



NEMZETBIZTONSÁGI SZEMLE

Kiemelt közlemények

LENDVAI TÜNDE – KRASZNAY CSABA: A SARS-CoV-2-vírus okozta fertőzés terjedését nyomon követő és karanténellenőrző applikációk

ERDÉLYI ÁKOS: Az online térben bekövetkező zaklatások lehetséges okai, dinamikai jellegzetességei és megoldási lehetőségei

ZOLTÁN LECHNER: *Opposing Discourses of Terror: The Use of the Terrorist Label by the Turkish and Russian Governments in the Northern Syrian Conflict*

9. évf. (2021)
3. szám

ISSN 2064-3756 (elektronikus)



LUDOVIKA
EGYETEMI KIADÓ

Impresszum

Nemzetbiztonsági Szemle

A Nemzeti Közszerológati Egyetem Nemzetbiztonsági Intézetének
elektronikus (online) megjelenésű tudományos folyóirata

HU ISSN 2064-3756 (elektronikus)

A szerkesztőbizottság elnöke

Dr. habil. Boda József, Nemzeti Közszerológati Egyetem

A szerkesztőbizottság tagjai

Dr. Béres János

Dr. Botz László

Dr. habil. Dobák Imre

Dr. Philipp Fluri, Svájc

Dr. Hazai Lászlóné

Dr. Kobilka István

Dr. Kovács Zoltán András

Dr. Ludek Michalék, Csehország

Prof. Dr. Padányi József

Dr. Regényi Kund Miklós

Prof. Dr. Resperger István

Prof. Dr. Szakály Sándor

Dr. Takács Tibor

Dr. Vida Csaba

Főszerkesztő

Dr. habil. Dobák Imre, Nemzeti Közszerológati Egyetem

Szerkesztőség

Nemzeti Közszerológati Egyetem, Nemzetbiztonsági Intézet

Szerkesztő: Dr. Deák József

Szerkesztőségi titkár: Mezei József

Internetes elérhetőség: <https://folyoirat.ludovika.hu/index.php/nbsz>

Kiadó

Nemzeti Közszerológati Egyetem | Ludovika Egyetemi Kiadó

Kapcsolat: www.ludovika.hu; kiadvanyok@uni-nke.hu

Székhely: 1083 Budapest, Ludovika tér 2.

A kiadásért felel: Koltay András rektor

Olvasószerkesztők: Gergely Zsuzsánna, Resofszki Ágnes, Zsávolya Zoltán

Tördelőszerkesztő: Kőrösi László



Tartalom

Lendvai Tünde – Krasznay Csaba

A SARS-CoV-2-vírus okozta fertőzés terjedését nyomon követő
és karanténellenőrző applikációk 3

Erdélyi Ákos

Az online térben bekövetkező zaklatások lehetséges okai, dinamikai
jellegzetességei és megoldási lehetőségei 18

Zoltán Lechner

Opposing Discourses of Terror: The Use of the Terrorist Label
by the Turkish and Russian Governments in the Northern Syrian Conflict 33

Eck Gábor

A terrorizmus és az információs tér kapcsolódási pontjai. 54

Majorosi Ádám

Az Oszmán Birodalom hírszerzése 65

Lendvai Tünde¹ – Krasznay Csaba²

A SARS-CoV-2-vírus okozta fertőzés terjedését nyomon követő és karanténellenőrző applikációk

Contact Tracing and Quarantine Control Applications against the Spread of SARS-CoV-2 Virus Infection

A koronavírus-applikációk, vagyis a kontaktusok nyomon követését és a karanténszabályok távoli ellenőrzését lehetővé tévő okostelefonos megoldások a világ számos államában strukturális elemét képezik a pandémia miatt szükségessé váló válságkezelési gyakorlatnak. A tanulmány a Kínai Népköztársaság és a Koreai Köztársaság által alkalmazott koronavírus-applikációk és kiegészítő, IT-re támaszkodó adminisztratív intézkedések bemutatásával és értékelésével javaslatokat fogalmaz meg Magyarország számára a technológiai alapú válságkezelési mechanizmusok integrálhatóságára vonatkozóan. A kutatás bemutatja a hazánkban elérhető alkalmazások körét, valamint a magán- és állami szféra fejlesztéseinek markáns jellemzőit, majd sorra veszi a kontaktuskövetési rendszer kialakítására irányuló európai uniós adatvédelmi előírásokat. Végül a koronavírus-alkalmazásokban rejlő további, hazánk számára a jövőben kiaknázható lehetőségek és felhasználási metódusok bemutatására kerül sor.

Kulcsszavak: karanténellenőrzés, kontaktuskövetés, Kínai Népköztársaság, Covid-19, adatvédelem, Európai Unió, Koreai Köztársaság

Coronavirus applications, the smartphone solutions that allow contact tracing and remote control of quarantine rules, have been used in pandemic crisis management practices in many states around the world. The study formulates proposals for Hungary on the integration of technology-based crisis management mechanisms by presenting and evaluating the coronavirus applications and additional IT-based administrative measures used by the People's Republic of China and the Republic of Korea. The paper

¹ Hallgató, Nemzeti Közszerológiai Egyetem Hadtudományi és Honvédtisztképző Kar, e-mail: lendvai.tunde.tunde@gmail.com

² Egyetemi docens, Nemzeti Közszerológiai Egyetem Eötvös József Kutatóközpont Kiberbiztonsági Kutatóintézet, e-mail: krasznay.csaba@uni-nke.hu

reviews the available applications in Hungary as well as the distinctive features of private and public sector coronavirus applications developments and presents an overview of the European Union's personal data protection recommendations of the development of contact tracking system. Finally, the research discusses the further methods of use in the future and exploitable opportunities of coronavirus applications for Hungary.

Keywords: quarantine control, contact tracing, People's Republic of China, Covid-19, data protection, European Union, Republic of Korea

1. A vírusfigyelő applikációkról általában

A SARS-CoV-2 vírus (a továbbiakban új típusú koronavírus vagy koronavírus) okozta, fertőző Covid-19-betegséget 2020 első negyedévéől világméretűként tartjuk számon.³ Az új típusú koronavírus rendkívül gyorsan képes terjedni, szövődményei pedig súlyos egészségi állapotot eredményezhetnek szinte bárkinél. Ellene azonban 2020 decemberétől hazánkban is fokozatosan elérhetővé váltak a különböző védőoltások. Ennek ellenére a lakosság kielégítő mértékű átoltottságának eléréséig, újbóli oltás igénye esetén vagy megelőzési céllal (például új variáns terjedésekor) továbbra is szükséges lehet számos, a mindennapi életvitelt korlátozó intézkedés bevezetése. Az államigazgatást és a lakosságot érő, pandémia okozta kihívások kezelését 2020 májusától hazánk, számos más államhoz hasonlóan, többek között olyan IT-technológiák támogatásával végzi, amelyek okostelefonos alkalmazások igénybevételével járulnak hozzá a kontaktusok nyomon követéséhez vagy a karantén szabályok betartásának távoli ellenőrizhetőségéhez. E mobilapplikációk gyűjtőneve a „koronavírus-applikációk”.⁴

A koronavírus-applikációk a felhasználók és a védekezésben részt vevők számára elsősorban biztonságot és rugalmasságot biztosítanak, ezenfelül megkönnyítik a válságkezelés során felmerülő igazgatási feladatokat, amely kettős funkcionalitás sikere egyaránt múlik a lakosság attitűdjén és az elérhető IT-alkalmazások széles körű használatán. A koronavírus-nyomkövető és karanténellenőrző alkalmazások használata azonban számos adatvédelmi kockázattal jár, illetve kihívás elé állítja a lakosság kormány iránti bizalmának töretlenségét az etikus válságkezelési gyakorlat tükrében, mivel a legtöbb esetben az államok ezen applikációk adatvédelmi garanciáinak letéteményesei. Ebből eredően a pandémia idején az európai államok számára kardinális kérdés az óvatos és átgondolt kormányzati kommunikáció, továbbá a technikai és adminisztratív védelmi garanciák biztosítása a kifejlesztett vírusfigyelő alkalmazások adatkezelési gyakorlatának felügyeletével párhuzamosan.⁵

³ 2020. március 11-én az Egészségügyi Világszervezet (WHO) világméretűvé nyilvánította az új típusú koronavírus (SARS-CoV-2) okozta COVID-19-betegséget. Lásd Európai Unió Tanácsa: *A koronavírus okozta Covid19-világméretű járvány. Háttér.* Európai Tanács Főtitkársága, 2020.

⁴ A nemzetközi szakirodalomban „Covid-19 tracking application” (magyarul kb. koronavírus-nyomkövető vagy vírusfigyelő alkalmazások).

⁵ Olivier Nay: Can a virus undermine human rights? *The Lancet Public Health*, 5. (2020), 5. 238–239.

2. Az Európai Uniót érintő adatvédelmi kérdések, technológiai és válságkezelési modellek

A víruskövető applikációk fejlesztésére és igénybevételére szigorú adatvédelmi előírások vonatkoznak az Európai Unió tagállamaiban. Az alkalmazások révén kezelt személyes adatokat, illetve a járvány terjedési tendenciáinak elemzéséhez felhasználható egészségügyi vonatkozású adatok körét különleges védelem illeti meg a GDPR (az EU általános adatvédelmi rendelete) értelmében. A világ számos más államában, köztük Kínában és Dél-Koreában azonban eltérő adatvédelmi és adatkezelési kultúra alakult ki e tekintetben, ami visszaköszön az IT-technológiák által támogatott válságkezelési gyakorlatban. Az Európai Unió tagállamaiban a GDPR- és egyéb, például bizottsági ajánlásoknak való megfelelés érdekében a *privacy by design* adatvédelmi irányzaton alapuló fejlesztések alkalmazhatók. A magyarul „beépített adatvédelem” gyanánt visszaadható elv azt a biztonságos eljárást képviseli, miszerint az adatvédelmi mechanizmusok adaptációjának már a digitális eszközök gyártása során meg kell valósulnia, annak érdekében, hogy a végfelhasználók személyes adatai és személyiségi jogai ne sérülhessenek a termék vagy szolgáltatás igénybevételekor.⁶ Claude-Étienne Armingaud és Natali Adison jogi szakértők útmutatót készítettek az EU tagállamainak szoftverfejlesztői részére azzal a céllal, hogy ennek nyomán az állami megrendelésre vagy az állami és magánszektorbeli közös fejlesztéssel készített nyomkövető alkalmazások megfeleljenek az adatvédelmi irányelveknek és a személyiségi jogok tiszteletben tartására irányuló európai ajánlásoknak.

„Ezen standardokat az EU intézményei által közzétett iránymutatásokban aszerint fektették le, hogy a nyomkövető alkalmazások használata önkéntes alapon történjen és meghatározott időkeretre vonatkozzon. Az adatok strukturálásába és gyűjtési mechanizmusainak kialakításába pedig a tagállamoknak be kell vonnia a nemzeti egészségügyi hatóságokat, melyek virológiai szempontból segítenek a rendszer kialakításában.”⁷

A három kritikus szempont, amelynek mentén a fejlesztéseknek végbe kell mennie, az anonimizálásra vonatkozó szabályozások betartása, az alkalmazás által támogatott válságkezelési célhoz való kötöttség és a létrehozott adatbázisok, illetve kiértékelt információ kezelésének és tárolásának állam általi ellenőrizhetősége. Az Európai Bizottság ajánlásai között a két legfőbb kritérium az önkéntes használat, valamint az állami részvétellel és kontroll megtartásával végbemenő fejlesztés és adatkezelés. Ez utóbbi keretében kizárólag aggregált adatbázisokban, anonimizáltan szabad a kontaktesetekre és egészségi állapotra vonatkozó adatokat gyűjteni. Ezeket a fertőzési hullámok kezelésének tervezési szakaszában lehet felhasználni, többek között prediktív statisztikai elemzések elkészítéséhez, amelyek szemléltetik, hogy miként

⁶ Nemzeti Adatvédelmi és Információszabadság Hatóság: *Adatvédelmi Értelmező Szótár – privacy by design*. 2020.

⁷ Claude-Étienne Armingaud – Natali Adison: *COVID-19. When EU Tracking Apps Meet the Pandemic, Trust and Privacy by Design Are the Hosts*. *National Law Review*, 10. (2020), 141.

alakulhat az új fertőzések számának változásával összefüggésben az egészségügyi szektorra nehezedő várható terhelés területi eloszlása. Az egészségügyi válsághelyzet megszűnésével ezen adatbázisokat törölni kell.⁸

Globális relációban alapvetően háromféle kontaktuskövető applikációs modell létezik. Az első modellt a Kínai Népköztársaság példája jeleníti meg, eszerint a kontaktusokra vonatkozó információk tárolása és nyomon követése az állam által történik, kötelező módon, univerzálisan alkalmazva. A második modellt képviseli például Magyarország is, ahol a technológia kifejlesztése és fenntartása állami támogatással valósult meg, az igénybevétele viszont önkéntes alapon történik. A harmadik modell magánszolgáltatók és vállalkozások által kifejlesztett applikációk csoportja, amelyek minden típusú állami közreműködéstől mentesek, ennél fogva használatuk az egyén döntésének függvénye. Ezt a modellt képviseli az Apple és a Google kontaktuskövető alkalmazása.

Az európai megoldások sarokkövei etikai és regulációs szempontból az alapjogok és a magánélet védelme, valamint az adatvédelemi standardok betartatása és állami ellenőrzése, ami együttesen a második típusú modellnek felel meg. Az ezen elvek által támasztott korlátok pedig a technológiai megvalósítás tükrében a következőkben merülnek ki:

- Adatok anonimizálási problematikája: A találkozásokra vonatkozó adatok körét (például geolokáció) olyan módon kell rögzíteni, hogy szükség esetén az érintett feleket személyesen lehessen értesíteni.
- A kontaktusokra vonatkozó adatok értékelése: A „kontaktusnak” minősülő eseményekre vonatkozó adatokat el kell látni különböző azonosítókkal, mint például időbélyeg és az érintettek elérhetősége.
- Az adatok tárolása: A begyűjtött adatokat összesíteni kell egy centralizált adatbázisban, amelynek tárhelyigénye folyamatosan változik a felhasználók és kontaktuseseményeik száma, illetve a vizsgált időtartam szerint (például 10–14 nap, az aktuális karanténszabályok szerint). Centralizáltan működő állami fenntartású tárhely hiánya (akár felhőszolgáltatás esetén) korlátozza az európai kormányok lehetőségeit.⁹

A fenti problémakörök feloldására Christina White, az amerikai Stanford Egyetem professzora a következő technológiai megoldások és adminisztratív kontrollok mellett érvel: „A geolokációs adatok begyűjtésére egyáltalán nem is lesz szükség, amennyiben a Bluetooth technológiát egyfajta távolságérzékelő-szenzorként használja az alkalmazás.” Vagyis az okoseszköz a kibocsátott Bluetooth-jeleket a közelben lévő, az alkalmazást használó okostelefonok felé továbbítja, mégpedig másfél méteren belül, egyben a társadalmi távolságtartási (*social distancing*) szabályok szerint. Ha tehát a két telefon ezen távolságon belül van legalább 15 percen keresztül, az kontaktusnak számít. Ennek hátránya, hogy a technológia nem tudja figyelembe venni a védekezőeszközök használatát (például szájmaszok), és nem érzékeli

⁸ European Commission: *Joint European Roadmap towards lifting COVID-19 containment measures*. Brussels, European Commission, 2020. 7.

⁹ Armingaud–Adison (2020): i. m.

a személyek közti elválasztó térelemeket, amelyek lehetnek – például ügyintézés esetén – üvegfalak. Az alkalmazás a kontaktusnak ítélt eseményekhez, a White által felvetett legbiztonságosabb technológiát használva „egyedi, véletlen számot generál, ezt rögzíti, és az adatokat továbbítja egy szerverre”, amely csak a kódszámokat egyezteti, és ez alapján küld ki figyelmeztetéseket a kódszámokhoz társított eszközökre. A megfertőződés bejelentését ennek megfelelően szintén egy fedő kódszámot generáló értesítésként töltik fel a szerverre, ezáltal az alkalmazás valójában kódszámok egyeztetését végzi és nem tárol személyes adatokat. A személyes adatokat az alkalmazás a felhasználó saját telefonján tárolja, ezáltal nem merülhet fel gondatlan adatkezelés és visszaélés lehetősége.¹⁰

3. Magyarországon igénybe vehető koronavírus-applikációk

Hazánkban a kontaktuskutatásért felelős rendészeti szerv az ORFK (Országos Rendőr-főkapitányság). Munkájának megkönnyítése érdekében vezették be az úgynevezett *VírusRadar*-alkalmazást. Az applikációt magáncég fejlesztette ki az Innovációs és Technológiai Minisztérium (ITM) és a Kormányzati Informatikai Fejlesztési Ügynökség közreműködésével, tehát államilag támogatott fejlesztésről van szó. A *VírusRadar* egy kontaktuskutatást segítő, Bluetooth-technológián alapuló, okostelefonos alkalmazás, amely jelenleg Android operációs rendszerrel működő eszközökkel kompatibilis.¹¹ A *VírusRadar*-alkalmazás adatvédelmi ismérvei közé tartozik, hogy csak egyetlen személyes jellegű adatot tárol a felhasználóról, a telefonszámot, egyéb személyes adatot nem. Az applikáció a telefonszámhoz egy véletlenszerűen generált regisztrációs kódot rendel, amelyet a Nemzeti Népegészségügyi Központ titkosított szerverén tárolnak, míg a kontaktusnak ítélt esetekhez (15 percen át kell tartózkodni két méteren belül) kapcsolódó azonosítók a felhasználók készülékén tárolódnak. A használat során ezen kódok egyeztetése történik.¹² Vagyis a *VírusRadar* nem gyűjt geolokációs adatokat, hanem a Bluetooth-technológia segítségével felméri a távolságot, és elmenti a közelben lévő készülék azonosító kódját. Ehhez azonban be kell kapcsolni a telefon saját hely-meghatározásra szolgáló funkcióját, emiatt kér az alkalmazás engedélyt a helyadatokhoz történő hozzáféréshez. További biztonsági funkció, amely egyúttal az állami visszaélés lehetőségét is csökkenti, hogy megfertőződés esetén az érintett döntésén múlik, hogy meg kívánja-e osztani kontaktusaival a *VírusRadar*-applikáción keresztül a megfertőződés tényét. A *VírusRadar*-applikáció 14 napos intervallumban kezeli a kontakteseteket, az ezen felüli napok adatait törli a készülékről. A fentiekben bemutatott kontrollok révén a magyarországi kontaktuskövetési gyakorlat teljes mértékben megfelel az Európai Unió adatvédelemre vonatkozó ajánlásainak.

¹⁰ Andy Greenberg: *Clever Cryptography Could Protect Privacy in Covid-19 Contact-Tracing Apps*. 2020.

¹¹ Kontextusba helyezve: Magyarországon az összesen 5,5 millió fő internetfelhasználónak megközelítőleg 4 millió Android rendszerű készüléke van.

¹² Miniszterelnöki Kabinetiroda: *Palkovics: A hatékony kontaktuskutatásban elengedhetetlen a mobiltelefonos applikációk használata*. Koronavírus Sajtóközpont, 2020.

A magyar hatóságok 2020. május 1-jével vezették be a karantén-ellenőrző applikációt, a Házi Karantén Rendszert (HRK). Államigazgatási szempontból ez az alkalmazás jelentősen csökkenti a hatóságok adminisztratív terheit és a rendőrség intézkedő állományának a létszám–esetszám arányból adódó nehézségeit, egyúttal elkerülhetővé teszi az eljáró személyek esetleges megfertőződését, az érintettek számára pedig kényelmi funkciókat biztosít.¹³ A HRK általi ellenőrzéshez regisztrációt és jelszó beállítását követően kötelező megadni olyan személyes adatokat, mint amilyen a teljes név, születési hely és idő, illetve anyja neve, e-mail-cím és telefonszám (magyarországi, vagyis +36-tal kezdődő), továbbá a készülékkel fotózott önarkép (szelfi), amit az ellenőrzési folyamat során egy mesterségesintelligencia-alapú arcfelismerő szoftver használ majd a hiteles biometrikus azonosításhoz. A rendőrség által működtetett HKR nyilvántartása összeköttetésben áll az applikációval, így a regisztráció csak azután hitelesíthető, hogy az érintett személyt a rendőrség is felvezette a hatósági házi karanténra kötelezettek jegyzékébe.

A sikeres regisztráció után az alkalmazás nappal, bármely időpontban, küld egy SMS-t, amelyben az Operatív Törzs nevében felkéri a használót, hogy 15 percen belül végezze el a távellenőrzést (a megadott időpontban az arckép azonosítása és helyadatok egyeztetése a karanténra kijelölt helyszín adataival), továbbá e-mailen keresztül emlékeztetőt, figyelmeztetést és visszaigazolást küld az ellenőrzés végrehajtásáról. Fontos, hogy a regisztrált felhasználók számára kötelező a napi gyakoriságú távellenőrzés elvégzése. Amennyiben az érintett már nem kívánja használni az alkalmazást a karanténkötelezettség során, a területileg illetékes rendőrkapitányságon kell kérelmeznie a törlését a HKR nyilvántartásából.¹⁴ Ha az érintett valamilyen okból elmulasztja a távellenőrzést,¹⁵ az alkalmazás automatikusan értesíti az Országos Rendőr-főkapitányságot, amely eljár az ügyben. A hatósági házi karantén kötelezettségének feloldásakor az alkalmazás nem küld több ellenőrzési felkérést. Az ügy lezárását követő 60 nap elteltével a felhasználó adatai törölődnek az adatbázisból. Ez alól kivételt képez az alkalmazás használata során naponta egyszer, önként kitölthető, egészségügyi állapotot felmérő kérdőív, amelynek adatait az érintett TAJ-számához rendelt, Elektronikus Egészségügyi Szolgáltató Tér (EESZT) elérhető profiljában is rögzítene, amelyhez a házi orvos férhet hozzá, elősegítve a beteg kezelését. Az egészségügyi állapotfelmérő kérdőív „az egészségügyi ellátórendszerekre háruló terhelés tervezhetőségének javítását”¹⁶ is szolgálja. Ennélfogva az Operatív Törzs szintén hozzáfér a kérdőívek anonimizált és aggregált adataihoz, amelyeket az egészségügyi ellátórendszerre nehezedő várható terhelés földrajzi eloszlásának prognosztizálására használnak fel.¹⁷

¹³ Miniszterelnöki Kabinetiroda: *Jól működik a hatósági házi karantén elektronikus ellenőrzése*. Koronavírus Sajtóközpont, 2020.

¹⁴ Hatósági Karantén Rendszer: *A Házi Karantén Rendszer működése*. Budapest, 2020.

¹⁵ Az elmulasztott távellenőrzés fakadhat olyan technikai okokból, mint a hálózati korlátok (maximum 3G), pontatlan helyadatok vagy például hogy az arcképek egyikéről sem ismerhető fel a személy. Az alkalmazás szintén elmulasztott ellenőrzésként tartja számon, ha az érintett romló egészségi állapota miatt nem tudja elvégezni a távellenőrzést.

¹⁶ Hatósági Karantén Rendszer: *Adatvédelmi irányelvek*. Budapest, 2020.

és Hatósági Karantén Rendszer: *Gyakran Ismételt Kérdések: Mi az applikáció célja?* Budapest, 2020.

¹⁷ Miniszterelnöki Kabinetiroda (2020): i. m.

A harmadik koronavírus-hullám kapcsán létrehozott alkalmazás tesztverziója 2021 májusától elérhető, ennek segítségével a beoltottság tényének elektronikus igazolása lehetséges. Az applikáció Android („EESZT applikáció”) és iOS („EESZT Lakossági”) eszközökkel kompatibilis, és az Ügyfélkapuhoz integrált EESZT-rendszer Lakossági Portáljával összehangoltan működik. Az alkalmazás PIN-kóddal védett bejelentkezést követően, internetkapcsolatot és QR-kódot használva megjeleníti a felhasználó nevét, TAJ-számát, a vakcina típusát és az oltás időpontját. A benne tárolt adatokat a piaci szolgáltatók egy külön erre a célra kifejlesztett alkalmazással, a QR-kód beolvasása alapján működő „EESZT Covid Control” applikációval kérdezhetik le (aminek eredménye: oltott vagy nem), például a beléptetés megkönnyítése céljából, illetve azon személyek egyszerűbb igazolása érdekében, akiknek az oltási igazolványát még nem kézbesítették.¹⁸

4. Koreai Köztársaság: a „COVID-19 Smart Management System”

A Covid-19-fertőzés elleni védekezés során használható IT-technológiák kiválasztása szorosan összefügg a felmerülő állam hálózati adottságaival, illetve lakosságának internetpenetrációjával (hány internetet használó lakosa van). A Statista adatai alapján Dél-Korea rendelkezik a világon az egyik legjelentősebb, 2021 januárjában 97%-os internetpenetrációval, amely érték a teljes lakossághoz mérten (2015-ben 51 millió, napjainkra körülbelül 51,29 millió fő) arányosítja az internetfelhasználók számát (2020-ban 49,75 millió fő).¹⁹ Ennek nyomán elmondható, hogy Dél-Korea nemzetgazdasága rendkívül hálózatosított, működéséhez a globális átlagnál (7 Mbps) jóval gyorsabb hálózati sebesség társul (27 Mbps).²⁰ Az országban 2019 áprilisában vezették be az 5G hálózatot, amely az év végére már közel 3 millió IT-eszköz felhasználója számára volt elérhető.²¹

Az új típusú koronavírus által okozott járvány 2020 januárjában az első országok egyikeként érintette Dél-Koreát. Rövid időn belül nagy létszámú fertőzési gócpontok keletkeztek, azonban az országnak sikerült szigorú intézkedések segítségével és széles körű gyorstesztelési kapacitás kiépítésével (gyalogosan vagy autóval elérhető mobil tesztpontok, úgynevezett „drive-thru”- és a „walk-thru”-tesztek) kijárási tilalom bevezetése nélkül is sikerült laposan tartani az esetszámokból generálható járványgörbét az első hullám végéig (nagyjából 2020 májusáig). A válságkezelés során Dél-Koreában, a legtöbb demokratikus államtól eltérően, kötelezően használandó IT-technológiák segítségével végezték az aktív esetek felderítését, a kontaktszemélyek izolációját, felügyelték a karantén betartását, továbbá a lakosság mozgásának (kontaktjainak) nyomon követését. Ezt az eljárásrendet egy 2015-ben pusztító járvány (MERS,

¹⁸ Miniszterelnöki Kabinetiroda: *Ingyenesen letölthető a koronavírus elleni védőoltást igazoló mobilalkalmazás a szolgáltatóknak és az oltottaknak is*. Budapest, Koronavírus Sajtóközpont, 2021.

¹⁹ Simon Kemp: *Digital 2021: South Korea*. 2021.

²⁰ Yasmin Waldeck: *Internet usage in South Korea – Statistics & Facts*. Statista Research Department, 2018.

²¹ Robert Clark: *Six Months of 5G. What We've Learned From South Korea*. Light Reading Asia, 2019.

közel-keleti légzőszervi szindróma járvány) kezelése során szerzett tapasztalatok, valamint az ezt követően megalkotott, járványügyi védekezés esetén alkalmazható törvény alapján vezették ismét be.²²

A dél-koreai járványügyi intézkedés centrumai (*Centers for Disease Control and Prevention*, magyarul visszaadva Koreai Betegség-ellenőrzési és Megelőzési Központok) fejlesztéseként jelent meg a koronavírus terjedését nyomon követő és menedzselő „COVID-19 Smart Management System” (Covid-19 SMS) nevű applikáció. A Covid-19 SMS rendszer implementációja személyes adatok széles körű állami kezelésével és egyes személyiségi jogok háttérbe szorításával járt, ám ezt a dél-koreai lakosság etikai szempontból arányos lépésként értékelte az áprilisi választási eredményekkel, az országgyűlésben ugyanis újra Mun Dzse-In elnök pártja, a kormányon lévő liberális Koreai Demokrata Párt szerzett többséget. A szinte korlátlan adatgyűjtés lehetővé tette, hogy a teljes lakosságot majdnem valós időben informálják a kontaktszemély esetleges pozitív Covid-tesztjének eredményéről, egy telefonra küldött értesítés formájában. Az értesítőrendszert a Big Data technológia, illetve a „nagy adatot” kiértékelő mesterségesintelligencia-alapú megoldások tették működőképpé, az 5G hálózat nagyobb adatforgalmat is kezelni képes erőforrásait kihasználva. A kontaktok azonosításához szükséges, „objektív forrásnak” nevezett adatokat térfigyelő kamerák rendszereiből, az okostelefonok és gépjárművek GPS-adataiból, valamint a bankkártyás fizetések lajstromából nyerték ki.²³ Ezen a ponton fontos megjegyezni, hogy Dél-Koreában a kontaktkutatás alapvetően nem masszív állami megfigyelésen alapszik. Csak szükség esetén kérhető le információ az „objektív forrásokból”, olyankor, ha az egészségügyi dolgozók által végzett kérdőíves felmérés alkalmával az érintett nem tudja biztosan megadni, hol, mennyi időt és kivel, milyen távolságban tartózkodott. A kapcsolati kör meghatározását követően az érintett személyek Covid-19 SMS rendszerben tárolt személyes adataihoz csak megfertőződés vagy kontaktus miatti karantén kijelölése esetén férhet hozzá egyetlen fő, aki egy speciális státuszban lévő köztisztviselő, úgynevezett epidemiológiai ügynök („epidemiological intelligence officer”). Egy eset kapcsán a személyes adatokba csak egyetlen epidemiológiai ügynök tekinthet be, s a karanténkötelezettség megszűnésével az adatokat törölni kell.²⁴ Dél-Koreában a karanténkötelezettség betartását is mobiltelefonos applikáció segítségével ellenőrzik, amely értesíti a hatóságokat az ellenőrzés elmulasztásáról.²⁵

Különösen érdekes a dél-koreai válságkezelés kapcsán, hogy 2020. április 15-én ebben az államban tartottak először választásokat a pandémiás helyzetben. A választáson a szavazásra jogosultak 66,2%-a vett részt. Az Asian Network for Free Elections, egy, a választások transzparenciájának megfigyelésére és értékelésére szakosodott nemzetközi szervezet álláspontja szerint a nagyarányú részvétel azt a bizalmat is reprezentálja, amelyet a lakosság az állam vírus elleni védekezési koncepciója

²² Hamar Balázs: *Dél-Korea sikere a COVID-19 járvány leküzdésében és annak hatása a 2020-as parlamenti választásokra*. AJTK, 2020.

