to experts from the Center for Strategic and International Studies (CSIS), Russian private military companies will have signed 16 agreements with governments in sub-Saharan Africa by 2021. In its attempts to expand, Chad could be its next target. *"Unlike other sub-Saharan countries, which have invited Wagner mercenaries, Chad could be Wagner's first attempt at overthrowing a sitting government, according to analysts."*[4]

The Sahel region

The Sahel region stretches from the Atlantic Ocean in the west to the Red Sea in the east and is home to diverse ethnic groups, languages, and cultures but remains one of the poorest regions in Africa. Countries in the region include Burkina Faso, Mali, Mauritania, Niger, Nigeria, Senegal, Sudan, and Chad. Some studies also include Northern Ethiopia and Eritrea.

[2] VALADE, Carol: Driven out of Niger, the French army takes refuge in Chad, Paris's last ally in the Sahel. Le Monde, 17 October 2023, https://www.lemonde.fr/en/le-monde-africa/article/2023/10/17/driven-out-of-niger-the-french-army-takes-refuge-in-chad-paris-s-last-ally-in-the-sahel_6179914_124.html (downloaded 9 November 2023)

[3] Saudi Press Agency: KSA, Chad sign Cooperation MOU in defense field. Saudi Press Agency. 2023, https://www.spa.gov.sa/w1844310?lang=en&newsid=2419918 (downloaded 18 November 2023)

[4] African Defense Forum: Wagner Group Targets Chad for Sahel Expansion. African Defense Forum. 28 March 2023, https://adf-magazine.com/2023/03/wagner-group-targets-chad-for-sahel-expansion/ (downloaded 18 November 2023)

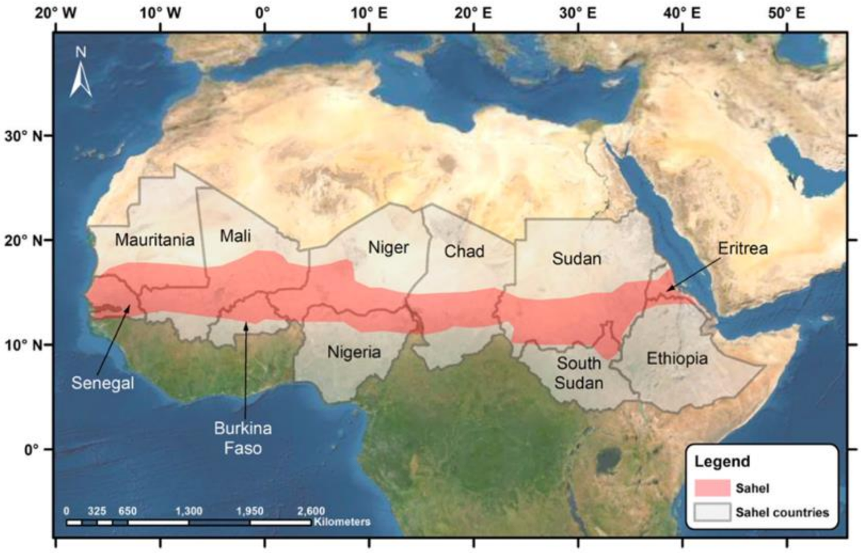


Figure 1: Map of the Sahel region and countries[5]

The security situation in the region

The region's countries face several security challenges in the shadow of the political turmoil, coups, and attempted coups[6], the effects of which pose a common threat to the countries of the Sahel region.

The instability of the region is demonstrated by the fact that in the last three years alone, there have been several successful military takeovers in the region, such as in Mali, Burkina Faso, Sudan, Chad, and Niger.[7]

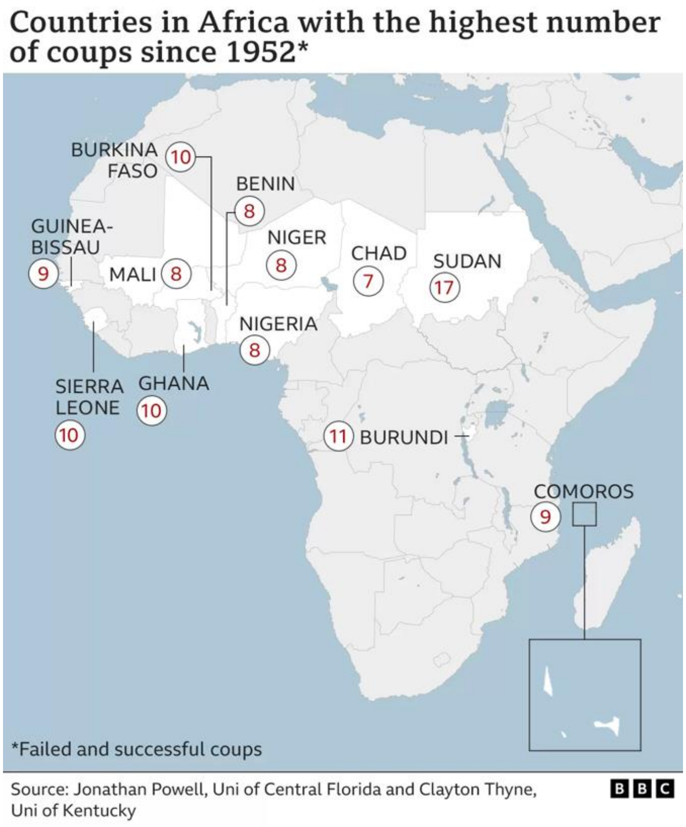
As shown in Figure 2, since 1952, there have been several successful and unsuccessful coups in the region. Sudan has had the highest number of coups and coup attempts, 17 in total, of which six were successful. [8]

[5] ALL-SAIDI, Mohammad – GAYOUM SAAD, Suhair A. – ELAGIB, Nadir A.: From scenario to mounting risks: COVID-19's perils for development and supply security in the Sahel. Springer, 2022, p. 25, DOI: 10.1007/s10668-022-02303-9 (downloaded 18 November 2023)

[6] POWELL, Jonathan M. – THYNE, Clayton L.: Global instances of coups from 1950 to 2010. A new dataset. Journal of Peace Research, 2011/2. pp. 249-259

[7] AJLABS: Mapping Africa's coups d'etat across the years. Al Jazeera. 30 August 2023, https://www.aljazeera.com/news/2023/8/30/mapping-africas-coups-detat-across-the-years (downloaded 24 October 2023)

[8] MWAI, Peter: Gabon coup: The latest in a series of military takeovers on the continent. BBC, 30 August 2023, https://www.bbc.com/news/world-africa-46783600 (downloaded 721 October 2023)



Countries in Africa with the highest number of coups since 1952*

*Failed and successful coups

Source: Jonathan Powell, Uni of Central Florida and Clayton Thyne, Uni of Kentucky

Figure 2: Countries in Africa with the highest number of coups since 1952[9]

In Mali, the escalation of unrest, coups, and coup attempts in the early 2020s led to the withdrawal of German troops in 2023, following the relocation of French troops in the country. Following a decision by the UN committee, the peacekeeping troops stationed there will also begin their withdrawal and leave the country by the 31st of December.[10]

[9] Ibid.

[10] Euronews – MTI: Kivonulnak az ENSZ-békefenntartók Maliból. Euronews.com 1 July 2023, https://hu.euronews.com/2023/07/01/kivonulnak-az-ensz-bekefenntartok-malibol (downloaded 21 October 2023)

The 12 camps of the UN MINUSMA[11] mission and a temporary operating base will be closed and handed over to the transitional authorities, and 12 947 uniformed personnel will leave the country.[12] The private military company, the Russian mercenary Wagner Group, currently provides security in Mali.[13]

The military leadership's failure to prevent the spread of extremist groups from 2013 to 2020 has made Mali a significant source of security risks in the region.[14] The military junta plans to hold elections in February 2024 to transfer power back to civilians.

Jonathan Powell, a US researcher on coups and former fellow at the University of Central Florida, pointed out that "The underlying causes of coups are present and getting worsening. Until these domestic dynamics improve, or regional or global actors can provide solutions, there is no reason to think coups should go away."[15]

G5 for development and security

The Group of Five (G5 Sahel) is a regional intergovernmental organization that was established in 2014 by Burkina Faso, Chad, Mali, Mauritania, and Niger to promote development and security in the Sahel region. In February 2017, the G5 Sahel took a further step and created the Joint Force to combat armed and violent extremist groups and address the worsening security situation in the area.[16]

Climate change poses a serious threat to the region, including land, vegetation, water resources, and food systems. The rising frequency of droughts, desertification, and floods, along with the expected shortening of the rainy season, is further degrading these resources. The desertification of the region is one of the major consequences of climate change, which will significantly impact the food supply in the area.[17] As a result of climate change, the Sahara is expanding, leading to a decrease in cultivation area and available land for the population.

[11] The United Nations: Multidimensional Integrated Stabilization Mission in Mali. https://minusma.unmissions.org/en/history (downloaded 8 November 2023)

[12] UN News: Mali: ‘MINUSMA is leaving, but the UN is staying’, Mission chief says. United Nations Africa renewal. 2023. augusztus 28. https://www.un.org/africarenewal/magazine/august-2023/mali-‘minusma-leaving-un-staying’-mission-chief-says (downloaded 22 October 2023)

[13] PÓSA, Tibor: Búcsú Malitól: az unió és a franciák után a németek is csomagolnak. Mandiner.hu, 19 August 2022, https://mandiner.hu/makronom/2022/08/mali-francia-nemet-katona-wagner-csoport-posa-tibor-makronom (downloaded 10 November 2023)

[14] SCHEFFER Joakim: Ha megtehetik, miért ne? – ezért van egyre több puccs Nyugat-Afrikában. Magyar Nemzet. 11 August 2023, https://magyarnemzet.hu/lugas-rovat/2023/08/ha-megtehetik-miert-ne-ezert-van-egyre-tobb-puccs-nyugat-afrikaban (downloaded 9 November 2023)

[15] DUZOR, Megan – WILLIAMSON, Brian: COUPS IN AFRICA. VOA News, 3 October 2023, https://projects.voanews.com/african-coups/ (downloaded 25 October 2023)

[16] Interpol [n.d.]: G5 Sahel. https://www.interpol.int/es/Delitos/Terrorismo/Proyectos-de-lucha-contra-el-terrorismo/G5-Sahel (downloaded 26 October 2023)

[17] International Fund for Agricultural Development (IFAD): Sahel. https://www.ifad.org/en/web/operations/regions/wca/sahel (downloaded 26 October 2023)

Political conflict and food insecurity have also made the Sahel the scene of various humanitarian crises, with millions of people needing assistance. The problem is exacerbated by the rapid population growth in the countries of the Sahel due to poor birth control and the influx of medicines from developed nations.
According to the UNHCR website, the figures for the refugee crisis in the Sahel are pretty telling. "As of 2023, more than 4.2 million people have been displaced across the region, and 3.7 million people are internally displaced, Furthermore, as of 2022 more than 10 million children need humanitarian assistance."[18]

The demographic explosion and climate change add to the Sahel region's instability and are also drastically straining the region's limited resources.

At the NATO Summit in June 2021, the Allies strongly expressed their alarm and deep concern regarding the situation in the Sahel region. The presence of jihadist and extremist groups remains a significant source of instability and poses severe security challenges and pressures on the region. The rise of extremist groups can be attributed to a number of factors, such as the lack of education, the absence of a social system, and underdeveloped infrastructure. Moreover, weak governance and tensions between different tribal and religious communities contribute to the strengthening of extremist organizations. These factors create a breeding ground for the recruitment of armed groups among communities that feel neglected by the authorities.[19]

Chad

The country is situated in the eastern region of Sahel and is recognized for its varied geography. It is the fifth largest nation in Africa. It was a French colony until it gained independence on 11th August 1960. The country has witnessed a long period of civil war and political instability since then. However, it has recovered and is now considered one of the most stable countries in the region.[20]

Based on the US government demographic estimates for 2014-15, 52.1% of Chad's population is Muslim.[21] Despite their presence, extremist Islamic fundamentalists do not have a significant following within the country.

There has been a significant population increase in recent decades. with the figures showing a population of 10.3 million [22] inhabitants in 2009, and 16.9 million inhabitants in a 2021 survey.

[18] The UN Refugee Agency [n.d. a]: SAHEL REFUGEE CRISIS. https://www.unrefugees.org/emergencies/sahel-crisis/ (downloaded 6 November 2023)

[19] BERGER, Chloé: NDC Policy Brief. Research Division – NATO Defense College, 22 December 2021, https://www.ndc.nato.int/news/news.php?icode=1644 (downloaded 6 November 2023)

[20] CIA: The World Factbook. Explore all countries – Chad. 2023, https://www.cia.gov/the-world-factbook/countries/chad/ (downloaded 25 October 2023)

[21] US Department of State: Report on International Religious Freedom: Chad. 2022, https://www.state.gov/reports/2022-report-on-international-religious-freedom/chad (downloaded 22 October 2023)

[22] BESENYŐ, János – HETÉNYI, Soma Ambrus – JAGADICS, Péter – RESPERGER, István: Országismertető: Csád. Sereg Szemle, Székesfehérvár, 2010

The CIA predicts that the population will reach 18.5 million in 2023.[23] As society continues to evolve, it is worth noting that currently, 65% of the population is under 25 years of age.[24]

In many African countries, families have up to 6-7 children. Chad follows this trend, with a median age of 16.1 years. This makes it one of the youngest countries in the world, alongside Niger, Uganda, Angola, and Mali.[25]

Chad's economic growth potential and international competitiveness are hindered by local obstacles, such as insufficient infrastructure and corruption. The high cost of importing and exporting often leads locals to resort to smuggling due to lengthy, slow administrative processes.[26] According to a 2015 study, the country earned over $11 billion from oil revenues but still cannot provide economic opportunities for its citizens.[27]

Food shortages and hunger in Chad

Food insecurity is a constant presence in extreme poverty. 165,080 people in Chad are severely undernourished, and 214,220 are moderately malnourished, according to a survey published by the Danube Institute. Compared to neighboring countries, Chad has an exceptionally high level of malnutrition.[28]

[23] CIA [n.d.]: The World Factbook. Country Summary – Chadk. https://www.cia.gov/the-world-factbook/countries/chad/summaries (downloaded 25 October 2023)

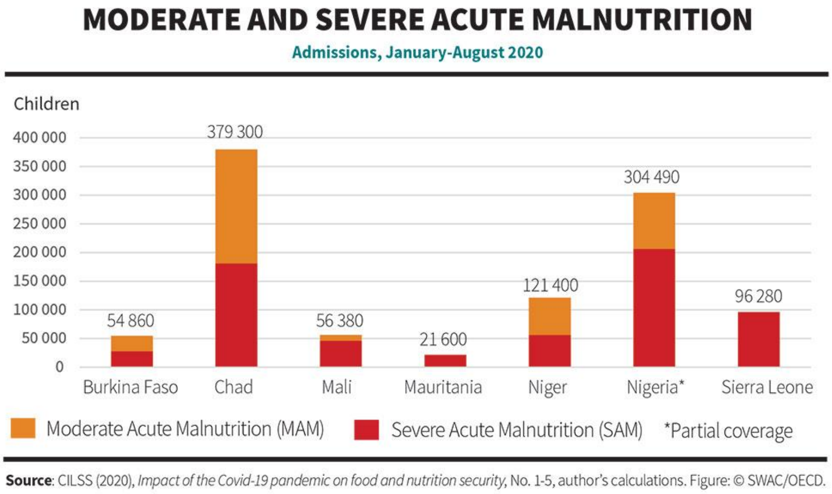
[24] United States Agency International Development (USAID)[n.d.]: Chad. https://www.usaid.gov/chad (downloaded 25 October 2023)

[25] WorldData.info: Median age by country. 2023, https://www.worlddata.info/average-age.php (downloaded 25 October 2023)

[26] Besenyő – Hetényi – Jagadics – Resperger op. cit.

[27] Hicks, Celeste: Chad and the West: Shifting Security Burden? Egmont Institute, 2015, http://www.jstor.org/stable/resrep06548 (downloaded 10 November 2023)

[28] Danube Institute: Egyre komolyabb kihívások jelentkeznek a Száhel-övezetben. 5 August 2023, https://danubeinstitute.hu/hu/blog/egyre-komolyabb-kihivasok-jelentkeznek-a-szahel-ovezetben (downloaded 10 November 2023)



Source: CILSS (2020), *Impact of the Covid-19 pandemic on food and nutrition security*, No. 1-5, author's calculations. Figure: © SWAC/OECD. Extract: SWAC/OECD (2020), Food and Nutrition Crisis 2020, Analyses & Responses, Maps & Facts, No. 3, November 2020.

Figure 3: Moderate and severe acute malnutrition[29]

The security situation in Chad

Migration

The security situation in the country is closely linked to the conflict in Sudan. Due to the ongoing civil war, hundreds of thousands of people have been forcibly displaced from the neighboring country to Chad.

Chad serves as both a country of transit for migration and a source country for emigrants.

There are one million forcibly displaced people in Chad, including 580,000 refugees from neighboring countries such as Sudan, the Central African Republic, and Cameroon, according to UNHCR. With the support of 40 NGOs and other UN agencies, UNHCR leads and coordinates refugee response to support the Chadian government.[30] *"The United Nations High Commissioner for Refugees (UNHCR) calls on the international community to urgently assist refugees in Chad, as the number of new arrivals has surpassed the 100,000 mark."*[31]

[29] RPCA – The food crisis prevention network: Moderate and severe acute malnutrition. 2020 November, https://www.food-security.net/en/map-library/prise-en-charge-de-la-malnutrition-aigue-severe-et-moderee/ (downloaded 28 November 2023)

[30] The UN Refugee Agency [n.d. b]: Chad. https://www.unhcr.org/countries/chad (downloaded 6 November 2023)

[31] The UN Refugee Agency (2023a): UNHCR urges for urgent support to Chad as refugee arrivals exceed 100,000. 2023. június 1. https://www.unhcr.org/africa/news/press-releases/unhcr-urges-urgent-support-chad-refugee-arrivals-exceed-100-000 (downloaded 9 November 2023)

Terrorist groups overshadowing the country

Chad is actively combating violent extremism, and the fight against terrorism and extremist groups represents one of its most significant challenges. A number of terrorist groups are active in the region, including Boko Haram, Al Shabab, Al Qaeda, and the African wing of ISIS.

Chad's security situation could be negatively affected by the fact that some of the weapons destined for Ukraine are already appearing on the African black market.[32] Boko Haram, which was initially active only in Nigeria, has now extended its terror activities to Chad. The proliferation of terrorist groups and criminal organizations is being facilitated by the porous borders of Chad, particularly around Lake Chad, making it difficult to secure the area.

Chad has a significant military presence in the region, boasting 33,250 active troops, which includes 350 members of the air force and 5,400 state security personnel.[33]

The Chadian forces coordinate with other regional countries to carry out counter-terrorism operations. In the effort to stabilize the region, Chad deployed 1,425 troops to Mali under MINUSMA,[34] and a total of 2,000 troops are being deployed to provide support for the MNJTF.[35] As a part of the G-5 Sahel Joint Force East Zone Command, 650 troops were deployed to Northern Chad. In addition, 1,200 troops were deployed to the tri-border region between Burkina Faso, Mali, and Niger, and 600 troops were contributed to the joint border security efforts with Sudan as part of the Chad-Sudan Mixed Force. In addition, it has deployed 1,200 troops to the Liptako-Gourma tri-border region between Burkina Faso, Mali, and Niger. Chad also supports the Chad-Sudan Mixed Force, contributing 600 troops to the joint border security efforts with Sudan.[36]

The Russian-Ukrainian war is also having a negative impact on the fight against terrorism on the African continent and on the financing of the G-5. Global powers have their attention on the ongoing Russia-Ukraine war and the consequent redeployment of resources. Moreover, the situation in the Gaza Strip is adding to the complexity, and it is crucial to stabilize and resolve the issues in Africa.

[32] CRI: Az Ukrajnának szánt fegyverek az afrikai feketepiacra kerülnek. China Radio International, 1 December 2022, https://hungarian.cri.cn/2022/12/01/ARTIzRKnLsy5UyFx7tlMWZBD221201.shtml (downloaded 10 November 2023)

[33] The International Institute for Strategic Studies: The Military Balance 2023. The International Institute for Strategic Studies, 2023. p. 442

[34] The United Nations: Multidimensional Integrated Stabilization Mission in Mali. https://minusma.unmissions.org/en/history (downloaded 8 November 2023)

[35] Multinational Joint Task Force, See: https://www.justice.gov/eoir/page/file/1292686/download (downloaded 8 November 2023)

[36] US Department of State: Bureau of counterterrorism. 2021, Country Reports on Terrorism 2021: Chad. https://www.state.gov/reports/country-reports-on-terrorism-2021/chad/ (downloaded 7 November 2023)

The impact of African migration on Europe

The influx of African migrants into Europe has led to a surge in illegal immigration facilitated by smugglers crossing the green borders.

The frequent and unchecked arrival of crowds in Europe has a hugely negative impact on the lives of its citizens. This can also lead to a feeling of insecurity among European residents. As a result, many countries have begun to reintroduce random border checks.[37]

It is worth considering whether ad-hoc monitoring, which is a great political communication tool, is enough to provide residents with real security, or whether it may give them a false sense of security without addressing the problem of insufficient screening. The European Union is currently focused on maintaining a prolonged war at a significant cost, but it has not yet recognized the importance of protecting its borders and its people.

It is particularly worrying that this trend is steadily increasing. A glaring recent example is the arrival of 8,500 new migrants in boats from Africa in just three days on the island of Lampedusa in southern Italy.[38] Furthermore, there needs to be a firm and decisive action on the arrival of the masses.

The threat of uncontrolled mass migration and the dramatic consequences of the infiltration of fundamentalist terrorists are already being seen in Western European countries. According to the European Parliament's website, "Jihadist terrorism remains the biggest threat to the EU, with more than twice as many terrorist attacks carried out in 2020 than failed."[39]

A few years ago, vehicles were driven into crowds as a means of intimidation, such as in the terrorist attack in Nice on 14 July 2016 that claimed 86 lives. The same year a hijacked truck was driven into the 2016 Berlin Christmas market, killing 12 people.[40]

[37] NÉMETH, Árpád: Sorra állítják vissza a határellenőrzést Európában. Index.hu, 1 October 2023, https://index.hu/kulfold/2023/10/01/hatarellenorzes-nemetorszag-lengyelorszag-csehorszag-szlovenia-horvatorszag-schengen/ (downloaded 7 November 2023

[38] HORVÁTH Ferenc: Lampedusa lakosai nem bírják tovább a migrációs nyomást. Euronews, 17 September 2023, https://hu.euronews.com/2023/09/17/lampedusa-lakosai-nem-birjak-tovabb-a-migracios-nyomast (downloaded 10 November 2023)

[39] Európai Parlament: Terrorizmus az EU-ban: támadások, halálesetek és letartóztatások 2020-ban. 20 August 2021, https://www.europarl.europa.eu/news/hu/headlines/society/20210628STO07262/terrorizmus-az-eu-ban-tamadasok-halalesetek-es-letartoztatasok-2020-ban (downloaded 23 October 2023)

[40] Index: A tömegbe hajtott egy kamion a berlini karácsonyi vásáron, 12 halott. Index.hu. 19 December 2016, https://index.hu/kulfold/2016/12/19/teherautoval_a_tomegbe_hajtottak_a_berlini_karacsonyi_vasaron/ (downloaded 8 November 2023)

Shortly before the writing of this article, on 16 October 2023. a terrorist rifle attack was carried out about 5 kilometers from the King Baudouin Stadium in Brussels, killing two fans wearing Swedish football jerseys.[41] The attack also affected the Belgium-Sweden European Championship qualifying match, which was abandoned at half-time at 1-1 at the request of the Swedish national team, and fans were not allowed to leave the stadium for a long time for security reasons. The perpetrator of the attack, a Tunisian man from the Schaerbeek district of Brussels, died of his injuries in hospital following a police operation to apprehend him. [42]

In addition to the current influx of uncontrolled migrants, the radicalization of first-, second, and third-generation refugees already living in Europe could pose an additional threat.

When the first generation of immigrants in a country face difficulty in finding their place, the resulting tension can linger. Furthermore, the authoritarian and religious upbringing they experienced at home can make it difficult for the second generation to assimilate into the dominant culture of their new country. As a result, young people in search of a sense of belonging and identity may feel like outsiders in their own country and may have an idealized view of their country of origin. These young people can become easy targets for terrorist organizations, particularly if they lack a clear sense of purpose and become ghettoized in large groups.[43]

International solutions and international presence

Threatening developments on the African continent and increasing migration could pose a real threat to Europe. The political situation in the Sahel region is becoming increasingly unstable. Unstable governments could lead to further civil wars in the region.

Back in 2015, Peter Maurer, the former head of the International Red Cross, had already drew attention to the refugee crisis in Chad and the need for more financial resources while the organization was helping on the ground.[44]

[41] ROBINSON, James: Brussels 'on highest terror alert' and football fans told to stay in the stadium after two shot dead. Skynews.com, 17 October 2023, https://news.sky.com/story/two-people-wearing-football-shirts-shot-dead-in-brussels-belgian-media-report-12985711 (downloaded 17 October 2023)

[42] Mandiner.hu: Iszlamista terror Brüsszelben, több halott – a belga rendőrség végzett az elkövetővel. Mandiner.hu 16 October 2023, https://mandiner.hu/kulfold/2023/10/breking-agyonlottek-ket-embert-brusszelben#google_vignette (downloaded 8 November 2023)

[43] BÁCS, Zoltán György: A radikalizáció és a terrorizmus kapcsolata, egyes formái, gondolatok a megelőzés lehetséges perspektíváiról. Nemzetbiztonsági Szemle, 2017/1, https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1721 (downloaded 8 November 2023)

[44] Európai Parlament: A Vöröskereszt Nemzetközi Bizottságának elnöke több segítséget vár az EU-tól. 28 May 2015, https://www.europarl.europa.eu/news/hu/headlines/eu-affairs/20150526STO59664/a-voroskereszt-nemzetkozi-bizottsaganak-elnoke-tobb-segitseget-var-az-eu-tol (downloaded 7 November 2023)

Following his visit to Chad in early September 2023, Filippo Grandi, UN High Commissioner for Refugees, said that the international community's assistance is insufficient to deal with the influx of refugees into the country.[45]

World Bank announced a new aid package of USD 340 million, but experts say that at least USD 1 billion would be needed to tackle this crisis.[46]

Hungarian solutions and Hungarian presence

„The Hungary Helps Agency was established on 14th April 2019 based on Act CXX of 2018 on the Hungary Helps Program. The Hungary Helps Agency is a governmental agency which works as a non-profit organization under the coordination of the Ministry of Foreign Affairs and Trade of Hungary."[47] The Program believes in helping people locally and along the vision of a *"[...] basic principle that help should go where the trouble is, not bring the trouble here."*[48] Thanks to this program, tens of thousands of people have been able to remain in their home country rather than migrating elsewhere.

In addition to international organizations, Hungary has also become active in the region. In Chad, Azbej Tristan, the State Secretary responsible for implementing the Program, said that *"under the program, a Hungarian humanitarian medical mission has started work in Chad, helping refugees arriving in the country - and internally displaced people – while also providing medical training to local professionals. Joining the mission, a team from the Hungarian University of Agricultural and Life Sciences is exploring ways to create long-term food security"*.[49]

In addition, the Hungarian government is establishing a humanitarian and development center in Chad, in the country's capital N'Djamena. The center, part of the Hungary Helps Program, will bring humanitarian and development programs into the country and throughout the Sahel, helping to prevent humanitarian disasters and maintain stability.[50]

[45] Hirado.hu: Több humanitárius segélyt követelt az ENSZ főbiztosa a Csádba érkezett szudáni menekülteknek. Hirado.hu, 11 September 2023, https://hirado.hu/kulfold/cikk/2023/09/11/tobb-humanitarius-segelyt-kovetelt-az-ensz-fobiztosa-a-csadba-erkezett-szudani-menekulteknek (downloaded 7 November 2023)

[46] The UN Refugee Agency (2023b): UNHCR's Grandi praises Chad's role hosting Sudanese; more aid urgently needed. https://www.unhcr.org/uk/news/press-releases/unhcr-s-grandi-praises-chad-s-role-hosting-sudanese-more-aid-urgently-needed (downloaded 9 November 2023)

[47] The Hungary Helps Agency: https://hungaryhelps.gov.hu/hungary-helps-program-main-page/ (downloaded 28 November 2023)

[48] Magyar Hírlap: A Hungary Helps Program példaként szolgálhat más kormányoknak is. 9 March 2021, https://www.magyarhirlap.hu/kulfold/20210309-a-hungary-helps-program-peldakent-szolgalhat-mas-kormanyoknak-is (downloaded 7 November 2023)

[49] M1 Híradó: Magyarország a Száhel övezetben is segít a Hungary Helps programon keresztül. YouTube, 24 September 2023, https://www.youtube.com/watch?v=SM8eyDben6Q (downloaded 10 November 2023)

[50] Hungary Helps: Hungary Helps humanitárium fejlesztési központ nyílik Csádban. https://hungaryhelps.gov.hu/2023/10/11/hungary-helps-humanitarius-fejlesztesi-kozpont-nyilik-csadban/ (downloaded 24 October 2023)

The Hungary Helps program will receive additional support from the Hungarian Defense Forces starting in the spring of 2024. This proposal was approved by the Hungarian Parliament on November 6, 2023, after being proposed by the Minister of Defense. According to the agreement, a maximum of 200 Hungarian military personnel will be deployed to Chad.[51]

According to Niccolò Machiavelli, having knowledge of one's surroundings is crucial, and he emphasized the significance of experience. An experienced person can assess their environment at a single glance, while those who lack this competency may be slow or even unable to navigate their surroundings.[52] The mission in Chad presents a great opportunity for Hungarian soldiers to gain valuable experience in a foreign environment. It also enables them to contribute to the fight against terrorism and reduce migratory pressure on Europe. The experience gained during this mission will benefit the Hungarian Armed Forces in various areas.

Conclusion

The Sahel region has seen a significant rise in population, leading to a reduction in living space due to the expansion of the Sahara. Additionally, public security has deteriorated, making emigration a pressing migration challenge and a potential threat to Europe. The emergence and spread of extremist groups flowing into Europe are out of control due to illegal migration.

In addition, the brain drain in Africa could be a significant problem. If people with the right skills leave their home countries, who will be able to lead and solve problems locally in crisis situations? The region's stability is not only in the interest of the local people but also in the shared global interest.

Since the beginning of the migration wave, the Hungarian government has warned of the dangers of uncontrolled illegal migration and the effects it has on Europe.

The war between Israel and Hamas has sparked a rise in anti-Semitism in some European countries, in some places revealing the radicalization of unintegrated populations.

According to former Austrian Chancellor Sebastian Kurz, *"[...] when he had similar views to the Hungarian government on migration, he was portrayed as a Nazi and heartless, but now the same phrases are being uttered by left-wing parties. But it is important that actions follow words"*.[53]

[51] Honvedelem.hu: A parlament jóváhagyta a magyar katonai misszió indítását Csádba. 2023, https://honvedelem.hu/hirek/a-parlament-jovahagyta-a-magyar-katonai-misszio-inditasat-csadba.html (downloaded 8 November 2023)

[52] MACHIAVELLI, Niccolo: Beszélgetések Titus Livius első tíz könyvéről. In: MACHIAVELLI, Niccolo: Machiavelli Művei. Európa kiadó, 1978, pp. 87-442

[53] Magyar Nemzet: Sebastian Kurz: Az európai migrációs politika egyre több halált okoz Magyar Nemzet. 08 November 2023, https://magyarnemzet.hu/kulfold/2023/11/sebastian-kurz-az-europai-migracios-politika-egyre-tobb-halalt-okoz (downloaded 9 November 2023)

The current European procedure is insufficient in addressing the issue at hand. The Sahel problem requires a localized solution, and Europe should prioritize its security and the preservation of its culture, whether it involves conflict or illegal migration. In order to achieve this, effective security measures, border protection, deportation, and appropriate penalties and political actions should be implemented immediately. This is how the EU can contribute to the long-term safety of its citizens.

Despite being one of the most stable countries in the region, Chad risks facing several unpleasant outcomes in the absence of significant economic and military aid. On the one hand, the continuous influx of refugees from Sudan may destabilize governance, while on the other hand, the military coups and anarchy that have taken place in neighboring countries over the past year could spill over into Chad.

The rise and spread of terrorism around Lake Chad is a major concern. The region's poverty and lack of education provide terrorist groups with a favorable opportunity to recruit new members. What's more, the growth of online communication has made it easier for terrorist organizations to spread their radical views and reach more people. This poses a significant threat not only to Chad but also to many other countries in the region. It could have severe global repercussions if not addressed promptly.

Despite the ongoing coverage of the events in Ukraine since 2022 and the Gaza Strip since October 2023, there is a pressing global crisis in the Sahel that is being overlooked by the more developed nations of the world. It urgently needs attention and help, but unfortunately, it is taking a back seat.

Europe needs to find innovative approaches to combat terrorism and reduce migration flows. The global community must acknowledge that providing more on-the-ground assistance in conflict zones is imperative rather than relocating the problem to other regions.