²³ Leesa Lin – Zhiyuan Hou: *Combat COVID-19 with artificial intelligence and big data*. *Journal of Travel Medicine*, 27. (2020), 5. 2.

²⁴ Hamar (2020): i. m.

²⁵ Sera Whiteclaw – Mamas A. Mamas – Eric Topol – Harriette G. C. Van Spall: *Applications of digital technology in COVID-19 pandemic planning and response*. *The Lancet Digital Health*, 2. (2020), 8. 438.

íránt érez.²⁶ A pandémia ideje alatt meghosszabbították a korai levélszavazatok leadásának időhatárát, a kórházban ápolott betegek és karanténban tartózkodók részére az „otthon-szavazási” (*home-voting*) program keretében. Az előzetes választáson részt vevő, otthonról, levélben vagy elektronikusan szavazók regisztrációját egy azonosító applikáció segítette.²⁷ A választás napján a korábban is alkalmazott megelőzési szabályok (távolságtartás és létszámkorlátozás, testhőmérés, maszkviselés, szavazóhelyiségek fertőtlenítése) voltak érvényben, míg a szavazatszámolás során élő közvetítés biztosította az átláthatóságot. A szavazás lebonyolításánál újdonság volt a védett időszáv bevezetése a karanténban tartózkodó tünetmentesek részére, akik egy elkülönített helyiségben szavazhattak (azok számára is külön helyiség állt rendelkezésre, akiknek testhőmérséklete túl magas volt), továbbá szavazóurnáknak a kórházakban történő felállítása.²⁸

Összességében elmondható, a dél-koreai parlamenti választások sikeres és biztonságos lebonyolítása példaként szolgálhatott a következő hónapokban világszerte esedékes különféle hasonló események megtervezése és kivitelezése számára, mint amilyen például az Amerikai Egyesült Államok elnökválasztása, az ázsiai régióban pedig a Srí Lanka-i parlamenti és a mianmari általános választás volt. Ez a modell elsősorban a járvány terjedésének korai szakaszában alkalmazható, a gócpontok elszigetelésére és a terjedési láncok megelőzésére. Legnagyobb előnye, hogy a teljes körű adatgyűjtés, továbbá a kontaktuskövető és karantén-ellenőrző eljárások alkalmazása következtében a lakosságra nehezedő információszolgáltatási kötelezettségekkel arányos benne a személyes adatok védelme, ami az epidemiológiai ügynöki rendszer adminisztratív kontrolljával is kiegészül.

5. Kínai Népköztársaság: „Health Barcode” rendszer

A Statista elemzőközpont adatai alapján 2020-ban 908 millió felhasználóval, 70%-os internetpenetráció mellett²⁹ a Kínai Népköztársaság rendelkezett a legnagyobb online közösséggel a világon. A kínai internet világának különlegessége, hogy arányosítva 10-ből 9,8 felhasználó mobiltelefonon keresztül csatlakozik a világháléhoz, amely 2019 óta 5G sávzélességgel is elérhető számára. A globális internetes tartalmakat a kínai állam szigorúan szabályozza és cenzúrázza, ezért a „kínai interneten” elérhető platformokat és egyéb szolgáltatásokat a három legnagyobb kínai IT-cég, a Baidu, az Alibaba Group és a Tencent (a továbbiakban, együttesen: BAT) szolgáltatásai határozzák meg.³⁰ Kínában 2020-tól éles üzemmódban vezettek be egy alkotmányos alapokon nyugvó, új, masszív állami megfigyelésen és IT-technológiákon alapuló közgazgatási szisztémát, a Társadalmi Kreditpontrendszert (kínaiul *Shehui Xinyong Tixi*),

²⁶ Asian Network for Free Elections: *COVID-19 and elections: the experience of South Korea*. ANFREL, 2020.

²⁷ Antonio Spinelli: *Managing Elections under the COVID-19 Pandemic. South Korea's Crucial Test*. IDEA, 2020.

²⁸ Asian Network for Free Elections (2020): i. m.

²⁹ A legfejlettebb nagyvárosok, például Sanghaj és Peking internetpenetrációja meghaladja az országos 70%-os átlagot, míg az elszigetelt és vidéki területeken 40–46% körüli az internetezők aránya.

³⁰ Lai Lin Thomala: *Internet usage in China – Statistics & Facts*. Statista Research Department, 2020.

amelynek használata az ország teljes területén, minden lakos és Kínában tartózkodó személy részére kötelező.

A BAT-óriáscégek monitorozzák a felhasználók online tevékenységét (pénzügyi- és online kereskedelmi tevékenység, közösségi média), és az így keletkező adatokat (Big Data) törvényi kötelezettséggel átadják az állam részére. Az adatszolgáltatás célja a Társadalmi Kreditpontrendszer személyi profiljainak létrehozása és működtetése, ami egyaránt épül a lakosság online magatartásának elemzésére és biometrikus adataira, amelyeket az országosan elhelyezett CCTV térfigyelő kamerák, ujjlenyomat-scanneerek és arcfelismerő rendszerek folyamatosan felvesznek. Továbbá az előbb említett forrásokat még egyéb kormányzati adatbázisok (például rendszám-nyilvántartás, egészségügyi adatok, jótékony célú felajánlások listája stb.) rögzítéseivel is integrálják. A Kreditpontrendszer a Kínai Kommunista Párt etikai és politikai szemléletmódja szerint meghatározott és közzétett értékelési kontrollok alapján osztályozza vagy pontozza az egyéneket a társadalmi megbízhatóság és becsületesség, valamint az üzleti és igazságügyi hitelesség jegyében. A társadalmi kreditpont értékéhez mérten az egyének többlétszolgáltatásokhoz és -jogosultságokhoz juthatnak (például a személy vállalkozásának kedvezményes hitelfelvétele, elérhető szolgáltatások és fogyasztási cikkek köre), vagy szankciók (például az utazás és a betölthető állások korlátozása) sújthatják őket, ha nem működnek együtt a hatóságokkal és politikailag nem elkötelezettek a rezsim iránt.³¹ A Társadalmi Kreditpontrendszer a totális kontroll által egyszerre valósítja meg a kommunista állampárt álláspontjának megfelelő szociális viselkedés ösztönzését és kikényszerítését, a kínai típusú piacgazdasági modell finomhangolását, továbbá a polgárjogi viszonyok transzparenciáját, magasabb szintű megbízhatóságának biztosítását.³²

A Társadalmi Kreditpontrendszer infrastrukturális alapjaira épül rá a „Health Barcode”-, más néven „Green Code”-rendszer,³³ amely a kínai államnak az új típusú koronavírus terjedését nyomon követő, egyéni egészségi állapotfelmérő kérdőívekre is támaszkodó, okostelefonnal működő modellje. Az alkalmazás célja a vírus országon belüli terjedésének megakadályozása (a járvány terjedési görbéjének laposan tartásával) és a kontaktuskutatás, valamint a karantén szabályok elrendelésének automatizálása. A modell lényege az utazási és kijárási szabályok egyéni korlátozhatósága. Ennélfogva a Health Barcode applikáció használata mindenki számára kötelező, aki Kína területére érkezik, nem csak a lakosság számára. Az applikáció mindennap a koronavírus tüneteire irányuló kérdőív kitöltését kéri. A kérdőív kiértékelése, a helyadatok, valamint a kontaktusokra vonatkozó információk (például a kontaktuszemélyek egészségi adatai) feldolgozása mesterséges intelligencia, gépi tanulás (*Machine Learning*, ML) és Big Data analízis segítségével történik, ami alapján a Health Barcode rendszer a fertőzés szempontjából hármasszínűskála szerint generál egy QR-kódot a felhasználó részére.³⁴

³¹ Amanda Lee: [What is China's social credit system and why is it controversial?](#) *South China Morning Post*, 2020.

³² Genia Kostka: *China's Social Credit Systems and Public Opinion Explaining High Levels of Approval*. MERICS, 2018; Kartal Kovalovszki: *A kínai társadalmi kreditrendszer*. 2019.

³³ Magyarul kb. „egészségi állapot”- vagy „zöld kódos” QR-kód rendszer, további elnevezése lehet még a „Quick Response” QR-kód rendszer.

³⁴ Whiteclaw et al. (2020): i. m. 435–440.



1. ábra

A Kínai Népköztársaságban használt Health Barcode elnevezésű, QR-kód alapú kontaktuskövető rendszer „egészséges” minősítéséhez tartozó zöld QR-kód

Forrás: a szerző szerkesztése

Az 1. ábrán látható zöld QR-kód jelentése, hogy a felhasználó egészségi állapota megfelelő, nem került kontaktusba fertőzött személlyel. Ebben az esetben az elkövetkező napon, a társadalmi távolságtartási szabályokat betartva, szabadon közlekedhet. A sárga értékelés jelentése, hogy a felhasználó újonnan érkezett a településre, és még nem töltötte le a karanténkötelezettség időtartamát. Vörös jelzéssel látják el azon QR-kódokat, ahol a felhasználónak karanténba kell vonulnia igazoltan pozitív Covid-19-tesztjének eredménye vagy kontaktus miatt. A karanténra kötelező kódok átlagosan 7–14 napig vannak érvényben, korlátozva a kijárást, ezen időtartam leteltével zöldre váltanak, ha a felhasználó sorozatosan normál egészségi állapotról számolt be. A technológia ennek alapján hatékonyan járult hozzá a teljes kijárási korlátozások feloldásakor a terjedési láncok és vírusgócok elszigeteléséhez.³⁵

³⁵ Lin–Hou et al. (2020): i. m. 1–3.

Az önbevalláson alapuló egészségi állapot-felmérő kérdőív hatékonyságát csökkenti az a tény, miszerint csak a tünetekkel rendelkező fertőzöttek esetén léptet életbe korlátozásokat, feltéve, hogy azok megfelelően jelentik be tüneteiket. Az ehhez hasonló válságkezelési gyakorlat akkor igazán hatásos, ha egyéb átfogó tesztelési stratégiákkal és kontaktuskövető vagy -ellenőrző mechanizmusokkal kombinálják. A kínai állam ezt a kockázatot a dél-koreai modell „objektív forrásaihoz” hasonló módon küszöbölte ki a további információk, méréseredmények bevonása révén. A tömegközlekedésben és lakóközösségek kijáratánál felállított ellenőrzőpontok csak a QR-kód beolvasását követően engedik tovább haladni a személyeket. Annak érdekében, hogy a kínai egyetemek működni tudjanak, egyes városokban a hallgatóknak egészségügyi állapotukat folyamatosan mutató, például a testhőt és a légzésszámot monitorozó karpereceket is viselniük kell a közös helyiségekben és egyes órákon, a fertőzékenység esetek kiszűrhetősége érdekében.³⁶ Összességében elmondható, hogy a Health Barcode szisztémája egy preventív jellegű intézkedéscsomag, aminek legnagyobb előnye az automatizált döntéshozatal és a magatartás-kikényszerítés lehetősége, a Társadalmi Kreditpontrendszer infrastruktúrájának felhasználásával.

6. Konklúzió

Az IT-technológiákon alapuló válságkezelési metódusok megkönnyítik a felmerülő adminisztratív feladatok elvégzését, sőt automatizálttá tehetik a karantén szabályok ellenőrzését és a kontaktusok nyomon követését, amit a kínai esetpélda mutat be. Emellett egy központosított egészségügyi adatbázis, amelyet Dél-Koreában is alkalmaznak, lehetővé teszi a gyors és hatékony lakossági tájékoztatást, a terjedési hullámok prognosztizálását és az egészségügyi szektorra nehezedő terhelés menedzselését, továbbá hozzájárulhat ahhoz, hogy a nagy létszámú rendezvények lebonyolítása és egyéb mindennapi tevékenységek ismét biztonságosak lehessenek. A kínai és dél-koreai, IT-technológiákra alapozott, komplex járványkezelési modellek bármely újabb járvány esetén alkalmazhatók, így a Magyarország számára átvehető nemzetközi megoldásokat érdemes tovább kutatni a jövőben az európai uniós és hazai adatvédelmi előírásoknak történő megfelelés jegyében. E meglévő tudásanyag és új lehetőségek nem csupán a járványok aktív időszakában könnyítik meg a közösség életét, hanem a nemzetgazdaság biztonságosabb újraindításában is szerepet játszhatnak, különösen a határokon átvelő kereskedelmi forgalom és turizmus területén. Az adminisztratív és technológiai adatvédelmi kontrollokkal ellátott kontaktuskövetés átgondolt, szabályozható és következetes monitorozást tesz lehetővé, amely a magyar és külföldi állampolgárok szabad mozgását egyaránt segíti, ezáltal ismét biztonságossá téve a turizmust és vendéglátást. Erre Európán belüli példaként Izland szolgálhat, amely a külföldi állampolgárok beutazását kontaktuskövető applikáció letöltéséhez köti. A különféle oltottsági igazolványok és vakcinatípusok adatainak opcionális felvezetését is érdemes lehetővé tenni a kontaktuskövető applikációk rendszerébe, függetlenül

³⁶ Emilia Jiang: Beijing uses temperature-monitoring bracelets to track students' body temperatures amid fears that reopening of schools could trigger a new wave of coronavirus infections. *Daily Mail*, 2020.

attól, hogy az egyes vakcinatípusok milyen időközönként igénylik az újbóli oltást, illetve, hogy az adott állam elismeri-e a vakcinát vagy oltási igazolványt. Ez egyrészt egészségügyi megfontolásból, másrészt adminisztratív szempontból lehet fontos. A hazai koronavírus-applikációk tekintetében a további elsődleges fejlesztési irány az okostelefonra készült összes operációs rendszerrel való kompatibilitás elérése, ezt követően a nemzetközi telefonszámok használatának engedélyezése és az idegen nyelvű beállítások lehetősége, esetlegesen a magánszolgáltatók (Apple, Google) fejlesztéseivel való kompatibilitás kiépítése az európai adatvédelmi standardok szerint.

A jelenleg Magyarországon elérhető államilag támogatott applikációk köre (karantén-ellenőrzés, beoltottság igazolása, kontaktuskövetés) funkcionálisan meg-egyezik a kínai és dél-koreai modellekben bemutatott rendszerek alapvető elemeivel. Emellett hazánkban, Európában egyedülálló módon, működik egy integrált elektro-nikus egészségügyi rendszer, az EESZT, amelyben olyan potenciál is rejlik, hogy egy, a Kínában vagy Dél-Koreában működő modellhez hasonló, automatizált és rendkívül gyors, rugalmas reagálás lehetőségét magában hordozó rendszert működtessen – természetesen az adatvédelmi követelmények betartásával – a koronavírus-applikációk körében. Állami oldalról nézve a karantén-ellenőrző és kontaktuskövető applikációk széles körű alkalmazása a járványhelyzet kezelésének tervezhetősége szempontjából elengedhetetlen, kifejlesztésük közép- és hosszú távon is megtérül. Az alkalmazásuk során létrejövő egészségügyi eljárások alapul szolgálhatnak a hasonló járványhelyzetek esetén követendő forgatókönyvek megírásához. Ezenfelül az adatkezelés és -feldolgozás, a jelenlegi válságkezelés során szerzett tapasztalatokkal kiegészülve, lehetővé teszi az IoMT-eszközök (Internet of Medical Things, okos egészségügyi eszközök internetje) működéséhez és további tökéletesítéséhez szükséges adatvagyron létrehozását és a diagnosztikai AI-technológiák folyamatos fejlesztését. Az ilyen irányú kutatás és innováció megvalósításához ugyanakkor kulcsfontosságú a személyes adatok védelme.

A tanulmány az Innovációs és Technológiai Minisztérium ÚNPK-20-2-i-nke-117 kód-számú „új nemzeti kiválóság” programjának szakmai támogatásával készült.



Felhasznált irodalom

- Armigaud, Claude-Étienne – Adison, Natali: COVID-19. When EU Tracking Apps Meet the Pandemic, Trust and Privacy by Design Are the Hosts. *National Law Review*, 10. (2020), 141. Online: www.natlawreview.com/article/covid-19-when-eu-tracking-apps-meet-pandemic-trust-and-privacy-design-are-hosts?
- Asian Network for Free Elections: *COVID-19 and elections. The experience of South Korea*. ANFREL, 2020. Online: <https://anfrel.org/covid-19-and-elections-the-experience-of-south-korea/>
- Clark, Robert: Six Months of 5G: What We've Learned From South Korea. *Light Reading Asia*, 2019. Online: www.lightreading.com/asia-pacific/six-months-of-5g-what-weve-learned-from-south-korea-/d/d-id/754562
- European Commission: *Joint European Roadmap towards lifting COVID-19 containment measures*. 2020. Online: https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf
- Európai Unió Tanácsa: *A koronavírus okozta Covid19-világjárvány. Háttér*. Brüsszel, Európai Tanács Főtitkársága, 2020. Online: www.consilium.europa.eu/hu/policies/coronavirus/
- Greenberg, Andy: Clever Cryptography Could Protect Privacy in Covid-19 Contact-Tracing Apps. *Wired*, 2020. Online: www.wired.com/story/covid-19-contact-tracing-apps-cryptography/
- Hamar Balázs: *Dél-Korea sikere a COVID-19 járvány leküzdésében és annak hatása a 2020-as parlamenti választásokra*. Budapest, Antall József Tudásközpont, 2020. Online: <https://ajtk.hu/hu/kutatas/kutato-i-blog/del-korea-sikere-a-covid-19-jarvany-lekuzdeseben-es-annak-hatasa-a-2020-as-parlamenti-valasztasokra>
- Hatósági Karantén Rendszer: *Adatvédelmi irányelvek*. 2020. Online: <https://hazikaranten.hu/adatvedelmi-iranyelvek/>
- Hatósági Karantén Rendszer: *A Házi Karantén Rendszer működése*. 2020. Online: <https://hazikaranten.hu/hogyan-mukodik-az-applicacio/>
- Hatósági Karantén Rendszer: *Gyakran Ismételt Kérdések: Mi az applikáció célja?* 2020. Online: <https://hazikaranten.hu/gyik/>
- Jiang, Emilia: Beijing uses temperature-monitoring bracelets to track students' body temperatures amid fears that reopening of schools could trigger a new wave of coronavirus infections. *Daily Mail*, 2020. Online: www.dailymail.co.uk/news/article-8306917/Beijing-school-students-trial-temperature-tracking-bracelets.html
- Kovalovszki Kartal: *A kínai társadalmi kreditrendszer*. 2019. Online: https://diplomaciablog.hu/2019/04/11/a_kinai_tarsadalmi_kreditrendszer
- Kostka, Genia: *China's Social Credit Systems and Public Opinion. Explaining High Levels of Approval*. MERICS, 2018. Online: <https://doi.org/10.2139/ssrn.3215138>
- Lee, Amanda: What is China's social credit system and why is it controversial? *South China Morning Post*, 2020. Online: www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial

- Lin, Leesa – Zhiyuan Hou: Combat COVID-19 with artificial intelligence and big data. *Journal of Travel Medicine*, 27. (2020), 5. 2. Online: <https://doi.org/10.1093/jtm/taaa080>
- Kemp, Simon: *Digital 2021: South Korea*. 2021. Online: <https://datareportal.com/reports/digital-2021-south-korea>
- Miniszterelnöki Kabinetiroda: *Ingyenesen letölthető a koronavírus elleni védőoltást igazoló mobilalkalmazás a szolgáltatóknak és az oltottaknak is*. Koronavírus Sajtóközpont, 2021. Online: <https://koronavirus.gov.hu/cikkek/ingyenesen-letoltheto-koronavirus-elleni-vedooltast-igazolo-mobilalkalmazas-szolgáltatoknak>
- Miniszterelnöki Kabinetiroda: *Jól működik a hatósági házi karantén elektronikus ellenőrzése*. Koronavírus Sajtóközpont, 2020. Online: <https://koronavirus.gov.hu/cikkek/jol-mukodik-hatosagi-hazi-karanten-elektronikus-ellenorzese>
- Miniszterelnöki Kabinetiroda: *Palkovics: a hatékony kontaktkutatásban elengedhetetlen a mobiltelefonos applikációk használata*. Koronavírus Sajtóközpont, 2020. Online: <https://koronavirus.gov.hu/cikkek/palkovics-hatekony-kontaktkutasban-elengethetetlen-mobiltelefonos-applikaciok-hasznalata>
- Nay, Olivier: Can a virus undermine human rights? *The Lancet Public Health*, 5. (2020), 5. 238–239. Online: [https://doi.org/10.1016/S2468-2667\(20\)30092-X](https://doi.org/10.1016/S2468-2667(20)30092-X)
- Nemzeti Adatvédelmi és Információszabadság Hatóság: *Adatvédelmi Értelmező Szótár – privacy by design*. 2020. Online: www.naih.hu/adatvedelmi-szotar.html
- Spinelli, Antonio: *Managing Elections under the COVID-19 Pandemic. South Korea's Crucial Test*. IDEA, 2020. Online: <https://doi.org/10.31752/idea.2020.15>
- Thomala, Lai Lin: *Internet usage in China – Statistics & Facts*. Statista Research Department, 2020. Online: www.statista.com/topics/2230/internet-usage-in-south-korea/
- Waldeck, Yasmin: *Internet usage in South Korea – Statistics & Facts*. Statista Research Department, 2018. Online: www.statista.com/topics/2230/internet-usage-in-south-korea/
- Whiteclaw, Sera – Mamas A. Mamas – Eric Topol – Harriette G. C. Van Spall: Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health*, 2. (2020), 435–440. Online: [https://doi.org/10.1016/S2589-7500\(20\)30142-4](https://doi.org/10.1016/S2589-7500(20)30142-4)

Erdélyi Ákos¹

Az online térben bekövetkező zaklatások lehetséges okai, dinamikai jellegzetességei és megoldási lehetőségei

Possible Causes, Dynamic Characteristics and Possible Solutions to Cyberbullying

A 21. században a technológiai újítások fénykorát éljük. Az online tér nagyban megkönnyíti mindennapjainkat, ugyanakkor számos előnye mellett a sötét oldalát is kénytelenek vagyunk megismerni. Nem kell a legdrasztikusabb cselekményekre gondolni ahhoz, hogy találkozzunk az internet veszélyeivel: elég csupán, ha zaklatásnak vagyunk kitéve a közösségi média egyes platformjain. Az online zaklatás, más néven cyberbullying olyan, agresszív és szándékosan ismétlődő cselekvés, amelyet egy egyén vagy csoport hajt végre elektronikus eszközök alkalmazásával (kép, videó eljuttatásával, telefonhívással, e-mailek küldésével, weboldalak és egyéb üzenetküldő programok használatával), s amellyel szemben az áldozat gyakran védtelen. Fontos feladat azonosítani az elkövetőket és feltárni az egyes zaklatások mögött meghúzódó dinamikai folyamatokat. Az elkövetők személyiségelemzése révén felkutatásuk és azonosításuk felgyorsulhat, az áldozatok jó esetben segítséget kapnak az átélt traumával való megküzdéshez és a reziliencia tudatos formálásával kapcsolatban, továbbá hatékony preventív és interventív módszerek kidolgozása is megvalósulhat.

Kulcsszavak: cyber, online zaklatás, cyberbullying, elkövetők, áldozatok, csoportdinamika, pszichológiai magyarázatok, protektív faktorok

In the 21st century, we are living in the heydays of technological innovations. The Internet makes our everyday lives a lot easier, but in addition to its many benefits, we also need to get to know its dark side. We don't have to think about the most drastic acts to face the dangers of the Internet: it's enough to just be harassed on various social media platforms. Online harassment, also known as cyberbullying, is an aggressive

¹ Szakügyintéző, Budapesti Rendőr-főkapitányság, V. Kerületi Rendőr-kapitányság, Vizsgálati Osztály, Gazdaságvédelmi Alosztály, e-mail: ErdelyiAk@budapest.police.hu

and repetitive intentional act committed by an individual or group using electronic means (sending pictures or videos, making phone calls, sending emails, using websites and other messaging programs) against the victim who is often unprotected. It is an important task to identify the perpetrators and to explore the dynamic processes behind each harassment. Personality and behaviour analysis of perpetrators can speed up their tracing and identification, help victims cope with the trauma they have experienced and consciously shape resilience, and develop effective preventive and interventional methods.

Keywords: *cyber, online harassment, cyberbullying, perpetrators, victims, group dynamics, psychological explanations, protective factors*

1. Bevezetés

Napjainkat áthatják a technológiai újítások. Még fel sem dolgoztuk, pontosabban nem is frissítettük a legutóbbi fejlesztést, máris van egy újabb verzió. A számítástechnikai fejlesztések és az információs rendszerek szerepe napjainkban felértékelődött – a pandémia időszakában nem csak ennek pozitív aspektusai, hiszen a bűnözés is jelentős mértékben áthelyeződött a kibertérbe. Az internethasználat során gyakran felmerül a kérdés: mi jó és hasznos, és mi az, ami már egyáltalán nem minősül annak. Sok előnye mellett – mint például a gyors információáramlás, a kapcsolatépítés és kapcsolattartás, a szórakozást biztosító website-ok – a kevésbé pozitív, sőt gyakran negatív tényezők is egyre nagyobb szerepet kapnak, főleg a Z generáció életében. A fejlődés számos ígéretes dologhoz segített hozzá bennünket, azonban itt is megtaláljuk az előnyök mellett a hátrányokat is, amelyek közé nem pusztán az addiktív állapot kialakulása, az önbizalom és önértékelés diszfunkcionalitása tartozik, de idesorolható számos jogi kérdést is felvető (bűn)cselekmény: az internetes pedofília, a személyes adatokkal való visszaélés, az online gyűlöletbeszéd és még lehetne folytatni a sort.

Különösen nagy hangsúlyt kap a zaklatás „21. századi” formája, a *cyberbullying*, azaz az online, elektronikus eszközök alkalmazásával történő zaklatás. Számos empirikus kutatás foglalkozott már ennek kérdéseivel, és igyekeztek meghatározni a cselekmény mentális mozgatórugóit, megrajzolni a személyiségprofilokat, és megfelelő preventív és intervenciós stratégiákat kidolgozni.² Jelen munkám célja nem az internet és az internetezés ellen irányuló tanulmány; sokkal inkább egy összefoglaló készítése, amelyben áttekintem e zaklatási mód típusait, a motivációkat, és összegzem az ismert és a lehetséges preventív megközelítéseket.

² Lásd összefoglalóan Domonkos Katalin: Cyberbullying. Zaklatás elektronikus eszközök használatával. *Alkalmazott Pszichológia*, 14. (2014), 1. 59–70.

2. Cyberbullying – definíciók

A negatív cselekmények összefoglaló megnevezésére alkották meg az elektronikus zaklatás definícióját, amely megjelenhet bántó és gyűlöletkeltő tartalmak formájában, nem kívánatos üzenetek és tartalmak küldéseként, valamint megszegyenyítésre alkalmas videók és képek megosztása gyanánt. A kutatók első ízben az ezredfordulót követő években kezdtek foglalkozni a kérdéssel. Az azóta eltelt idő során a *cyberbullyingra* számtalan definíció született, egyre többet írnak megjelenési formáiról és a már vizsgált területeiről. Az alábbiakban az egyes definíciós kontextusokat tekintem át:

1. táblázat

Patchin és Hinduja, 2006	Internet vagy mobiltelefon használatával elkövetett ismételt károkozás különböző típusú (szövegi, képi) tartalom küldésével.
Smith és munkatársai, 2008	Olyan agresszív és ismétlődő szándékos cselekvés, amelyet egy egyén vagy csoport hajt végre elektronikus eszközök alkalmazásával, s amellyel szemben az áldozat gyakran védtelen.
Basley, 2009	Egy egyén vagy csoport által követett ellenséges és szándékos viselkedés, amelyet kommunikációs eszközök által hajtanak végre annak céljából, hogy másnak kárt okozzanak.
Slonje, 2012	SMS, kép, videó eljuttatásával, telefonhívással, e-mailek küldésével, weboldalak és egyéb üzenetküldő programok használatával megvalósuló cselekmény.

Forrás: Domonkos (2014): i. m.

Jól látható, hogy a zaklatásra jellemző motívumok az online zaklatás definiálása során is helyet kapnak: a *szándékosság*, az *ismétlődés* és a *tudatosság* tehát az a három kulcsfogalom, amelynek meghatározását és detektálását követően adott eseményt zaklatásként azonosítunk.

Egyes kutatók a zaklatásnak olyan jelzőket tulajdonítanak, mint az ismételt, negatív verbális és fizikai viselkedés, az informatikai és egyéb kommunikációs eszközök által folytatott cselekvés.³ Az egyén vagy csoport által végrehajtott ellenséges viselkedés a legkülönbözőbb módokon valósulhat meg: mobilhívások, e-mailek, blogok adják az online zaklatás eszköztárát. Módszereit vizsgálva hasonló differenciáltságot fedezünk fel: az ellenséges viselkedés megnyilvánulhat hazugság, becsapás, rágalmozás által. Gyakori az anonimitás megőrzése, a másik személy bőrébe bújás (vagyis amikor magunkat egy másik, létező személyként azonosítjuk, és az ő nevében osztunk meg valótlan állításokat), a mások fényképének engedély nélküli felhasználása és terjesztése, a fenyegetés és megfélemlítés, valamint az ugratás.

Látható továbbá, hogy valamennyi definícióban központi szerephez jut a cselekmény időszakos, többszöri előfordulása, az életvitelben lehetségesen bekövetkező negatív változások,⁴ ami érthető, hiszen zaklatásról csak ezek megállapítását

³ Tolga Aricak et al.: *Bullying, Cyberbullying and Suicide. Cyberpsychology & Behavior*, 11. (2008), 3. 253–261.

⁴ Domonkos Katalin – Ujhelyi Adrienn: Az online zaklatás médiareprezentációja. *Neveléstudomány*, (2015), 1. 77–92.

követően beszélhetünk. Valamennyi elméletalkotó kiemeli, hogy cyberbullying során az infokommunikációs eszközök alkalmazása felértékelődik, szerepüket a felhasználók felülreprezentálják.

3. Átfedés az offline és az online zaklatás között

Kutatók szerint jelentős a *kapcsolat* és az *átfedés* a két típus között. Azok, akik az offline, tehát a fizikai világban elkövetők, nagyobb valószínűség szerint lesznek azzá az online világban is. Az áldozatok szemszögéből vizsgálva a kérdést szintén megállapítható, hogy azok, akik az offline térben bűncselekmény áldozatai, a kibertérben is nagyobb eséllyel válnak sértetté. A cselekményekhez kapcsolódó morális érzelmek megjelenése és átélése csökken: a hagyományos zaklatási esetekben több lehetőség adódik az empátia átélésére, mint a virtuális térben (ennek okait lásd a következő fejezetben). Azok a fiatalok, akik a zaklatás mindkét típusában érintettek, inkább számolnak be depressziós időszakokról és magasabb arányban követnek el öngyilkosságot, mint azok, akik csak az egyikben áldozatok.⁵

Aricak és munkatársai véleménye szerint⁶ a zaklatások két jól elkülöníthető típus mentén azonosíthatók attól függően, hogy *nyílt* vagy *rejtett* zaklatásról van-e szó. Amennyiben a zaklatás nyílt, tehát mások bevonásával, mások előtt történik, akkor *direkt* zaklatásról van szó, amelynek során a zaklató olyan eszközöket használ célja elérése érdekében, mint az erőszakos viselkedés verbális kifejezése vagy a direkt fizikai abúzus, például verekedés kezdeményezése vagy a másik ugratása. Ezzel szemben az indirekt zaklatás során (rejtett zaklatáskor) az elkövető az áldozatok szociális kapcsolatait, társas interakciót semmisíti meg. Ennek érdekében pletykákat, rosszindulatú és hamis híreszteléseket kelt és terjeszt, elszeparálja, kizárja áldozatát a társas közegből. A zaklatások elkövetési módjai között a verbális (fenyegetés, ugratás), a fizikai (ütlegelés, rugdosás), illetve a manipulatív stratégiák (kiközösítés, kierőszakolás) alkalmazása gyakori.⁷ A bullying egy agresszív cselekvés, ilyenkor egy egyén vagy csoport direkt vagy indirekt formában abuzál másokat.⁸ A továbbiakban, mielőtt rátérnék a cyberbullying általános jellemzőire, fontos látni, hogy a büntetőjog hogyan kezeli a zaklatás bűncselekményét.

4. A zaklatás és a Btk.

A zaklatás, hasonlóan más típusú bűncselekményekhez, törvénykönyvben rögzített bűncselekmény, amely a személy elleni erőszakos bűncselekmények kategóriájába

⁵ Domonkos (2014): i. m.

⁶ Aricak et al. (2008) i. m.

⁷ Sameer Hinduja – Justin W. Patchin: Bullying, cyberbullying and suicide. *Archives of Suicide Research*, 14. (2010), 206–221.

⁸ Rosario Ortega-Ruiz et al.: The Emotional Impact on Victims of Traditional Bullying and Cyberbullying. *Journal of Psychology*, (2009), 4. 197–204.

tartozik. A Büntető Törvénykönyvről szóló 2012. évi C. törvény a 222. §-ban rögzíti a zaklatás törvényi tényállását. Ennek értelmében:

„Aki abból a célból, hogy más megfélemlítsen, vagy más magánéletébe, illetve mindennapi életvitelébe önkényesen beavatkozzon, őt rendszeresen vagy tartósan háborgatja, ha súlyosabb bűncselekmény nem valósul meg, vétség miatt évig terjedő szabadságvesztéssel büntetendő.”⁹

A (2) bekezdés folytatólagosan így fogalmaz:

„Aki félelemkeltés céljából

- a) más vagy rá tekintettel hozzátartozóját személy elleni erőszakos vagy közveszélyt okozó büntetendő cselekmény elkövetésével megfenyeget, vagy
- b) azt a látszatot kelti, hogy más életét, testi épségét vagy egészségét sértő vagy közvetlenül veszélyeztető esemény következik be, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.”¹⁰

A (3) bekezdésben – hasonlóan, mint a legtöbb bűncselekményt illetően – a törvénykönyv minősített eseteket fogalmaz meg, amelyek értelmében:

„Aki a zaklatást

- a) házastársa, volt házastársa, élettársa vagy volt élettársa sérelmére,
- b) nevelése, felügyelete, gondozása vagy gyógykezelése alatt álló személy sérelmére,
- c) hatalmi vagy befolyási helyzetével visszaélve, illetve
- d) hivatalos személy sérelmére, hivatali tevékenységével össze nem egyeztethető helyen vagy időben követi el, az (1) bekezdésben meghatározott esetben két évig, a (2) bekezdésben meghatározott esetben büntett miatt három évig terjedő szabadságvesztéssel büntetendő.”¹¹

Mint látjuk, a jogalkotó itt is él azzal a lehetőséggel, hogy úgynevezett minősített eseteket fogalmazzon meg a zaklatás tényállásával kapcsolatban, ezzel lehetőséget adva a bűncselekmény súlyosabban történő szankcionálásához. A jogalkotó ebben a tényállásban úgy fogalmaz, hogy a jogi tárgy (= a védendő érték) a személy *magánélethez, mindennapi életviteléhez való joga*, valamint *az élet, egészség és testi épség sértetlensége*. Elkövetési tárgya (= amire vagy akire nézve a bűncselekményt elkövetik, vagyis ami vagy aki a bűncselekmény sértettje) és elkövetője bárki lehet – erre az *aki* személyes névmással utalva.

Az elkövetési magatartás az első fordulatban a más életébe való önkényes beavatkozás, a második fordulatban pedig a félelemkeltés. Tehát a zaklatás csak *tevőlegesen* elkövethető bűncselekmény. Az elkövetés módja az első fordulatban

⁹ Btk. 222. § (1).

¹⁰ Btk. 222. § (2).

¹¹ Btk. 222. § (3).

a megfélemlítés, míg a második fordulatban az erőszakos vagy közveszélyt okozó cselekménnyel való fenyegetés.

A hazai esetszámokat tekintve¹² láthatjuk, hogy 2018 II. féléve óta napjainkig összesen több mint 11 ezer eset történt meg. A legtöbb a fővárosban (1713 eset), megyei szinten az első két helyezett Borsod-Abaúj-Zemplén (1302 eset) és Pest megye (1242 eset), míg a legkevesebb eset Vas (263) és Zala megyében (223) fordult elő. Azt is látjuk, hogy több mint 4800 esetben felnőtt korúval szemben indult eljárás, és a fiatalokkorúakkal szemben csupán 209 esetben foganatosítottak ilyet. A nemek megoszlásakor az a tendencia látszik, hogy többnyire férfiak követték el a bűncselekményt, közülük is főként felnőtt korúak. Ami viszont a statisztikából nem látszik: milyen típusú zaklatásról van szó? Offline vagy online, esetleg mindkettő?

5. A cyberbullying általános jellemzői

A hazai diskurzusban is gyakran csak angol nevével illetett „cyberbullying” vizsgálata interdiszciplináris terület, mivel nem pusztán pszichológusok, hanem pedagógusok, jogi szakemberek és szociológusok is foglalkoznak a téma kérdéskörével. A nemi érintettségéről nincs egységes konszenzus a kutatók között. Domonkos és Ujhelyi¹³ – a releváns kutatások áttekintése után – úgy vélik, hogy a zaklatás során az elkövető és az áldozat szerepeit betöltő fiatalok között jól körbejárható módon nemi eltérés van: a lányok sokkal kevesebb alkalommal válnak elkövetővé és sokkal nagyobb eséllyel válnak sértetté, mint a fiúk. Fiúk esetében mindez fordított. A tanulmányban azonban arról olvashatunk, hogy nincs összefüggés a nemek magasabb arányú érintettsége és a zaklatás között, vagyis a fiúk és a lányok egyenlő arányban válhatnak elkövetővé és áldozattá.¹⁴

Az internetes zaklatás legveszélyesebb jellemzője, hogy tartalma gyakorlatilag azonnal *terjeszthetővé* válik, így a sértő bejegyzéssel az áldozat újra és újra találkozik – ezzel újabb és újabb traumatizációnak és viktimizációnak válva kiszolgáltatottá –, mindez pedig az esetek többségében a nyilvánosság bevonásával zajlik. Aricak úgy fogalmaz, hogy „a számítógépek megjelenése előtt a gyerekek biztonságban érezhették magukat a szobájukban a zaklató aktusok elől, de ma már a cyberbullying képes oda is behatolni”.¹⁵

Manapság a mobilinternetnek, a wifihálózatoknak és egyéb hot spotoknak köszönhetően bármikor csatlakozni tudunk a világhálóra. Ha eltévedünk, semmi gond, nem esünk kétségbe, csak megnyitjuk a Google Maps vagy a Waze alkalmazásokat, és már meg is oldottuk a problémánkat. Gyakorlatilag 0–24 órában elérhetővé váltunk. Az állandó *elérhetőség*, az online eltöltött idő nagy mennyisége a cyberbullying kialakulásának másik kedvező feltétele. A sértett bármikor célkeresztbe kerülhet. Kutatók szerint ez azért is veszélyes, mert nehezebbé válik az elmenekülés, és az érzelmi

¹² Forrás: Egységes Nyomozóhatósági és Ügyészségi Bűnügyi Statisztika. 2021. 01. 23.

¹³ Domonkos–Ujhelyi (2015): i. m.

¹⁴ Heidi Vandebosch – Katrien van Cleemput: *Cyberbullying among youngsters. Profiles of bullies and victims. New Media & Society*, 11. (2009), 8. 1349–1371.

¹⁵ Aricak et al. (2008): i. m. 253.

bevonódás sokkal megterhelőbb, mint a zaklatás offline változatában. A virtuális tér egyik hátránya az anonimitás lehetősége, ami keltheti azt a látszatot, hogy az elkövető „megússza” a felelősségre vonást, ez pedig elősegítheti a zaklató tevékenység megismétlődését. A térbeli távolság a zaklató és áldozata között szintén hozzájárul ahhoz, hogy a zaklatás gyakoribbá váljon, továbbá hatással van az empátia átélésére is: „a nonverbális jelek hiánya miatt az elkövető nem látja áldozata reakcióját, nem szembesül a zaklatás következményeivel, csökken az áldozattal való együttérzés esélye, ami növeli az ismétlődés lehetőségét és a büntudat hiányához vezet”.¹⁶ Az online zaklatás során az elkövető és az áldozat között több kilométer távolság is lehet, így a zaklató, ahogy Domonkos is írja, nem szembesül közvetlenül áldozatának reakciójával. Addig, amíg offline esetekben nagyobb az esély az empátia átérzésére – hiszen az elkövető látja, hogy tette milyen emocionális válaszokat váltott ki áldozatából –, az online térben jelentősen kevesebb. A hagyományos zaklatás megvalósításánál szükséges feltétel volt a fizikai közelség, a kontaktusteremtés; a zaklató és áldozat viszonylag közel tartózkodtak egymáshoz, vagyis az elkövető a reakciót közvetlenül tapasztalta meg, amely közvetlen tapasztalás elősegítette a morális érzelmek, köztük az empátia megélését. Online térben azonban a reakcióról az elkövető csak közvetetten kap visszajelzést: az általa megtettek elhárítására irányuló aktust látja mindössze (például üzenet törlése, személy letiltása vagy blokkolása), de a mögötte húzódozó érzelmi töltetet nem, így a morális érzelmek kiváltódása nehezebben megy végbe.

6. Személyiségprofilok

6.1. Az elkövetők személyiségrajza

A résztvevők személyiségét áttekintve mindenekelőtt megállapíthatjuk, hogy az online agresszorokra a pszichoszociális karakterisztikumok tekintetében az alacsony elköteleződés jellemző, és gyakori, hogy fizikailag is inzultálják társaikat. Igyekeznek megszerzeni a másik személy feletti kontrollt, és dominanciát gyakorolni. Általában nemcsak a kortársaikkal szemben agresszívek, hanem a felnőttek irányában is. Gyakran szegik meg az iskolai szabályokat, előírásokat – esetenként a törvénnyel is szembekerülnek. Alacsony iskolai elköteleződéssel jellemezhetőek, továbbá esetükben gyakoriak a kriminalizáló aktusok (például a szerhasználat és a lopás). Általában extrovertáltak. A családjukban ritka a feléjük irányuló szülői ellenőrzés, azonban a fizikai büntetés gyakori. Csoportjuk viszonylatában (osztályon belül) központi helyet foglalnak el. Jellemzően olyan személyek, akik előzetes provokáció nélkül támadnak áldozatukra, társaiktól pedig fizikailag erőteljesebbnek érzik magukat. Önbizalmuk határtalan, szelf-percepciójuk jellemzően pozitív irányba torzít. *Énképük – én-ideáljuk – elvárt énjük* között nagyfokú kongruencia figyelhető meg. Az elkövetők többsége úgy jellemezi magát, mint domináns személy, amely kijelentéssel az *énképéről* ad visszajelzést. Elbeszéléseik szerint azonban még nagyobb dominanciára vágynak (*én-ideál*),

¹⁶ Domonkos (2014): i. m. 62.

sőt, úgy gondolják, hogy a domináns viselkedést mások is elvárják tőlük (*elvárt én*). Az elkövetővé válás az alacsony szocioökonómiai státuszt betöltő és idősebb fiatalok körében magasabb, kiindulópontjának a 10–12 éves kort jelölik meg a szakemberek. Lányok inkább a zaklatás indirekt módját választják (pletykák terjesztése, rágalmazás), míg a fiúk a nyílt és direkt formát preferálják, amely agresszív viselkedés nemcsak az iskolában nyilvánul meg, hanem otthon, vagy akár a szomszédban, sőt a közösségi oldalakon is.¹⁷

6.2. Az áldozatok profilja

Alacsony önértékeléssel és önbizalommal rendelkeznek, társaiknál fizikailag gyengébbek vagy annak tekintik magukat. Barátaik száma kevés, introvertált, elszigetelt személyek, akikre bizonytalanság jellemző. Interperszonális kapcsolataik lazák, osztálytársaikkal nem tudnak szoros kapcsolatot kialakítani. Nagyobb a viktimizáció esélye azoknál a fiataloknál, akik nem heteroszexuálisak; azoknál, akik több információt osztanak meg magukról a közösségi oldalakon, ugyanakkor a nem, az etnikai és faji hovatartozás, a szocioökonómiai státusz mind rizikófaktorok. Ha a szülői háttér túlságosan védelmező, a gyerekek a fejlődési és szocializációs folyamatok során nem sajátítják el a megfelelő védekező- és megküzdési stratégiákat. Szorongóvá, depresszívú válnak, és nem ritka az önbántalmazás vagy a szuicidium sem – főleg azoknál, akik a zaklatás mindkét formájában érintettek. Tanulmányi teljesítményük romlik, az iskolához nem fűzi őket szorosabb kötelék. Kevésbé népszerű személyek.

Megkülönböztetett szerepet tölt be az áldozatok egy speciális csoportja, az *agresszív áldozatok*. Ők azok, akik reaktív agresszióval reagálnak egy-egy zaklató eseményre, ezzel képezve meg a zaklató áldozatok csoportját. Viselkedésük impulzív, aminek következtében a provokáló tényezőket és a fenyegetést jelentő személyeket intuitív módon rögtön ellenséges képzetekkel ruházzák fel.¹⁸

Ezen a ponton fontos néhány szót ejteni az agresszióról. Az agresszió evolúciós pszichológiai megközelítésből adaptív viselkedésmód, amely a túlélést szolgálta, szolgálja. Az agresszió szót meghallva sokakban egy negatív színezetű viselkedésről kialakult reprezentáció aktivizálódik, és az agresszióval sok esetben az erőszak asszociálódik. Azonban fontos megjegyezni, hogy létezik proszociális agresszió,¹⁹ vagyis olyan agresszív magatartás, amely a társadalom védelme érdekében aktivizálódik – gondoljunk

¹⁷ Vö. Ann Frisén – Anna-Karin Jonsson – Camilla Persson: Adolescents' perception of bullying. Who is the victim? Who is the bully? What can be done to stop bullying? *Adolescence*, 42. (2007), 749–761; Aricak et al. (2008): i. m.; Vandebosch – Van Cleemput (2009): i. m.; Esther Calvete et al.: Cyberbullying in adolescents. Modalities and aggressors' profile. *Computers in Human Behavior*, 26. (2010), 1128–1135; Körmendi Attila: A szemlélődők szerepe az iskolai zaklatásban. *Alkalmazott Pszichológia*, 14. (2014), 2. 105–121; Domonkos (2014): i. m.; Domonkos–Ujhelyi (2015): i. m.

¹⁸ Vö. Aricak et al. (2008): i. m.; Shari Kessel Schneider et al.: Cyberbullying, school bullying, and psychological distress. A regional census of high school students. *American Journal of Public Health*, 102. (2012), 1. 171–177; Sheri Bauman – Russel B. Toomey – Jenny L. Walker: Associations among bullying, cyberbullying, and suicide in high school students. *Journal of Adolescence*, 36. (2013), 341–350; Domonkos (2014): i. m.; Domonkos–Ujhelyi (2015): i. m.

¹⁹ Haller József – Fogarasi Mihály – Ivaskevics Krisztián: Agresszió és erőszakos bűncselekmények. In Haller József (szerk.): *Bűntettek kriminálpszichológiája*. Budapest, Dialóg Campus, 2020. 17–58.

csak a rendvédelemben dolgozó személyek magatartására, amikor egy fegyverrel felszerelkezett bűnözővel szemben intézkednek.

A stressz kezelésének egyik lehetséges formája az érzelmi alapú megküzdés, aminek során a szituációt érzelmeink irányításával próbáljuk megoldani, míg egy másik formája a problémaközpontú megküzdés, amikor az elénk táruló akadályokra és azok megszüntetésére összpontosítunk. Elmondható, hogy azok az áldozatok, akik az utóbbi stratégiát preferálták és alkalmazták a zaklatással szemben, „kevesebb egészségügyi problémáról számoltak be”,²⁰ továbbá, hogy az életkor előrehaladtával csökken az áldozattá válás kockázata. Narratív elemzésekből kiderül, hogy az áldozatok azért váltak célponttá, mert *mások* voltak a többiekhez képest, például különböztek külső megjelenésükben. Néhány áldozat arról számolt be, hogy a bullying megszakadt abban a pillanatban, amikor változtattak a külsejükön, és ennek következtében már nem tértek el nagymértékben társaiktól.²¹

7. Csoportdinamikai folyamatok iskolai közegben

Amennyiben a zaklatás folyamata direkt és nyílt módon zajlik, úgy a környezet akarva-akaratlanul is belevonódik a cselekmények sorába, és különböző pozíciókat vesz fel. Három lehetséges csoportszerep azonosítható az áldozat és a zaklató személyén kívül, akik részt vesznek a folyamatban. Elsőként említendő a *védelmeső*, aki mindent megtesz azért, hogy a sértettet megvédje és leállítsa a zaklatást, másodikként a *zaklató segítő*, akik mindenben támogatják őt: az offline térben ők azok, akik elfogják és leteperik az áldozatot, míg a virtuális térben megosztásokkal segítik a negatív tartalom terjedését. A harmadik csoport azután a *megeősítő*ké. Ennek tagjai tevélegesen nem vesznek részt a zaklatásban, azonban a zaklatónak verbális megerősítést nyújtanak, esetenként még kommentekkel is hergelve őt a kibertérben. Megjegyzendő ugyanakkor, hogy a fent említett három csoport képviselői az úgynevezett *szemlélők* közül kerülnek ki. Ezek a diákok formailag semlegesek, és egyik oldal mellett sem foglalnak állást, csak figyelemmel kísérik az eseményeket. Közbelépésük meggátolhatja a zaklatást, annak hiánya viszont megerősítheti a zaklató cselekvését.

A prevenció és intervenció során a cél tehát az, hogy a csoportban minél több védelmeső és minél kevesebb támogató személy legyen. Egyes elméletek ennél jóval összetettebbek. Ezek a teóriák egy kontinuum mentén helyezik el a különböző szerepeket felvevő és betöltő személyeket, mely kontinuum két végén az elkövető és az áldozat helyezkedik el. Ha a zaklató szerepétől indulunk el, akkor őt követik a *csatlósok*, akik a zaklatás aktív támogatói, de maguk soha nem kezdeményeznek. Utánuk jönnek a *passzív zaklatók*, akik pusztán helyeslő hozzászólásokkal tarkítják az agresszív viselkedést. E passzív támogatók azok, akik ugyan élvezik a zaklatást, de nem támogatják azt. Nagyjából középen helyezkednek el a *szemlélők*, akik állásfoglalás nélkül figyelik az eseményeket. A *passzív védelmesők* ellenzik a zaklatást, mégsem lépnek közbe, míg az *aktív védelmesők* minden lehetséges módon igyekeznek meggátolni azt.

²⁰ Domonkos–Ujhelyi (2015): i. m. 78.

²¹ Frisén – Jonsson – Persson (2007): i. m.

Jellemző rájuk a morális érzelmek (empátia) magas szintje, az erőteljesen funkcionáló én-hatékonyság, a felsőbb szociális státusz, az altruizmus és a proszocialitás, az adaptív megküzdési stratégiák megléte és alkalmazása.²²

Kutatásokat elemezve „az a kép körvonalazódott, hogy a zaklatások gyakoriságát befolyásolhatja a szemlélők reakciója, vagyis a segítők részvétele a bántalmazásban, a védelmezők közbelépése és általánosságban a közösség reakciója. Egyrészt a szemlélők hatékonyak lehetnek a bántalmazás leállításában [...], másrészt a zaklatás az esetek 85–90%-ában a kortársak jelenlétében zajlik, tehát a szemlélők szinte minden esetben jelen vannak a zaklatáskor”.²³

Jól látjuk tehát, hogy a zaklatás folyamatában nem pusztán az elkövető–áldozat szerepkör betöltőit kell azonosítani, hanem a csoportszerepek többi tagját is, hiszen az intervenció szempontjából nekik is óriási szerepük lesz a folyamat kezelésében.

A közbelépés elmaradásának oka lehet a zaklatótól, valamint az áldozattá válástól való félelem, a bizonytalan interperszonális kapcsolatok, ugyanakkor a fiatalabb csoportokban a zaklató egy idő után követendő modellé válhat. Bandura szociális tanuláselméletében a modell szerepe igen jelentős. Ha a modell szabadon cselekszik, tehát viselkedése nem kontrollált, vagy a viselkedését – legyen az akár proszociális, akár antiszociális – pozitív megerősítés követi, az általa tanúsított viselkedés követendő példává válik. Ellenkező esetben: ha a nemkívánatos viselkedésre negatív válaszreakció érkezik, akkor a nemkívánatos viselkedés ellenkezője fog a „tanuló” viselkedésében reprezentálódni. Ahhoz, hogy a modellel a gyermek azonosulni tudjon, az alábbi feltételek szükségesek:

- a modell és a megfigyelő között hasonlóság álljon fenn;
- a modell társadalmilag elfogadott szerepet töltsön be;
- a modell viselkedését jutalmazza vagy legalábbis ne büntessék.

8. Pszichés funkcióvesztés

A zaklatások következményeivel a fiatalok nem mindig számolnak. Nincsenek vele pontosan tisztában, hogy az általuk elkövetett cselekedet milyen hatást vált ki az áldozatból. Ezek a következmények éppúgy lehetnek mentális jellegű (például stressz, szorongás, krónikus depresszió), mint testi tünetek (például emésztőrendszeri és kardiológiai problémák), amelyek kölcsönösen hatnak egymásra, interakcióban állnak. Kutatók elsőként a depresszív szimptomákat hozták kapcsolatba a cyberbullying jelenségével: szignifikánsan magasabb depressziós tüneteket detektáltak azoknál a fiataloknál, akik internetes zaklatásnak voltak kitéve. Természetesen a hatások nem pusztán lelki-fizikális diszfunkciók lehetnek: azok a gyerekek, akik a világhálón különböző negatív eseményeknek voltak kitéve, a későbbiekben rosszul működő szociális kompetenciákkal rendelkeztek és kevésbé tudtak sikeresen reflektálni önmagukra.²⁴ A pszichológiai „distressz”-állapotra adott válasz Schneider

²² Vö. Körmendi (2014): i. m.

²³ Körmendi (2014): i. m. 107.

²⁴ Aricak et al. (2008): i. m.

és munkatársai szerint²⁵ lehet a teljesítmény drasztikus romlása, az alacsony iskolai elköteleződés, az önkárosítás vagy akár öngyilkosság elkövetése.

Hinduja és Patchin tanulmányukban²⁶ azt írják, hogy a mindennapi zaklatás meg tapasztalása az iskolában vagy annak környezetében jelentős mértékben összefügg az öngyilkossági képzetek egyre gyakoribb megjelenésével. Ugyanakkor kiemelik: nem pusztán az áldozatok, de az elkövetők körében is kockázatot jelent a szuicídium. Ok-okozati összefüggést tárnak fel a különböző viselkedéses komponensek között: a zaklatás által kialakult depressziós szimptomák – reménytelenség-érzés, elmagányosodás, egyre csökkenő önértékelés – mind prediktív tényezőként jelennek meg az öngyilkossági fantáziák kialakulása és gyakorivá válása során.

Vessünk külön pillantást a zaklatásokra adható extrém válasz, az iskolai *ámokfutás* meghatározására és kiindulópontjaira. A kriminológia a több ember sérelmére elkövetett életellenes bűncselekményeket négy kategóriában tárgyalja, a differenciálás szempontjai a következők:²⁷

- *ámokfutás*: több helyszínen történő folyamatos elkövetés, az áldozatok személye kiszámíthatatlan és véletlenszerű; „rosszkor volt rossz helyen” – éppen akivel találkozik az elkövető (az egyes elméletek szerint ennek a típusnak az egyik altípusát adják a terroristatámadások);²⁸
- *tömeggyilkosság*: ha egy helyszínen négy vagy több ember hal meg;
- *sorozatgyilkosság*: legalább három különböző időpontban kerül sor a cselekmények végrehajtására;
- *kiterjesztett öngyilkosság (családirtás)*: egy alkalommal több ember életének kioltása.