Bibliography:

- African Defense Forum: Wagner Group Targets Chad for Sahel Expansion. African Defense Forum. 28 March 2023, https://adf-magazine.com/2023/03/wagner-group-targets-chad-for-sahel-expansion/ (downloaded 18 November 2023)
- AJLABS: Mapping Africa’s coups d’etat across the years. Al Jazeera. 30 August 2023, https://www.aljazeera.com/news/2023/8/30/mapping-africas-coups-detat-across-the-years (downloaded 24 October 2023)
- ALL-SAIDI, Mohammad – GAYOUM SAAD, Suhair A. – ELAGIB, Nadir A.: From scenario to mounting risks: COVID-19’s perils for development and supply security in the Sahel. Springer, 2022, DOI: 10.1007/s10668-022-02303-9 (downloaded 18 November 2023)

- BÁCS, Zoltán György: A radikalizáció és a terrorizmus kapcsolata, egyes formái, gondolatok a megelőzés lehetséges perspektíváiról. Nemzetbiztonsági Szemle, 2017/1, https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1721 (downloaded 8 November 2023)
- BBC: Nice: Eight guilty over the deadly Bastille Day lorry attack. BBC.com, 13 December 2022, https://www.bbc.com/news/world-europe-63954860 (downloaded 8 November 2023)
- BERGER, Chloé: NDC Policy Brief. Research Division – NATO Defense College, 22 December 2021, https://www.ndc.nato.int/news/news.php?icode=1644 (downloaded 6 November 2023)
- BESENYŐ, János – HETÉNYI, Soma Ambrus – JAGADICS, Péter – RESPERGER, István: Országismertető: Csád. Sereg Szemle, Székesfehérvár, 2010
- BORSI, Gergely: Terrorriadó Brüsszelben: megöltek két svéd szurkolót. Index.hu, 16 October 2023, https://index.hu/sport/futball/2023/10/16/labdarugas-gyilkossag-lovoldozes-brusszel-belgium-svedorszag-eb-selejtezo-europa-bajnoksag-terror/ (downloaded 8 November 2023)
- CIA: The World Factbook. Explore all countries – Chad. 2023, https://www.cia.gov/the-world-factbook/countries/chad/ (downloaded 25 October 2023)
- CIA [n.d.]: The World Factbook. Country Summary – Chadk. https://www.cia.gov/the-world-factbook/countries/chad/summaries (downloaded 25 October 2023)
- CRI: Az Ukrajnának szánt fegyverek az afrikai feketepiacra kerülnek. China Radio International, 1 December 2022, https://hungarian.cri.cn/2022/12/01/ARTIzRKnLsy5UyFx7tlMWZBD221201.shtml (downloaded 10 November 2023)
- Danube Institute: Egyre komolyabb kihívások jelentkeznek a Száhel-övezetben. 5 August 2023, https://danubeinstitute.hu/hu/blog/egyre-komolyabb-kihivasok-jelentkeznek-a-szahel-ovezetben (downloaded 10 November 2023)
- DE LEÓN COBO, Beatriz: Russian influence in the Sahel: Wagner and the support of military juntas Friedrich Naumann Foundation. 1 May 2022, https://www.freiheit.org/spain-italy-portugal-and-mediterranean-dialogue/russian-influence-sahel-wagner-and-support-military (downloaded 16 October 2023)
- DUZOR, Megan – WILLIAMSON, Brian: COUPS IN AFRICA. VOA News, 3 October 2023, https://projects.voanews.com/african-coups/ (downloaded 25 October 2023)
- Euronews – MTI: Kivonulnak az ENSZ-békefenntartók Maliból. Euronews.com 1 July 2023, https://hu.euronews.com/2023/07/01/kivonulnak-az-ensz-bekefenntartok-malibol (downloaded 21 October 2023)

- Európai Parlament: A Vöröskereszt Nemzetközi Bizottságának elnöke több segítséget vár az EU-tól. 28 May 2015, https://www.europarl.europa.eu/news/hu/headlines/eu-affairs/20150526STO59664/a-voroskereszt-nemzetkozi-bizottsaganak-elnoke-tobb-segitseget-var-az-eu-tol (downloaded 7 November 2023)
- Európai Parlament: Terrorizmus az EU-ban: támadások, halálesetek és letartóztatások 2020-ban. 20 August 2021, https://www.europarl.europa.eu/news/hu/headlines/society/20210628STO07262/terrorizmus-az-eu-ban-tamadasok-halalesetek-es-letartoztatasok-2020-ban (downloaded 23 October 2023)
- HICKS, Celeste: Chad and the West: Shifting Security Burden? Egmont Institute, 2015, http://www.jstor.org/stable/resrep06548 (downloaded 10 November 2023)
- Hirado.hu: Több humanitárius segélyt követelt az ENSZ főbiztosa a Csádba érkezett szudáni menekülteknek. Hirado.hu, 11 September 2023, https://hirado.hu/kulfold/cikk/2023/09/11/tobb-humanitarius-segelyt-kovetelt-az-ensz-fobiztosa-a-csadba-erkezett-szudani-menekulteknek (downloaded 7 November 2023)
- Honvedelem.hu: A parlament jóváhagyta a magyar katonai misszió indítását Csádba. 2023, https://honvedelem.hu/hirek/a-parlament-jovahagyta-a-magyar-katonai-misszio-inditasat-csadba.html (downloaded 8 November 2023)
- HORVÁTH Ferenc: Lampedusa lakosai nem bírják tovább a migrációs nyomást. Euronews, 17 September 2023, https://hu.euronews.com/2023/09/17/lampedusa-lakosai-nem-birjak-tovabb-a-migracios-nyomast (downloaded 10 November 2023)
- Hungary Helps: Hungary Helps humanitárium fejlesztési központ nyílik Csádban. https://hungaryhelps.gov.hu/2023/10/11/hungary-helps-humanitarius-fejlesztesi-kozpont-nyilik-csadban/ (downloaded 24 October 2023)
- Index: A tömegbe hajtott egy kamion a berlini karácsonyi vásáron, 12 halott. Index.hu. 19 December 2016, https://index.hu/kulfold/2016/12/19/teherautoval_a_tomegbe_hajtottak_a_berlini_karacsonyi_vasaron/ (downloaded 8 November 2023)
- International Fund for Agricultural Development (IFAD): Sahel. https://www.ifad.org/en/web/operations/regions/wca/sahel (downloaded 26 October 2023)
- Interpol [n.d.]: G5 Sahel. https://www.interpol.int/es/Delitos/Terrorismo/Proyectos-de-lucha-contra-el-terrorismo/G5-Sahel (downloaded 26 October 2023)
- M1 Híradó: Magyarország a Száhel övezetben is segít a Hungary Helps programon keresztül. YouTube, 24 September 2023, https://www.youtube.com/watch?v=SM8eyDben6Q (downloaded 10 November 2023)
- MACHIAVELLI, Niccolo: Beszélgetések Titus Livius első tíz könyvéről. In: MACHIAVELLI, Niccolo: Machiavelli Művei. Európa kiadó, 1978, pp. 87-442

- Magyar Hírlap: A Hungary Helps Program példaként szolgálhat más kormányoknak is. 9 March 2021, https://www.magyarhirlap.hu/kulfold/20210309-a-hungary-helps-program-peldakent-szolgalhat-mas-kormanyoknak-is (downloaded 7 November 2023)
- Magyar Nemzet: Sebastian Kurz: Az európai migrációs politika egyre több halált okoz Magyar Nemzet. 08 November 2023, https://magyarnemzet.hu/kulfold/2023/11/sebastian-kurz-az-europai-migracios-politika-egyre-tobb-halalt-okoz (downloaded 9 November 2023)
- Mandiner.hu: Iszlamista terror Brüsszelben, több halott – a belga rendőrség végzett az elkövetővel. Mandiner.hu 16 October 2023, https://mandiner.hu/kulfold/2023/10/breking-agyonlottek-ket-embert-brusszelben#google_vignette (downloaded 8 November 2023)
- Multinational Joint Task Force, https://www.justice.gov/eoir/page/file/1292686/download (downloaded 8 November 2023)
- MWAI, Peter: Gabon coup: The latest in a series of military takeovers on the continent. BBC, 30 August 2023, https://www.bbc.com/news/world-africa-46783600 (downloaded 721 October 2023)
- NÉMETH, Árpád: Sorra állítják vissza a határellenőrzést Európában. Index.hu, 1 October 2023, https://index.hu/kulfold/2023/10/01/hatarellenorzes-nemetorszag-lengyelorszag-csehorszag-szlovenia-horvatorszag-schengen/ (downloaded 7 November 2023)
- PÓSA, Tibor: Búcsú Malitól: az unió és a franciák után a németek is csomagolnak. Mandiner.hu, 19 August 2022, https://mandiner.hu/makronom/2022/08/mali-francia-nemet-katona-wagner-csoport-posa-tibor-makronom (downloaded 10 November 2023)
- POWELL, Jonathan M. – THYNE, Clayton L.: Global instances of coups from 1950 to 2010. A new dataset. Journal of Peace Research, 2011/2. pp. 249-259
- Rédaction Africanews with AFP: Africa: the 7 military coups over the last three years. 30 August 2023, https://www.africanews.com/2023/08/30/africa-the-7-military-coups-over-the-last-three-years// (downloaded 26 October 2023)
- ROBINSON, James: Brussels 'on highest terror alert' and football fans told to stay in the stadium after two shot dead. Skynews.com, 17 October 2023, https://news.sky.com/story/two-people-wearing-football-shirts-shot-dead-in-brussels-belgian-media-report-12985711 (downloaded 17 October 2023)
- RPCA – The food crisis prevention network: Moderate and severe acute malnutrition. 2020 November, https://www.food-security.net/en/map-library/prise-en-charge-de-la-malnutrition-aigue-severe-et-moderee/ (downloaded 28 November 2023)
- Saudi Press Agency: KSA, Chad sign Cooperation MOU in defense field. Saudi Press Agency. 2023, https://www.spa.gov.sa/w1844310?lang=en&newsid=2419918 (downloaded 18 November 2023)

- SCHEFFER Joakim: Ha megtehetik, miért ne? – ezért van egyre több puccs Nyugat-Afrikában. Magyar Nemzet. 11 August 2023, https://magyarnemzet.hu/lugas-rovat/2023/08/ha-megtehetik-miert-ne-ezert-van-egyre-tobb-puccs-nyugat-afrikaban (downloaded 9 November 2023)
- The Heritage Foundation: CHAD – 2023 Index for economic freedom. 2023, https://www.heritage.org/index/country/chad (downloaded 26 October 2023)
- The Hungary Helps Agency: https://hungaryhelps.gov.hu/hungary-helps-program-main-page/ (downloaded 28 November 2023)
- The International Institute for Strategic Studies: The Military Balance 2023. The International Institute for Strategic Studies, 2023.
- The United Nations: Multidimensional Integrated Stabilization Mission in Mali. https://minusma.unmissions.org/en/history (downloaded 8 November 2023)
- The UN Refugee Agency (2023a): UNHCR urges for urgent support to Chad as refugee arrivals exceed 100,000. 2023. június 1. https://www.unhcr.org/africa/news/press-releases/unhcr-urges-urgent-support-chad-refugee-arrivals-exceed-100-000 (downloaded 9 November 2023)
- The UN Refugee Agency (2023b): UNHCR's Grandi praises Chad's role hosting Sudanese; more aid urgently needed. https://www.unhcr.org/uk/news/press-releases/unhcr-s-grandi-praises-chad-s-role-hosting-sudanese-more-aid-urgently-needed (downloaded 9 November 2023)
- The UN Refugee Agency [n.d. a]: SAHEL REFUGEE CRISIS. https://www.unrefugees.org/emergencies/sahel-crisis/ (downloaded 6 November 2023)
- The UN Refugee Agency [n.d. b]: Chad. https://www.unhcr.org/countries/chad (downloaded 6 November 2023)
- UN News: Mali: 'MINUSMA is leaving, but the UN is staying', Mission chief says. United Nations Africa renewal. 2023. augusztus 28. https://www.un.org/africarenewal/magazine/august-2023/mali-'minusma-leaving-un-staying'-mission-chief-says (downloaded 22 October 2023)
- United States Agency International Development (USAID)[n.d.]: Chad. https://www.usaid.gov/chad (downloaded 25 October 2023)
- US Department of State: Report on International Religious Freedom: Chad. 2022, https://www.state.gov/reports/2022-report-on-international-religious-freedom/chad (downloaded 22 October 2023)
- US Department of State: Bureau of counterterrorism. 2021, Country Reports on Terrorism 2021: Chad. https://www.state.gov/reports/country-reports-on-terrorism-2021/chad/ (downloaded 7 November 2023)

- VALADE, Carol: Driven out of Niger, the French army takes refuge in Chad, Paris's last ally in the Sahel. Le Monde, 17 October 2023, https://www.lemonde.fr/en/le-monde-africa/article/2023/10/17/driven-out-of-niger-the-french-army-takes-refuge-in-chad-paris-s-last-ally-in-the-sahel_6179914_124.html (downloaded 9 November 2023)
- WorldData.info: Median age by country. 2023, https://www.worlddata.info/average-age.php (downloaded 25 October 2023)

INFORMATION AND COMMUNICATION SECURITY

ANDRÁS JÓZSEF ÜVEGES[1]

PROTECTION OF PERSONAL DATA IN THE VIEW OF ALLIED NATIONAL CYBER SECURTY STRATEGIES 2022-2023

Abstract

The cyber-defence and the protection of personal data represent rapidly and dynamically developing areas in cyberspace, as more and more risks arise with regard to personal data stored, processed and transferred in cyberspace. Globally, it can be said that one of the priorities of the strategies of individual governments is to build and develop resilience against cyberthreats, and to ensure that the population and the economy can effectively take advantage of the benefits of reliable digital technologies. The National Cybersecurity Strategies published in 2022 also include and emphasize the protection of personal data in several different cases and ways.

Keywords: cyber security, personal data protection, information security, national cyber security strategy

Introduction

In my article, I continue my previously started research,[2] where I investigated how the protection of personal data appears in national cyber security strategies. In my actual study, I examined the strategies, published in the years between 2022 and 2023, in order to have a more detailed view of the connection between the protection of personal data and the mentioned strategic documents. In the mentioned period of time, the Icelandic, Romanian, Italian and Danish governments also published a new national cyber security strategy. In addition, it is very important to emphasize that the United States Department of Defense is also issued its document entitled "2023 Department of Defense Cyber Strategy", during the period under review.

Regarding cyber-defence, it can be said that the highest level of planning and conceptual thinking are at the level of strategic documents, since they contain the main concepts of governments.

This can also be seen by the fact that the European Union adopted its first security strategy in December 2003, which lists the global and specific challenges threatening the Union, among which the concept of cyber threats is not yet directly included, but is already appearing as a critical issue.

[1] ORCID: 0000-0002-5860-2405

[2] ÜVEGES, András: A személyes adatok védelme a kiberbiztonsági stratégiák tükrében, Felderítő Szemle, 2021/3, p. 17

After the announcement of the Digital Agenda, cyberspace and cyber security became prominent, and this became noticeable in EU documents as well.[3]

In 2012, the European Parliament adopted a resolution entitled "Critical information infrastructure protection: towards the creation of global cyber security".[4]

After this, in 2013, the Union published its comprehensive cyber security strategy under the title "Open, safe and reliable cyber space – Cyber security strategy of the European Union.". In 2016, the Union's data protection regulation was adopted and the NIS directive was also published.[5]

Subsequently, in 2016, the European Union published a new document which called "Common vision, common action: a stronger Europe." Also, the Union's new security strategy was published under the title "EU Global Foreign and Security Policy Strategy", in which cyberspace has already appeared like a new dimension, which will later become a battlefield.[6]

Demarcation

The examined period is only approximate one, as the preparation-publication-entry into force date is partially different on ENISA's electronic web[7] page as well as in the electronic copy of the strategic documents.

In the article, I tried to examine only publications where the personal data are actually mentioned. I did not deal with indirect ways, such as cybercrime, where personal data clearly appear as the object of the crime.

General objectives of cyber security strategies

Typically, cybersecurity strategies describe – but do not regulate – how the government concerned can utilize and strengthen all of its available tools and resources to remain cyber-sovereign, in the rapidly evolving digital ecosystem.

[3] https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf (downloaded 01 November 2023)

[4] European Commission: Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – 'Achievements and next steps: towards global cyber-security'. Brussels, 31 March 2011, Procedure number: 200304 (downloaded 05 November 2023)

[5] KOVÁCS, László: Kiberbiztonság és -stratégia, Dialóg Campus Kiadó, Budapest, 2018 p. 86.

[6] BISCOP, Sven: Global and Operational: A New Strategy for EU Foreign and Security Policy, IAI-CSF, 2015 July https://www.iai.it/sites/default/files/iaiwp1527.pdf (downloaded 01 November 2023)

[7] ENISA: National Cyber Security Strategies – Interactive map. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map (downloaded 15 September 2023)

These documents also address how the country concerned can strengthen its cooperation globally (bilaterally or multilaterally) with partners who share national values related to democracy, the rule of law and human rights.