Rátérve az iskolai ámokfutások áttekintésére: Mark Leary és munkatársai úgy gondolják,²⁹ az egyre szélesebb körben és egyre gyakrabban megjelenő iskolai erőszak mögött a társadalom morális értékeinek hanyatlása áll. Elképzelésük értelmében a mai világ felértékeli a halál szerepét, az agresszív számítógépes játékok tárháza pedig végtelen. Összefoglalójuk szerint az iskolai ámokfutók – mint amilyen az 1999-es littletoni lövöldöző (Colorado, Egyesült Államok) volt – magányosak, társaiktól elszigetelten élik mindennapjaikat; osztálytársaiktól, iskolatársaiktól elutasítást kapnak; kívülállónak érzik magukat. Az állandó és ismétlődő zaklatás során elfojtott frusztrációjuk fokozódik, kifejeződése azonban gátlás alá kerül. Az elkövetők többsége azzal magyarázza tettét, hogy társai kiközösítették, bántalmazták őket, és csak a sérelmek miatt reagáltak extrém módon. Az egyik lövöldöző a vele készített interjúban azt mondja, azért ölt, mert mindennaposak voltak a megaláztatásai, és senkit nem érdekelt,

²⁵ Schneider et al. (2012): i. m.

²⁶ Hinduja–Patchin (2010): i. m.

²⁷ Bolyky Orsolya: *Az emberölések jogi és kriminológiai jellemzői, különös tekintettel a mentális tényezők büntetőjogi értékelésére*. Doktori értekezés. Budapest, Pázmány Péter Katolikus Egyetem Állam- és Jogtudományi Kar, 2018.

²⁸ Kulcsár Gabriella: *Az iskolai ámokfutások etiológiája és a prevenció lehetőségei*. Doktori értekezés. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2014; Katherine S. Newman: *Rampage. The Social Roots of School Shooting*. New York, Basic Books, 2004.

²⁹ Mark R. Leary et al.: Teasing, rejection and violence. Case studies of the school shootings. *Aggressive Behavior*, 29. (2003), 202–214.

hogyan mi lesz vele. Vagyis az ámokfutást a társak felől érkező erőteljes szeparációs folyamat előzte meg.

Tanya Beran és Qing Li párhuzamot von az iskolai ámokfutások és az internetes zaklatás között.³⁰ A társas csoportok, így az iskolai csoportok is hierarchikus szerveződést mutatnak, amelyben néhány csoporttag úgy próbál minél magasabbra jutni, hogy dominanciát gyakorol a többi tag felett. A dominancia kifejezésének módja sokféle lehet. Amikor ez a dominanciakifejezés olyan eszközöket hív segítségül, amelyek az individuuum számára károsak – ilyen mondjuk az individuuum életének külső kontrollálása –, akkor az egyén viselkedésmintázatába beemeli a *cry for help* reakciót. Ez egyfajta énvédő mechanizmusnak tekinthető; a személy külső segítségért kiált. Ha a segítség késve vagy egyáltalán nem érkezik meg, az egyén – jelen esetben a tanuló, diák – internalizálja a fokozott stresszhelyzet által kiváltottakat, például a stresszt, a magányosságérzést, a szomorúságot, ami életvitelére, teljesítményére és koncentrációs készségeire is negatív hatást fejt ki.

9. Prevenációs lehetőségek

Majd a tanár megoldja. Vagy: Ez az iskola feladata. Bizonyára sokak számára ismertek ezek a kijelentések. Ahogy minden iskolához kapcsolatos kötelezettséget, úgy a zaklatás kivédését, kiiktatását is sokan elsődleges vagy akár kizárólagosan az intézmény feladatai közé sorolják. Pedig ez nem feltétlen van így. Természetesen elengedhetetlen a tájékozottság és tájékoztatás, ugyanakkor a közvetetten érintett képviselők (pedagógusok) helyett célszerűbb a közvetlenül érintett csoportok (diákok) bevonása a prevencióba.

Domonkos szerint³¹ a megelőzés elsősorban az iskolapszichológus feladata. Meg kell ismertetni a diákokat a lehetséges beavatkozásokkal,³² és fel kell vértetni őket a szükséges tudással. Ennek eszköze lehet egy brosúra vagy az iskola által kialakított eljárási protokoll. Azonban nem minden intézményben dolgozik iskolapszichológus, ha mégis, elképzelhető, hogy egyszerre több iskolában lát el pszichológusi feladatkört, így nincs mindig „helyben”, hogy azonnal reagálni tudjon az eseményekre. Körmendi³³ az edukáció fontosságát emeli ki, amelynek „célközönségét” alkotják a diákokon túl a pedagógusok és a szülők is. Utóbbiak edukációja azért is fontos, mert a zaklatás különböző típusairól kevés információval rendelkeznek, mint ahogyan annak káros hatásairól is. A kívülállók pozitív megerősítéseit meg kell akadályozni a zaklató felé, ezek ugyanis facilitálják az ismételt cselekményt. A cél az kell legyen, hogy a kortársak beavatkozási lehetőségét emeljük ki, amihez a diákok edukációja

³⁰ Tanya N. Beran – Qing Li: The Relationship between Cyberbullying and School Bullying. *Journal of Student Wellbeing*, 1. (2007), 2. 15–33.

³¹ Domonkos (2014): i. m.

³² Mi az eljárás a nyílt, illetve a privát felületeken? Előbbi esetén az azonnali beavatkozás szükséges, míg az utóbbi esetben először a zaklató személyének figyelmen kívül hagyása javasolt mindamelllett, hogy a zaklató tartalmakat mentsük le.

³³ Körmendi (2014): i. m.

szorosan kapcsolódik: hatékony kommunikációs technikák, megküzdési stratégiák oktatása segítően hathat.

Mind a prevenció, mind az intervenció szempontjából elengedhetetlen, hogy az iskolákban kialakítsanak egy széles körű, átfogó válaszstratégiát a bullyinggal szemben. Az igazságszolgáltatás nyújtotta eljárások mellett – polgári peres eljárás, büntetőeljárás, mediáció – az iskoláknak is ki kellene dolgozniuk egy iskolai protokollt, amelyben lefektetik az iskola zaklatással kapcsolatos vélekedését, illetve, hogy zaklatás esetén milyen szankciókat érvényesít az elkövetővel szemben az intézmény.

Fontos, hogy a prevenció célcsoportja ne csak az iskolában tanító pedagógus legyen: a zaklatás aktív és passzív résztvevőit is be kell vonni a megelőzésbe. A tanár nem tud mindig jelen lenni minden konfliktusnál, és ez nem is várható el tőle. Az online zaklatásnak pedig nem kritériuma, hogy iskolaidő alatt történjen meg. Véleményem szerint fontosabb, hogy a diákokra helyezzük a hangsúlyt, hiszen ők a folyamat aktív ágensei. Az edukációs elképzelés nagyon jó kiindulópont, amit érdemes lenne multidiszciplináris perspektívából megközelíteni.

Az egyik ilyen lehetőség egy *face to face*, formális oktatási forma. Ennek keretében alapvető jogi ismereteket kellene átadni és pszichoedukatív tevékenységet lehetne folytatni. Megismertetni a diákokat néhány alapvető büntetőjogi ténnyel, mint amilyen például a büntethetőség kérdése, és azzal, hogy bizonyos cselekedeteik esetleg kimeríthetik valamelyik büntetőjogi tényállást. A pszichoedukáció során a mentális jó- és jóllétről, a rezilienciáról, illetve az általánosan vett csoportdinamikai folyamatokról lehet érdemes párbeszédet folytatni, kiegészítve kommunikációs és asszertivitási tréningekkel, agressziókezeléssel.

A másik lehetőség olyan informális, aktív, csoportfoglalkozás-jellegű események szervezése, ahol a diákok játékos formában sajátítanak el egyes ismereteket és tapasztalatot szereznek.

Az online zaklatás elleni fellépés jól szervezett lehetősége a DGYS (Magyarország Digitális Gyermekvédelmi Stratégiája), amelyet a Kormány a szakmai és társadalmi szervekkel szorosan együttműködve dolgozott ki. Mint fogalmaznak, a DGYS megalkotása során elsődleges szempont volt, hogy a fiatalok naprakész információ birtokába kerüljenek az internethasználat veszélyeit illetően, valamint, hogy felkészítsék a tanulókat, a szülőket és a tanárokat a tudatos és biztonságos internethasználatra. A DGYS keretében kidolgoztak egy kortárs segítő képzési rendszert is, aminek keretein belül az internet előnyeit, valamint annak kockázatait a leginkább érintettek számára a velük egykorú társaik prezentálják – ezáltal hitelesebbé válik az informátor és az általa közölt információ is.

Véleményem szerint a DGYS és az általa képviselt irány példaértékű és hiánypótló, ugyanakkor annak figyelembe kellene vennie azt is, hogy a cyberbullying nem korosztály-specifikus jelenség: a felnőttek körében éppúgy jelen lehet, mint a fiatalok esetében. Így célszerű lenne a DGYS mentén egy felnőttekre szabott, hasonló platform kidolgozása is.

Felhasznált irodalom

- Arıcak, Tolga – Sinem Siyahhan – Aisegül Uzunhasanoglu – Sevda Saribeyoglu – Songul Ciplak – Nesrin Yılmaz – Cemil Memmedov: Cyberbullying among Turkish Adolescents. *Cyberpsychology & Behavior*, 11. (2008), 3. 253–261. Online: <https://doi.org/10.1089/cpb.2007.0016>
- Bauman, Sheri – Russel B. Toomey – Jenny L. Walker: Associations among bullying, cyberbullying, and suicide in high school students. *Journal of Adolescence*, 36. (2013), 341–350. Online: <https://doi.org/10.1016/j.adolescence.2012.12.001>
- Beran, Tanya N. – Qing Li: The Relationship between Cyberbullying and School Bullying. *Journal of Student Wellbeing*, 1. (2007), 2. 15–33. Online: <https://doi.org/10.21913/JSW.v1i2.172>
- Bolyky Orsolya: *Az emberölések jogi és kriminológiai jellemzői, különös tekintettel a mentális tényezők büntetőjogi értékelésére*. Doktori értekezés. Budapest, Pázmány Péter Katolikus Egyetem Állam- és Jogtudományi Kar, 2018.
- Calvete, Esther – Izaskun Orue – Ana Estévez – Lourdes Villardón – Patricia Padilla: Cyberbullying in adolescents. Modalities and aggressors' profile. *Computers in Human Behavior*, 26. (2010), 1128–1135. Online: <https://doi.org/10.1016/j.chb.2010.03.017>
- Domonkos Katalin: Cyberbullying: zaklatás elektronikus eszközök használatával. *Alkalmazott Pszichológia*, 14. (2014), 1. 59–70.
- Domonkos Katalin – Ujhelyi Adrienn: Az online zaklatás médiareprezentációja. *Neveléstudomány*, (2015), 1. 77–92.
- Frisén, Ann – Anna-Karin Jonsson – Camilla Persson: Adolescents' perception of bullying: Who is the victim? Who is the bully? What can be done to stop bullying? *Adolescence*, 42 (2007), 749–761.
- Haller József – Fogarasi Mihály – Ivaskevics Krisztián: Agresszió és erőszakos bűncselekmények. In Haller József (szerk.): *Büntettek kriminálpszichológiája*. Budapest, Dialóg Campus, 2020. 17–58.
- Hinduja, Sameer – Justin W. Patchin: Bullying, cyberbullying and suicide. *Archives of Suicide Research*, 14. (2010), 206–221. Online: <https://doi.org/10.1080/1381118.2010.494133>
- Körmenyi Attila: A szemlélődők szerepe az iskolai zaklatásban. *Alkalmazott Pszichológia*, 14. (2014), 2. 105–121.
- Kulcsár Gabriella: *Az iskolai ámokfutások etiológiája és a prevenció lehetőségei*. PhD-értekezés. Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2014.
- Leary, Mark R. – Robin M. Kowalski – Laura Smith – Stephen Phillips: Teasing, rejection and violence: case studies of the school shootings. *Aggressive Behavior*, 29. (2003), 202–214. Online: <https://doi.org/10.1002/ab.10061>
- Newman, Katherine S.: *Rampage. The Social Roots of School Shooting*. New York, Basic Books, 2004.
- Ortega-Ruiz, Rosario – Paz Felipe – Joaquín Mora-Merchán – Juan Calmaestra – Esther Vega: The emotional impact on victims of traditional bullying and cyberbullying. *Journal of Psychology*, 217. (2009), 4. 197–204. Online: <https://doi.org/10.1027/0044-3409.217.4.197>

- Schneider, Shari Kessel – Lydia O’Donnell – Ann Stueve – Robert W.S. Coulter: Cyberbullying, school bullying, and psychological distress. A regional census of high school students. *American Journal of Public Health*, 102. (2012), 1. 171–177. Online: <https://doi.org/10.2105/AJPH.2011.300308>
- Vandebosch, Heidi – Katrien van Cleemput: Cyberbullying among youngsters. Profiles of bullies and victims. *New Media & Society*, 11. (2009), 8. 1349–1371. Online: <https://doi.org/10.1177/1461444809341263>
- Wölfner, R. – A. Schultze-Krumbholtz – P. Zagorscak – A. Jäkel – K. Göbel – H. Scheithauer: Prevention 2.0: Targeting Cyberbullying@School. *Prevention Science*, 15. (2014), 6. 879–887. Online: <https://doi.org/10.1007/s11121-013-0438-y>

Zoltán Lechner¹

Opposing Discourses of Terror: The Use of the Terrorist Label by the Turkish and Russian Governments in the Northern Syrian Conflict

The primary goal of the paper is to examine how the Turkish and Russian Governments are using the term terrorist in their diplomatic communication towards the Syrian conflict. Following the introduction, the study outlines the theoretical framework – namely the securitisation theory –, then presents a concept of terrorism, which is focusing on the instrumentalisation of the terrorist label in discursive processes. Henceforward, the paper attempts to accomplish the aforementioned goal by examining the Turkish and Russian security discourses on two interrelated issues of the Syrian war: Turkey’s Operation Peace Spring in October 2019, and the Russian–Syrian offensive codenamed Operation Dawn of Idlib between April 2019 and March 2020. Based on the detailed analysis of relevant speeches and articles given or written by high-ranking Russian and Turkish diplomats, the paper displays how the two states justified their military interventions, defined their own roles, and framed the non-governmental actors involved in the conflicts. According to the conclusion of the author, despite the numerous similarities in their discourses, Turkey and Russia define oppositely, who is, and who is not a terrorist in Syria, which constitutes a major collision point between their geostrategic perspectives.

Keywords: Turkey, Russia, Syria, terrorism, security, diplomacy

1. Introduction

In October 2019, shortly after the Turkish Armed Forces conducted a military incursion in northern Syria, Turkey’s United Nations envoy Feridun Sinirlioğlu described the intervention as a ‘limited cross-border counter-terrorism operation’, and condemned

¹ PhD student, Interdisciplinary Doctoral School of the University of Pécs, e-mail: zoltan.lechner@gmail.com

‘any representation of our counter-terrorism operations as an offensive or aggression’.² His Russian counterpart, Vassily Nebenzia, on the other hand, refused to designate the groups targeted by the intervention as terrorists and described the Turkish campaign as an ‘illegal occupation and [...] dangerous experiment in demographic engineering’.³ Based on the exchange of words between the diplomats, we can presume that the two states define the meaning of terrorism differently, and are using the word “terrorist” arbitrarily, which constitutes a major collision point between their narratives. The primary aim of the paper is to test this hypothesis through the detailed analysis of Turkish and Russian security discourses on the northern Syrian conflict. The central question of the research is how the terrorist label is being used by the two governments, and how the two discourses relate to each other.

Geographically, the research is narrowed down to two subregions within Syria: Turkey’s “peace corridor” in northern Syria, and Idlib governorate. Chronologically, the research is focusing on the time period from April 2019 to March 2020 but takes the antecedents of the examined events also into consideration. Thematically, the study focuses on two specific and interrelated issues. On the one hand, it analyses how the Turkish diplomatic communication justified Operation Peace Spring, and how the Turkish and Russian perspectives differ on the Syrian Kurdish political/paramilitary groups. On the other hand, the research examines how the Russian diplomatic communication justified Russia’s active participation in Operation Dawn of Idlib, and how the Russian and Turkish perspectives differ on the radical Islamist group Hayat Tahrir al-Sham. The two issues have been chosen because of three reasons: 1. both interventions generated a fervent international reaction and criticism; 2. in both cases, the motif of terrorism played a major role in the intervention’s official justification; 3. the two interventions are important not only regarding the endgame of the Syrian war but also the Turkish–Russian bilateral relations.

The theoretical basis of the study is the securitisation theory, which explains how political leaderships frame security issues. In the second half of the theoretical framework, a securitisation-inspired concept of terrorism is presented, which focuses on the instrumentalisation of the terrorist label in discursive processes. Accordingly, the methodology used in the research is discourse analysis. As the primary aim of the study is to examine how the two governments framed the interventions in front of the international community, relevant speeches and articles given or written by high-ranking Russian and Turkish diplomats are analysed, to identify recurring elements in the two discourses. Special attention is paid to the analysis of speeches given at the United Nations Security Council and General Assembly during the aforementioned period, obtained from the United Nations Digital Library.

² United Nations General Assembly, Seventy-fourth session 3rd plenary meeting (United Nations Digital Library, 2019), 25.

³ Ibid. 11.

2. Theoretical framework: the theory of securitisation

When the Warsaw Pact and shortly after the Soviet Union collapsed, and the bipolar structure of the cold war ceased to exist, the security agenda which had dominated international affairs for over forty years has seemingly come to an end. The following uncertainty around the nature of international relations prompted a newfound debate on the very meaning of the term *security*. The rise of economic and environmental agendas, the growing role of non-governmental actors, and the concerns regarding identity issues and transnational challenges resulted in the popularity of a new approach, whose proponents argued that the narrow, state- and military-centred perspective of traditionalist theories must be exceeded by adding such issues as climate change, social injustice, water-scarcity and migration to the security agenda.⁴ According to this line of thinking, in the age of intensified globalisation the state loses its monopoly over conducting international affairs, therefore the relevance of security studies can be preserved only if the scope of national security is complemented with human and global aspects.⁵ Responding to these innovative ideas, the main counterargument of the traditionalist thinkers is that the progressive widening of the agenda endangers the intellectual merits of security studies, as it deprives the notion of security of its defined meaning. As a result of expanding its scope, the concept becomes the synonym for potentially ‘everything’, thus losing all its coherence and usefulness.⁶ Traditionalists, therefore, claim that the sole focus of the field must remain national security.

The securitisation theory, created and expanded by the Copenhagen School of Security Studies – Ole Wæver and Barry Buzan among others – offers a third interpretation, which constitutes the theoretical basis of the present study. While it takes the traditionalists’ complaint about incoherence seriously, it nevertheless problematises their clinging to the exclusively state- and military-centred perspective. Instead of seeking coherence by confining the definition to the military sector, it focuses on the inner logic of security, the process through which political leaderships decide what is, and what is not a security threat. The key argument of the theory is that an issue – which can be for instance a minority’s pursuit of greater autonomy, migration or the spreading of certain ideologies – becomes a security matter when it is identified as an existential threat to a referent object – usually the state – by a securitising actor – usually the government – which thereby gains legitimacy and endorsement for extreme measures beyond the scope of ordinary politics,⁷ for example suspending the separation of power branches, conducting large-scale secret surveillance programs, or launching otherwise controversial military campaigns.

Accordingly, the term *securitisation* refers to a discursive instrument utilised by political actors, which enables them to “move” a particular problem into a specific area, thereby claiming special rights to use any means necessary to solve it. This is

⁴ Viktor Glied, ‘Migrációs diskurzus a poszt-multikulturális Európában’, *Pólusok* 1, no 1 (2020).

⁵ Barry Buzan, ‘Rethinking Security after the Cold War’, *Cooperation and Conflict* 32, no 1 (1997).

⁶ Ole Wæver, ‘Securitization and Desecuritization’, in *On Security*, ed. by Ronnie D Lipschutz (New York: Columbia University Press, 1995).

⁷ Ole Wæver, ‘Politics, security, theory’, *Security Dialogue* 42, no 4–5 (2011).

realised through the power of language: by framing an issue in a certain way, one can shape public perceptions according to their political interests.⁸ The utterance is therefore an act in itself, which constitutes social and political reality: labelling something as an imminent threat can generate an intersubjective sense of danger, which changes the accepted rules of politics. What is decisive in this regard is not whether the expressed statements about the issue are factually true, but whether the securitising actor has the resources, channels and skills to convince the target audience. Thus, the process of securitisation has two key components: the designation of an existential threat requiring emergency measures and the acceptance of that designation by the audience.⁹

2.1. *Understanding the effect of the terrorist label through securitisation theory*

Especially since the September 11 attacks, terrorism has been one of the most important subjects of security studies. Although the need for a common understanding of the problem is widely acknowledged, there is a seemingly endless debate among experts over the precise meaning of the term. As Alex Schmid, one of the leading scholars in the field points out, the word *terrorism* refers to a complex and multidimensional phenomenon, and is used in so many different contexts that it is questionable whether a unitary and all-inclusive definition can be reached. The fundamental reason for the difficulty to determine the objective meaning of terrorism is ontological: there is no intrinsic essence of the concept, as it is a man-made construct, not an object in the material sense.¹⁰

The lack of consensus constitutes not only an analytical problem but also a practical one. Boaz Ganor, the director of the Israel-based International Policy Institute for Counter-Terrorism convincingly argues, that it is necessary to find an exhaustive and objective definition of terrorism, as it is indispensable to any attempt to make sufficient countermeasures. Only based on such a definition, he claims, can the global struggle against terror be organised and implemented. The concept he offers is simple yet compact: ‘...terrorism is the intentional use of, or threat to use, violence against civilians or against civilian targets, in order to attain political aims.’¹¹ Although creating a precise definition certainly has some scientific value, what Ganor refuses to acknowledge is that in practice, identifying the terrorist always takes place in a political context, as the ability to do so constitutes power. Therefore, solving the problem created by the aforementioned lack of agreement does not depend on

⁸ Ole Wæver, ‘Security, the Speech Act: Analysing the Politics of a Word’, *Working Paper* no 19 (Copenhagen Peace Research Institute, 1989).

⁹ Buzan, ‘Rethinking Security’.

¹⁰ Alex Schmid, ‘Terrorism – The Definitional Problem’, *Case Western Reserve Journal of International Law* 36, no 2 (2004).

¹¹ Boaz Ganor, ‘Defining Terrorism: Is One Man’s Terrorist another Man’s Freedom Fighter?’ *Police Practice and Research: An International Journal* 3, no 4 (2002), 294.

whether we can find the perfect definition of terrorism, but whether the involved actors – in most cases governments of states – can make a political compromise.

It is precisely the political nature of the matter, why it makes sense to approach it using securitisation theory: instead of making an effort to determine who is and who is not a terrorist based on objective factors, the research should focus on describing which actors are involved in defining terrorism, how they frame the threat, why they do so, and how the utterance of the term changes the boundaries between self and other.¹² What the *political* in this case refers to is that publicly identifying a group as a terrorist organisation or using expressions like “Axis of Evil” to describe certain countries are not neutral acts, but powerful discursive instruments which convey disapproval, appeal to emotions, and serve as mobilisation tools.¹³

In social sciences, discourse is defined as a structure of knowledge, conveyed through language, designed to exclude or invalidate alternative forms of knowledge and practice, justify a particular political and social order, and sustain a hegemonic interpretation of reality.¹⁴ Accordingly, a terror discourse applies labels, images, narratives, arguments and analogies related to the notions of terrorism and counterterrorism, and appeals to a target audience – which, depending on the circumstances, can vary from a domestic voting bloc to the international community – with the aims of de-legitimising particular actors, and legitimising the use of particular actions. Labelling the opponents as terrorists prevents the recognition of their political legitimacy, as it suggests that they are enemies of the civilised world, with whom negotiation is not acceptable.¹⁵ This implies that the challenge they pose to the security of the domestic and/or international community requires the adoption of uncompromising methods. The acceptance of the message by the target audience thus means that the political leadership receives moral and legal justification for using practices otherwise deemed inhumane or illegal.¹⁶ Acknowledging that the identified threat may be real and indeed requires special solutions should therefore not make us overlook the possibility that suspending human rights and the rule of law in the name of countering terrorist activities will result in the abuse of power and have the effect of increasing the citizens’ insecurity.¹⁷

Consequently, the understanding of terrorism based on securitisation theory is more pessimistic than the traditional one, as it questions the practical value of a precisely formulated definition. The process of identifying the terrorists takes place in a discursive context, and the definitions used by governments are adjusted to their domestic or geopolitical interests. The adequate methodological approach

¹² Jørgen Staun, ‘When, how and why elites frame terrorists: a Wittgensteinian analysis of terror and radicalisation’, *Critical Studies on Terrorism* 3, no 3 (2010).

¹³ Schmid, ‘Terrorism – The Definitional Problem’.

¹⁴ Richard Jackson, ‘Knowledge, Power and Politics in the Study of Political Terrorism’, in *Critical Terrorism Studies: A New Research Agenda*, ed. by Richard Jackson, Marie Breen Smyth and Jeroen Gunning (Abingdon: Routledge, 2009), 66–83.

¹⁵ Fred Vultee, ‘Securitization: A new approach to the framing of the “war on terror”’, *Journalism Practice* 4, no 1 (2010).

¹⁶ André Barrinha, ‘The political importance of labelling: terrorism and Turkey’s discourse on the PKK’, *Critical Studies on Terrorism* 4, no 2 (2011).

¹⁷ Priya Dixit, ‘Securitization and Terroristization: Analyzing States’ Usage of the Rhetoric of Terrorism’, in *State Terror, State Violence: Global Perspectives*, ed. by Bettina Koch (Wiesbaden: Springer VS, 2016).

is therefore discourse analysis, a form of critical theorising aiming to examine the relationship between textual and (geo)political processes. Accordingly, the critical analysis of a terror discourse analyses relevant sources – speeches, articles or media contents – in a broader context, to identify linguistic elements directly or indirectly related to terrorism, examining what is and what is not addressed, and attempting to understand the political motivations behind the rhetoric.

3. Operation Peace Spring and the Turkish discourse of terror

In a phone conversation on the 6th of October 2019, U.S. President Donald Trump informed Turkish President Recep Tayyip Erdoğan about his decision to withdraw the American troops from Northeast Syria, thus providing the opportunity for Turkey to initiate a cross-border military intervention. Three days later, the Turkish Armed Forces and its Syrian allies launched Operation Peace Spring, a limited incursion into the 100 km stretch between the towns of Tal Abyad and Ras Al-Ayn, in order to clean the territory from “terrorist elements” and to create a “safe zone” which enables the repatriation of the Syrian refugees residing in Turkey.¹⁸ Within four years, this was the third major campaign conducted by the Turkish state in the Kurdish-controlled region commonly called Rojava.

The military containment of the Syrian–Kurdish Democratic Union Party (PYD) and its armed wing, the People’s Protection Units (YPG) became a priority for Ankara in 2015, as a result of three interrelated developments: 1. In June 2015, Turkey’s governing Justice and Development Party (AKP) lost its parliamentary majority for the first time, partially because of the unexpected success of the Peoples’ Democratic Party, a progressive-socialist party, which was able to obtain the support of a large part of Turkey’s Kurdish community. Following the elections, President Erdoğan and the AKP started informally cooperating with a far-right opposition party, while embracing an exclusivist, nationalist rhetoric. 2. This coincided with the final collapse of the peace process – initiated in 2008 then restarted in 2013 – between the Turkish state and the Kurdistan Workers’ Party (PKK),¹⁹ after a PKK-related group murdered two Turkish police officers in the town of Ceylanpınar in July 2015.²⁰ 3. In parallel with the domestic processes in Turkey, the YPG – with the military support provided by the U.S. Army – achieved successes in the fight against the so-called “Islamic State” (Daesh), and started continuously expanding the territory under its control in northern Syria, thereby awakening the greatest fear of many Turks, an uninterrupted Kurdish belt along Turkey’s southern border, controlled by PKK-related militias.²¹ In order to

¹⁸ Krisztián Manzinger and Péter Wagner, ‘Syrian Kurds, Rojava and Alternative Society Building in Middle East’, *Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata* 148, no 1 (2020).

¹⁹ A Kurdish militant political organisation and armed separatist movement, established in 1978 in Southeast Turkey. In 1984, the PKK launched a full-scale insurgency against the Turkish state. Since then, approximately 40,000 people have died in the conflict.

²⁰ Arin Savran, ‘The Peace Process between Turkey and the Kurdistan Workers’ Party, 2009–2015’, *Journal of Balkan and Near Eastern Studies* 22, no 6 (2020).

²¹ H Akin Ünver, ‘Schrödinger’s Kurds: Transnational Kurdish Geopolitics in the Age of Shifting Borders’, *Columbia Journal of International Affairs* 69, no 2 (2016).

prevent that scenario, Turkey launched its first major military intervention in Syria, Operation Euphrates Shield in August 2016. Although the official aim of the campaign was to push back Daesh, by capturing several towns including Jarablus and Al-Bab, Turkey has also prevented the YPG from gaining more ground and merging the two Kurdish cantons of Afrin and Kobane.²² Turkey's second military intervention, Operation Olive Branch launched in January 2018, has resulted in the occupation of Afrin and led to the displacement of approximately 150,000 people.²³

Turkey's 2019 intervention generated a wide and fervent international outburst. It triggered extensive criticism in Washington, followed by a bipartisan rebuke to the President for his decision in the House of Representatives.²⁴ In a declaration by the High Representative, the European Union called upon Turkey to cease the unilateral military action and expressed its concern that the operation is endangering the progress achieved by the International Community to defeat Daesh.²⁵ Arab League Secretary-General Ahmed Aboul Gheit has also condemned the operation, calling it an invasion of Arab land and aggression on the territorial sovereignty of the Syrian state.²⁶ The Turkish troops and their rebel allies were accused of committing war crimes including summary killings and unlawful attacks on non-combatants. According to the Kurdish-led administration's health authority in Northeast Syria, in the period between 9 and 17 October at least 218 civilians – among them, 18 children – have been killed.²⁷

Having no other options to stop the incursion, the PYD/YPG has made a Moscow-brokered deal with Syrian President Assad on the 15th of October, which resulted in the movement of Russian and Syrian troops into Kurdish-controlled areas not yet reached by Turkish forces. The major military clashes between the Turkish army and the Kurdish militias lasted until the 17th of October when U.S. Vice President Pence and President Erdoğan agreed on a ceasefire over Turkey's operation. The agreement gave 120 hours for the YPG to withdraw its forces from an approximately 100 km long strip along the Turkey–Syria border, the aforementioned safe zone area between the towns of Tal Abyad and Ras al-Ain.²⁸ It was a clear sign of growing Russian influence that five days later President Erdoğan met President Putin in Sochi to discuss the post-operation state of affairs in northern Syria. The memorandum of understanding signed by the two leaders *inter alia* gave an additional 150 hours to the YPG to complete the withdrawal from the safe zone; reiterated the parties'

²² Zoltán Egeresi, 'Törökország konfliktusa az észak-szíriai kurdokkal', *KKI-Elemzések* E-2020/11.

²³ United Nations High Commissioner for Refugees, Syria Factsheet (January–November 2018) Situation Report, 2018.

²⁴ Catie Edmondson, 'In Bipartisan Rebuke, House Majority Condemns Trump for Syria Withdrawal', *The New York Times*, 16 October 2019.

²⁵ Council of the European Union, Declaration by the High Representative on behalf of the EU on recent developments in north-east Syria, 2019.

²⁶ Reuters, 'Turkey's Syria offensive an 'invasion': Arab League secretary general', 12 October 2019.

²⁷ Amnesty International, 'Syria: Damning evidence of war crimes and other violations by Turkish forces and their allies', 18 October 2019.

²⁸ Umut Uras, 'Turkey's Operation Peace Spring in northern Syria: One month on', *Aljazeera*, 08 November 2019.

commitment to preserving the territorial integrity of Syria; and emphasised their determination to fight terrorism in all forms.²⁹

3.1. *The Turkish discourse of terror*

If we examine the Operation Peace Spring-related speeches and articles given or written by high-ranking Turkish diplomats, we can identify five recurring arguments, which constitute the backbone of the official justification for the intervention. The first element of the discourse is designating the presence of PYD/YPG as an existential threat to the national security of Turkey, which implies that the intervention was an act of self-defence. This is evident for instance in the letter addressed to the President of the Security Council by Turkey's envoy to the UN: 'Turkey's national security has been under the direct and imminent threat of terrorist organizations operating in the east of the Euphrates in Syria.'³⁰ The securitisation of the "Kurdish issue" resonates well with the collective threat perceptions of the Turkish public, as the majority of Turks believes that the efforts of the Kurdish minority to gain more autonomy and the support provided by outside (Western) powers for these efforts endanger the unity of the state. This intersubjective fear is not confined to the Turkish borders: as the population along both sides of the Turkish–Syrian border is mostly Kurdish, many Turks are concerned about the possibility that the level of autonomy achieved by northern Syrian Kurds will revive separatist tendencies in Southeast Turkey. From a legal perspective, however, the argument has yet another meaning: in case the operation is recognised as an act of self-defence by the International Community, it is in line with international law. Accordingly, Sinirlioğlu cites Article 51 of the Charter of the United Nations as legal justification, which declares that individual or collective self-defence is legitimate if an armed attack occurs against a member state.

The second discursive element is the designation of the PYD/YPG as a force occupying Northeast Syria and oppressing the various communities living under its rule.³¹ In a speech given at the UN Security Council in October 2019, Sinirlioğlu said that the area controlled by the Kurdish militias is a 'testing ground for a new totalitarian terrorist State'.³² Similarly, in an article published by *The New York Times*, Foreign Minister Mevlüt Çavuşoğlu characterised the rule of PYD/YPG as 'tyranny of terrorist organisations'.³³ The implication, in this case, is twofold. On the one hand, by emphasising the dictatorial nature of the PYD/YPG authorities, the Turkish Government frames the operation as a humanitarian intervention aiming

²⁹ President of Russia, 'Memorandum of Understanding Between Turkey and the Russian Federation', 22 October 2019.

³⁰ Feridun H Sinirlioğlu, *Letter dated 9 October 2019 from the Permanent Representative of Turkey to the United Nations addressed to the President of the Security Council* (United Nations Digital Library, 2019), 1.

³¹ The Turkish accusations against the PYD are not baseless. According to a report conducted by the Human Rights Watch in 2014, the PYD has committed a range of human rights abuses, including arbitrary arrests, abuse in detention, unsolved disappearances and killings, and the use of children in PYD security forces (Human Rights Watch, 2014).

³² United Nations Security Council, 8645th meeting (United Nations Digital Library, 2019), 26.

³³ Mevlüt Çavuşoğlu, 'Why Turkey Took the Fight to Syria', *The New York Times*, 11 October 2019.

to liberate oppressed and terrorised civilians. On the other hand, the argument can be interpreted as a response to the criticism that Turkey has violated the territorial integrity of the Syrian state: by emphasising the separatist agenda of the PYD/YPG, Ankara frames Operation Peace Spring as an intervention aiming not to violate, but to preserve Syria's integrity. This narrative appeared for instance in a speech given by Çavuşoğlu at the TRT World Forum 2019, in which the minister said that one of the goals of the operation was to 'enforce Syrian territorial integrity, which we are very much committed to. And the aim of this terrorist organization and the countries who were supporting this terrorist organization was to divide Syria and to create a terror state along our border'.³⁴

The third and arguably most important discursive element is the almost constant use of the term "PKK/PYD" or "PKK/PYD/YPG" in speeches and articles alike, which clearly indicates that according to Ankara's narrative, the PKK and the PYD are in fact one organisation. This claim has its basis, as the history of the two groups is tied together, and the ideological connections between them are undeniable. After the 1980 military coup in Turkey, the PKK moved its headquarter to northern Syria, and organised the armed struggle against the Turkish state mainly from there until 1998, when Ankara and Damascus normalised their relations and signed the Adana Security Agreement, which obligated the Syrian regime to recognise the PKK as a terrorist organisation, and prohibit all activities of the group on its territory. Following the millennium, the PKK has established regional "sister parties" in the countries with significant Kurdish minority;³⁵ one among them being the PYD, inheriting the organisational resources left behind by the "mother party". These branches remained under the PKK's indirect control; some scholars, however, argue that the exceptional circumstances in Syria since 2011 have given the PYD a more distinctive purpose and identity, which may have resulted in the loosening of its ties with the PKK.

According to Kaya and Lowe, the priorities of the two groups started to diverge in 2015, when the PKK returned to the low-level guerrilla warfare against Turkey, while the PYD remained focused on the efforts to implement an autonomous administration in northern Syria and gain more international legitimacy.³⁶ This narrative however is debatable, as, during the second half of the decade, the PKK reportedly carried out attacks on the Turkish state with American weapons provided to the YPG, which suggests that the ties between the groups are still strong.³⁷ The Turkish discourse which consistently refers to them as one serves two main purposes. On the one hand, by emphasising that the PYD/YPG is inseparable from the PKK, Ankara points out the contradiction in the U.S. discourse, which approves the former while condemning the latter as a terrorist organisation. On the other hand, according to Ankara the inseparability of the two groups means that the Adana Agreement can be applied to the PYD/YPG as well. This is especially relevant because of the 4th annex of the document, which declares that the Syrian Government's 'failure to take the necessary

³⁴ Mevlüt Çavuşoğlu, 'Demystifying Turkey's Operation Peace Spring', *TRT World Forum*, 12 November 2019.

³⁵ International Crisis Group, 'The PKK's Fateful Choice in Northern Syria', 04 May 2017.

³⁶ Zeynep Kaya and Robert Lowe, 'The Curious Question of the PYD-PKK Relationship', in *The Kurdish Question Revisited*, ed. by Mohammed Shareef and Gareth R V Stansfield (London: Hurst & Company, 2017).

³⁷ Daily Sabah, 'US weapons given to PYD used by PKK in attacks in Turkey', 28 April 2017.

measures and security duties, stated in this agreement, gives Turkey the right to take all necessary security measures within 5 km deep into Syrian territory'.³⁸ Therefore, it is not surprising that Turkish diplomats refer to the agreement as legal justification.

The fourth recurring argument is placing the PYD/YPG in the same definitional category as Daesh; thereby criticising the U.S. efforts to counter Daesh through Kurdish proxies. The implication is that as both are terrorist organisations, supporting one to defeat the other is unacceptable. As Sinirlioğlu put it: '...some Member States have provided heavy weapons, ammunition and training to PKK/YPG under the assumption that it was acceptable to use a terrorist organization against another terrorist organization [...]. Unsurprisingly, those weapons have been used to target Turkey and civilians in Syria.'³⁹ Although the Turkish Government's official standpoint is that the conflict in Syria can only be resolved by finding a political solution, it nevertheless vehemently opposes the inclusion of the PYD in any political negotiation. By labelling the PYD as terrorists, Ankara not only attempts to prevent the military support provided for the group but simultaneously legitimises its own decision to veto the Kurdish participation in both the Geneva and the Astana processes. Turkish politicians and diplomats have criticised the efforts made by the U.S. to "rebrand" the YPG, thus making it more acceptable for Turkey. The term "rebrand" mainly concerns the name "Syrian Democratic Forces", under which the YPG is acting since late 2015. In this regard, Ankara's recurring point of reference is a segment from a speech given by General Raymond Thomas in 2017: "We literally played back to them: 'You have got to change your brand. What do you want to call yourselves besides the YPG?' With about a day's notice, they declared that they were the Syrian Democratic Forces. I thought it was a stroke of brilliance to put democracy in there somewhere. But it gave them a little bit of credibility."⁴⁰

The last element is framing the intervention as a precondition for solving the refugee crisis in Turkey. With 3.6 million people, the country indeed hosts the largest refugee community in the world, which creates a wide range of social, administrative, educational and economic challenges for the Turkish state.⁴¹ As the rapidly increasing number of refugees in the second half of the decade has evoked growing displeasure in the Turkish population, the government is interested in solving the problem also from a political perspective. Two weeks before the start of the operation, President Erdoğan gave a speech at the UN's General Assembly, in which he announced that Turkey intends 'to establish a peace corridor in Syria, 30 kilometres wide by 480 kilometres long, where we hope, with the support of the international community, to facilitate the settlement of 2 million Syrians'.⁴² The Turkish discourse thus depicts the result of the intervention with a pair of antonyms: it designates the area prior to the intervention as a "terror corridor", while describing the post-intervention

³⁸ Voltaire Network, 'The Adana Security Agreement', 20 October 1998.

³⁹ United Nations Security Council, 8645th meeting, 25.

⁴⁰ The Aspen Institute, 'SOCOM: Policing the World', 2017.

⁴¹ Sára Gibárti, 'Assisting Syrian refugees in Turkey: International approaches and domestic policies', *Security and Defence Quarterly* 33, no 1 (2021).

⁴² United Nations General Assembly, 'Seventy-fourth session 3rd plenary meeting'.

situation as a “peace corridor”. It is undeniable that since the intervention, the Turkish state has been making great efforts to provide infrastructure, education and health services for the people settled in the “safe zone”.⁴³ Critics, however, claim that through the relocation of the mostly Arab population into the stretch of territory along the Turkish border, Erdoğan also intends to change the ethnic composition of the area, thereby creating an “Arab corridor” between Southeast Turkey and the region controlled by the PYD/YPG.⁴⁴

4. Operation Dawn of Idlib and the Russian discourse of terror

On the 30th of April 2019, the Syrian regime, backed by Russian airpower, has launched a military campaign to recapture the last remaining province in Syria under the control of rebel forces.⁴⁵ The antecedent of the campaign was an agreement between Russia and Turkey, signed in September 2018 in Sochi, which can be considered a diplomatic attempt to uphold the ceasefire in the Idlib de-escalation zone.⁴⁶ The deal prescribed the establishment of a demilitarised zone 15–20 km deep in the de-escalation area from where all radical terrorist groups must be removed within a month, and the restoration of transit traffic on the routes M4 and M5 by the end of 2018. Furthermore, the signatories reiterated their commitment ‘to combat terrorism in Syria in all forms and manifestations’.⁴⁷ As Şaban Kardaş points out, the Sochi Agreement has created a very unstable equilibrium, which constituted a “mission impossible” for Ankara; and justification for the launch of the 2019 offensive for Damascus and Moscow.⁴⁸

The deal has indeed posed a serious dilemma for Turkey: although it had to prevent a Syrian–Russian attack, causing a humanitarian disaster and generating a new wave of refugees towards the Turkish border, it was unwilling to start a military conflict with Hayat Tahrir al-Sham (HTS), which by then has side-lined or subdued other rebel groups, and successfully consolidated itself as a hegemon in Idlib governorate.⁴⁹ HTS is the successor organisation of Jabhat al-Nusra, a group openly aligned with Al-Qaida. In July 2016, it changed its name to Jabhat Fatha al-Sham, thereby signalling that its ties with Al-Qaida have been broken. In January 2017, when Jabhat Fatha al-Sham merged with several smaller groups, HTS was established, whose leaders officially

⁴³ Carlotta Gall, ‘In Turkey’s Safe Zone in Syria, Security and Misery Go Hand in Hand’, *The New York Times*, 16 February 2021.

⁴⁴ Fehim Tastekin, ‘Turkey’s occupation of northern Syria includes population transfers’, *Al-Monitor*, 07 May 2020.

⁴⁵ Vivian Yee and Hwaida Saad, ‘Syrian Government Starts Campaign to Retake Last Opposition Stronghold of Idlib’, *The New York Times*, 20 May 2019.

⁴⁶ In the framework of the Astana process, launched by Russia, Iran and Turkey in January 2017, four de-escalation zones have been established in Syria. By 2018, Idlib was the last remaining zone, as the other three had been captured by the Assad regime.

⁴⁷ Feridun H Sinirlioğlu and Vassily Nebenzia, *Letter dated 18 September 2018 from the Permanent Representatives of the Russian Federation and Turkey to the United Nations addressed to the President of the Security Council* (United Nations Digital Library, 2018), 2.

⁴⁸ Şaban Kardaş, ‘Turkey’s Mission Impossible in Sustaining Idlib’s Unstable Equilibrium’, *German Marshall Fund of the United States*, 09 April 2020.

⁴⁹ International Crisis Group, ‘In Syria’s Idlib, Washington’s Chance to Reimagine Counter-terrorism’, 03 February 2021.

declared that they have cut all the connections with the formal ally, and gave up on the international jihadist agenda.⁵⁰ Unsurprisingly, Syria and Russia did not affirm this, and designated HTS as a terrorist organisation. According to their narrative, Turkey could have fulfilled its obligations only if it had separated HTS from moderate groups and taken military action against the former.⁵¹ For Ankara, however, it was clear that HTS was already too entrenched in Idlib to be defeated without suffering mass casualties.⁵² Having no better options, Turkey thus started to cooperate with the group on pragmatic grounds, while officially including the group on its list of terrorist organisations.⁵³

Turkey's inaction regarding HTS and the continuous attacks by various radical groups against Russian military assets at the Hmeimim airbase constituted a narrative basis for Moscow and the Assad regime to launch military campaigns – first Operation Dawn of Idlib in April 2019, then Operation Dawn of Idlib 2 in December 2019 – to retake Idlib governorate and the surrounding area in Northwest Syria. According to Human Rights Watch, the attacks carried out by the Russian–Syrian alliance during the period from April 2019 to March 2020 have killed at least 1,600 civilians, destroyed or damaged schools, markets and medical facilities, and forced approximately 1.4 million people to leave their homes.⁵⁴ This is reinforced by a report conducted by the United Nations Human Rights Council, which claims that based on the available evidence it is reasonable to believe that Russian aircraft have participated in attacks deliberately and systematically targeting civilian areas in order to depopulate the zone, and accelerate its capture.⁵⁵ During spring 2019, the Syrian–Russian forces first advanced eastward on villages and towns in northern Hama, followed by a westward push in August, resulting in the capture of the strategically important town of Khan Sheikhoun on the M5 highway.

With the support of Russian airpower, regime forces intensified the campaign in December and proceeded towards the city of Idlib. In January 2020, Turkey responded with the deployment of 9,000 additional soldiers to observation points in the area, which raised the conflict to a new level and increased the risk of direct Turkish–Russian confrontation.⁵⁶ On 27 February, a most probably Russian airstrike has killed 34 Turkish soldiers. To avoid the escalation with Moscow, Ankara chose to blame the Syrian regime and upgraded its military presence in the area into a self-standing operation targeting regime troops.⁵⁷ The unfolding violence was halted on 5 March, when an additional protocol to the 2018 Sochi Agreement was signed by President Putin and President Erdoğan, which ceased military actions along the actual

⁵⁰ International Crisis Group, 'Silencing the Guns in Syria's Idlib', 14 May 2020.

⁵¹ Ekaterina Stepanova, 'Russia's Foreign and Security Policy in the Middle East: Entering the 2020s', *Istituto Affari Internazionali*, 2020.

⁵² International Crisis Group, 'In Syria's Idlib'.

⁵³ Ercan Çitlioğlu, 'A Turkish Perspective on Syria', *Konrad Adenauer Stiftung*, 27 October 2020.

⁵⁴ Human Rights Watch, 'Targeting Life in Idlib', 15 October 2020.

⁵⁵ United Nations Human Rights Council, 'Rampant human rights violations and war crimes as war-torn Idlib faces the pandemic UN Syria Commission of Inquiry report', 07 July 2020.

⁵⁶ Stepanova, 'Russia's Foreign'.

⁵⁷ Kardaş, 'Turkey's Mission Impossible'.

line of contact; and prescribed the establishment of a security corridor on both sides of the M4 highway, monitored by joint Turkish–Russian patrols.⁵⁸

4.1. *The Russian discourse of terror*

Given the high number of civilian casualties, it is worth examining how Russia justified its active participation in the offensive. Based on the analysis of relevant speeches and articles given or written by high-ranking diplomats, three main recurring arguments can be identified in the Russian discourse. The first one is designating the West as a single entity, deliberately blocking the peace process by supporting and “whitewashing” terrorists in Idlib. According to the discourse, Moscow is committed to the political solution of the Syrian crisis, nevertheless believes that the precondition of the successful negotiations is the eradication of the last remaining terrorist stronghold in the country. Thus, the most pressing task is to fulfil the 2018 Sochi Agreement, which prescribes the separation of moderate opposition from terrorist forces.⁵⁹ The greatest obstacle to these efforts, Russian diplomats claim, is that “Western colleagues” are still pursuing the goal of regime change; therefore, they are providing support to the enemies of the regime regardless of their extremist agenda, and taking steps to rebrand a terrorist organisation, namely HTS, as a legitimate actor. This was put forward for instance by Vassily Nebenzia, the permanent representative of Russia in the UN: “As the Syrian Government forces move closer to the strongholds of the terrorists, [...] we increasingly hear that Hayat Tahrir Al-Sham has allegedly become an emancipated responsible structure, a kind of civilian administration that is striving to allow people to live peacefully in those areas.”⁶⁰

The argument was used by Nebenzia to justify the Russian decision to veto a draft resolution submitted by Germany, Belgium and Kuwait, which called upon all parties, in particular the Syrian regime, to immediately cease hostilities and undertake confidence-building measures. Although the document emphasised the importance of combating terrorism, Nebenzia claimed that the real objective of the draft was “to save the international terrorists who are entrenched in Idlib from their final defeat”.⁶¹ The Russian portrayal of the West is unquestionably a manipulative generalisation, it is, however, not entirely baseless. Although the United States designates HTS as a terrorist organisation and an “Entity of Particular Concern”,⁶² some prominent figures in American diplomatic circles are indeed suggesting a more flexible U.S. policy towards the group. In an interview in March 2021, former ambassador and former Special Presidential Envoy James Jeffrey for instance said that HTS could be

⁵⁸ Ministry of Foreign Affairs of the Russian Federation, ‘Additional Protocol to the Memorandum on Stabilization of the Situation in the Idlib De-Escalation Area’, 06 March 2020.

⁵⁹ Ministry of Foreign Affairs of the Russian Federation, ‘Foreign Minister Sergey Lavrov’s answers to media questions following the 56th Munich Security Conference, Munich, February 17, 2020’, 17 February 2020.

⁶⁰ United Nations Security Council, 8623rd meeting (United Nations Digital Library, 2019), 3.

⁶¹ *Ibid.* 2.

⁶² Sultan Al-Kanji, ‘Despite attempt at makeover, Syria’s HTS remains on US terror list’, *Al-Monitor*, 21 December 2020.

an asset for U.S. strategy, and claimed that “[t]hey are the least bad option of the various options in Idlib”.⁶³

The second key element of the discourse is portraying Russia as a benign power committed to international law, and associating those who question this narrative with terrorism. According to the Russian diplomatic communication, Moscow did everything to “prevent violence and resolve the situations peacefully”;⁶⁴ because of the terrorist activities of HTS, however, it had no other options besides launching an offensive on Idlib. On several occasions, Nebenzia emphasised that while conducting attacks, Russia always acts according to the norms of international law, and uses precision airstrikes to avoid civilian casualties.⁶⁵ This self-designation is complemented by the framing of HTS as a group of terrorists, bandits and hostage-takers; which implies that it is illegally occupying a territory of the Syrian state and causing suffering to the civilians under its rule.⁶⁶ The discourse thus depicts Operation Dawn of Idlib as a humanitarian intervention aiming to liberate the terrorists’ civilian hostages.

Russian accusations against HTS have a basis. According to the United Nations Human Rights Council, the group escalated attacks on government-controlled areas causing civilian casualties; recruited and used children to participate in hostilities; and persecuted activists and media workers critical of its activity.⁶⁷ What the Russian narrative “forgets” to add, however, is that nearly half of the population in Idlib consists of internally displaced persons, who were inclined to flee there by their fear of the regime. Given the centrality of international law in the discourse, it is not surprising that those who question or disprove the Russian narrative have become the targets of disinformation campaigns. One of the prime subjects of these campaigns is the White Helmets, a group of rescue workers attempting to save victims of military strikes while documenting the consequences of the attacks. After the group had publicised video footage and documentary evidence of war crimes committed by Russian and Syrian forces, Russian propagandists responded by associating the members of the White Helmets with terrorist organisations and accusing them of faking attacks to besmirch Russia’s reputation.⁶⁸ Although the main platform of the campaign is social media, high-ranking diplomats have also accused the group of terrorism-related activities. Nebenzia for instance claimed that the group is “working with Al-Nusra Front, and [...] preparing acts of provocation using chemicals”.⁶⁹

The third element, which places the Russian narrative in a wider context, is portraying the Syrian conflict with the antonyms of order and chaos. The argument is embedded in the Russian discourse on the post-bipolar world order, which emphasises the growing tension between liberal interventionism, and the traditional Westphalian approach to state sovereignty. In his 2019 speech at the General Assembly of the

⁶³ Priyanka Boghani, ‘Syrian Militant and Former Al Qaeda Leader Seeks Wider Acceptance in First Interview With U.S. Journalist’, *Frontline*, 02 April 2021.

⁶⁴ United Nations Security Council, 8527th meeting (United Nations Digital Library, 2019).

⁶⁵ *Ibid.*

⁶⁶ United Nations Security Council, ‘8623rd meeting’.

⁶⁷ United Nations Human Rights Council, ‘Rampant human rights violations’.

⁶⁸ Matthew Levinger, ‘Master Narratives of Disinformation Campaigns’, *Columbia Journal of International Affairs* 71, no 1.5 (2018), 125–134.

⁶⁹ United Nations Security Council, 8553rd meeting (United Nations Digital Library, 2019), 15.

United Nations, Foreign Minister Sergey Lavrov said that Western nations are making desperate attempts to “prevent the establishment of a polycentric world, restore their positions of privilege and impose standards of conduct on everyone else based on their own narrow interpretation of liberalism”.⁷⁰ In another speech, given at the Valdai International Discussion Club, Lavrov claimed that the geographical distance between the United States and the Middle East enables Washington to pursue its geopolitical and geo-economic interests by conducting interventions, overthrowing regimes, and creating safe havens for terrorists.⁷¹ Russia on the other hand is directly impacted by the Middle Eastern turmoil, not only because of the strategic partnerships between Moscow and Damascus, but also because of the spread of Islamic radicalism, which can potentially revive separatist and extremist tendencies in the North Caucasus, and thus poses a threat to the territorial integrity of the Russian state. Accordingly, Moscow’s discourse claims that the Western emphasis on human rights and liberal values is merely a cover-up for the real intention of the West: to destabilise the region and undermine Russia’s geopolitical position.⁷²

As both the U.S. invasion of Iraq in 2003 and NATO’s Libyan intervention in 2011 had negative impacts on regional stability and contributed to the emergence and expansion of Jihadist factions, the argument has a solid basis – by pointing at the devastating consequences of Western adventurism, Russian diplomats can effectively demonstrate, who is the real “agent of chaos” in the Middle East. According to Moscow’s dichotomy-based narrative, the only alternative to liberal interventionism is the concept of *sovereign democracy*, created by former Kremlin ideologue Vladislav Surkov as a response to the “colour revolutions” of the post-soviet periphery. As Richard Sakwa points out, the concept has a binary meaning. Internationally, it demands autonomy and independence for individual states vis à vis Western hegemony; calls for a more democratic, polycentric world order; and argues for the right of every nation to a democratic development process that is compatible with its specific traditions and political culture. Domestically, however, it prioritises political and social stability over the rights of the individual, thereby rationalising the technocratic suppression of competitive and pluralistic politics.⁷³ Consequently, the discursive application of the concept has two implications regarding Syria. On the one hand, it denies the International Community’s right to question Assad’s legitimacy, which in practice manifests in the Russian vetoes of Security Council resolutions targeting the regime. On the other hand, the discourse justifies the regime’s efforts to restore its sovereignty over the entire territory of the country regardless of the brutality of the measures it is using, which in practice manifests in the active participation of the Russian army in Operation Dawn of Idlib.

⁷⁰ United Nations General Assembly, Seventy-fourth session 9th plenary meeting (United Nations Digital Library, 2019).

⁷¹ Ministry of Foreign Affairs of the Russian Federation, ‘Foreign Minister Sergey Lavrov’s remarks and answers to questions during the Valdai International Discussion Club’s panel on Russia’s policy in the Middle East, Sochi, October 2, 2019’, 02 October 2019.

⁷² Hannah Notte, ‘Russia in Syria: Domestic Drivers and Regional Implications’, *Konrad Adenauer Stiftung*, January 2017.

⁷³ Richard Sakwa, ‘Sovereignty and Democracy: Constructions and Contradictions in Russia and Beyond’, *Region: Regional Studies of Russia, Eastern Europe and Central Asia* 1, no 1 (2012), 3–27.

5. Conclusion

If we compare the Turkish and Russian discourses, we can find many similar or even identical elements. Both accuse the United States of supporting terrorism, claim that the precondition of a successful political peace process is the elimination of terrorists, stress that no differentiation can be made between good and bad terrorists, and underline the importance of preserving Syria's territorial integrity. It is also remarkable that despite the differences between their geostrategic interests, both Ankara and Moscow emphasise the potentiality of Turkish–Russian cooperation. In the period examined by this paper, diplomatic efforts have resulted in two agreements, creating a situation in northern Syria that is – at the moment – acceptable for both sides. The aforementioned similarities, the relatively friendly-toned communication towards each other, and the diplomatic achievements, however, do not resolve the sharp contradiction between the Turkish and Russian terror discourses.