The creators of cyber security strategies also address the cyber security of essential services, such as elements of vital infrastructures, such as the protection of IT systems of healthcare institutions, energy networks and their service infrastructure, rail traffic and transport, as well as the rapidly expanding Industry 4.0[8] or smart solutions applying operating units, and protection of personal data.[9]

During the examined period (approximately between 2021 and 2023), the Danish, Romanian, Icelandic and Italian governments also published their National Cyber Security Strategy.

It is also important to note what László Kovács states in his book, if we look „, *national-level cyber strategies approach cyberspace and its security differently from country to country. Researching the reasons for the differences in the different approaches, we can come to the conclusion that they can be discovered primarily in whether the given country previously considered the development and smooth operation of technology and technology, the information society, and the protection of critical information infrastructures as a starting point. At the same time, several common factors are present in the cyber security strategies of different European countries. One of these common factors is that every country without exception sees cyber security as a basic and defining element of national security".*[10]As a result, I did not compare the strategies against each other, as it would give a wrong research result.

Danish National Strategy for Cyber and Information Security

Denmark is one of the leading countries in terms of digitization processes. The Danish government system and society itself rely heavily on digitized solutions in many areas of the private sector, government and industry.

[8] Industry 4.0 is revolutionizing the way creators, facories, improve and distribute their products. Manufacturers are integrating new technologies, like Internet of Things (IoT), cloud computing or analytics, and AI and ML into their production hubs.

[9] ENISA: Raising awareness of cybersecurity – A Key Element of National Cybersecurity Strategies. November 2021, ISBN 978-92-9204-544-9, DOI 10.2824/36362. (downloaded 15 September 2023)

[10] Kovács (2018) p. 8

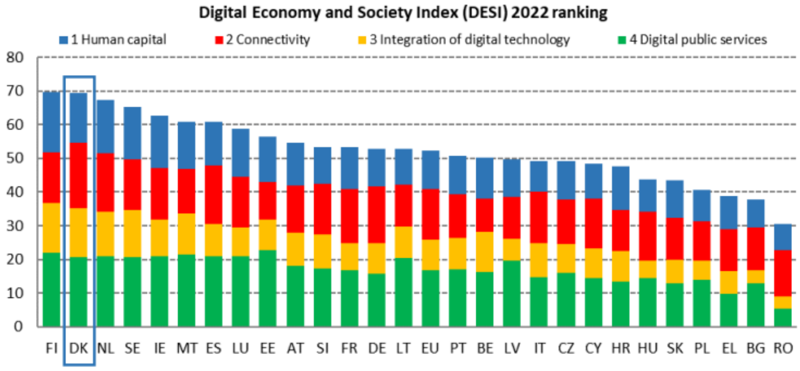
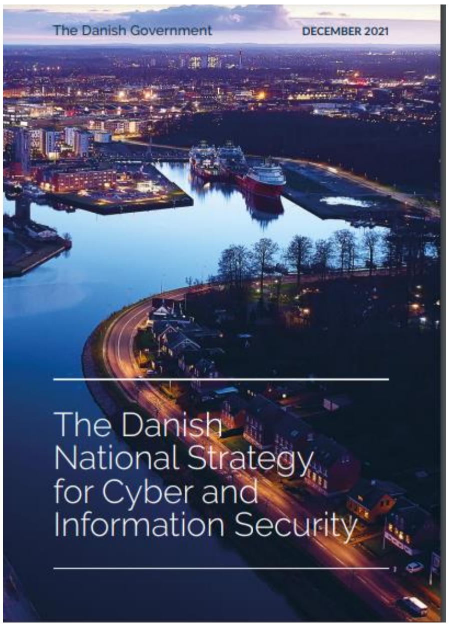


Figure 1: 2022 DESI index – Denmark[11]

According to the DESI index, Denmark[12] ranks second in this regard. The defining concept of the Danish National Cybersecurity Strategy is to create a reliable and safe cyberspace for industry, the economy and, above all, the population. This concept is naturally in line with the EU strategic concept and the recommendations of ENISA.[13]



The Danish Government

DECEMBER 2021

The Danish National Strategy for Cyber and Information Security

Figure 2: Danish Cyber and Information Security Strategy 2022-2024[14]

[11] Source: European Commission op. cit.

[12] Denmark in the Digital Economy and Society Index https://digital-strategy.ec.europa.eu/en/policies/desi-denmark (downloaded 04 November 2023)

[13] National Cybersecurity Strategies Guidelines & tools. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools (downloaded 01 November 2023)

[14] Source: https://www.cfcs.dk/globalassets/cfcs/dokumenter/2022/ncis_2022-2024_en.pdf (downloaded 01 November 2023)

The strategy is for the period 2022-2024. The strategy sets out a number of objectives as follows:

- Management of fight against cybercrime;
- Strengthening citizen's internet security awareness;
- Protection of critical information infrastructure;
- Development of national cyber preparedness plans;
- Increasing international cooperation;
- Development of an incident-response capability;
- Definition of basic security requirements;
- Create incident reporting mechanisms;
- Upgrade R&D events;
- Organization of cyber defence exercises;
- Development of training and educational programs.

In terms of the Danish strategy, the protection of personal data appears in relation to the protection of social values, although the concept of personal data is not mentioned here literally. After that, in point 1.16, the concept of personal data appears in connection with the Central Population Registration System. According to point 1.16 of the document, the up-to-datedness of personal data stored in the government's Central Population Registration System must be increased. More precisely „*Training efforts will be launched for control staff of relevant authorities to ensure more valid personal data in the Central Population Register, which is a prerequisite for trust in the personal data used by many public and private bodies"*[15]

The protection of personal data also appears indirectly in chapter 2.1 of the strategy, according to which, the ICT competencies of senior government officials must be strengthened, where it specifically refers to personal ICT capabilities. Quoted verbatim „*Increased demands are placed on the personal ICT security of top government leaders, and competence initiatives are strengthened so that security will become a integral part of the management task in the future.", which presumably means the PAN network in this case.*[16]

In summary, it can be said that, according to the Danish point of view, the protection of personal data is also important, but the strategy typically focuses more on external risks threatening the country. In the majority of the strategic documents, countries and organizations with counter-interests and the fight against cybercrime are mentioned, where personal data can be clearly seen as a means of abuse.

It is also important to note that this strategy mentioned the cyber security and information security separately. If we consider the information security to be the set of security procedures and tools that broadly protect confidential data (usually corporate) from misuse, unauthorized access, service interruption and destruction, then this includes personal data protection as well. From this point of view, the customer/employee data managed by the companies should also be classified here. It is enough to think that when applying the algorithm-based method of securing communication, we ensure that the given message can only be viewed and deciphered by its recipients.

[15] Danish Cyber and Information Security Strategy 2022-2024 op. cit. p. 46

[16] Ibid. p. 47

Romanian Cyber Security Strategy and Action Plan 2022-27

As a result of increased global threats, the Romanian government wants to become one of the most competent NATO members, in terms of cyber capabilities. The Romanian government is regrouping more and more resources for the training of IT engineers. Despite being the second poorest member of the EU, based on gross domestic product, it ranks sixth globally, in terms of the number of certified IT workers per capita. In addition, Romania ranks first in the EU in terms of the number of IT freelancers. With one of the fastest growing economies in the EU, Romania's IT&C sector accounted for almost 7 percent of the country's GDP in 2021, compared to 6 percent in 2018.[17]

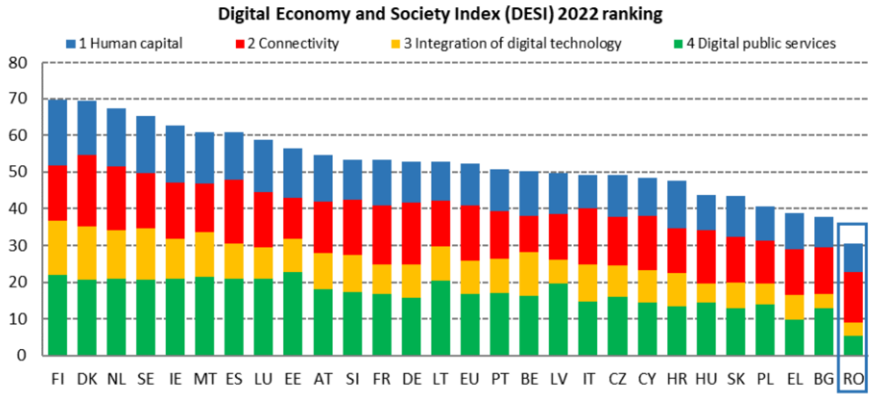


Figure 3: 2022 DESI index – Romania[18]

Yet, according to the DESI index, Romania ranks last in this regard.

On 30 December 2021, the Romanian Government adopted the Decision No. 1321/2021, approving Romania’s Cybersecurity Strategy and Action Plan for 2022-2027. The new Strategy mainly aims to ensure a higher level of cybersecurity, so that Romania should be able to, deter, prevent, and respond effectively to hostile actions in cyberspace.[19]

The strategy sets out a number of objectives as follows:

- Management the fight against the cybercrime;
- Adoption of information security standards;
- Strengthening citizens' safety awareness on the internet;
- Protection of critical information infrastructure;
- Development of national cyber preparedness plans;

[17] International Trade Administration: Romania Country Commercial Guide. https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict (downloaded 01 November 2023)

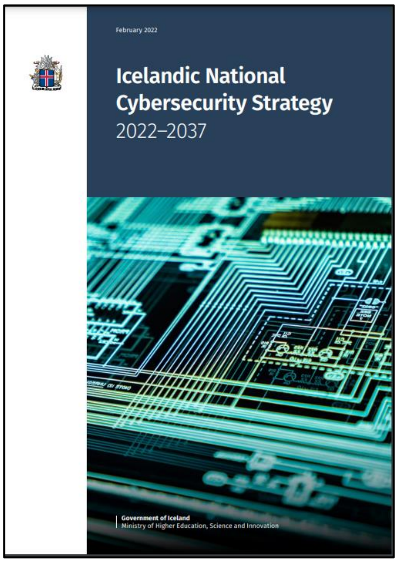
[18] Source: European Commission

[19] INFORMAŢIE DE PRESĂ: privind actele normative aprobate în şedinţa Guvernului României din 30 decembrie 2021 https://gov.ro/ro/guvernul/sedinte-guvern/informatie-de-presa-privind-actele-normative-aprobate-in-sedinta-guvernului-romaniei-din-30-decembrie-2021 (downloaded 04 November 2023)

- Strengthening international cooperation;
- Developing cooperation between the public and private sectors;
- Creating an incident response capability;
- Establishing an institutionalized form of cooperation between state bodies;
- Development and implementation of policies and regulatory capabilities;
- Definition of basic security requirements;
- Creation of incident reporting mechanisms;
- Creating reliable information sharing mechanisms;
- Stimulating R&D;
- Increasing the number of cyber defence practices;
- Strengthening the training and education programs;
- Improving supply chain cyber security.

In the Romanian strategic document, the emphasis on the protection of personal data does not appear clearly separately, despite the fact that close relationship between data protection and cyber security results from Art. 5 of the European Union’s General Data Protection Regulation, which outlines one of the most important principles relating to processing of personal data: “integrity and confidentiality”. One of the most frequent cyberattacks that we can see in general are phishing or email fraud, in which the attackers gain access to an organization’s network using a direct hit on the email accounts of a business and their clients. Phishing just edges out scanning for and exploiting vulnerabilities and unauthorized use of credentials. Among the main goals, there are many points for which the protection of personal data could have been emphasized in the strategy.[20]

Icelandic National Cyber Security Strategy



February 2022

Icelandic National Cybersecurity Strategy 2022–2037

Government of Iceland
Ministry of Higher Education, Science and Innovation

Figure 4: Icelandic National Cybersecurity Strategy[21]

[20] ENISA: National Cyber Security Strategies – Interactive map. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map (downloaded 15 September 2023)

[21] Ibid.

The Icelandic government currently has a new National Cybersecurity Strategy,[22] which includes the concept of the period 2022-2037. The strategy replaced the 2015 document. The Icelandic National Cyber Security Strategy contains the government's vision for the future, as well as the determination of the capabilities necessary to create and maintain a secure cyber environment for the society. The strategy is regulated by the Law 78/2019 on Cyber and Data Security. s. approved by law for Transportation and Minister responsible for local governments and part of the government's Electronic Communication Plan[23] too.

The strategy 2022-37 will cover a significantly long period, where it defines a number of goals as follows:

- Fight against the cybercrime;
- Strengthening citizens' safety awareness;
- Protection of critical information infrastructure;
- Strengthening international cooperation;
- Stimulating R&D;
- Strengthening of training and education programs.

The Icelandic leadership wants to build a secure internet infrastructure for the population and economy, based on a strong security culture. But they still respect the individual's freedom and human rights. The society is also well-prepared to deal with cybercrime, cyberattacks, cyber-intelligence, and the misuse of personal and business data.

It is important to note that data protection legislation in Iceland has been implemented with the adoption of Act No. 77/2000 on the Protection of Privacy, as regards the Processing of Personal Data,[24] which implements the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals, with regard to the processing of personal data and on the free movement of such data. The Act No. 77/2000 on Privacy as regards to the Processing of Personal Data has been in force since 2000 and implements the provisions of Directive 95/46/EC. On grounds of Art. 11 and 12 of the Data Protection Act the Icelandic Data Protection Authority (DPA) has set forth the Rules No. 299/2001 on the Security of Personal Data. Iceland is also in the process of implementing the EU General Data Protection Regulation (GDPR). The above-mentioned legislation already appears in the preliminary strategy, so it can be said that the GDPR basically already appears in the strategic thinking as well.

Italian National Cyber Security Strategy

In Italy, as in other European states, the number of cyber-attacks that have occurred represents an increasing risk and challenge.

[22] Icelandic National Cybersecurity Strategy 2022-2037. Ministry of Higher Education, Science and Innovation, 2022, National Cyber Security Strategies – Interactive Map, ENISA (europa.eu)

[23] Electronic Communications Plan.

[24] Data Protection Act

In terms of the number of malware attacks, the situation is no better in Italy, while the government and healthcare institutions are increasingly targeted by ransomware attacks.[25]

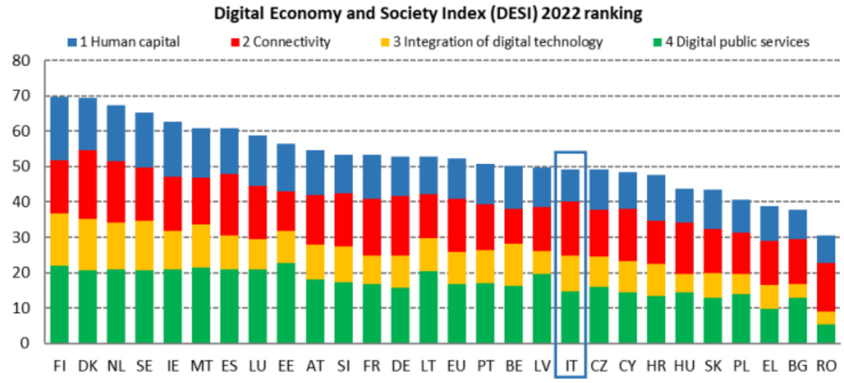


Figure 5: 2022-es DESI index – Italy[26]

Figure 6: Italian CyberSecurity Strategy 2022-2026[27]

[25] https://www.trade.gov/country-commercial-guides/italy-cybersecurity (downloaded 15 September 2023)

[26] Source: European Commission op. cit.

[27] Source: ENISA, https://www.enisa.europa.eu/events/enisapolicyconference-v2_pub.pdf (downloaded 15 September 2023)

Italian users were also hit by a number of cyber-attacks, which were carried out with malicious software.[28] In January 2023, in several cases in Italy, malicious software was delivered to victims' IT devices via phishing emails, in order to obtain sensitive data from it, such as system information, cryptocurrency wallet data, browsing history and cookies.

It cannot be ruled out that the protection of personal data was included in the strategic document, as there was also an application in 2023, the data management of which did not comply with the rules of the GDPR. The Italian Data Protection Authority[29] has imposed a temporary ban of OpenAI's ChatGPT service[30] in the country, because data protection concerns.[31] More important, there appears to be no legal basis underpinning the massive collection and processing of personal data, in order to upgrade algorithms on which the platform relies. In response to the order, OpenAI has blocked its generative AI chatbot from being accessed by users with an Italian IP address. End it is issuing refunds to subscribers of ChatGPT Plus, in addition to pausing subscription renewals.[32,33,34]

The San Francisco-based company further emphasized that it provides ChatGPT in compliance with GDPR and other privacy laws. ChatGPT is already blocked in China, Iran, North Korea, and Russia.[35]

The strategy covers the period 2022-2026. Similar to the Danish strategy, the strategy defines a number of goals as follows:

- Increasing the fight against cybercrime;
- Adoption of new information security standards;
- Harmonization of privacy protection and cyber security;
- Strengthening the population's safe internet usage;
- Protecting of critical information infrastructure;
- Increasing international cooperation;
- Strengthening the cooperation between the authority and the population;
- Creating an incident response capability;

[28] The multi-stage infection sequence commences with an invoice-themed phishing email which containing a link. After you clicked, downloads a password-protected ZIP archive file, and after it contains two files. A shortcut (.LNK) file and a batch (.BAT) file.

[29] Garante per la Protezione dei Dati Personali – Garante - is an independent administrative authority established by the so-called privacy law (Law No. 675 of 31 December 1996) and regulated subsequently by the Personal Data Protection Code (Legislative Decree No. 196 of 30 June 2003) as amended by Legislative Decree No. 101 of 10 August 2018, which also established that the Italian DPA is the supervisory authority responsible for monitoring application of the General Data Protection Regulation (pursuant to Article 51 of Regulation No. 2016/679).

[30] ChatGPT is an AI-powered language model developed by OpenAI, capable of generating human made text based on context and conversations (chats)

[31] https://www.garanteprivacy.it/home

[32] https://twitter.com/sama/status/1641897800236687360 (downloaded 04 November 2023)

[33] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847#english (downloaded 04 November 2023)

[34] https://www.reuters.com/technology/italy-data-protection-agency-opens-chatgpt-probe-privacy-concerns-2023-03-31/ (downloaded 04 November 2023)

[35] https://www.digitaltrends.com/computing/these-countries-chatgpt-banned/ (downloaded 04 November 2023)

- Establishing an institutionalized form of cooperation between state bodies;
- Development and implementation of policies and regulatory capabilities;
- Definition of basic security requirements;
- Creation of incident reporting mechanisms;
- Creating reliable information sharing mechanisms;
- R&D development;
- Improving supply chain cyber security;
- Organization of exercises;
- Increasing training and educational activities.

  In the strategy, personal data are mentioned from the point of view that politicians, journalists, and public figures can be shown in a negative light, with their illegal use. Here, the strategy presumably aims to leak sensitive personal data (gender identity, for example) about the targeted person.

US Department of Defence Cyber Security Strategy

The IT infrastructure of the United States of America is exposed to continuous attacks in cyberspace, the attackers aim to map the vulnerabilities of American systems and eliminate the current competitive advantage of the armed forces.

The document is of course already an updated version of a preliminary series of documents. The first such cyber security strategy can be traced back to the Bush era. In 2003, the administration issued its first strategy that already mentioned the cyberspace.[36] In 2009, the Obama administration issued a document entitled Review of Cyberspace Policy.[37] In 2011, the International Strategy for Cyberspace of the United States of America was also published.[38] In 2018, the Trump administration released the US National Cyber Security Strategy.[39] This strategy can be called as a cyber security strategy in the classical sense. Its structure follows the structure of the 2018 American National Security Strategy. This strategy was updated on March 3, 2023.[40]

At the same time, the Ministry of Defense also started publishing its own concept. Starting in 2011, the Department of Defense issued a separate cyber strategy. This was updated in 2015 and again in 2018. In the American National Cyber Security Strategies, the protection of personal data typically appears in terms of the protection of privacy.

[36] Nemzeti Stratégia a Kibertér Védelmére – National Strategy to Secure Cyberspace

[37] Cyberspace Policy Review

[38] International Strategy for Cyberspace

[39] National Cyber Strategy

[40] TheWhiteHouse: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, 01 March 2023 (downloaded 01 November 2023)

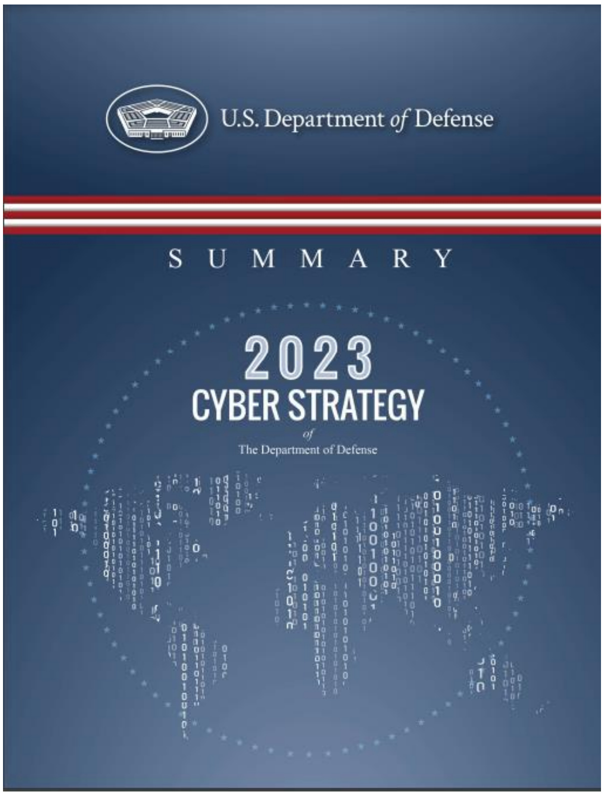


Figure 7: US Department of Defense Cyber Strategy[41]

The protection of personal data in the document promotes cyber awareness.[42] According to the document, attacks carried out with malicious software – in addition to affecting the entire defence sector – include also the entire personnel of the armed forces. The primary goal of the attacks, in such cases, is to gain access to the personal data of the staff members, with which they can later carry out further abuses. This destroys and reduces the military capability and readiness of the given military unit. The idea that appeared in the strategy is presumably a consequence of the fact that, in the entire concept, it views human resources as the most significant capability/capacity of cyber security/cyber protection.

[41] Source: https://www.defense-aerospace.com/pentagon-releases-2023-cyber-strategy-summary/ (downloaded 04 November 2023)

[42] Foster Cyber Awareness

Cyber security in practice

Whatever cybersecurity strategy governments develop, the battle will be fought at the ends, and the organizations must deal with both attacks and cybersecurity issues, caused by human error.

"The organizations, regardless of their size, need to prepare for a breach in their cyberdefence, but this often requires more than "superhuman" efforts, like in the case of the supply chain attacks. Like these kinds of actions, the attackers launch an attack against the weakest links in the supply chain, in such a way that the target is not actually them, but the strongest member of the chain. The organizations must trust the professional knowledge and caution of those with authorized access to their cyberdefence, but this can only be achieved by introducing, educating and consistently following and enforcing comprehensive internal policies.

In the case of the EEA[43] *member states, a high level of protection is also required by the data protection and data security regulations of the GDPR, and data protection incidents, due to breaches of security, must also be reported to the data protection supervisory authorities. The authorities investigate these incidents and, where appropriate, impose administrative fines, depending on the risk posed to the rights and freedoms of those involved. Of course, the affected parties can also take their grievances to court, asking for compensation for the damage they have suffered.*

In addition to "traditional" cyber defence systems, the new technologies of IPAR 4.0 also present new challenges that organizations must prepare for, for example, the rise of connected (IoT) systems or artificial intelligence systems and models. The organizations are not yet fully aware of the operating mechanisms and risks of these ecosystems, so their preparedness does not always reach the expected level in the field of cyber security, even posing a national security risk to a given state. That is why the governments must not only create a cyber security strategy, but also actively participate in supporting the cyber security of the organizations."[44]

Conclusion

In my opinion, the emphasis on the protection of personal data clearly appears indirectly in the strengthening of the fight against cybercrime. It is interesting that, in addition to mentioning the fight against cybercrime, the documents do not make a clear reference to this.

The concept of the protection of personal data appears clearly in some cases, where I indicated this beforehand in the article, but it can be seen that the strategic documents – presumably due to their nature – form a more comprehensive picture and typically do not cover this in the period under review.

[43] European Economic Area was established with the Agreement on the European Economic Area, international agreement which enables the extension of the European Union's single market to member states of the European Free Trade Association. EEA was established on 1 January 1994.

[44] Dr. Ágota Albert LL.M, lawyer specialized in data security and data protection, data protection officer (4-IN-1 Ltd., https://gdprszakszeruen.hu/ujtechnologiak.php) and deputy president of the Data Protection Trade Association (https://www.aszake.hu/)

Bibliography:

- BISCOP, Sven: Global and Operational: A New Strategy for EU Foreign and Security Policy, IAI-CSF, 2015 July https://www.iai.it/sites/default/files/iaiwp1527.pdf (downloaded 01 November 2023)
- Danish Cyber and Information Security Strategy 2022-2024 https://www.cfcs.dk/globalassets/cfcs/dokumenter/2022/ncis_2022-2024_en.pdf (downloaded 01 November 2023)
- Denmark in the Digital Economy and Society Index https://digital-strategy.ec.europa.eu/en/policies/desi-denmark (downloaded 04 November 2023)
- ENISA: National Cyber Security Strategies – Interactive map. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map (downloaded 15 September 2023)
- ENISA: Raising awareness of cybersecurity – A Key Element of National Cybersecurity Strategies. November 2021, ISBN 978-92-9204-544-9, DOI 10.2824/36362. (downloaded 15 September 2023)
- European Commission: Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – 'Achievements and next steps: towards global cyber-security'. Brussels, 31 March 2011, Procedure number: 200304 (downloaded 05 November 2023)
- European Security Strategy – A secure Europe in a better world. General Secretariat of the Council (Council of the EU), 2009, ISBN 978-92-824-2421-6, DOI 10.2860/1402
- GrantePrivace: https://www.garanteprivacy.it/home (downloaded 01 November 2023)
- INFORMAŢIE DE PRESĂ: privind actele normative aprobate în şedinţa Guvernului României din 30 decembrie 2021 https://gov.ro/ro/guvernul/sedinte-guvern/informatie-de-presa-privind-actele-normative-aprobate-in-sedinta-guvernului-romaniei-din-30-decembrie-2021 (downloaded 04 November 2023)
- International Trade Administration: Romania Country Commercial Guide. https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict (downloaded 01 November 2023)
- KOVÁCS, László: Kiberbiztonság és -stratégia, Dialóg Campus Kiadó, Budapest, 2018
- Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Brüsszel, 2013.2.7. JOIN(2013) 1 final.

- National Cybersecurity Strategies Guidelines & tools. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools (downloaded 01 November 2023)
- Romanian Cyber Secuirty Startagie. ENISA Interactive Map, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Romania (downloaded 01 November 2023)
- TheWhiteHouse: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, 01 March 2023 (downloaded 01 November 2023)
- ÜVEGES, András: A személyes adatok védelme a kiberbiztonsági stratégiák tükrében. Felderítő Szemle, 2021/3, pp. 145-162

LAJOS ZÁHONYI[1] – ENDRE SZŰCS[2]

EXAMINING INFORMATION SECURITY EDUCATIONAL TOOL SYSTEMS, IN THE LIGHT OF JUVENILE CYBER SECURITY RISKS

Abstract

The biggest national defense and military development program of recent years, the ”Zrínyi 2026 program”[3], has been currently taking place. The success of this program depends significantly on the success of recruitment and on the way how the young people entering the system find their place. Today's primary school-age group will soon enter the labor market and may even be a part of the national defense staff to be recruited in the future. All of this coincides with the time, when the most populous 40-50-year old working-age group living today will be in their 60s. Our future is dependent on the socialization of this age group. We owe them a responsibility, so that when the time comes, they also owe us the same. A part of our responsibility is to be able to convey appropriate answers to the challenges generated by digital technology, since the conscious use of the Internet by young people also produces national security benefits, when it consciously protects the Internet data. We can state that the age-related aspects of cyber defense, such as the information security-awareness and conscious data protection of young people, contribute significantly to national defense. One way to do this is to try to use the tools of education and knowledge dissemination, in conformity with the current information security[4] and data protection challenges. “Equipping” educational materials, expanding the National Basic Curriculum, publishing informative materials, holding preventive lectures and extending national defense educational materials in this direction can provide a kind of answer to the problems, so the tools and their measures can improve young people's knowledge of data protection, information security and network security point of view.

In this scientific article, we will examine the aspects and tools that can currently be found in the Hungarian education system; we analyze the relevant international research and educational tools, which help the young generation to deal properly with today's information security and data protection challenges, and provide answers to the challenges of the present day.

Keywords: information security, data protection, development history of information security, information protection, information security education, young people of primary school age

[1] ORCID: 0000-0001-9999-9624

[2] ORCID: 0000-0003-2818-262X

[3] https://honvedelem.hu/hirek/hazai-hirek/zrinyi-2026-2026.html download time: 19 June 2023

[4] Definition available: https://edps.europa.eu/data-protection/data-protection/reference-library/information-security_en

Research methodology tools for writing this study

In the writing of this study, some research principles were particularly emphasized. Given that the examination of information security among elementary school-aged youth is one of the current topics that affects many people. During the writing of the study, we tried to enforce the principle of objectivity, to examine – based on the available data – the response system of the education to the problem and the teaching materials that affect our research subject.

The examination of a relevant effective method was preceded by a historical research, which consisted of several parts, during which, we examined the events associated with the development of information technology, and then, we scrutinized the legal regulatory environment surrounding young people, as well as the reaction of some international organizations to the subject. In this study, we will examine what subject-content and possibly other means of dissemination of knowledge are available within the education system, in response to the main technological challenges related to information protection and data protection of the age group.

In the processing of the topic, great emphasis was placed on incorporating the methods of empirical research into the adaptation of the topic. Based on request, two experts – who can be regarded as experts in the field – were approached during an in-depth interview, and in the process of elaborating this topic, we analyzed the data appearing and available on many relevant institutional internet portals, such as questionnaire research, statistics and scientific articles. The use of secondary data was based on the data from the Central Statistical Office and the Education Office. All of this contributed to the scientific foundation of the research on which this article is based.

In writing our article, we did not examine educational technology, pedagogical and methodological issues, we only dealt with the objective examination of the teaching materials, issued by the education office, i.e. we looked for whether some appropriate aspects related to the data protection, information protection and information security of young people could be found.

Introduction

According to the latest educational data available on the website of the Central Statistical Office (hereinafter: KSH), in the 2023/2024 academic year in Hungary, 1 million 462 thousand young people will participate in some level of public education, vocational training and higher education. 714,000 of them study in primary school. Also, based on the data available on the KSH website, 91.4 percent of Hungarian households have internet downloaded. This means that the examination of the use of Internet by this age group and the relevant information security challenges is practically inevitable.

In the European Union in 2020, the annual cost of cybercrime committed against the global economy was €5.5 billion. If we examine the issue of information security awareness among minors from this point of view, it can be said that the topic raises national security issues also in the long term.

If, as a senior age group, we do not take care of the information security protection of young people, and we and “let them go” on their own way, in the absence of proper knowledge and protection, we expose them to a huge danger, and in the long term, it may indirectly, harmfully affect also the field of national defense.

Cyber security threats across the ages

As defined by the United Nations Children's Fund (UNICEF): *“Millions of children around the world are spending more and more time online...children's increased exposure to the digital environment poses both risks and challenges. Harmful misinformation, child sexual exploitation and harassment, online bullying and violence, and mental health issues threaten the health, safety and rights of children.”*

The digital environment surrounding today's young generation hides countless challenges. Due to the large number of young people and the prevalence of digital devices, the issue of information security and data protection must also be addressed at institutional level. *“On the one hand, the protection of personal data is the right of every living person, regardless of age - as the dangers also affect – on the other hand, the age limit for the use of digital devices is sliding down more and more.”*

This age group is more exposed to information security threats, from among which we have identified the following ones:

- Data protection: These young people share data during their activities on the Internet, which can be used by online criminals or other malicious persons. Lack of data protection makes them vulnerable to data breaches. Free online content, movies, games and applications, which often have limited data protection regulations, deserve special attention. This makes them easily exposed to inappropriate content, data collection and manipulation that can have a detrimental effect on their lives.
- Cybersecurity threats: During the Internet and online activities, the age group can face threats such as viruses, malware, phishing, which allow online attackers to infect or steal the personal data of young people.
- Online bullying: Online bullying, i.e. cyberbullying, is one of the dangers that young people of primary school age often face. Due to the widespread use of social media and communication technologies, young people of elementary school age can easily become victims of online bullying.

The topic is very fresh and at the same time very current. In response to the challenges of digital society, knowledge materials that increase and develop young people's digital knowledge have also appeared in Hungarian education, which also affect the age group's information protection and data protection issues. One of the pillars of this is the 110/2012. (VI. 4.) Government Decree’s promulgation on public surfaces, as well as the introduction and application of the National Core Curriculum, in which, the term of digital culture has already appeared in its technology chapter. In 2020, the National Core Curriculum has been introduced, in which the name of the subject “Digital Culture” has already appeared, and age-specific textbooks will be prepared, which will then be approved.