In Idlib governorate, the central question concerns the status of HTS – an Islamist organisation aiming to prove that it has left its Jihadist past behind and become a moderate rebel group. For Turkey, the priority regarding Idlib is to maintain the status quo by preventing a new Syrian–Russian offensive, which would further aggravate the humanitarian crisis in the area, and launch a new wave of refugees towards the Turkish borders. This motivates Ankara's pragmatic cooperation with HTS and explains the Turkish discourse which emphasises that “the killing of civilians under the pretext of fighting against terrorism cannot be accepted”.⁷⁴ Consequently, the best-case scenario for Ankara would be the one in which Russia recognises HTS as a moderate rebel group that can be involved in the negotiations. This scenario, however, seems highly unlikely. In northern Syria, Russia is carefully balancing between two conflicting goals: on the one hand, Moscow supports the regime's efforts to retake the entire territory of Syria; on the other, it tries to maintain its fragile partnership with Turkey. The latter is important for Russia not only economically, but also strategically, as it is interested in deepening the internal fractures within the Euro-Atlantic Alliance – this explains the Russian discourse which unequivocally detaches Turkey from the West, using a friendlier tone with the former while harshly criticising the latter.

The text of the 2018 Sochi Agreement already reflected the Russian balancing, as the document contains two contradictory instructions, which were reaffirmed in the 2020 additional protocol: to take all necessary measures to maintain the existing status quo; and to combat terrorism in all forms and manifestations.⁷⁵ Because of the now fortified presence of the Turkish Armed Forces in Idlib, and not least because of Russia's interest in sustaining the partnership with Turkey, the status quo seems stable in the short- and perhaps medium-term. In the long-term, however, Moscow will probably support the regime's efforts to retake the region, and the fact that HTS is still on the UN Security Council's list of terrorist organisations may provide the narrative basis for a new offensive. In other words, the 2018 and 2020 agreements

⁷⁴ United Nations Security Council, ‘8645th meeting’.

⁷⁵ Sinirliođlu and Nebenzia, *Letter dated 18 September 2018*.

between Moscow and Ankara have only frozen the conflict, without tackling the deep-seated contradiction between their narratives.

The situation in north-eastern Syria is no less complicated. Regarding the PYD/YPG, the roles played by Turkey and Russia are reversed compared to the attitudes towards HTS. Ankara designates the Kurdish group as a terrorist organisation, and vehemently opposes its inclusion in the peace process. Moscow on the other hand does not identify it as a terrorist group and cooperates with it on a pragmatic basis. Accordingly, Russian diplomats have not hidden their displeasure with Operation Peace Spring. Shortly after the intervention had ended, UN envoy Nebenzia stated that the “illegal occupation and the dangerous experiment in demographic engineering” in north-eastern Syria has destabilised the region, which necessitates a dialogue between Syrian Kurds and the regime.⁷⁶ This indicates that a central element of the scenario pushed by Moscow is a deal between Assad and the PYD, which grants the regime sovereignty over the Kurdish territories while providing some form of regional autonomy for the Kurds.

For Ankara, however, it is a strategic priority, and because of the nationalist sentiments at home, it is also a domestic political goal to hinder any form of Kurdish autonomy in Syria, especially if that means that the region is de facto governed by the PYD/YPG. The October 22 Sochi Agreement, similarly to the documents on Idlib, did not tackle the obvious contradiction between Russian and Turkish discourses. It emphasised the parties’ “determination to combat terrorism in all forms and manifestations”,⁷⁷ it did not, however, specify whether the PYD/YPG should be considered a terrorist organisation. It has not cleared the air either that the memorandum reaffirmed the importance of the Adana Agreement, as the two sides interpret the relevance of the 1998 document differently. Ankara considers it a legal justification for the Turkish presence in Syria. For Russia, however, working in the framework of the agreement means that the legitimacy of the regime in Damascus must be recognised by Turkey. Although the existing status quo seems relatively stable, it reasonably concerns Ankara, that the 22 October memorandum provided the opportunity for Moscow to put pressure on Turkey by playing the “Kurdish card”.

We can conclude that the discursive practices used by the Turkish and Russian Governments regarding the northern Syrian conflicts clearly demonstrate, why the efficiency of a positivist, definition-based approach is questionable, to say the least. Both Turkey and Russia define the notion of terrorism according to their (geo) political interests and are using the terrorist label to de-legitimise the actors they perceive as threats to their strategic priorities. In practice, this inevitably results in the meaninglessness of the provisions emphasising their commitment to fighting terrorism in all forms and manifestations. The two terror discourses show several similarities, furthermore, through their diplomatic efforts Moscow and Ankara were able to create a status quo that at the moment seems stable. These factors, however, do not resolve the central collision point between Turkish and Russian narratives on northern Syria, namely, that the two governments define oppositely, who is and

⁷⁶ United Nations Security Council, ‘8645th meeting’.

⁷⁷ President of Russia, ‘Memorandum of Understanding’.

who is not a terrorist in the region. As long as this interest-driven contradiction is not tackled, the potentiality of recurring conflict remains high.

References

- Aktürk, Şener, 'Turkey's Operation Peace Spring and the Battle for a Free Syria'. *TRT World Research Centre*, 09 December 2019.
- Al-Kanj, Sultan, 'Despite attempt at makeover, Syria's HTS remains on US terror list'. *Al-Monitor*, 21 December 2020.
- Al-Khateb, Khaleb, 'Hayat Tahrir al-Sham intensifies campaign against al-Qaeda affiliate in Idlib'. *Al-Monitor*, 25 February 2021.
- Amnesty International, 'Syria: Damning evidence of war crimes and other violations by Turkish forces and their allies', 18 October 2019.
- Barrinha, André, 'The political importance of labelling: terrorism and Turkey's discourse on the PKK'. *Critical Studies on Terrorism* 4, no 2 (2011), 163–180. Online: <https://doi.org/10.1080/17539153.2011.586203>
- Boghani, Priyanka, 'Syrian Militant and Former Al Qaeda Leader Seeks Wider Acceptance in First Interview With U.S. Journalist'. *Frontline*, 02 April 2021.
- Buzan, Barry, 'Rethinking Security after the Cold War'. *Cooperation and Conflict* 32, no 1 (1997), 5–28. Online: <https://doi.org/10.1177/0010836797032001001>
- Çavuşoğlu, Mevlüt, 'Why Turkey Took the Fight to Syria'. *The New York Times*, 11 October 2019.
- Çavuşoğlu, Mevlüt, 'Demystifying Turkey's Operation Peace Spring'. *TRT World Forum*, 12 November 2019.
- Çitlioğlu, Ercan, 'A Turkish Perspective on Syria'. *Konrad Adenauer Stiftung*, 27 October 2020.
- Council of the European Union, 'Declaration by the High Representative on behalf of the EU on recent developments in north-east Syria', 2019.
- Daily Sabah, 'US weapons given to PYD used by PKK in attacks in Turkey', 28 April 2017.
- Dixit, Priya, 'Securitization and Terroristization: Analyzing States' Usage of the Rhetoric of Terrorism', in *State Terror, State Violence: Global Perspectives*, ed. by Bettina Koch. Wiesbaden: Springer VS, 2016. Online: https://doi.org/10.1007/978-3-658-11181-6_3
- Edmondson, Catie, 'In Bipartisan Rebuke, House Majority Condemns Trump for Syria Withdrawal'. *The New York Times*, 16 October 2019.
- Egeresi, Zoltán, 'Törökország konfliktusa az észak-szíriai kurdokkal'. *KKI-Elemzések* E-2020/11.
- Gall, Carlotta, 'In Turkey's Safe Zone in Syria, Security and Misery Go Hand in Hand'. *The New York Times*, 16 February 2021.
- Ganor, Boaz, 'Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter?' *Police Practice and Research: An International Journal* 3, no 4 (2002), 287-304. Online: <https://doi.org/10.1080/1561426022000032060>

- Gibárti, Sára, 'Assisting Syrian refugees in Turkey: International approaches and domestic policies'. *Security and Defence Quarterly* 33, no 1 (2021). Online: <https://doi.org/10.35467/sdq/132027>
- Glied, Viktor, 'Migrációs diskurzus a poszt-multikulturális Európában'. *Pólusok* 1, no 1 (2020). Online: <https://doi.org/10.15170/PSK.2020.01.01.02>
- Human Rights Watch, 'Under Kurdish Rule: Abuses in PYD-run Enclaves of Syria', 18 June 2014.
- Human Rights Watch, 'Targeting Life in Idlib', 15 October 2020.
- International Crisis Group, 'The PKK's Fateful Choice in Northern Syria', 04 May 2017.
- International Crisis Group, 'Silencing the Guns in Syria's Idlib', 14 May 2020.
- International Crisis Group, 'In Syria's Idlib, Washington's Chance to Reimagine Counter-terrorism', 03 February 2021.
- Jackson, Richard, 'Knowledge, Power and Politics in the Study of Political Terrorism', in *Critical Terrorism Studies: A New Research Agenda*, ed. by Richard Jackson, Marie Breen Smyth and Jeroen Gunning. Abingdon: Routledge, 2009, 66–83. Online: <https://doi.org/10.4324/9780203880227>
- Kardaş, Şaban, 'Turkey's Mission Impossible in Sustaining Idlib's Unstable Equilibrium'. *German Marshall Fund of the United States*, 09 April 2020.
- Kaya, Zeynep and Robert Lowe, 'The Curious Question of the PYD–PKK Relationship', in *The Kurdish Question Revisited*, ed. by Mohammed Shareef and Gareth R V Stansfield. London: Hurst & Company, 2017.
- Levinger, Matthew, 'Master Narratives of Disinformation Campaigns'. *Columbia Journal of International Affairs* 71, no 1.5 (2018), 125–134.
- Manzinger, Krisztián and Péter Wagner, 'Syrian Kurds, Rojava and Alternative Society Building in Middle East'. *Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata* 148, no 1 (2020), 15–40. Online: <https://doi.org/10.35926/HDR.2020.1.2>
- Ministry of Foreign Affairs of the Russian Federation, 'Foreign Minister Sergey Lavrov's remarks and answers to questions during the Valdai International Discussion Club's panel on Russia's policy in the Middle East, Sochi, October 2, 2019', 02 October 2019.
- Ministry of Foreign Affairs of the Russian Federation, 'Foreign Minister Sergey Lavrov's answers to media questions following the 56th Munich Security Conference, Munich, February 17, 2020', 17 February 2020.
- Ministry of Foreign Affairs of the Russian Federation, 'Additional Protocol to the Memorandum on Stabilization of the Situation in the Idlib De-Escalation Area', 06 March 2020.
- Notte, Hannah, 'Russia in Syria: Domestic Drivers and Regional Implications'. *Konrad Adenauer Stiftung*, January 2017.
- President of Russia, 'Memorandum of Understanding Between Turkey and the Russian Federation', 22 October 2019.
- Reuters, 'Turkey's Syria offensive an 'invasion': Arab League secretary general', 12 October 2019.
- Sakwa, Richard, 'Sovereignty and Democracy: Constructions and Contradictions in Russia and Beyond'. *Region: Regional Studies of Russia, Eastern Europe and Central Asia* 1, no 1 (2012), 3–27. Online: <https://doi.org/10.1353/reg.2012.0004>

- Savran, Arin, 'The Peace Process between Turkey and the Kurdistan Workers' Party, 2009–2015'. *Journal of Balkan and Near Eastern Studies* 22, no 6 (2020). Online: <https://doi.org/10.1080/19448953.2020.1801243>
- Schmid, Alex, 'Terrorism – The Definitional Problem'. *Case Western Reserve Journal of International Law* 36, no 2 (2004), 379–380.
- Sinirlioğlu, Feridun H, Letter dated 9 October 2019 from the Permanent Representative of Turkey to the United Nations addressed to the President of the Security Council. United Nations Digital Library, 2019.
- Sinirlioğlu, Feridun H and Vassily Nebenzia, Letter dated 18 September 2018 from the Permanent Representatives of the Russian Federation and Turkey to the United Nations addressed to the President of the Security Council. United Nations Digital Library, 2018.
- Staun, Jørgen, 'When, how and why elites frame terrorists: a Wittgensteinian analysis of terror and radicalisation'. *Critical Studies on Terrorism* 3, no 3 (2010), 403–420. Online: <https://doi.org/10.1080/17539153.2010.521642>
- Stepanova, Ekaterina, 'Russia's Foreign and Security Policy in the Middle East: Entering the 2020s'. *Istituto Affari Internazionali*, 2020.
- Tastekin, Fehim, 'Turkey's occupation of northern Syria includes population transfers'. *Al-Monitor*, 07 May 2020.
- The Aspen Institute, 'SOCOM: Policing the World', 2017.
- United Nations High Commissioner for Refugees, *Syria Factsheet (January–November 2018) Situation Report*, 2018.
- United Nations General Assembly, *Seventy-fourth session 3rd plenary meeting*. United Nations Digital Library, 2019.
- United Nations General Assembly, *Seventy-fourth session 9th plenary meeting*. United Nations Digital Library, 2019.
- United Nations Human Rights Council, 'Rampant human rights violations and war crimes as war-torn Idlib faces the pandemic UN Syria Commission of Inquiry report', 07 July 2020.
- United Nations Security Council, *8645th meeting*. United Nations Digital Library, 2019.
- United Nations Security Council, *8623rd meeting*. United Nations Digital Library, 2019.
- United Nations Security Council, *8527th meeting*. United Nations Digital Library, 2019.
- United Nations Security Council, *8553rd meeting*. United Nations Digital Library, 2019.
- Uras, Umut, 'Turkey's Operation Peace Spring in northern Syria: One month on'. *Aljazeera*, 08 November 2019.
- Ünver, H Akın, *Schrödinger's Kurds: Transnational Kurdish Geopolitics in the Age of Shifting Borders*. *Columbia Journal of International Affairs* 69, no 2 (2016), 65–98.
- Voltaire Network, 'The Adana Security Agreement', 20 October 1998.
- Vultee, Fred, 'Securitization: A new approach to the framing of the "war on terror"'. *Journalism Practice* 4, no 1 (2010), 33–47. Online: <https://doi.org/10.1080/17512780903172049>
- Wæver, Ole, 'Security, the Speech Act: Analysing the Politics of a Word'. *Working Paper* no 19. Copenhagen Peace Research Institute, 1989.

- Wæver, Ole, 'Securitization and Desecuritization', in *On Security*, ed. by Ronnie D Lipschutz. New York: Columbia University Press, 1995.
- Wæver, Ole, 'Politics, security, theory'. *Security Dialogue* 42, no 4–5 (2011), 465–480. Online: <https://doi.org/10.1177/0967010611418718>
- Yee, Vivian and Hwaida Saad, 'Syrian Government Starts Campaign to Retake Last Opposition Stronghold of Idlib'. *The New York Times*, 20 May 2019.

Eck Gábor¹

A terrorizmus és az információs tér kapcsolódási pontjai

Links between Terrorism and the Information Space

A digitális kultúra, a mobileszközök és a közösségi média nélkülözhetetlen részévé vált az életünknek. A legfrissebb felmérések szerint a Föld népességének 60 %-a használja az internetet, így a közösségi média alkalmazóinak száma meghaladja a 3,8 milliárdot. Egy átlagos internetező naponta közel 6 óra 45 percet tölt el a világhálón, ebből közel 2 óra 30 percet közösségi média használatával. Ezek a számok folyamatosan emelkedő tendenciát mutatnak. A világ népességének jelentős része elérhető a virtuális térben, ezért érdemes megvizsgálni, hogy a terrorizmus és az abban érintett személyek hogyan viszonyulnak a digitalizáció nyújtotta lehetőségekhez, és ez milyen kihívások elé állítja a biztonságért felelős szerveket.

Kulcsszavak: internet, közösségi média, biztonság, terrorizmus

The digital culture, the use of cellular devices and the use of the social media have become an essential part of our lives. According to the latest surveys, 60 percent of the world's population uses the Internet, which means that there are more than 3.8 billion social media users. The average internet users spend nearly 6 hours and 45 minutes a day on the web, including nearly 2 hours and 30 minutes using social media. These figures show an upwarding trend. A significant part of the world's population is available in the cyberspace, so it is worth to see how terrorism and people affected by this phenomenon react to the potential of digitalisation and what kind of new challenges security bodies face.

Keywords: internet, social media, security, terrorism

¹ Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: eck.gabor@icloud.com

1. Bevezetés

Manapság olyan világban élünk, amelyben a számítógépek, az okoseszközök és a rajtuk keresztül elérhető hálózatok aktív és nem elkerülhető részei mindennapjainknak, segítik, támogatják szervezik azt, ám ha nem figyelünk kellően oda, irányíthatják is tevékenységünket.² Természetesen e technikai vívmányok tudatos használatával kényelmesebben tarthatunk lépést felgyorsult világunkkal. Minél jobban átszövi életünket a technika, annál inkább megjelennek biztonsági kérdések is a használattal, valamint a felhasználókkal kapcsolatban, hiszen minden új, az életünk részét képező dolognak vannak árnyoldalai, „alternatív felhasználási” lehetőségei.

Tanulmányomban rá kívánok világítani a terrorizmus elleni küzdelem és az információ tér, valamint az ott használt eszközök kölcsönhatásaira, be kívánom mutatni a terrrorszervezetek internetes törekvéseit, az azokhoz kapcsolódó fenyegetéseket és kihívásokat.

Célom, hogy a fogalmi meghatározások tisztázása, a terrorizmus kibertérben zajló mozzanatainak bemutatása és az azokra adható válaszok révén élesem a képet az online világban tapasztalható biztonsági kihívásokról.

2. Terrorizmus – kiberterrorizmus

A terrorizmus meghatározásával kapcsolatban sok álláspont született, de nemzetközileg elfogadott terminust nem sikerül még alkotni. Érdemes a teljesség igénye nélkül néhány definíciót ismertetni.

Benjamin Netanjahu szerint: „A terrorizmus a polgárokon gyakorolt szándékos, módszeres erőszak, amely az általa kiváltott félelmen keresztül politikai célokat kíván megvalósítani.”³

A NATO által használt definíció szerint a terrorizmus „[e]rőszak jogellenes alkalmazása, vagy azzal való fenyegetés, amely félelmet vagy rettegést kelt, egyének vagy tulajdon ellen, kormányok vagy társadalmak kényszerítésére vagy megfélemlítésére, vagy a lakosság feletti ellenőrzés megszerzésére, politikai, vallási vagy ideológiai célok elérésére”.⁴

Korinek László meghatározásában:

„A terrorizmus eltérő eszmerendszerekből merítő, sajátos logikának engedelmeskedő, változatos formákat öltő módszeres erőszak alkalmazása, vagy ezzel való fenyegetés, melynek célja politikai törekvések elérése azáltal, hogy az áldozatban, a nézőközönségben, az államban, a társadalomban megalkuvó magatartás alakuljon ki. A meghirdetett cél általában politikai, ideológiai, vallási, etnikai tartalmú radikális változás kikényszerítése, a cél elérésére alkalmazott

² Vö. *Global Digital Overview. Digital in 2020.*

³ Benjamin Netanjahu: *Harc a terrorizmus ellen.* Pécs, Alexandra, 1995. 20.

⁴ Nato Unclassified: MC 0472/1 Military Committee Concept For Counter-Terrorism.

cselekménysor. Az eszköz viszont jogi lényegét tekintve köztörvényes, erőszakos bűncselekmény.”⁵

Resperger István úgy véli: „A terrorizmus terroristák (egyének vagy csoportok) által, politikai célok elérése érdekében, főként a polgári lakosságon, erőszakos eszközökkel folytatott tevékenység, abból a célból, hogy akaratukat az ellenfélre kényszerítsék.”⁶

A fogalom vizsgálata során joggal merül fel a kérdés, hogy a virtuális téren keresztül hogyan lehetséges erőszakot alkalmazni, vagy azzal olyan módon fenyegetni, hogy az alkalmas legyen a kitűzött célok elérésére. Az elmúlt évek terrortámadásai megismertették velünk a félelemnek azon szegmenseit, amelyek képesek a tőlünk nagyobb távolságra lévő borzalmakat is érezhetővé tenni. Egy bekövetkezett támadás híre szinte azonnal eljut a világ bármelyik részére, a helyszínen tartózkodó emberek élő, egyenes adásban közvetítik a történéseket, így a technika segítségével jóformán a saját bőrünkön érezzük a következményeket, az események részeseivé válunk. Érdemes elgondolkodni azon, hogy a mindenáron érvényesülő közléskényszerünk, a rettenet ilyen módon való transzportálása mennyire segíti a terroristákat céljaik elérésében, gondolok itt a megfélemlítésre, kényszerítésre, valamint az irányítás átvételére. Bruce Schneier amerikai biztonsági szakértő szerint a terrorizmus valódi lényege nem maga a cselekmény, hanem az arra adott reakció.”⁷

Természetesen a terroristák számára nem csak a korábban említett közvetett módon érhető el az információs tér nyújtotta potenciál, annak pozitívumait aktívan is használják céljaik megvalósítása érdekében. Ezen a ponton elkerülhetetlen egy újabb fogalom, a kiberterrorizmus definíciójának a vizsgálata. A terrorizmushoz hasonlóan a kiberterrorizmusnak sincs egy egységesen elfogadott és kiforrott meghatározása. A téma szakértői egyetértenek abban, hogy a terrorizmus és a kibertér fogalmaiból kell kiindulni, és azokat ötvözve lehet legközelebb jutni a keresett értelmezéshez.

A terrorizmus fentebb említett fogalmát tehát ki kell egészítenünk a kibertér fogalmával, ami egy újabb komoly kihívás, hiszen minden terület a saját maga számára jelentős tényezőket emeli ki. Munk Sándor ebből a gondolatból kiindulva a következőket mondja: „egyes alkalmazás- vagy szakterületek a kérdések megválaszolásával (ha eddig nem tették volna meg) maguk és mások számára is pontosabban meg tudják határozni kibertér-értelmezésük részletes tartalmát, illetve, hogy a különböző értelmezések összehasonlíthatók, eltéréseik feltárhatók”.⁸ Ettől függetlenül szükséges egy olyan fogalmi meghatározás, amely felülemelkedik a fenti problémán, és ad egy általános, mindenki számára elfogható definíciót. Haig Zsolt és Kovács László álláspontja szerint a kibertér az elektronikus kommunikációs technológiák, valamint az azokon megtalálható szolgáltatások és információk, adatok alkotta virtuális tér.⁹

⁵ Gönczöl Katalin et al.: *Kriminológia – Szakkriminológia*. Budapest, CompLex, 2006. 447.

⁶ Resperger István: A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In Resperger István (szerk.): *A nemzetbiztonság elmélete a közszolgálatban*. Budapest, Dialóg Campus, 2018. 76.

⁷ Bruce Schneier: *A biztonsággról*. Budapest, HVG, 2010. 16.

⁸ Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Haditechnika*, (2018), 1. 114.

⁹ Haig Zsolt – Kovács László: Fenyegetések a cybertérből. *Nemzet és Biztonság*, 1. (2008), 5. 61–69.

Dorothy E. Denning amerikai információbiztonsági kutató a kiberterrorizmusra mint a terrorizmus és a kibertér fúziójára tekint. Véleménye szerint azokat a számítógépek, hálózatok és az azokban tárolt információk elleni jogellenes támadásokat és támadásokkal való fenyegetéseket lehet általában kiberterrorizmusnak nevezni, amelyek a kormányzatok vagy azok szervei ellen irányulnak, illetve a politikai vagy társadalmi céljaikkal, érdekeikkel szemben igyekeznek őket valamire kényszeríteni. Ahhoz, hogy a jelenséget vagy a tevékenységet kiberterrorizmusnak minősíthessük, a támadásnak személyekkel vagy vagyonnal szembeni erőszakkal kell járnia, illetve elegendő kárt kell okoznia a félelem kiváltásához.¹⁰

3. Hacker – kiberterrorista – online terrorista

Meg kell vizsgálnunk, hogy a fenti meghatározásokkal összefüggésbe hozható személyek között hogyan lehet különbséget tenni. Ahogyan a valós körülmények között is igen komoly feladatot, elhatárolási problémát jelenthet a felkelőt a terroristától megkülönböztetni,¹¹ ugyanúgy a virtuális térben megjelenő szereplők között is elengedhetetlen az eltérések megállapítása. De kik is ezek a szereplők, van-e közöttük kapcsolat, és ha igen, akkor ennek mik a jellemzői?

Kazári szerint a *hacker* olyan kimagasló számítástechnikai tudású személy, aki szigorúan segítő jelleggel feltárja a számítógépes rendszerek/alkalmazások előnyeit és hibáit, illetőleg javít azokon.¹² A meghatározásból ki kell emelnünk a segítő jelleget, tehát a hackerek a meglévő többlettudásukat a közjó, az internet népének boldogulása szolgálatába állítják. A hackerkultúra nem gazdasági vagy társadalmi formáció, egy valódi hacker szabadelvű, a hierarchikus viszonyokat erősen tagadó, a materiális javak megszerzését figyelmen kívül hagyó entitás, aki megelégszik a többiek figyelmével, elisméréssel, és ezért minden alkotását szabadon hozzáférhetővé teszi.¹³

Természetesen ebben a szubkultúrában is megjelentek, megjelennek olyanok, akik a fenti etikai szemléletet nem vagy nem teljesen gondolják követendőnek, és céljuk az anyagi haszonszerzés vagy egészen egyszerűen csak kellemetlenség, probléma okozása másoknak, illetőleg ezek kombinációja. Ennek a morális határnak az átlépésével sokkal inkább beszélhetünk kiberbűnözőkről, mint a közösséget önérdek nélkül támogató, magas színvonalú specialistákról. Ezek a személyek ideális alanyai lehetnek egy terrorszervezet célkitűzéseit – akár a valódi cél ismerte nélkül – támogató, a virtuális térben a szükséges háttértudást biztosító sejtnek. Elmondhatjuk, hogy kiberterrorista az, aki a speciális számítástechnikai tudásával a valódi célok ismeretével vagy azok tudta nélkül terrortevékenységet támogat. Így a terrorizmus, a kiberterrorizmus és a kiberbűnözés elleni fellépésnek egy közös, bűnüldözői és nemzetbiztonsági szegmensekkel is rendelkező feladatrendszernek kell lennie.

¹⁰ *Statement of Dorothy E. Denning*. Georgetown University, (é. n.).

¹¹ Lásd bővebben: Resperger István: Az aszimmetrikus hadviselés és a terrorizmus jellemzői. *Hadtudomány*, (2010), 4. 74.

¹² Kazári Csaba: *Hacker, cracker, warez. A számítógépes alvilág titkai*. Budapest, Computer Panoráma, 2003. 18.

¹³ Eric S. Raymond: *How To Become A Hacker*.

Természetesen nem szabad megfeledkeznünk arról a kategóriáról sem, amikor a terrorcselekményekhez köthető személyek az informatikai, technikai, infokommunikációs eszközök biztosította lehetőségeket használják célkitűzéseik elérése érdekében. A fenti lehetőségek használata során technikailag nincs különbség a „rendes” (rendeltetésszerű) és a rosszindulatú igénybevétel között. Az ilyen esetekben a külső szemlélő számára teljes az azonosság, és a használatban rejlő anomáliák sok esetben még az alapos adatelemzés során sem, vagy csak részben kimutathatók.

4. Lehetőségek a kibertérben

A fogalmak tisztázását követően érdemes áttekinteni, hogy a terrrorszervezetek szervezői, a terrorcselekmények tervezői, elkövetői mennyire közvetlen módon látják hasznát a kibertérhez kapcsolódó infokommunikációs eszközök és hálózatok által kínált technikai újdonságoknak.

4.1. Toborzás – ideológiaterjesztés – támogatás

Tevékenységük során a terroristák a toborzás, a kapcsolattartás, a támogatások megszerzése és továbbítása (terrorfinanszírozás), valamint az ideológia-terjesztés (indoktrináció) területén is támaszkodhatnak a kibertér által biztosított lehetőségekre. Ezek értelmezhetők úgy is, mint a mindenki számára elérhető és használható technológia fejlődésében rejlő esély, és úgy is, mint egy állandóan változásban lévő és fejlődő területen fellelhető, az átlagos, hétköznapi ember tudását meghaladó, speciális szakértelmet kívánó lehetőségek.