Examining the teaching materials of the digital culture subject

"Since the development of IT tools constantly reveals new possibilities that we have not encountered before, the development of students' digital competence does not only mean the transfer of IT knowledge, but also requires the versatile development of students' digital culture. Of course, this appears in all learning areas, but the necessary professional and methodological background and coherence is provided by the digital culture subject" – says the explanation in the framework of curriculum.

Digital culture textbook for elementary school-age youth by grade:

Grade	Year of publication	Duration of license
8	2023	2022. 12. 02-től 2027. 08. 31-ig
7	2022	2022. 03. 11-től 2027. 08. 31-ig
6	2020	2027. 08. 31-ig
5	2020	2020. 06. 10-től 2025. 08. 31-ig
4	2022	2022. 12. 19-tôl 2027. 08. 31-ig
3	2021	2022. 02. 02-tôl 2027. 08. 31-ig

Table 1: Publication of digital culture subject textbooks
(Author's own edition)

In the case of elementary school-aged youth, the children encounter the Digital Culture subject for the first time in the third grade. We examined what references and knowledge materials are available in some teaching materials, in the area of information security and data protection in a broader sense, in connection with the awareness of cyber security.

- The third-grade textbook clarifies that *"here is a lot of data and information that reveals personal things about you."* You also name these: name, date of birth, residential address, student ID number, and education ID. That is, *"all data that allow them to know who you are, that is, to identify you."* In the textbook, the children are informed that, in addition to personal data, the consent of their parents is required to take photos and videos. It draws attention to the fact that, in addition to physical dangers, children must also pay attention to other dangers. However, the dangers can be avoided with a smart use and an adult's help. The curriculum emphasizes that the Internet does not only contain information and data that are correct in all cases. In the age-group textbook, we come across additional related concepts:

- In the case of elementary school-aged youth, in the fourth grade-textbook, the handling of fake news and the reaction to it, in the area of information protection, is explained in a very detailed manner. In addition, adapted to the age group, playful tasks are used to demonstrate what to do in the case of a lost password, as well as how to handle the influencing information.
- In the fifth grade, the approach to data protection and information protection is slightly neglected, and the focus of other areas of age-specific knowledge comes to the fore, e.g.: robotics, programming or making presentations.
- In the sixth grade, the concepts of data protection and data security already appear concretely. They define the data protection as protecting our data against unauthorized downloaded. They draw the students' attention to the fact that they can have downloaded to their data only with their own name and password. They also explain the concept of data security, which is protecting your data from being damaged or destroyed, and they recommend the saving and the backing up. For this age group, under the heading of "Ethical and healthy device use in the cloud and on the ground"; knowledge materials on the ethics of the Internet has been introduced, and an explanation is provided about the concepts of Internet addiction and gaming addiction.
- In the seventh grade, an entire chapter is devoted to the field of data protection. The textbook suggests how young people should manage their data, while using the Internet and defines what is considered personal data. A special feature of this year's course material is that it discusses which rule applies to the registration on the websites for the children under the age of fourteen and under the age of eighteen. Otherwise, in the case of the subject, the main focus is on word processing and presentation.
- The last part of the examined study materials is the eighth grade, which is also the most recent subject. The textbook was published in 2023. In this, a separate chapter "The e-world and online communication" deals with information security and data protection. In the eighth grade, the biggest content deals with the ways of editing tables, through 27 pages of the 113-page textbook, in a great detail. The textbook, edited for eighth graders, contains the most pages from among the examined books. At the end of the textbook, you can also find a summary collection of concepts, and it also contains a three-page summary chapter on the development of the computer.

The digital culture subject is a part of the curriculum, from the third to the eighth grade of elementary school. The subject, methodology and curriculum are very new. But in today's world, the concept of "new" is relative expression. In the digital age, we have to process more and more of the ever-accelerating information, so the curriculum is expected to need updating within a few years.

International projects researching cyber security awareness of young people and good practices

The concept of cyber security clearly includes a set of steps aimed at protecting digital data and devices. The timeliness of the topic is shown by the fact that there are many cross-border initiatives at the domestic and international level that examine the information security awareness of primary school-aged children, the situation of children's information protection and data protection. In this article, we present some of these initiatives that we consider relevant to our research.

DQ Institute

On September 24, 2020, the IEEE Standards Council approved the IEEE 3527.1 Standard for Digital Intelligence (DQ), the world's first global standard for digital literacy, digital skills, and digital readiness.

Digital intelligence (DQ) is a comprehensive set of technical, cognitive, metacognitive and socio-emotional competencies that are based on universal moral values, and enable individuals to face the challenges and take advantage of the opportunities of digital life. The DQ is based on three levels, eight areas and 24 competencies, which are composed of a system of knowledge, different skills, attitudes and values. The organization's senior officials are composed of Korean, Singaporean, American and European researchers.

The aim of the Singapore-based organization is to introduce and raise awareness of digital intelligence and assess its current state. The campaign specifically addresses young people and children, in order to draw their attention to the dangers of information protection and data protection. In 2022, they published their 29-question global assessment questionnaire for children.

The DQ Institute's children's online safety index, based on data from a survey of children aged 8-18 in 30 countries, concludes that 71 percent of children have experienced at least one cyber risk, including cyber abuse, some kind of addiction or just encountered risky content.

It categorizes five types of child attitudes, using age-appropriate pictogram styles. These are:

- Comfortable user: feels more comfortable online than offline. Potentially involved in various cyber risks.
- Ordinary user: average technology user who is not necessarily aware of either the risks or the opportunities. You tend to passively follow the algorithm or click on pop-ups.
- Always on: you communicate a lot with others online and don't pay much attention to potential cyber risks.
- Cautious: You're aware of potential cyber risks, but you're not fully exploring the digital world. You are likely to take low risks in the digital world.
- Digilog: A well-educated digital citizen who balances online and offline life and uses technology consciously.

The Office of Communications - Ofcom (United Kingdom)

The London-based Office of Communications (abbreviated and its commonly used name: Ofcom) is a public institution that publishes a report on children's information security and digital awareness every year, which is based on the surveys of the given year.

In the Ofcom's 2022 research, the digital media usage habits of children and their parents were examined. Based on this, in terms of early childhood data, prior to the relevant age group of this article, the percentage of 3-4-year-old children, living in the United Kingdom already have their own mobile device, 18 percent play games online and 24 percent have a profile on social media. In the age group 5-7, 28 percent already have their own mobile phone, 38 percent play online and 33 percent have a profile.

Data for the primary school age group:

60 percent of children aged 8-11 already have their own mobile phone, 84 percent use some messaging application, and 69 percent play games online. 32 percent of children have experienced some disturbing event – harmful for their age group – while using the Internet.

97 percent of the 12-15-year-old children have a mobile phone, 89 percent have some kind of social media profile, 76 percent play games online and 37 percent have seen something harmful for their age group, while using the Internet.

The statistics highlighted in the survey clearly show that research into the age group is relevant, and changes in the device systems can be continuously monitored.

SANGO project

SANGO is a cyber protection-preventive-educational publication for children, supported by the International Telecommunication Union (ITU), based on the research of the Young and Resilient Research Center of the University of Western Sydney. Its protagonist is SANGO, which playfully introduces children of preschool and primary school age to the use of digital devices and safe operation on online interfaces. The publication deals exclusively with the data protection and information security issues of minors, naturally with age-appropriate wording and pictorial (narrative) materials. The multi-part material can be called a gap-filler in its field. In the course of our research, we contacted internet lawyer Dr. Katalin Baracsi, who took care of the Hungarian translation, in a personal interview. The expert said that *"translations of seven SANGO materials have been completed, which include workbooks for children between the ages of 9-12, teacher's employment booklets, and handbooks for parents-teachers-political decision-makers-industry players.*".

Conclusion

In this article, we have examined what teaching materials are available in the field of domestic education, in order to raise the awareness of information security and data protection among young people of primary school age, and we have also briefly displayed some surveys and initiatives, related to domestic and international information security.

In order to protect the information security of primary school-aged youth, more and more educational programs and informative materials have been published. In this framework, there are information-protection and data-protection educational materials that are existing, modified and constantly developed, which raise awareness and protect the children's media usage habits, improves their knowledge of information security and the management of their personal data. These knowledge-materials try to help and create such frameworks that ensure for the data to be secured and protected against unauthorized downloaded and data breaches.

However, the creation of educational materials for the age groups dealing with cyber protection is not sufficient in itself to manage information security risks and prevent incidents. Knowledge must be passed on, and knowledge must be attained. In addition, it is necessary to start as many educational programs as possible, which help the conscious use of the Internet. Maintaining information security requires constant attention and commitment from all relevant actors, including public education organizations, national defense actors, non-profit organizations and initiatives. It is necessary to constantly monitor and research the current situation, which shows the protection of the online safety of young people and children, because based on the research, it is possible to react to the trends that generate new and new challenges and dangers, dictated by the IT world. Of course, all of this does not necessarily mean the creation of new teaching materials, because awareness and application of existing knowledge may be sufficient, with some supplementing and expanding steps. Educational programs should teach young people about the importance of internet safety, their legal protection, and should enlighten them about data protection and online security risks, so that they become protected against online harassment or cybercrime, as conscious digital device users.

Bibliography:

- ÇUBUKÇU, Ceren – AKTÜRK Cemal: The Rise of Distance Education during Covid-19 Pandemic and the Related Data Threats: A Study about Zoom. June 2020, https://dergipark.org.tr/en/download/article-file/2154547
- Ofcom: Children and parents: media use and attitudes report, 2022. 30 march 2022
- Overview OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Hungarian translation, OECD, 2003, https://www.oecd-ilibrary.org/docserver/9789264196391-sum-hu.pdf?expires=1700142236&id=id&accname=guest&checksum=08108BBFE9B5524DBCE41DA9B9434C94

- PINTÉR, Gergely (Ed.): Digital culture textbook 5, Office of Education, 2020
- PINTÉR, Gergely (Ed.): Digital culture textbook 6, Office of Education, 2020
- SZÉLL, Szilvia (Ed.): Digital culture textbook 7, Office of Education, 2022
- SZÉLL, Szilvia (Ed.): Digital culture textbook 8, Office of Education, 2023
- SZIKLAY, Júlia (Ed.): Key to the world of the net! NAIH's study on the safe and legal use of the Internet by children. NAIH, Budapest, 2013, ISBN: 978-963-08-7724-4
- SZŰCS, Endre – ZÁHONYI, Lajos: Historical development of information security – Milestones, events and answers. Security Science Review, 2021/3, pp. 81-91.
- VITÉZ, Annamária (Ed.): Digital culture textbook 3, Office of Education, 2021
- VITÉZ, Annamária (Ed.): Digital culture textbook 4, Office of Education, 2022
- WYLIE, Christopher – NIELSEN, E. S. – VOGT, B.: Cambridge Analytica and the Manipulation of Political Opinion: Implications for Privacy, Autonomy, and Democratic Principles. Journal of Social and Political Psychology, 2019

Internet links:

- https://edps.europa.eu/data-protection/data-protection/reference-library/information-security_en (downloaded 19 June 2023)
- https://edps.europa.eu/data-protection/data-protection/reference-library/information-security_en (downloaded 19 June 2023)
- https://honvedelem.hu/hirek/hazai-hirek/zrinyi-2026-2026.html (downloaded 19 June 2023)
- https://standards.ieee.org/beyond-standards/new-standard-will-help-nations-accelerate-digital-literacy-and-digital-skills-building/ (downloaded 23 May 2023)
- https://statinfo.ksh.hu/Statinfo/haViewer.jsp (downloaded 23 May 2023)
- https://www.dqinstitute.org/news-post/digital-citizenship-test-cyber-risk-and-digital-skills-assessment-launch/?fbclid=IwAR3s9_gtj5uHJoM9t-R5mM6ckDqN1sx9LE7Ns7W1nZ7YRcMzit1jTxpd1wE (downloaded 23 May 2023)
- https://www.europarl.europa.eu/news/hu/headlines/society/20211008STO14521/miert-fontos-a-kiberbiztonsag-es-mibe-kerulhet-egy-kibertamadas-az-erintettnek (downloaded 23 May 2023)
- https://www.ksh.hu/infografika/2023/becsongettek_2023.pdf (downloaded 23 May 2023)
- https://www.ofcom.org.uk/research-and-data/online-research (downloaded 23 May 2023)
- https://www.oktatas.hu/pub_bin/dload/kozoktatas/kerettanterv/Digitalis_kultura_K.docx (downloaded 23 May 2023)

- Protecting the rights of every child in the digital environment july 5. 2022. https://hlpf.un.org/2022/programme/protecting-the-rights-of-every-child-in-the-digital-environment-public-and-private (downloaded 23 May 2023)

Authors' personal interviews with:

- BARACSI, Katalin Dr. LL.M infocommunications lawyer Dr. Attila Péterfalvi, President of the National Authority for Data Protection and Freedom of Information (NAIH)

Legislation:

- 110/2012. (VI. 4.) Government decree on the publication, introduction and application of the National Core Curriculum
- GDPR, general data protection regulation: adopted by the European Parliament and the Council (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free flow of such data, and on the repeal of Directive 95/46/EC
- CXII of 2011 on the right to information self-determination and freedom of information law
- Directive 2011/93/EU of the European Parliament and of the Council (December 13, 2011) on combating the sexual abuse, sexual exploitation and child pornography of children and replacing Council Framework Decision 2004/68/JHA
- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - EU Children's Rights Strategy, Brussels 2021
- Regulation of the EUROPEAN PARLIAMENT and COUNCIL establishing rules for preventing and combating sexual abuse of children, Brussels 2022, proposal

FERENC BÁLINT[1]

ANTI-MONEY LAUNDERING WITH A SPECIAL FOCUS ON THE CYBER SECURITY THREATS AND VULNERABILITIES

THE ROLE OF INTERNAL CONTROL FUNCTIONS OF HUNGARIAN FINANCIAL INSTITUTIONS FOR AML COMPLIANCE

Abstract

Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CTF) refer to a set of tightening regulations and practices designed to prevent and detect illegal activities related to money laundering and terrorist financing.

Keywords: cybersecurity, financing, anti-money laundering, risk, control, fraud

Introductions

Money Laundering is the illegal process of taking funds generated from criminal activity, such as trafficking in narcotics, weapons, fraud, gambling, and making it appear to have originated from a legal source.

The United Nations estimates that between 2% and 5% of the world's GDP (Gross Domestic Product) is laundered every year. Roughly 10% of the laundered money is detected.

The money is typically laundered in the following three stages to make it appear legitimate:

- Placement: criminal proceeds are entered into the financial system.
- Layering: is the process of disguising the origin of criminal proceeds by making complex financial transactions or through accounting tricks.
- Integration: the process means reinserting the funds into the legitimate financial system.

Terrorism financing is the process of funneling funds to support the operational activities of different terrorist groups. Charitable organizations are considered as higher risk for the supporting of terrorism. Many countries worldwide have implemented measures to counter terrorism financing, integrating in their AML control framework.

Pursuant to the Hungarian Criminal Code, Money Laundering and Terrorist Financing are considered act of crime.

[1] ORCID: 0009-0009-8970-762X

Legal and Regulatory Requirements

Financial institutions worldwide are not only required by law to prevent criminals from using their platforms, but it is also the well-understood interest of the firms to act accordingly. Money Laundering and Terrorist Financing pose a significant risk to the stability not only on the level of the individual financial institutions, but even for the entire financial sector. Money laundering scandals caused banks' collapse and shocked countries. Ultimately, society pays the cost through an erosion of trust in the integrity of the financial system.

Introducing proper AML/CFT control framework is essential to avoid high supervisory fines, regulatory penalties, financial losses and reputational damage. Regulatory penalties may include limitation on conducting business activities or even the license revocation of the financial institution.

Applicable AML Laws and Regulations in Hungary[2]

Financial institutions in Hungary need to comply with the following laws and regulations:

- Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing;
- Act LII of 2017 on the Implementation of Restrictive Measures Imposed by the European union and the UN Security Council Relating to Liquid Assets and Other Financial Interest;
- 26/2020 (VIII.25.) MNB (Central Bank of Hungary) Decree on Anti-Money Laundering and Terrorist Financing;
- 21/2017 (VIII.3.) MNE (Ministry of National Economy) Decree on the Mandatory Substantive Elements of the Internal Code.

The objective of these laws and regulations is to prevent the cross-border laundering of proceeds of criminal activities through the financial system, the capital markets and other areas exposed to ML operations as well as to help combat the flow of funds financing terrorism.

Hungarian financial institutions are supervised by the Central Bank of Hungary (MNB).

One of the main focuses of the inspection of the supervisory bodies is the adequacy of the operation of the AMF/CTF. The fine imposed in the event of any related deficiency discovered by the MNB is detailed as a separate item.

[2] Central Bank of Hungary – Supervision, Anti-Money Laundering. https://www.mnb.hu/felugyelet/szabalyozas/penzmosas-ellen (downloaded 02 July 2023)

The role of the Financial Action Task Force (FATF)[3]

The Financial Action Task Force, FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against illegal activities caused by money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

The FATF sets international standards to ensure national authorities detecting illicit funds linked to drug trafficking, illicit arms trade, cyber fraud and other serious crimes. In total, more than 200 jurisdictions have committed to implement the FATF's Standards to prevent organized crime, corruption and terrorism.

Hungary's Vulnerability for Money Laundering[4]

In June 2022, MONEYVAL, the anti-money laundering body of the Council of Europe has published a follow-up report on Hungary's compliance with the FATF (Financial Action Task Force) standards. Consequently, Hungary has improved measures in fighting Money Laundering and Terrorist Financing, demonstrating good progress in the level of compliance with the FATF standards. Hungary fully complies with 32 out of the 40 FATF recommendations.

Hungary has been upgraded from potentially compliant to largely compliant in three areas related to the following:

- Correspondent banking: introduction of Enhanced Customer Due Diligence (EDD) measures, before the establishment of correspondent relationship with financial institutions of EU member states.
- High standards in the hiring process and providing ongoing trainings: Hungarian financial institutions are expected to adopt internal rules and measures to ensure that professionals with adequate skills are responsible for the AML/CTF measures.
- Transparency and beneficial ownership: Hungary introduced measures such as the requirement for companies to disclose all directors in the Companies Register, maintain up-to-date information on beneficial ownership, and adhere to a 30-day deadline for submitting registration data updates.

Hungary has to improve its AML/CFT measures related to the following areas: non-profit organizations, new technologies and cash couriers.

[3] Financial Action Task Force (FATF). https://www.fatf-gafi.org/en/the-fatf/who-we-are.html (downloaded 03 August 2023)

[4] Council of Europe – Newsroom – MONEYVAL report on Hungary: improvements in fighting money laundering and terrorist financing have led to upgraded ratings. https://www.coe.int/en/web/moneyval/-/moneyval-report-on-hungary-improvements-in-fighting-money-laundering-and-terrorist-financing-have-led-to-upgraded-ratings (downloaded 03 August 2023)
Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – MONEYVAL (monitoring body of the Council of Europe) – Anti-money laundering and counter-terrorist financing measures Hungary, 5th Enhanced Follow-up Report, May 2022. https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-fur/Moneyval-FUR-Hungary-2022.pdf.coredownload.pdf (downloaded 15 July 2023)

The Three Lines of Defense – AML Related Responsibilities[5]

The first line of defense function's AML related responsibilities are linked to client onboarding. Related business unit is performing due diligence measures during onboarding of clients.

Compliance, as a second line of defense function, is primary responsible for preventing Money Laundering and Terrorism Financing. The responsibility of Compliance is the ongoing monitoring of AML suspicious clients and transactions, and overall the compliance of the firm with the relevant laws and regulations.

Risk Management, being also a second line of defense function, also plays an important role in assessment and detection of risks, fraud management and cyber operations.

The role of *Internal Audit* (IA), being the third line of defense, is to provide independent assurance to the financial institution by assessing the legal and regulatory compliance and operational effectiveness of its AML policies, processes and control framework. Internal Audit is seeking sufficient mitigating controls to address ML/TF risks and reduce them to an acceptable level. Most importantly, IA is issuing recommendations on how identified weaknesses can be addressed by the management of the financial institution.

AML Internal Control Framework[6]

All risks associated with financial crime involve three kinds of countermeasures: identifying and authenticating the customer, monitoring and detecting transaction and behavioral anomalies, and mitigating risks.

The AML internal control framework consist of the below elements:

AML Governance – Organization, Written Guidelines, Awareness

A designated *AML Compliance Officer* has to be appointed who oversees the entire AML program. Additionally, financial institutions must provide adequate resources appropriate to the level of risk and size of the organization.

[5] The Institute of Internal Auditors – The IIA's Three Lines Model. https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf (downloaded 15 July 2023)

[6] Wolters Kluwer Legal and regulatory research – Anti-money laundering https://net.jogtar.hu (downloaded: 30 July 2023);
International Monetary Fund – ANTI-MONEY LAUNDERING/COMBATING THE FINANCING OF TERRORISM (AML/CFT). https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm#typologies (downloaded: 30 July 2023);
Trulioo – KYC: 3 Steps to Achieving Know Your Customer Compliance. https://www.trulioo.com/blog/kyc (downloaded 09 August 2023)
Central Authority of the National Tax and Customs Administration, the Hungarian Financial Intelligence Unit (HFIU) - NAV PEI. https://nav.gov.hu/penzmosas (downloaded 11 August 2023)

Each financial institution shall develop *AML policy and procedures* reasonably designed and introduce appropriate internal controls accordingly to detect money laundering and terrorism financings. These internal policies and procedures are binding on all employees.

Periodic AML training needs to be developed for all staff, tailored to the risk profile and activities of the financial institution. Employees have to familiarize themselves with the applicable AML/CTF legal rules and prescriptions, to recognize business relationships and transaction orders enabling money laundering or terrorist financing.

Know Your Customer (KYC)

The KYC check is an upmost crucial process of identifying and verifying the client's identity during client onboarding and periodically afterwards.

The KYC process includes to collect and store data and documents, required by law, to verify the adequacy and effectiveness of the identity card (Proof of Identity), document verification such as utility bills (Proof of Address).

The application of rigorous KYS processes, biometric identification during the digital onboarding process, multi-factor authentication mechanism for customer verification and identification of mobile device to authenticate online banking transactions are preventive control measures for financial institutions.

Customer Due Diligence (CDD)

According to the relevant Hungarian legal rules, the customer due diligence is mandatory in the legally defined cases. Specifically, CDD measures have to be conducted upon the establishment of a client relationship, in case of cash transactions equal to or exceeding HUF 4.5 million, and in case of currency conversion above the equivalent of HUF 300,000.

Financial institutions require to adopt a risk-based approach for conducting ongoing customer due diligence to understand the nature and the purpose of the customer relationships. CDD measures include the collection, identification and verification of all AML relevant data and documentation of the potential or existing customer (client, his/her representative, beneficial owner). It includes the analysis of the customer's identity source of funds, source of wealth, employment, history, etc.

In order to meet these requirements, financial institutions have to keep all client identification data and documents up to date at all times. Consequently, ongoing monitoring on the compliance with the various laws and regulations is essential.

Enhanced Due Diligence (EDD) process provides a greater level scrutiny and more comprehensive understanding of the risks associated with the clients. EDD is expected to perform on high risk ranked clients of the financial institution.

Customers with *Politically Exposed Person* (PEP) status, clients from high risk third countries with strategic deficiencies, clients from high risk business sectors and customers with unnecessary complex business relationships are examples for the high-risk classification.

Different in-house and external software of third-party vendors are relied on to verify client information, which are designed to identify potential suspicious and fraudulent data and/or document. Depending on the risk classification of the client, CDD can be performed by means of direct and indirect way of electronic means of communication.

Sanction Screening

The Financial Action Task Force (FATF) keeps a list of jurisdictions that are strategically deficient regarding their AML/CFT practices (also called as Grey and Black lists).

Monitoring of suspicious transactions by automated screening system including international sanction list (e.g. UN, EU, OFAC), PEP lists, bad actor screening and adverse media are essential elements of fighting against Money Laundering and Terrorist Financing.

Transaction Monitoring and Reporting of Suspicious Transactions

Definition and set of suspicious scenarios in the monitoring system (based on the number of transactions, amounts, types of counterparties, countries involved) are required detective controls to filter out and even block suspicious transactions as well as tightening of fraud detection rules.

Typical transaction patters are: immediate high or low value transactions after account opening, immediate cash withdrawals or transfers of large amounts, transfers of funds to and from high-risk ML jurisdictions, third party transactions, etc.

Ongoing real-time transaction monitoring will enable financial institutions to identify suspicious activity, eliminate false positive hits of alerts through the automatic monitoring system, and report promptly suspicious transactions in a timely manner, within five business days.

The process for identifying, investigating and reporting suspicious transactions to the Financial Intelligence Unit (FIU) should be clearly documented in the AML policy and procedures.

The suspicious activity report (SAR) is a mechanism that tracks suspicious activities that are unusual. It should include relevant records about the client, and data related to AML-suspicious transactions.

In Hungary, the Central Authority of the National Tax and Customs Administration, the Hungarian Financial Intelligence Unit (HFIU) is responsible for the receipt, analysis and transmitting of reports of suspicious transactions.

Record Keeping

Institutions must keep records of all customer transactions throughout the business relationship and for eight years afterwards.

Cyber Risk and Illicit Financial Flows[7]

In today's digital world, the integration of technology into the financial systems provides tremendous efficiency. However, with these developments, new risks and challenges, especially in the field of AML, cannot be avoided. Cyber security plays a vital role in the fight against Money Laundering by protecting financial institutions and the clients from cyber threats.

Cyber Risk and Cybersecurity Measures

Risks for financial institutions arise from different factors, not only the vulnerabilities to fraud and financial crime inherent in automation and digitalization, but also the increased growth in transaction volumes. Cybercrime and malicious hacking have also intensified. Digital services became integrated part of the daily life. As more citizens are participating in various online activities, consequently also jurisdictions are increasingly connected with information and funds moving across the borders.

The COVID-19 pandemic accelerated the transition from in-person activities into digitalization, such as on-line client identification and verification, account opening, payments, etc. Fraudulent activities have significantly increased through social media. This change also impacted the ML landscape, including the increase use of digital banking, payment platforms and remote transactions.

Financial institutions are required to collect and store sensitive information about their customers and their transactions and store such data and documents in their systems. The vulnerability in such systems and applications can lead to data breaches.

Institutions have to introduce proper cybersecurity measures to protect their data, systems, devices and networks from unauthorized access, and ensure confidentiality, integrity and availability of information. Besides, an effective and continuously improving fraud and cybersecurity risk management necessitates an ongoing assessment and adjustment of the internal risk management and control framework of the financial institutions.

[7] FAFT – Illicit Financial Flows from Cyber-Enabled Fraud, November 2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf (downloaded 11 October 2023)
McKinsey & Company – Risk & Resilience: Financial crime and fraud in the age of cybersecurity. October, 2019. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity#/ (downloaded 20 August 2023)
Cybergate International – Exploring how Cyber security and Anti Money Laundering go hand-in-hand. https://cybergateinternational.com/blog/exploring-how-cyber-security-and-anti-money-laundering-go-hand-in-hand/ (downloaded 23 August 2023)

While information security risks can vary depending on the specific implementation and systems involved, there are several common risks associated with AML processes. Some information security risks in the area of AML include the following:

- Data Breaches: A significant risk is the unauthorized access or disclosure of sensitive customer information, including personal identification details and financial records. If attackers gain access to such data, they can exploit it for criminal purposes or sell it on the dark web.
- Inadequate Identity Verification: Weak identity verification processes can lead to the creation of false or fraudulent customer accounts, allowing money launderers to hide their true identities. If AML systems fail to properly authenticate customers, it becomes easier for criminals to bypass detection measures.
- System Vulnerabilities: AML systems can be vulnerable to various cybersecurity threats, such as malware, phishing attacks, or ransomware. If attackers successfully exploit these vulnerabilities, they may gain unauthorized access to AML systems, compromise their integrity, or disrupt their operations.
- Insider Threats: Employees or individuals with authorized access to AML systems can pose a significant risk. Insiders with malicious intent may manipulate or misuse AML systems to facilitate money laundering activities or compromise the integrity of the system.
- Disinformation / Misinformation: The increasing use of social media platforms and online media has led to a rise in campaigns spreading disinformation and misinformation. The aim is to cause fear and uncertainty.
- Lack of Timely Data Analysis: Effective AML systems rely on real-time monitoring and analysis of financial transactions to detect suspicious patterns or activities. If there are delays or gaps in data analysis, potential money laundering activities may go unnoticed, reducing the effectiveness of the AML program.
- Regulatory Compliance: AML regulations are continuously evolving, and organizations must keep up with changes to remain compliant. Failure to comply with regulatory requirements can result in penalties, legal consequences, and reputational damage.

Any cyber incident is to be considered as a suspicious transaction. To mitigate cyber risks, organizations should implement robust security measures, such as encryption, access controls, secure data storage, and regular security assessments. Cybersecurity technologies can help financial institutions identify suspicious patterns or anomalies in the financial transactions. Additionally, staff training, strict identity verification procedures, and continuous monitoring of AML systems are essential to enhance information security in AML/CTF processes.

Cyber-Enabled Fraud (CEF)

Cyber-enabled fraud is a growing transnational organized crime. CEF criminal syndicates are often well structured into distinct sub-groups with specialized areas of criminal expertise, including money laundering. These sub-groups may also be loosely organized and de-centralized across different jurisdictions. As illicit proceeds may be laundered through the financial systems of multiple third-party jurisdictions, it further complicate efforts to investigate CEF activity.

The digitalization has allowed CEF criminals to develop and enhance the scale, scope, and speed of their illicit activities. Criminals are taking advantage of social media and messaging platforms to recruit money mules across borders at scale. The Virtual Private Networks (VPNs) and 'The Onion Router' can allow criminals to process illicit activities anonymously, making difficult for authorities to identify criminals performing the ML activities.

Proceeds can be laundered quickly through a network of accounts, which often spread across multiple jurisdictions and financial institutions. Jurisdictions must collaborate multi-laterally to effectively and expeditiously detect and avoid CEF proceeds that are laundered across borders. To do so, jurisdictions should leverage and support existing (and any future) multi-lateral mechanisms (such as INTERPOOL) for rapid international co-operation and information exchange to more effectively combat CEF.

INTERPOOL maintains global databases containing police information on criminals and crime, moreover it provides operational and forensic support to prevent financial crime and corruption, counter-terrorism, cybercrime and organized crime.

Project on Countering Illicit Financial Flows from CEF

The first strong collective commitment to tackling transnational organized criminals and their networks is the joint project among the Egmont Group, FATF and INTERPOL.

The Egmont Group of Financial Intelligence Units (Egmont Group) serves as a forum for financial intelligence units (FIUs) around the world to improve co-operation in the fight against ML.

The transnational illicit fund flows and the deceptive social engineering techniques can lead to the following different types of criminal activities:

- Business Email Compromise (BEC) fraud: Based on email instructions victims tare asked to transfer funds to new payments accounts.
- Phishing fraud: Victims are deceived into revealing sensitive information such as personal data, banking details or account login credentials. The criminal will then use the information to drain the victims' money from their payment's accounts, open new payment accounts or make fraudulent transactions.

- Social media and telecommunication impersonation fraud: Victims are contacted via mobile or social media applications by criminals pretending to be government officials, relatives or friends, and prey on the victims' emotions to induce payment or hand over control of payments accounts or to carry out financial activities such as a loan application or an account opening to receive criminal proceeds.
- Online trading/ trading platform fraud: Victims are deceived by fake advertisements or advisors online to non-existent or fake (fraudulent) platforms for trading or investment.
- Online romance fraud: Victims are convinced into sending money to criminals after being convinced that they are in a romantic relationship.
- Employment scams: Fake job offers on social media platforms trick victims to pay scammers upon various excuses.

Consequently, criminals may steal identities through various techniques and information technological tools, including phishing, purchasing, or deceiving someone to voluntarily hand over their identity. One of such technological tools is the deepfake technology. With the help of machine learning algorithms, a fraudster might create a deepfake of someone's voice or video, which can then be used to impersonate that person over the phone or in biometric authentication systems. Criminals then directly set up and control accounts using these stolen or falsified identities. This makes it more difficult to trace ML activities as the account holders may not even be aware of their involvement.

According to the INTERPOOL Global Crime Trend Report 2022, online scams are one of the cybercrime trends perceived as posing 'high' or 'very high' threats globally.

Countering CEF and Related ML

Based of FATF study, experiences from both private and public sectors begin to demonstrate that anti-fraud and AML processes are complementary. Anti-fraud measures include leveraging technology to help users automatically reject the reception of fraudulent messages, creating account security features, controls and rules, warning messages in anti-virus software for potential phishing sites, as well as introduction of real- time transaction monitoring.

The effective prevention of CEF and related ML has been managed on national and international levels, while enhancing the various preventive and detective control measures, as detailed below.

Enhancing domestic co-ordination across public and private sectors:

- Jurisdictions should develop co-ordination mechanisms to bring together relevant competent authorities to tackle CEF and the laundering of related proceeds. This includes technical cybercrime experts as well as non-traditional sectors such as social media platforms, e-commerce, telecommunication and internet service providers. Jurisdictions should also leverage public-private partnerships to improve detection and investigations, and accelerate operational asset recovery responses.