Az új technológiák drámai mértékben megnövelik a terrorizmussal összefüggésbe hozható online tartalmak globális elérhetőségét. A közösségi média lehetővé teszi a terrrorszervezetek, -csoportok számára, hogy propagandájukat terjesszék, és azonnal, költség és nagyobb fáradtság nélkül toborozzanak követőket a világ bármely pontjáról. Néhány évtizeddel ezelőtt az egyéni radikalizációs folyamat személyes kontaktust igényelt, ezt követően a radikális imámok audió-felvételek terjesztésével próbálták minél szélesebb körben terjeszteni tanaikat, Oszáma bin Láden faxot használt vallási rendeleteinek továbbítására.¹⁴

Mára ez megváltozott, a szimpatizánsok nemcsak a terrrorszervezetek által működtetett honlapokon, online magazinokon keresztül – mint például az Iszlám Állam által üzemeltetett Dabiq, Rumiya, Dar al-Islam vagy a Konstantinápoly –, hanem a közösségi média segítségével biztosított csatornákon is iránymutatást kaphatnak az ideológia elsajátítására, a szervezethez történő fizikai csatlakozásra, a támadások kivitelezésére. A közkedvelt közösségimédia-platformok „egy kattintással” lehetőséget biztosítanak felhasználók százezreinek elérésére, vagy akár nagy terjedelmű fényképek, videóanyagok továbbítására is. Az Iszlám Állam (ISIS) nevű terrrorszervezet felismerte a közösségi média erejét és azt, hogy a toborzásuk szempontjából érdekes

¹⁴ Kate Zernike – Michael T. Kaufman: *The Most Wanted Face of Terrorism*.

korosztályú személyek elsősorban ezekről a platformokról tájékozódnak. Az ISIS propagandistái 2015-ben egy hónap alatt 1146 bejegyzést tettek a Twitteren, amelyek között volt fotó, esszé, videó, nyilatkozat, rádiótájékoztató, szöveges összefoglaló; magazinok, plakátok, brossúrák, teológiai értekezések láttak napvilágot, és mindez oroszul, törökül, arabul, kurdul, franciául és angolul egyaránt megjelent.¹⁵

Ez a kiterjesztett világ komoly lehetőséget nyújt azoknak is, akik nem akarnak, mernek valódi, kézzelfogható segítséget nyújtani a terroristák toborzásához, ideológiájuk terjesztéséhez, de helyeslő magatartásukkal, a hirdetett tanokkal való rokonszenvük kimutatásával meghatározó ösztönzői lehetnek a radikalizációs folyamatoknak. Ezzel a tevékenységükkel pótolják a radikalizálódási folyamat érzelmi és pszichológiai részét, erősítve magukban az „egyetlen helyes út” szellemiségét. Sok esetben ebből a szerepkörükből tovább lépve, már közvetítőként funkcionálnak, kapcsolatot biztosítanak a már megnyert, beszerzett személyek és a terroristák között, illetőleg segítséget nyújtanak a terrorcselekmény elkövetőinek a célterületre való bejutáshoz, az ott-tartózkodáshoz és rejtőzködéshez. Természetesen a segítségnyújtás, támogatás megjelenhet egyéb, anyagi jellegű – a terrorizmus finanszírozásának klasszikus forrásain, lehetőségein túlmutató – formában is. A közösségi média és az online felületek alkalmazása nagyon sokrétű lehetőséget biztosít a terrorizmus pénzügyi támogatásának területén. Például amikor az egyik terrorszervezethez kapcsolódó személyek a Twitteren keresztül igyekeztek adományokat gyűjteni, arra kérték az adományozókat, hogy Skype-on vegyék fel velük a kapcsolatot. Itt aztán arra kérték az adományozókat, hogy szerezzenek be valamilyen nemzetközi feltöltőkártyát (ez lehet mobiltelefon-jóváírás, programok vásárlását vagy az internetes tartalom elérését biztosító vásárlás), és küldjék el nekik a jogosultságot igazoló azonosítókat. Az adománygyűjtő elküldte az azonosítókat Szíriába, ahol alacsonyabb áron értékesítették azokat, az ebből származó készpénz pedig a terrorszervezethez került.¹⁶

Az Iszlám Állam kötelékébe tartozó külföldi harcosok folyamatosan használták az internetet, posztjaikban törekedtek bemutatni a csatlakozó dzsihadistákra váró „kihagyhatatlan” lehetőségeket, így erősítve az esetleges kétkedőket.¹⁷

4.2. Kapcsolattartás

A terroristák egymás közötti kommunikációjuk során az átlagemberek számára is elérhető, alkalmazható és használatukhoz kiemelkedő informatikai tudást nem igénylő kommunikációs hálózatokat, valamint az azokon működő és/vagy hozzájuk kapcsolódó eszközök kínálta lehetőségeket használják ki és alkalmazzák rossz szándékkal. Bármely szokványos készülék a hozzá tartozó hálózati elérésekkel és néhány konspirációs jellegű rendszabállyal jelentős segítséget nyújthat egy terrorcselekmény előkészítése, illetve végrehajtása során szükséges kommunikáció megkönnyítéséhez. A kapcsolattartásra kiváló lehetőséget biztosítanak a különböző infokommunikációs eszközök,

¹⁵ Charlie Winter: *Fishing and ultraviolence*. *BBC News*, 2015. augusztus 1.

¹⁶ Lásd a Pénzügyi Akciócsoport nevű kormányközi szervezet (Financial Action Task Force, FATF) jelentését: *Emerging Terrorist Financing Risks*.

¹⁷ Aris Roussinos: *Jihad selfies, these british extremists in Syria love social media*. *Vice*, 2013. december 5.

a közösségi oldalak és chatalkalmazások, mint ahogyan ezt a 2015. november 13-án Párizsban és 2016. március 22-én Brüsszelben végrehajtott terrortámadások után páratlan nemzetközi összefogással végrehajtott nyomozás adatai alátámasztották.¹⁸

A hétköznapi eszközök, technológiák, hálózatok terroristák, terrorszimpatizánsok általi használata komoly lehetőséget biztosít a terrorellenes fellépés hatékonyságának fokozására. A platformokon kihelyezett privát üzenetek lehetővé teszik a nemzetbiztonsági szolgálatoknak, hogy az adatok elemzése során terroristákat azonosítsanak és figyeljenek meg, kapcsolati hálókat térképezzenek fel, terrorizmushoz köthető tevékenységek mintázatait ismerjék fel. A nemzetbiztonsági szolgálatok e tevékenységük során az egyszerű, formális logikai és a kötött elemző-értékelő eljárásokra, valamint a komplex elemző-értékelő modellekre egyaránt támaszkodnak. Az eljárások és modellek – a terroristák azonosításán, megfigyelésén, kapcsolataik megismerésén túl – lehetőséget biztosítanak korai előrejelző rendszerek kiépítésére is.¹⁹

A kibertérben folytatott kommunikációjukban rejlt biztonsági deficitekkel a terror-szervezetek vezetői is tisztában vannak, voltak. Oszáma bin Láden az 1990-es években felhagyott műholdas telefonkészüléke használatával, miután sajtóhírek jelentek meg arról, hogy az amerikai nemzetbiztonsági szolgálatok ellenőrzik azt.²⁰ A sors fintora ugyanakkor, hogy rejtkehelyének felderítéséhez jelentősen hozzájárult testőre műholdas telefonhívásainak megfigyelése, rögzítése.²¹ A Snowden-botrány kirobbanása előtt is jellemző volt a digitális konspiráció a terrorszervezetekre. Az al-Káida 2007-ben adta ki a „Mujahedeem Secrets”²² nevű titkosító programját, amelyet hosszú időn keresztül használtak a szervezeten belül a szenzitív adatok védelmére.²³

Az Edward Snowden által kitergetett információk rávilágítottak arra, hogy az amerikai hatóságok mennyire támaszkodnak a terrorizmussal összefüggésbe hozható személyek megfigyelése során az interneten folytatott – sok esetben titkosítatlan – információcserékre, illetőleg az azok feldolgozásából és elemzéséből nyert adatokra.²⁴

Ennek hatására a terroristaszervezetek rendkívüli gyorsasággal változtatták meg az internetes kommunikációjukhoz kapcsolódó biztonsági előírásokat. Az információcseréjük védelme érdekében többféle módszert alkalmaznak, ilyenek például a végpontok közötti titkosítás, a teljes eszköz titkosítása, VPN²⁵ és TOR²⁶ használata.

¹⁸ Mágó Károly: 14 terrorista járt Magyarországon a párizsi és brüsszeli merénylek közül. *Origo*, 2016. szeptember 30.

¹⁹ Kenedli Tamás – Vida Csaba: Elemző-értékelő tevékenység. In Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete*. Budapest, Nemzeti Közsolgálati Egyetem, Nemzetbiztonsági Intézet, 2014.

²⁰ Ronald Kessler: *Why Osama bin Laden stopped using his intercepted phone*. *The Washington Times*, 2018. augusztus 5.

²¹ Owais Tohid: *Bin Laden bodyguard's satellite phone calls helped lead US forces to hiding place*. *The Christian Science Monitor*, 2011. május 2.

²² Nyílt forráskódú titkosító software, elsősorban e-mailen folytatott kommunikáció biztosítására.

²³ See Morten Storm et al.: *My Life Inside al Qaeda and the CIA*. New York, Atlantic Monthly Press, 2014. 182–183.

²⁴ Eric Schmitt – Ben Hubbard: *ISIS Leader Takes Steps to Ensure Group's Survival*. *The New York Times*, 2015. július 21.

²⁵ Virtual Private Network: az adatokat megosztott vagy nyilvános hálózaton keresztül úgy küldik, fogadják, mintha a használt eszköz közvetlenül kapcsolódna a helyi hálózathoz, ezzel az eredeti kapcsolódási hálózat rejtve marad.

²⁶ The Onion Router: az internetes forgalmat több proxykiszolgálón keresztül továbbítja, így akadályozva meg a forgalom eredetének azonosítását.

E lehetőségek megismerése és elsajátítása érdekében az ISIS kiadott egy kézikönyvet,²⁷ támogatva a szimpatizánsok, tagok, kapcsolódó személyek biztonságos és a hatóságok előtt rejtett kommunikációját. A leírás segítséget nyújt a titkosított kommunikációt biztosító programok, applikációk használatához, a geolokációs információk azonosításához vezető adatok titkosításához, tanácsokat ad az adatvédelmi alkalmazások kezeléséhez. Az útmutató ajánlásokat tesz arra vonatkozóan, hogy mely levelezési platformokat, közösségi oldalakat kerüljék el az olvasói, valamint felhívja a figyelmet az eszközök biztonságos használatához szükséges beállításokra. Az ISIS tevékenységének digitális támogatása terén a platformot használók számára rendkívül nagy segítség volt az állandó jelleggel működő helpdesk szolgáltatás kialakítása is. Ez lehetővé tette, hogy magasan képzett informatikai szakemberek szakmai támogatást nyújtsanak a terrorszervezettel kapcsolatban álló személyek biztonságos kommunikációjához.²⁸

4.3. Támadás

A kibertérből érkező fenyegetések következő, magasabb szintje, amikor egy terrorszervezethez köthető, annak céljait támogató hackerek támadnak meg kormányzati platformokat. Ilyen volt a 2015 januárjában az Amerikai Egyesült Államok Központi Katonai Parancsnokság²⁹ Twitter- és YouTube-fiókjait ért célzott támadás.³⁰ A parancsnokság Twitter-fiókját felhasználva az ISIS üzenetet tett közzé, amely szerint az USA szíriai, afganisztáni és iraki tevékenysége miatt támadni fogják a katonai és az ahhoz köthető hálózatokat, eszközöket. Hatékonyságuk bizonyítékául a Pentagonból származó katonai információkkal kiegészített térképeket, valamint nyugalmazott amerikai tábormokok adatait tartalmazó táblázatokat tettek közzé. Az esetet követően az említett fiókok elérhetetlenné váltak. Az amerikai Védelmi Minisztérium elismerte a támadások tényét, de tagadta, hogy minősített információ került volna a terroristák kezébe.³¹

Ez az incidens rámutat arra, hogy a terroristaszervezetek műszaki, informatikai fejlettsége már komoly fenyegetést jelent, és a védelmi intézkedések tervezése során nem szabad figyelmen kívül hagyni az ilyen jellegű támadások megelőzésére, elhárítására való felkészülést. Még megválaszolandó a kérdés, hogy – mivel a fentebb leírt informatikai támadó műveletekhez hasonló méretű és hatékonyságú akció jelenlegi ismereteink szerint azóta nem történt – a terrorszervezetek jelenleg vajon rendelkeznek-e megfelelő forrásokkal és eszközökkel ilyen jellegű műveletek végrehajtására?

²⁷ Madhumita Murgia: Islamic State uses detailed security manual, revealing its cyber strategy. *The Telegraph*, 2015. november 20.

²⁸ Aaron Brantly – Muhammad al-Ubaydi: Extremist Forums Provide Digital OpSec Training. *CTC Sentinel*, 8. (2015), 5. 10–13.

²⁹ US Central Command.

³⁰ Everett Rosenfeld: FBI investigating Central Command Twitter hacked. *CNBC*, 2015. január 12.

³¹ Audrey Alexander – Bennett Clifford: Doxing and Defacements: Examining the Islamic State's Hacking Capabilities. *CTC Sentinel*, 12. (2019), 4. 22–28.

4.4. Válaszok

Az online térben rejlő lehetőségek megkönnyítik a terroristák kommunikációját, segítik szélsőséges gondolataik és terveik mind szélesebb körben való terjedését. Az online terrortartalmak terjedésének megakadályozása, a véleménynyilvánítás és az információk, eszmék megismerési és közlési szabadságának maradéktalan szem előtt tartásával együtt – talán korunk legnagyobb biztonsági kihívása.

Az internetes platformokat üzemeltető technológiai cégóriások, mint amilyen a Facebook, Microsoft, YouTube és a Twitter – politikai szintekről érkező kritikák hatására – létrehozták a Terrorizmus Elleni Globális Internet Fórumot, abból a célból, hogy megakadályozzák a terroristákat és az erőszakos szélsőségeket a digitális felületek kihasználásában. A fórum küldetése a technikai együttműködés elősegítése a kutatások eredményeinek és a tudás megosztásának előmozdítása, illetve a terrorista és erőszakos, szélsőséges tartalmak online terjedésének megakadályozása érdekében.³² Ezt az összefogást erősíti az a tény is, hogy az Európai Unió Tanácsának 2021. március 16-án elfogadott rendelete alapján a tagállami hatóságok 2022-t követően felhatalmazást kapnak a terroristatartalmak egy órán belüli eltávolítására vagy az összes tagállamban való hozzáférhetetlenné tételére.

Hazai viszonylatban az elsődlegesen médiaszabályozással foglalkozó hatóság a Nemzeti Média- és Hírközlési Hatóság, amely 2014-óta működteti a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisát.³³ Itt kell elhelyezni az azokra a jogellenes tartalmakra vonatkozó határozatokat, amelyek elérhetetlenné tételét az eljáró hatóságok szükségesnek látják. A szolgáltatóknak a Nemzeti Média- és Hírközlési Hatóság közlését követően egy munkanap áll rendelkezésre a határozatban foglalt tartalmak blokkolására, elérhetetlenné tételére. Az adatbázisban elhelyezett információk nem nyilvánosak, azokba betekinteni csak a bíróságnak, a külön törvényben meghatározott hatóságnak, az ügyésznek, a nyomozó hatóságnak, az Országgyűlés illetékes bizottsága tagjainak és az NMHH-nak van joga.

5. Összefoglalás, következtetés

Kijelenthetjük, hogy a napjainkat átszövő információk – és az azokhoz kapcsolódó eszközök – védelme, a velük való gazdálkodás világunk teljes spektrumát áthatja. Így a terrorizmus irányítóit, szervezőit, támogatóit és végrehajtóit is. Kiváló példa erre Rajib Karim esete, aki a British Airways informatikai mérnökeként öngyilkos merénylőnek jelentkezett, vállalva, hogy robbanóanyagot juttat fel egy, az Egyesült Államokba tartó járatra. Al-Awlaki, az Egyesült Államokban született és tanult jemeni sejk rábeszélte, hogy inkább számítástechnikai ismereteit használja a szent cél érdekében. Karim letartóztatását követően a lefoglalt számítástechnikai eszközein tárolt tartalmak feltöréséhez több hónapi szakértői munkára volt szükség a többszintű titkosítási és védelmi rendszerek miatt.

³² Global Internet Forum to Counter-Terrorism.

³³ Az elektronikus hírközlésről szóló 2003. évi C. törvény 159/B. § (3) bekezdés.

Megállapítható, hogy a terrorizmus aktivitása az információ térben elsősorban a kommunikációra, toborzásra és a finanszírozásra terjed ki. Ezek hatékony ellenszere a terrortartalmú közleményeket érintő tiltás, eltávolítás, illetve a gyanús pénz- és eszközmozgások szűrése, figyelése. A kormányzatok komoly nyomást helyeztek az internetes cégekre és a közösségi médiát üzemeltető vállalkozásokra ebben a vonatkozásban.

Erre válaszul a közösségimédia-platformokat üzemeltető informatikai társulások létrehozta egy globális kezdeményezést a terroristatartalmak eltávolítása érdekében. Az illegális tartalmak megjelenése, kontroll nélkülsége komoly veszélyt és hátrányt jelent a gazdasági folyamatokra, az információk szabad áramlására és az emberi kapcsolatokra nézve.

Ezeket a veszélyeket felismerve az Európai Unió intézményei – a hasonló irányú tagállami fellépést is támogatva – ajánlások, irányelvek és rendeletek alkotásával törekszenek gátolni a törvényellenes tevékenységeket és magatartásmódokat. Ez a törekvés 2022-től újabb mérföldkőhöz fog érkezni a tagállami hatóságok tartalomeltávolítási jogkörének végrehajtására vonatkozó időbeli szűkítéssel.

Felhasznált irodalom

- Alexander, Audrey – Bennett Clifford: Doxing and Defacements. Examining the Islamic State's Hacking Capabilities. *CTC Sentinel*, 12. (2019), 4. 22–28.
- Gönczöl Katalin – Kerezi Klára – Korinek László – Lévay Miklós: *Kriminológia-Szakkriminológia*. Budapest, Complex Kiadó, 2006.
- Haig Zsolt – Kovács László: Fenyegetések a cybertérből, *Nemzet és Biztonság*, 1. (2008), 5. 61–69.
- Kazári Csaba: *Hacker, cracker, warez. A számítógépes alvilág titkai*. Budapest, Computer Panoráma, 2003.
- Kenedli Tamás – Vida Csaba: Elemző-értékelő tevékenység. In Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete*. Budapest, Nemzeti Köszolgálati Egyetem, Nemzetbiztonsági Intézet, 2014. 191–206.
- Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Haditechnika*, (2018), 1. Online: <https://doi.org/10.17047/HADTUD.2018.28.1.113>
- Netanjahu, Benjamin: *Harc a terrorizmus ellen*. Pécs, Alexandra, 1995.
- Resperger István: A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In Resperger István (szerk.): *A nemzetbiztonság elmélete a közszolgálatban*. Budapest, Dialóg Campus, 2018.
- Resperger István: Az aszimmetrikus hadviselés és a terrorizmus jellemzői. *Hadtudomány*, (2010), 4. 68–77.
- Schneier, Bruce: *A biztonságáról*. Budapest, HVG, 2010.
- Storm, See Morten – Paul Cruickshank – Tim Lister – Agent Storm: *My Life Inside al Qaeda and the CIA*. New York, Atlantic Monthly Press, 2014.

Internetes források

- Brantly, Aaron – Muhammad al-Ubaydi: Extremist Forums Provide Digital OpSec Training. *CTC Sentinel*, 8. (2015), 5. Online: <https://ctc.usma.edu/wp-content/uploads/2015/05/CTCSentinel-Vol8Issue53.pdf>
- Emerging Terrorist Financing Risks*. FATF Report, October 2015. Online: www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf
- Global Digital Overview. Digital in 2020*. Online: www.wearesocial.com/digital-2020
- Kessler, Ronald: Why Osama bin Laden stopped using his intercepted phone. *The Washington Times*, 2018. augusztus 5. Online: www.washingtontimes.com/news/2018/aug/5/why-osama-bin-laden-stopped-using-his-intercepted/
- Mágó Károly: 14 terrorista járt Magyarországon a párizsi és brüsszeli merénylők közül. *Origo*, 2016. szeptember 30. Online: www.origo.hu/itthon/20160930-tobb-terrorista-is-jart-magyarorszagon.html
- Murgia, Madhumita: Islamic State uses detailed security manual, revealing its cyber strategy. *The Telegraph*, 2015. november 20. Online: www.telegraph.co.uk/technology/internet-security/12007170/Islamic-States-detailed-security-manual-reveals-its-cyber-strategy.html letöltés ideje: 2021.04.25.
- Nato Unclassified: *MC 0472/1 Military Committee Concept For Counter-Terrorism*. Online: www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160817_160106-mc0472-1-final.pdf
- Raymond, Eric: *S. How To Become A Hacker*. Online: <http://catb.org/~esr/faqs/hacker-howto.html>
- Rosenfeld, Everett: FBI investigating Central Command Twitter hack. *CNBC*, 2015. január 12. Online: www.cnbc.com/2015/01/12/us-central-command-twitter-hacked.html
- Roussinos, Aris: Jihad selfies, these british extremists in Syria love social media. *Vice*, 2013. december 5. Online: www.vice.com/en/article/gq8g5b/syrian-jihadist-selfies-tell-us-a-lot-about-their-war
- Schmitt, Eric – Ben Hubbard: ISIS Leader Takes Steps to Ensure Group's Survival. *The New York Times*, 2015. július 21. Online: www.nytimes.com/2015/07/21/world/middleeast/isis-strategies-include-lines-of-succession-and-deadly-ring-tones
- Statement of Dorothy E. Denning*. Georgetown University. Online: https://fas.org/irp/congress/2000_hr/00-05-23denning.htm
- Tohid, Owais: Bin Laden bodyguard's satellite phone calls helped lead US forces to hiding place. *The Christian Science Monitor*, 2011. május 2. Online: www.csmonitor.com/World/Asia-South-Central/2011/0502/Bin-Laden-bodyguard-s-satellite-phone-calls-helped-lead-US-forces-to-hiding-place
- Winter, Charlie: Fishing and Ultraviolence. *BBC News*, 2015. augusztus 1. Online: www.bbc.co.uk/news/resources/idt-88492697-b674-4c69-8426-3edd17b7daed
- Zernike, Kate – Michael T. Kaufman: The Most Wanted Face of Terrorism. *The New York Times*, 2011. május 2. Online: www.nytimes.com/2011/05/02/world/02o-sama-bin-laden-obituary.html

Majorosi Ádám¹

Az Oszmán Birodalom hírszerzése

Intelligence of the Ottoman Empire

Az Oszmán Birodalom hírszerzése decentralizált volt és rendkívül nagy területet kellett átfognia. Elsősorban a nagyúri udvarokon (háztartásokon) nyugodott, ezért tanulmányom első nagyobb egysége ezekkel foglalkozik. A következő egységben a hírszerzést végző, különböző háttérű csoportokról lesz szó. Így például a mórokról, a zsidókról vagy a kereskedőkről. Majd írok a postai rendszerről, amely gyorsan célba juttatta az elhárító tevékenységgel kapcsolatos híreket. Ez is decentralizált volt, ami azonban semmit nem von le hatékonyságából. Következtetésekkel zárom a munkát. Ezek legfontosabbika: a rendszer hasonló problémákkal küzdött, mint például a központosított nyugati hírszerző szervezetek.

Kulcsszavak: Oszmán Birodalom, hírszerzés, mórok, kereskedők, kalózok,

In this essay I am writing about the intelligence network of the Ottoman Empire. This system was decentralised and it has had agents in all over the Mediterranean area. It was made to operate through the courts of the main officers of the empire. So I have dedicated the first part to them. In the next chapter I would like to examine the agents of the Ottoman Empire. They have served the Empire with different backgrounds (moriscos, merchants, pirates). After that, I will write about the postal system, which transferred the news to the capital quickly. My last chapter will examine the counter-intelligence system. This was also decentralised, which, however, does not detract from its effectiveness. I will finish this essay with the conclusion. Although the system was decentralised, it was very effective, because the centre had to examine fewer information, than the centralised Western services. However, they had similar systemic problems also (competitor bosses, lack of control over them, delivery of contradictory news).

Keywords: Ottoman Empire, intelligence, moors, merchant, pirates

¹ PhD-hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: majorosiadam@gmail.com

1. Bevezetés

Tanulmányomban az Oszmán Birodalom hírszerzéséről adok áttekintést, főképpen a 16. századról. Az Oszmán Birodalom ekkor érte el legnagyobb kiterjedését, ezért egy olyan hírszerző rendszert kellett kialakítania, amely képes a megnövekedett hírigényeket kielégíteni. A 16. században indult meg a mai, modern államalakulatok kifejlődéséhez vezető intézmények kiépülése, így ez a periódus vált a hírszerző szervezetek kialakulásának legfontosabb időszakává. A szerveződést a diplomácia kapcsolatok felélélnkülése és az állandó követségek megalakulása segítette. Ekkor főleg az itáliai városállamok kezdtek állandó követségeket létrehozni egymás udvarában. Ezek a követek a saját országuk érdekeit képviselték, és igyekeztek a fogadó állam területén információkat szerezni a politikai, gazdasági, katonai fejleményekről. Ezt a megoldást Velence és a Pápai Állam alkalmazta elsőként. Azonban a Nyugat-európai államok követték a példájukat, így a 16. századtól kezdve állandó követségek alakultak meg Európa főbb országaiban. Ezek nagykövetei hozták létre azokat a hírszerző hálózatokat, amelyek a modern titkosszolgálatok alapjaivá váltak.²

Az Oszmán Birodalom hírszerzésének születése is a 16. századra datálható. Bár korábban is igyekeztek információkat szerezni, ezek még inkább katonai jellegűek voltak, és a felderítés tárgykörébe estek. Ezeket a műveleteket főleg a segéderők kategóriába tartozó akindzsik, vagy martalócok hajtották végre. Fő céljuk pedig az ellenséges haderő kikémlése, valamint az úgynevezett „nyelvfogás” volt. Később azonban a birodalom növekedése megkövetelte egyfajta hírszerző szervezet kialakítását. Ez a szervezet azonban nem hasonlítható a nyugati országok (Habsburg-birodalom, Velence) által kialakított hírszerző apparátusokhoz. Míg az utóbbiak központilag ellenőrzött és irányított szervezetet tartottak fent, addig az oszmánoknál a hírszerzés decentralizált formában állandósult. Ez azt jelentette, hogy a különböző udvarok eltérő hírszerzési tevékenységet folytattak, és akár együttműködhetnek más államokkal saját politikai céljaik elérése érdekében. Sőt, a határvidékeken tartózkodó szandzsákbégek hírszerző tevékenységét sem irányította napi rendszerességgel az isztambuli kormányzat. Ők csak az ellenőrző tevékenységben vettek részt, esetleg jutalmat osztottak ki a megfelelő sikerrel járó tevékenységért, illetve ritka esetekben részt is vettek benne (foglyok kihallgatása, esetleg helyi ellenőrzések lefolytatása).³

Magyarul eddig kevés összegzés jelent meg a témával kapcsolatban. Kiemelhetjük Ágoston Gábor, Szakály Ferenc, Fodor Pál munkásságát, akik főképpen a hódoltság hírszerző tevékenységével foglalkoztak. Ágoston Gábor azonban a központ információszerező tevékenységét is elemezte. Ennek a területnek a legkiválóbb kutatója Emrah Safa Gürkan, aki főleg külföldi levéltári források alapján igyekezett rekonstruálni azt. Korábbi doktori disszertációját összegző munkája a *Szultán kémei* címmel jelent meg.

Tanulmányom első nagyobb egységében a hírszerzői szervezetet mutatom be. Itt főleg a szervezet decentralizáltságára összpontosítok, illetve azokra a hírszerzői hálózatokra, amelyeknek jelentős befolyásuk volt az oszmán döntéshozatalra.

² Ágoston Gábor: *Európa és az oszmán hódítás*. Budapest, Hadtörténeti Intézet – Európa Könyvkiadó, 2014. 67–68.

³ Gürkan, Emrah S.: *A szultán kémei, Oszmán hírszerzési módszerek és ügynökhálózatok a 16. században*. Budapest, Gondolat, 2020. 129–141.

Így érintem majd Szokollu Mehmed pasa, nagyvezír, Uludzs Ali, kapudán pasa, flotaparancsnok, József Nászi zsidó kémfőnök és Alvise Gritti hírszerző szervezeteit is.⁴ Ezek különböző érdekek mentén gyűjtöttek híreket, amelyeket más országok hálózataival is megoszthattak. Utána szólok pár szót azokról az elemekről, akik a hírszerzést végezték. Idesorolhatók például a szandzsákbégek, az akindzsik, a korzárók (kalózok), martalócok, pribékek, akik igyekeztek megfelelő információkkal ellátni a központot. Azonban gyakran előfordult, hogy kettős játékot játszottak, és például a Habsburgoknak is küldhettek híreket. Itt szeretném érzékeltetni a szervezetek kiterjedtségét, hiszen az oszmánok a Földközi-tenger teljes területét lefedték, sőt még az angol királyi udvarban is voltak embereik. Így számos helyről szerezhettek adatokat.

Az oszmán hírszerzést a külpolitikai folyamatok is befolyásolták. Így az oszmán vezetés hírszerzői tevékenységet folytathatott a spanyol területeken élő moriszkók körében, vagy például Nápolyban is jelentős csoportot tudott kialakítani, köszönhetően a helyiek ellenállásának a Habsburg birodalmi törekvésekkel szemben. Tanulmányomban azt is vizsgálni fogom, hogy milyen volt az együttműködés más államok hírszerző tevékenységével. Például az oszmán hírszerzés rendre kapott híreket Velencén keresztül, amely nem akart kiszolgáltatott lenni egy esetleges támadással szemben, ezért készségesen adott át információt az isztambuli bailón keresztül.⁵ A dolgozatomban természetesen a hódoltsági információgyűjtést szintén igyekszem majd vizsgálni, amely főleg katonai felderítést jelentett, elsődleges célja pedig az ellenséges hadmozdulatok kikémlelése volt.