- A good practice involves the creation of a dedicated centralized unit that can control relevant information and co-ordinate actions across various public and private sectors, including investigations, asset recovery and fraud prevention.

Supporting multi-lateral international collaboration:

- Jurisdictions should work together to intercept CEF-proceeds expeditiously. Intervention is showed to be generally most effective within 24 to 72 hours of a CEF incident. A global united approach is required to effectively trace and recover CEF-proceeds, which are being laundered and distributed across multiple jurisdictions.
- To do so, jurisdictions should leverage and support existing (and any future) multi-lateral mechanisms (such as INTERPOL's I-GRIP and the Egmont Group BEC Project) for rapid international co-operation and information exchange to combat CEF. Such multi-lateral mechanisms also allow jurisdictions to collaborate and collectively dismantle transnational CEF syndicates.

Strengthening detection and prevention:

- To enhance detection, jurisdictions should ensure ease of victim reporting, for example, through dedicated platforms that allow streamlined reporting. Jurisdictions should also work with the private sector to improve suspicious transaction reporting.
- Jurisdictions should promote awareness and vigilance against CEF through public education, including to share tell-tale signs of CEF and enhancing cyber literacy. Prevention plays a key role in reducing the overall profitability for CEF syndicates. Jurisdictions can also collaborate with the private sector to support CEF prevention strategies, such as consumer protection and removal of criminal instrumentalities.

Crowdfunding for Terrorism Financing[8]

Crowdfunding is an innovative fundraising solution, used by people from all over the world to fund legitimate ideas, projects or business ventures, but it can be exploited by bad actors.

Although the majority of crowdfunding activity is legitimate, Financial Action Task Force (FATF) research has shown that the Islamic State of Iraq and the Levant (ISIL), Al-Qaeda and ethnically or racially motivated terrorist (EoRMT) individuals and groups have exploited it to raise money for terrorist financing (TF) purposes.

[8] FATF – FAFT Report Crowdfunding for Terrorism Financing, October 2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf (downloaded 11 October 2023)

Based on the FATF Report, the below four main ways can be identified in which crowdfunding platforms can be abused for TF purposes:

- Abuse of humanitarian, charitable or non-profit causes: Humanitarian, charitable and non-profit causes can serve as effective covers for financial solicitation and are in some cases abused for TF purposes.
- Use of dedicated crowdfunding platforms or websites: EoRMT individuals and groups use crowdfunding platforms or website for raise money for various activities, some of which are protected by law, other are promoting hate or violence.
- Use of social media platforms or messaging apps: Social media sites and online messaging services are used strategically by terrorist actors for TF purposes. These actors share campaign links or payment instructions with their followers, recruit supporters, share advice on how to avoid detection, and take advantage of features like encryption to transmit sensitive details.
- Interaction of crowdfunding with virtual assets (VA): As digital forms of payment continue to evolve globally; the crowdfunding industry has also incorporated funding options tied to VA. While Bitcoin has been the most visible, other types of VAs such as privacy coins are increasingly noted and pose unique challenges for investigators.

In practice, criminals and terrorists rely on multiple methods and various techniques combinations to raise funds.

While certain jurisdictions and industry participants proactively implement measures to mitigate these risks, anti-money laundering and counter-terrorist financing (AML/CFT) regulation is not consistent across the globe. The complexity of crowdfunding operations, lack of data, and the use of anonymizing techniques also complicate tracing efforts for law enforcement, reporting entities and supervisors. Jurisdictions and stakeholders involved in the crowdfunding industry need to identify and understand TF risks associated with this activity and introduce risk-based measures to mitigate potential abuses.

Conclusion

The digital transformation has inevitably led to new cybersecurity treats due to the COVID-19 pandemic and the war in Ukraine. The changed political and economic environment have created more possibilities for cybercriminals, while the compliance with the AML/CTF laws and regulations are crucial in the protection of the financial sector.

The cyber-enabled fraud is expected to grow with the rising trend of digitalization across the globe. Jurisdictions should be prepared of the vulnerabilities across various sectors that criminals may exploit to enhance ML techniques. Besides the importance of the preventive and detective controls, and because of the de-centralized nature of CEF and related ML, jurisdictions need to enhance collaboration between various sectors and entities both on domestic and international level.

The implementation of sound AML/CFT policies and procedures and robust cybersecurity measures are crucial in protecting the safety, soundness, stability and integrity of the financial system. The impact; however, is not limited to monetary losses; it can have devastating social and economic implications.

Hungary is continuously working to strengthen its AML/CTF internal control framework to ensure an increased security for the clients and the entire financial sector. Based on the follow-up report of the Council of Europe AML body MONEYVAL, Hungary has demonstrated good progress in the level of compliance with the FATF standards.

Bibliography:

- Central Authority of the National Tax and Customs Administration, the Hungarian Financial Intelligence Unit (HFIU) - NAV PEI. https://nav.gov.hu/penzmosas (downloaded 11 August 2023)
- Central Bank of Hungary – Supervision, Anti-Money Laundering. https://www.mnb.hu/felugyelet/szabalyozas/penzmosas-ellen (downloaded 02 July 2023)
- Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – MONEYVAL (monitoring body of the Council of Europe) – Anti-money laundering and counter-terrorist financing measures Hungary, 5th Enhanced Follow-up Report, May 2022. https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-fur/Moneyval-FUR-Hungary-2022.pdf.coredownload.pdf (downloaded 15 July 2023)
- Council of Europe – Newsroom – MONEYVAL report on Hungary: improvements in fighting money laundering and terrorist financing have led to upgraded ratings. https://www.coe.int/en/web/moneyval/-/moneyval-report-on-hungary-improvements-in-fighting-money-laundering-and-terrorist-financing-have-led-to-upgraded-ratings (downloaded 03 August 2023)
- Cybergate International – Exploring how Cyber security and Anti Money Laundering go hand-in-hand. https://cybergateinternational.com/blog/exploring-how-cyber-security-and-anti-money-laundering-go-hand-in-hand/ (downloaded 23 August 2023)
- FAFT – Illicit Financial Flows from Cyber-Enabled Fraud, November 2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf (downloaded 11 October 2023)
- FATF – FAFT Report Crowdfunding for Terrorism Financing, October 2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf (downloaded 11 October 2023)
- Financial Action Task Force (FATF). https://www.fatf-gafi.org/en/the-fatf/who-we-are.html (downloaded 03 August 2023)

- International Monetary Fund – ANTI-MONEY LAUNDERING/COMBATING THE FINANCING OF TERRORISM (AML/CFT). https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm#typologies (downloaded: 30 July 2023)
- McKinsey & Company – Risk & Resilience: Financial crime and fraud in the age of cybersecurity. October, 2019. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity#/ (downloaded 20 August 2023)
- The Institute of Internal Auditors – The IIA's Three Lines Model. https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf (downloaded 15 July 2023)
- Trulioo – KYC: 3 Steps to Achieving Know Your Customer Compliance. https://www.trulioo.com/blog/kyc (downloaded 09 August 2023)
- Wolters Kluwer Legal and regulatory research – Anti-money laundering https://net.jogtar.hu (downloaded: 30 July 2023)

ISTVÁN TALIÁN[1]

WINDS OF CHANGE ‐ ON THE SUBJECT OF 4 IMPORTANT RECENT AMERICAN ARTICLES

Recently, 4 very important articles were published in the official journal of the American National Defense University, Joint Forces Quarterly (abbreviated: JFQ). The line was opened by General Mark A. Milley, former chairman of the Joint Chiefs of Staff, whose article, "Strategic Inflection Point," appeared in JFQ Issue 110 (Q3 2023). The tone of all four articles is set by the foreword of General Milley's article: *"Geostrategic competition and rapidly advancing technology are driving fundamental changes to the character of war. Our opportunity to ensure that we maintain an enduring competitive advantage is fleeting. We must modernize the Joint Force to deter our adversaries, defend the United States, ensure future military advantage, and, if necessary, prevail in conflict. The Joint Force has taken the first step by developing and publishing the Joint Warfighting Concept (JWC) and updating Joint Publication 1, Doctrine for the Armed Forces of the United States. The JWC is a joint, combined vision for how the U.S. military will operate across all domains. The next step is to create a leadership structure that turns concepts into capabilities. The Joint Force must make fundamental changes now to win the next war and, by doing so, we will deter the war from happening in the first place."*[2]

General Milley provides the American and allied armed forces with the theoretical basis for evaluating the situation in the future world and, as a result, the future of the Western armed forces, and in the situation that has occurred, sets the framework for the further development of our forces. He writes about the "change in the character of war", the "change in the global world order", the "unification of views on the concept of joint-force warfare", the "results of concept development so far", the "Joint Warfighting Concept" defining warfare at a strategic level and JP 1 (Joint Publication 1), i.e. about the most important cornerstones of the "Doctrine of the Armed Forces of the United States", the necessary "Capability Development", the "Future-Focused Organization of Force Development and Planning" and states that the Joint Force Requirements Oversight Committee must be filled with new life in order the future force and its own doctrinal environment governing the way of warfare can operate successfully.

The following article exploring the topic of change is written by Thomas A. Walsh and Alexandra L. Huber and was published in JFQ Issue 111 (2023, Issue 4) entitled "A symphony of capabilities".

[1] ORCID: 0000-0002-1817-3247

[2] https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-110/jfq-110_6-15_Milley.pdf?ver=XE5o7a8f80Ro99ue8Vh-IQ%3d%3d (downloaded 05 November 2023)

This article breaks down the tasks assigned to each military force from the situation outlined in General Milley's article and from the strategic force development situation, along the lines of the “Joint Military Concept”.[3]

The third article in a row is from the pen of Admiral Christopher W. Grady, Vice Chairman of the Joint Chiefs of Staff.[4] The article was published in JFQ issue 111 (Q4 2023).

In the article, Admiral Grady explains how the American side visions to transfer the “Joint Warfare Concept” into the daily practice, as well as how this process is envisioned to be accelerated; what role is assigned to innovation; how important a role is assigned to continuous experimentation and the continuation of war games in this process; and finally, it rephrases the eternal question of all armed forces: who will be responsible for all this? After all, regardless of the nationality, one of the most comprehensive common characteristics of all armies in the world is that the enlisted soldiers, petty officers, the non-commissioned officers, the subordinate officers, the senior officers and the generals are also responsible for everything they do or fail to do.

The tasks of preparing for future warfare are concluded in the 4th part of the article series, which comes from the pen of General Philippe Lavigne, of the French Air Force, currently Commander of the Allied Command transformation (ACT).[5]

The message of the article is that, in addition to the U.S. Joint Warfighting Concept (JWC), several other allied concept developments are taking place in parallel, so that the Allied forces can meet the challenges and warfare expectations of the future – but NATO's overall expectation to deepen the cooperation between the member states in all areas makes it especially necessary for the Allies to jointly develop the concept of future warfare, which is mostly dictated by the challenges of the increasingly digitized world. The article presents the “control of new realities”, at the strategic level, a concise but comprehensive presentation of the novelties within the new realities (“more, faster and everywhere”), that it is necessary to prepare for the implementation of “multidomain operations”, that the NATO must also develop a new, basic, joint warfare concept, that handling new situations must be flexible and agile, that massive changes and changes must preserve the interoperability of allied forces, and then, as a final word, it states that the forces of NATO member countries must either accept and implement the necessary changes at a high level – or, in the long run, they will be the losers of the change process.

With General Lavigne's article, the three American articles on the long-term, forward-looking, adequate reform of the armed forces and warfare become a joint NATO task.

[3] https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-111/jfq-111_4-15_Walsh-Huber.pdf?ver=TwePyLVymtN8924udhzIxQ%3d%3d (downloaded 05 November 2023)

[4] https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-111/jfq-111_16-24_Grady.pdf?ver=mSwZtHE-hBpGdgBxlYkhQg%3d%3d (downloaded 05 November 2023)

[5] https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-111/jfq-111_25-31_Lavigne.pdf?ver=ggnzk36Wtq6gxEZgLOC27w%3d%3d (downloaded 05 November 2023)

The reform of the Hungarian Armed Forces is underway, and the defence budget in proportion to GDP has risen to a height not seen since the since the change of the political system in 1990, which also enabled military technology modernization not seen ever since. At the same time, based on what was read in the article, it has become a common expectation among NATO allies that the Hungarian Defence Forces (and the entire legal, doctrinal, force organization and defence industry environment that supports it) go in the same direction as the development and concepts of the military and warfare methods paved by the Americans. and be realized in such a way that the Hungarian Defence Forces meet all the expectations of the interoperable implementation envisioned by General Milley and made a task and expectation of NATO by General Lavigne. The Honvédség is the army of a country that is on NATO's external, militarily most endangered border, so its protection can clearly only be ensured by military means if, in addition to maximizing the human, economic and military potential of the Hungarian people and Hungary, they are ready and able at a strategic level, to carry out multinational defence activities in the entire territory of the country, and in the entire spectrum of these strategic-level defence activities, if the Honvédség is interoperable with the supporting Allied forces arriving here in case of a joint defence need - based on NATO's strategic-level plans.

The American and top-level NATO senior management formulated the tasks, the bar was set high, but so far, the Hungarian Defence Forces and the Hungarian Military National Security Service and its legal predecessors, which support the general execution of the defence of the Homeland and through that, the Allied territories have always managed to meet it reassuringly. It is somewhat urgent for all domestic stakeholders to break the big tasks defined by the above four guiding articles into small change as soon as possible.

And how the expected future developments formulated by the authors of the articles will affect the military intelligence and the counterintelligence, as well as the cyber offensive and defensive activities now accepted as the latest national security domain, cannot yet be known, since these are the war fighters, “the forces” envisioned above that will set the frameworks for the special services and their activities. One thing can be known though: that the changes in the activities of the joint forces will require immediate changes in the legal and professional regulation of both military intelligence and military counterintelligence, as well as the adaptation of the “usual” intelligence and counterintelligence activities will have to be adjusted to expectations and the realities of the future.

AUTHORS OF THIS ISSUE

- **ANDRÁS ÁRPÁD NOVÁK** is a scientific fellow of the National Security Institute of the University of Public Service, Budapest;
- **ENDRE SZŰCS** is an assistant professor of the Institute of Mechanical and Safety Sciences at the University of Óbuda, Budapest;
- **ÁRON TARKÓ** is a student of the doctoral school of University of Public Service, Budapest;
- **ANDRÁS JÓZSEF ÜVEGES** is a PhD student of the Doctoral School of Military Engineering of the as well as a scientific associate of the National Security Institute of the University of Public Service, Budapest;
- **FERENC BÁLINT** is a PhD student of the Óbuda University, Budapest;
- **ISTVÁN TALIÁN** is the editor of the National Security Review magazine;
- **KATALIN TAKÁCS-GYÖRGY** PHD, is a professor of the Keleti Faculty of Business and Management, Department of Business Development and Infocommunications at the Óbuda University, Budapest;
- **LAJOS ZÁHONYI** is a PhD student of the Óbuda University Doctoral School on Safety and Security Sciences, Budapest;
- **MADINA IGIBAYEVA** is a student of the UPS Ludovika, PhD School of Military Science;
- **RUDOLF NAGY** PhD. habil, is a professor of the Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Institute of Mechanical Engineering and Security Sciences, Budapest;
- **TAMÁS SOMOGYI** is a PhD student of the Óbuda University Doctoral School on Safety and Security Sciences, Budapest;
- **TIBOR BABOS** is a PhD student of the Óbuda University, Doctoral School of Safety and Security Sciences, Budapest;
- **TIBOR SZILVÁGYI** PhD, is a free-lance security and defence policy analyst;
- **WU YUE** is a PhD student of the Óbuda University, Doctoral School of Safety and Security Sciences, Budapest.

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, reconnaissance, 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. pp. 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. KOVÁCS, Jenő: Roots of the Hungarian Military Science, ideological problems of its development. p. 6.
2. ÁCS, Tibor: Military culture in the reform era. p. 34.
3. BEREK, Lajos: Basic elements of research work in Military Science. p. 33.
4. www.globalsecurity.org/army/iraq (downloaded: 19 April 2012)

List of biographical references (biography):

We have to fill the list by arranging the authors' name in alphabetical order.

Examples:

1. ÁCS, Tibor: Military culture in the reform era. Zrinyi Publishing House, Budapest, 2005, ISBN 963 9276 45 6
2. BEREK, Lajos: Basic elements of research work in Military Science. In: Tivadar SZILÁGYI (Ed.): Excerptions. Zrínyi Miklós Military Academy, Budapest, 1944. pp. 31-50.
3. KOVÁCS, Jenő: Roots of the Hungarian Military Science, ideological problems of its development. New Defense Review, 2005/3. pp. 1-7, ISSN 1216-7436
4. www.globalsecurity.org/army/iraq (downloaded: 19 April 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.