Végezetül a következtetések sorában összegezem az oszmán hírszerző tevékenységet. Az oszmán hírszerző szervezet, bár nem állt szorosabb központi irányítás alatt, mégis képes volt felvenni a versenyt a többi hírszerző szolgálattal, és felül is tudta múlni azokat. Ennek fő oka, hogy a decentralizáltság miatt a helyi szandzsákbég képes volt előzetesen értékelni az információkat, és helyben felhasználni azokat, így a központnak jelentős beavatkozással nem kellett élnie. Csak az igazán fontos információk kerültek a központ elé. Ebben természetesen szerepet játszott a *menzil* postarendszer, amelynek használatát a hivatalnokok részére erősen korlátozták.⁶ Így csak a legfontosabb információkat küldték tovább. Valamint az oszmánok több külföldit alkalmaztak hírszerzői feladatokra, ez pedig segítette a hírszerzést és az idegen környezetbe való beépülést is. Bár az oszmánok nem alkalmaztak állandó nagyköveteket, de a folyamatos diplomáciai interakciók következtében állandó kapcsolatban voltak más országokkal, így képesek voltak fontos információkat szerezni. Ebben segítette őket Isztambul multikulturális légköre is, amelyben sok információ cserélt gazdát.⁷ Így az előbb említett hátrányt képesek voltak bizonyos szinten kiküszöbölni. Az sem jelentett számukra különösebb gondot, hogy az oszmánok nem sajátították el a rejtjelezést, s így dokumentumaik könnyen olvashatókká váltak. Sőt, a birodalom

⁴ Emrah S. Gürkan: *Espionage in the 16th Century Mediterranean. Secret Diplomacy, Mediterranean Go-Betweens and the Ottoman–Habsburg Rivalry*. Doktori értekezés. Washington D.C., Georgetown University, 2012. 369–396.

⁵ Erről lásd bővebben Hahner Péter: A velencei hírszerző és biztonsági szolgálatok. In Boda József – Regényi Kund (szerk.): *A hírszerzés története az ókortól napjainkig*. Budapest, Dialóg Campus, 2019. 66–68.

⁶ Gürkan (2012): i. m. 410–412.

⁷ Ágoston Gábor: Információszerzés és kémkedés az Oszmán Birodalomban a 15–17. században. In Petercsák Tivadar – Berecz Mátyás (szerk.): *Információáramlás a magyar és a török végvári rendszerben*. Eger, 1997. 138–139.

határain kívül az oszmán üzenetváltásokat Velence szállította, a dózse emberei így olvashatták azokat. Átléptek afelett is, hogy az Oszmán Birodalom nem rendelkezett újságokkal, amelyek információk megosztásával gyakorolhattak volna hatást lakosaikra. A nyugati újságokat ugyanakkor gyakran használták arra, hogy befolyásolják az európai közvéleményt.⁸

2. Az oszmán hírszerző szervezet

2.1. A rendszerről

Az Oszmán Birodalomban is a 16. századtól kezdve alakult ki a központi hatalomra jellemző államigazgatás. Az átalakulás kezdetben a vallási intézményekben volt megfigyelhető, ahol szétvált a vallási és a pénzügyi adminisztráció. A pénzügyi adminisztrációból vált ki később az államigazgatás. Ekkor már a vallási hivatalnokoknak fontosabb volt a pénzkereset, mint az egyház működtetése, így ők a pénzügyben, később az államigazgatásban kaptak állást. A továbbiakban pedig titkárok lehettek, akik az oszmán hírszerzés legfőbb irányítóinak számítottak, ők gondozták a kémek levelezését és irányították a kémszervezeteket. Az adminisztráció átalakulása nem érintette a diplomáciai testület létrehozását, már csak azért sem, mert az európai államok ekkor még ellenségnek számítottak, így az iszlám szerint oda nem küldhettek követeket. Ezért az oszmán vezetésnek másként kellett megoldani a problémát.⁹

Természetesen az oszmán vezetés is küldött nagyköveteket idegen udvarokba. Ezek azonban ideiglenes nagyköveteknek számítottak, akik csak bizonyos ügyekben képviselték a Portát. Ráadásul nem beszélhetünk hivatalos, a feladatra kiképzett nagykövetről sem. Legtöbbször portai tolmácsokat vagy renegátokat (átállt külföldieket, vagy a szultáni udvarban fiataloktól nevelkedett idegeneket) küldtek külföldi országokba követnek. Őket azért, mert beszélték az illető ország nyelvét és ismerték a kultúráját is.¹⁰ Így jobban eligazodtak a fogadó országban, és megfelelőképpen képviselheték a Portát. Azonban az oszmánok is alkalmaztak követeket hírszerzésre és a kémeikkel való kapcsolattartásra egyaránt. Követeik egyébként rendkívül kíváncsiak voltak, sokat kérdezősködtek. Ezért például Velence igyekezett őket házi őrizet alatt tartani, és elzárni az információs forrásaiktól. Az izolációs kísérlet azonban többnyire nem volt sikeres, a követ gyakran képes volt megoldani azt, hogy közvetítőkön keresztül kapcsolatot tartson az adott országban tevékenykedő oszmán kémeikkel. Egyébként az érintkezés nehezítésének módszerét az oszmánok is alkalmazták a külföldi kémek informálódásának megakadályozására, kevés sikerrel.¹¹

A 16. században az egyes államok igyekeztek központosított adminisztrációt létrehozni, hogy hatékonyabban foglalkozhassanak az államügyekkel. Ennek eredményeként

⁸ Ágoston (2014): i. m. 113–114.

⁹ Gürkan (2020): i. m. 128.

¹⁰ Ágoston (1997): i. m. 141–144.

¹¹ Gürkan (2020): i. m. 112–113.

az állami hírszerzés is központi irányítás alá került. Ezt igyekeztek különböző bizottságokon keresztül irányítani.

A spanyol korona alatt például különböző tanácsok foglalkoztak a hírszerző tevékenységgel, sőt II. Fülöp létrehozta a Legfőbb Kémhivatalt is, amely az információkat begyűjtve igyekezett azok valóságtartalmát is ellenőrizni. Ebben a munkában több tanács is segítette, azonban a jelentős információmennyiséget sokszor lehetetlen volt teljességgel ellenőrizni. Velencében a hírszerzés legfőbb irányítója a Tízek Tanácsa volt. Tagjai a nagykövetektől kérték be az aktuális információkat, amelyeket rejtjelezve, tömören küldtek meg számukra. Ők az információkat megrostálták és ellenőrizték, azok így kerültek a szenátus elé. A Tízek Tanácsa igyekezett a kémekre vonatkozó minden információt eltüntetni, mert nem akarták, hogy nyilvánosságra kerüljenek.¹²

Az Oszmán Birodalomban effajta centralizáció nem létezett, ott teljesen másfajta hírszerző rendszert valósítottak meg. Központosítás helyett igyekeztek decentralizált információgyűjtő rendszert létrehozni, amelynek irányítását a helyi szandzsákbégek irányítása alá helyezték. Ennek több oka volt. Egyrészt a birodalom területe óriásira duzzadt, ami jelentős információmennyiséget jelentett. Ezt pedig lehetetlen volt egészében ellenőrizni. Több hétbe került, míg ezek az információk vidékről elérték a fővárost, így mire a megfelelő intézkedéseket meghozhatták volna, az információ elavult, értéktelenné vált. A jelentős információt postával küldhették fel, a küldemények azonban késedelmet szenvedhettek az úton, sőt a sok üzenet esetleg túlterhelte a rendszert, így pedig maguk a kommunikációs csatornák használhatatlanná válhattak. Az tűnt a leglogikusabb módszernek, ha az információgyűjtést és -feldolgozást a helyi szintre korlátozzák. Így a határbégek, kormányzók határozhatták meg a számukra fontos információk körét, amelyekhez időben hozzájutva gyorsan képesek voltak a lehetséges fenyegetéseket, problémákat elhárítani. Csak olyan híreket küldtek fel a fővárosba, amelyek a szultáni udvar számára igazán fontossá válhattak. A szultáni udvar gyakran követelt információkat a szandzsákbégektől, ezek elmaradását szankcionálhatta is. Ha elégedetlen volt az információk mennyiségével, minőségével, akkor beavatkozhatott, és akár még csauzt (ellenőrt) is küldött az adott kormányzóságba, aki ellenőrizte az információgyűjtő tevékenységet.¹³

A hírszerző tevékenységet helyi szinten sem egy központi szervezet végezte, hanem valamelyik nagyobb úr udvartartása. Ez a megoldás még a törzsi időszakból maradt meg, amikor a törzsfők személyes szolgálatra különböző pozíciókban alkalmaztak szolgálókat. Az Oszmán Birodalom ilyen udvartartásokon alapult. Ezek az udvarok láttak el bizonyos adminisztrációs, de hírszerzési feladatokat is.¹⁴

A legnépesebb udvar természetesen a szultáné volt, ám több főméltóság és hivatalnok (nagyvezír, kapudán pasa) szintén rendelkezett ilyen udvartartással, amelyek a határterületek kormányzóságaiban is megtalálhatók voltak. Ezeken belül dolgozhattak katonák, titkárok, mérnökök, külföldről származó különböző hivatalnokok is. Az udvartartás tagjai több idegen nyelvet is beszélhettek, így megfelelő hírszerzőként szolgáltak. Általában őket küldték el különböző megbízatások elvégzésére, amelyek

¹² Hahner (2019): i. m. 67.

¹³ Gürkan (2012): i. m. 348–351.

¹⁴ Emrah S. Gürkan: L'Idra del sultano. Lo spionaggio ottomano nel cinquecento. *Mediterranea*, 13. (2016), 12. 449.

mindig az adott udvar céljait szolgálták.¹⁵ Az oszmán államigazgatásban ugyanis frakciók alakultak ki bizonyos stratégiai célok elérése érdekében (például Uludzs Ali kapudán pasa, flottaparancsnok a tengeri terjeszkedés mellett lobbizott). Így a főbb személyek, tisztségviselők alá tartozó udvarok e különféle stratégiai érdekek szerint igyekeztek befolyásolni az uralkodót. Így pedig felnagyíthattak bizonyos veszélyeket, vagy el is hallgathattak másokat azzal a céllal, hogy az uralkodót az elképzeléseik megvalósítására ösztönözzék. Így lényegében a szultán számára gyakran küldtek információkat, ezek azonban reális hírértékük mellett bizonyos fokú manipulálásra is szolgálhattak, és egyben a külpolitikai irányvonalat is alakítani igyekeztek. Megtörtént, hogy ezek a szervezetek idegen államok számára küldtek használható információt, hogy ezáltal is a saját befolyásukat növeljék. A határterületeken ugyancsak az ő soraikból kerültek ki azok a hírszerzők, akik a túloldalon lévő politikai-katonai tevékenységekről szolgáltak információkkal. Ezen udvartartások, adminisztrációk tagjait az azokat fenntartó főhivatalnokok, magas rangú tisztségviselők pénzelték, így a szultántól birtokokat és pénzt is kaphattak. Azonban a fenntartó halála után ezek a javak visszaszálltak az udvarra. Az udvar ennek segítségével tudta korlátok között tartani az udvartartások hírszerző tevékenységét, megőrizve felettük befolyását.¹⁶

Az egyik ilyen udvartartás a nagyvezír volt. Szulejmán szultán első nagyvezíre, Pargali Ibrahim is jelentős hírszerző szervezetet hozott létre. Legfőképpen a Habsburg csapatmozgásokat és az európai államok külkapcsolatait figyelte. Egyik legfontosabb hírszerző főnöke Alvise Gritti, a velencei dózse fia volt. Ő 1506-ban került a fővárosba, és hamar összebarátkozott a leendő szultánnal és Ibrahimmal. Később az európai ügyekkel kapcsolatos tanácsadóvá vált, és jelentős hírszerző szolgálatot alakított ki. Nagy diplomáciai befolyása volt, több udvarban rendelkezett kapcsolatokkal. Legnagyobb hírforrása Velence volt, ahonnan az apja révén jelentős értékű információkat szerezhetett meg. Azonban nemcsak hírszerző tevékenységet látott el, hanem titkos műveleteket szintén végrehajtott, például támogatta a Habsburgok elleni protestáns lázadásokat. De provokálta a franciákat is Milánó megtámadására, hogy ezzel segítse az oszmán térnyerést. Gritti a hírszerző tevékenységbe saját testvéreit is belevonta.¹⁷ Fivére, Zorzi órásmesterként járta be Európa nyugati felét, ahonnan sok információt küldött Isztambulba. A hálózat ellen a keresztény országok nem sokat tehettek, mivel Gritti apja volt a dózse. Bár Zorzi Grittit le is tartóztatták a Habsburgok, végül el kellett engedniük az apja befolyásának köszönhetően.¹⁸

A másik jelentős hálózat Szokollu Mehmed alatt épült ki. A nagyvezír számára fontos volt a megfelelő információk megszerzése, ezért nagyfokú kémtevékenységet folytatott. Mindig gondot fordított a kémeire, így, amikor Velence elfogta az egyiküket, mindent megtett a kiszabadítása érdekében. A nagyvezír halála után a kémek végül kivégezték. Szokollu Mehmed kiterjedt hálózatot működtetett, amely kiterjedt egész Európára, voltak emberei Spanyolországban, Németországban, Itáliában is. Még a Németalföldön dúló függetlenségi háborúba is küldött kémeket, akik a hadi-eseményeket figyelték. A folyamatosan érkező információkat pedig úgy igyekezett

¹⁵ Gürkan (2020): i. m. 132–133.

¹⁶ Gürkan (2016): i. m. 451–452.

¹⁷ Gürkan (2012): i. m. 370–373.

¹⁸ Gürkan (2016): i. m. 455–457.

felhasználni a béketárgyalásokon, hogy előnyre tegyen szert. Szinte minden hír érdekelte, a katonai-politikai újdonságok mellett a stratégiai szempontból kulcsfontosságú földrajzi ismereteket is gyűjtötte. Így például a folyók, városok elhelyezkedése, a várak, erődök védelmi szerkezete egyaránt érdekelte.¹⁹

Ebbe a kategóriába, tehát a hálózatok működtetői közé tartoznak még a zsidó kémek irányítói is. Ők a reconquista megvalósulása után menekültek az Oszmán Birodalomba, miután korábbi hazájukban erőszakos áttérítést kezdtek alkalmazni velük szemben. Az egyik legmagasabb beosztást betöltő személy körükből József Nászi volt. Bankár családból származott, majd pedig összebarátkozott Szelim²⁰ herceggel, akinek későbbi uralkodása alatt magas pozíciót töltött be. Legfontosabb feladata a hírszerzési információk begyűjtése volt.²¹ Olyan fontos információkat játszott a szultán kezére, hogy Szulejmán egy tükörhöz hasonlította, amelyen keresztül a gyaurok elméjébe is beláthat. József Nászi jelentős kapcsolatokkal rendelkezett, még V. Károlyral is kapcsolatot tartott fenn. Mindez annak volt köszönhető, hogy mint a században a kémek többsége, ő más országoknak is dolgozott, nem csak az oszmánoknak. Nászi hálózata legfőképpen az Európában jelentős zsidó közösségekre alapozott, amelyek számos fővárosban előfordultak, így kiváló információforrásnak számítottak. Bizonyos emberei befolyásos kereskedők, bankárok lehettek, akik még királyi udvarokba is bejáratosak voltak. Hálózata olyan kiterjedt volt és annyira sikeresen dolgozott, hogy az európai államok paranoiásokká váltak miatta, és egy idő után már mindenhol Nászi tevékenységét vélték felfedezni. Erre példa az 1569-es tűzvész. Ekkor valószínűleg Nászi egyik embere gyűjtötte fel a velencei arzenált.²²

Ezután Velence kitiltotta a zsidókat a városból. Olyan rémhírek is keringtek Násziról, hogy a móriskó felkelés alkalmával el akarja foglalni Spanyolországot. Mindezt annak köszönhetné, hogy támogatta a Habsburgokkal szembeni megmozdulásokat szerte Európában, például a spanyol uralom alatt álló németalföldi tartományok Madrid-ellenes felkelését is. Ezzel pedig óriási pénzügyi kárt okozott a Habsburg Birodalomnak.²³

A másik fontos zsidó vallású kémfőnök Alvaro Mendes volt, aki portugál kereskedőcsaládból származott. Hazájában kapcsolatot ápolt a trónkövetelővel, Dom Antoniával, amiért menekülnie kellett. Raguzába ment, majd felajánlotta a szolgálatait az oszmánoknak. Gyorsan befolyásos emberré vált, például igyekezett megvalósítani az angol–oszmán diplomáciai közeledést, és rávenni a Portát arra, hogy beavatkozzon Dom Antonio oldalán a portugál örökösödési harcokba. Jelentős tevékenységet folytatott a tizenöt éves háború során, amikor Angliát igyekezett meggyőzni arról, hogy maradjon semleges a konfliktus alatt. Ez nem esett nehezére, mivel a sógora Erzsébet királynő orvosa lett, így a legfelső társadalmi szinttel volt közvetlen összeköttetése. Később Pijávus pasa portugál szakértőjévé vált, és jelentős információkkal látta el főnökét az Indiai-óceán térségében található portugál erődökkel kapcsolatban.²⁴

¹⁹ Gürkan (2020): i. m. 130–132.

²⁰ A trónon majd mint II. Szelim (1566–1574).

²¹ Ágoston (1997): i. m. 43–144.

²² Gürkan (2012): i. m. 380.

²³ Gürkan (2020): i. m. 132.

²⁴ Gürkan (2012): i. m. 384–385.

A birodalomban még egy magas beosztású hivatalnok rendelkezett jelentős hírszerző szolgálattal, a kapudán pasa (oszmán főadmirális). Több, a pozíciót betöltő személy korábban korzáró, vagyis kalóz volt. Ők észak-afrikai bázisaikról indítottak támadásokat Európa part menti területei ellen, ahol különféle értékeket és foglyokat zsákmányoltak. Ha a foglyok áttértek, akkor belőlük is kalóz válhatott. Az észak-afrikai területek a növekvő Habsburg nyomás miatt az oszmán szultánnál kerestek menedéket, aki cserébe autonómiát adott nekik, egyben kötelezővé tette számukra a hírszerzést. Később az áttért renegátokból lett kalózok magas pozíciókba kerülhettek a szultáni udvarban, sőt némelyikük a főadmirális kinevezést is elnyerte. Ilyen volt például Barbarossa Hayreddin. Egy másik, jelentős befolyást nyerő renegát Uludzs Ali volt, aki Dél-Itáliából származott, és a fogságban tért át az iszlám hitre. Ő egy, a Földközi-tenger nyugati medencéjébe és Észak-Afrikába indítandó hadjárat mellett kardoskodott a szultánnál, ezért információkra volt szüksége ahhoz, hogy a hadjáratra az uralkodót rávegye. Ennek érdekében nagy volumenű hírszerző hálózatot hozott létre, amely lefedte az egész kontinenst. Főképpen az európai hatalmak haditengerészeti mozgásait kémlelte.²⁵

Uludzs Ali elsősorban az előző bekezdésben részletesebben tárgyalt kalózokra támaszkodott hírszerző tevékenysége során. Ezek az emberek ismerték a Földközi-tenger medencéjét, így akár észrevétlenül is képesek voltak megfigyelni az ellenséges haditengerészet mozgását. Erről pedig naprakész információkat tudtak küldeni a kapudán pasának vagy magának a birodalmi központnak. Az is előnyükre szolgált, hogy Tunisz vagy Algír kereskedelmi központok voltak. Ide érkeztek a rabszolgakereskedők vagy rabszolgák kiváltásában érdekelt követek. Tőlük is naprakész információkat szerezhettek, ami szintén az oszmánok érdekeit szolgálta. A kalózok többször foglaltak el értékes gályákat vagy akár katonai fregattokat. A foglyoktól értékes információkat tudtak kicsikarni, esetleg a hajó által szállított dokumentumok is jelentős értéket képviseltek. A velenceiek gyakran panaszkodtak arra, hogy a kalózok elfogták a külügyi postájukat szállító hajóikat. A hajókon általában muszlim rabszolgák is voltak, akik kiszabadításuk után szintén híreket szolgáltatnak Isztambulnak. A kalózok ráadásul földrajzi ismereteiket sem ártallották az oszmán haditengerészet szolgálatába állítani, így azok naprakész információkkal rendelkeztek az ellenséges hadihajók mozgásával, a part menti ellenséges erődökkel kapcsolatban.²⁶ A kalózok gyakran fosztogatták a part menti településeket, amelyeknek áttért foglyai újabb információkat adhattak. A kalózok még a szállítókapacitásukat sem tagadták meg az oszmán hírszerzéstől. Így például ők juttatták célba azokat a hírszerzőket, akik a dél-italiai erődöket kémlelték ki. Így Uludzs Alinak bőségesen állt rendelkezésére információforrás, híreivel pedig a szultánnál lobbizott a Földközi-tenger nyugati medencéjében lefolytatandó hadjáratral kapcsolatban. Attól sem riadt vissza, hogy hamis információkkal próbálja meg az általa remélt eredményt elérni. Így előfordult, hogy egy papot bízott meg, aki nagy közönség előtt könyörgött neki, hogy tegyen valamit a velencei gályák fosztogatásai ellen. Végül a nagyvezírhez kísérték a papot, aki előtte mindent bevallott. Ám a nagyvezír ezt nem használta fel később Uludzs Ali ellen. A főadmirális maga is

²⁵ Gürkan (2016): i. m. 454–455.

²⁶ Gürkan (2012): i. m. 355–360.

tartotta a kapcsolatot a nyugati hírszerző hálózatokkal, akik igyekeztek őt rávenni az átállásra. Erre nem volt hajlandó, olyan értelmű információt viszont bőségesen továbbíthatott, amellyel a saját politikai céljait erősítette, a többi, más célokért küzdő frakció törekvéseit ellenben aláásta.²⁷

2.2. Hírszerzők

Mint minden állam a 16. században, az oszmánok is igyekeztek különböző forrásokra támaszkodni a hírszerzés terén. Így több, különböző háttérű és feladatú ügynököt alkalmaztak. A hírszerzés legfőképpen a határterületek feladata volt, és az információkat is ott, helyben dolgozták fel. Így azonnali intézkedéseket tudtak hozni, és nem kellett a központi utasításokra várniuk. A határterületeken a legfőbb információs forrást az elfogott ellenséges katonák, tisztviselők, civilek jelentették. Őket nevezték „nyelveknek”, és portyák során, hadjáratok alkalmával gyűjtötték be őket az irreguláris katonai alakulatok (akindzsik, tatárok). Tőlük lehetett megtudni az aktuális katonai-politikai eseményeket.²⁸ Őket általában helyben hallgatták ki, és az általuk adott információt összevették más értesülésekkel. Majd erről egy rövid jelentést írtak, amit a központba küldtek. A központ válaszüzenetében nyugtázta az információt, és további hírszerző tevékenységre szólított fel. Ez nemcsak a határterületek, de az autonómiával rendelkező egyéb területek feladata is volt (Egyiptom, kalózállamok). A portyákat egyébként nemcsak az akindzsik vagy a tatárok, hanem martalócok is végrehajthatták. Őket főleg a Balkán szláv és görög népcsoportjaiból toborozták, fő feladatuk a portyák mellett a rendfenntartás volt. Csapataikat a Balkánon kívül a Perzsiával közös határszakaszon szintén alkalmazták.²⁹ A segédhadak bizonyos részének is volt saját hírszerzése. Portyáik során a tatárok például kalauzokat alkalmaztak, akik az ismeretlen terepen eligazították őket. A vezető általában a tatárok közül került ki, de helyieket is alkalmazhattak. Valamint ők is használtak korábbi hadifoglyokat kémtevékenységre. Ezek általában jól beszélték az adott térség nyelvét, jól be tudtak illeszkedni, és információkat gyűjtöttek az ellenséges erődökről, hadseregekről. Sőt, a tatárok az oszmánok ellen is kémkedtek, igyekeztek kipuhatolni, vajon mi a véleménye a szultánnak a tevékenységükről.³⁰

A határterületek kormányzóinál is megfigyelhető az udvartartás, csak kisebb mértékben, mint a Díván magas rangú tagjainál. Itt is voltak olyan szolgálók (zsidók, mérnökök, papok) akiket át lehetett küldeni a határ túoldalára kémkedni. Ezek az emberek természetesen beszélték a helyi nyelveket, és jelentős információkat szerezhettek a helyi vezető számára az esetleges hadjáratok előkészületeiről, a politikai, katonai eseményekről. Ezek az emberek különböző háttérrel rendelkeztek. Egyebek mellett voltak köztük kereskedők, írnokok, katonai mérnökök.³¹ Katonai

²⁷ Gürkan (2020): i. m. 133–134.

²⁸ Ágoston (2014): i. m. 95–96.

²⁹ Gürkan (2020): i. m. 145.

³⁰ Ivanics Mária: Tatár kémiszolgálat az 1663-as magyarországi hadjáraton. In: Petercsák–Berecz (szerk.): i. m. 1997. 207–225.

³¹ Gürkan (2012): i. m. 351.

mérnököket a Habsburgok és az oszmánok egyaránt alkalmaztak. Fontos szerepük volt, mivel ismerték az erődítési munkálatok során alkalmazott legújabb stílusokat, és képesek voltak megtalálni ezen építmények gyenge pontjait. Továbbá a katonák diszlokációját, a vízlelőhelyeket ugyancsak meg tudták mondani. Általában kísérővel együtt mentek, és a megfigyeléseikről vázlatot készítettek. Az oszmánok igyekeztek az ilyesfajta tevékenységre külföldieket alkalmazni, akik beszélték a helyi nyelveket, így el tudtak vegyülni. A problémát az erődök megfigyelése jelentette. Sokszor úgy buktak le, hogy a többszöri látogatásukra az őrség felfigyelt, és letartóztatta őket. Volt olyan mérnök is, például II. Mehmed egyik német származású kémje, Nürnbergi Jörg, aki egyiptomi megbízatását használta fel arra, hogy elmeneküljön. A hírszerző mérnök által összegyűjtött anyagot később elemezték, adatait összevetve korábbi információkkal, és terepasztalt készíthettek mindezek alapján. Így készültek az esetleges ostromokra.³²

A kémek másik fontos csoportját alkották a kereskedők. Őket is alkalmazta mind a két fél információszerezésre. A Habsburgok isztambuli hírszerzésénél például többségben voltak azok az ügynökök, akik kereskedői tevékenységgel álcázták magukat. A magyar végvári kapitányok szintén főleg a kereskedőkre támaszkodhattak, ha információhoz akartak jutni. A kereskedők azért voltak megfelelők, mert fedőtevékenységük révén több jelentős városban megfordultak, és észrevétlenül gyűjthettek híreket a piacokon, kocsmákban egyaránt. Egyébként a kereskedőknek nem feltétlenül kellett fizetett kémeknek lenniük ahhoz, hogy információt szolgáltatassanak. Az oszmánok például minden kereskedőt igyekeztek kikérdezni, akiktől csak tájékozódhattak a nyugati világ történéseiről. De ugyanígy jártak el a Habsburgok is, tehát a kereskedők mind a két felet ellátták információval. Természetesen a tengeri kereskedőktől is lehetőség volt információkat szerezni. Így például a városok kikötőibe érkező hajók kapitányait és legénységét egyaránt azonnal kikérdezhették, amint kikötöttek. A kereskedők azonban nem csak saját érdekeik mentén adhattak át híreket az oszmánoknak. A Földközi-tengeren szolgáló kalózok az elfogott kereskedőhajók kapitányait, személyzetét ugyancsak rendszeresen kifaggatták, az így kapott információkat pedig tovább küldték a központba. A kereskedőhajók viszont levelezést is szállíthattak, ennek dokumentumait a kalózok megint csak előszeretettel továbbították Isztambulba. Jelentős szerepe volt a rabszolgakiváltó kereskedőknek. Ezek az emberek a kalózok által elfogott vagy a hadjáratok során fogságba eső katonák, civilek kiszabadításával foglalkoztak, és az ehhez szükséges váltságdíjat szállították.³³ Azonban ez nem utolsósorban kiváló fedőtevékenységet jelentett számukra, mivel a tárgyalásaik során bőséges lehetőségük volt a legkülönfélébb információkhoz jutni, mint ahogyan maguktól a hadifoglyoktól is. Így nem egy ilyen kereskedő volt kém a maga korában. A magyar végvári kapitányok is alkalmaztak kiváltó kereskedőket hasonló célokra. Feladatuk az ellenséges erődítmények, csapatok kikémlelése és az információk továbbítása volt.³⁴

³² Ágoston (2014): i. m. 107.

³³ Gürkan (2020): i. m. 103–105.

³⁴ Pálffy Géza: Hírszerzés és hírközlés a törökkori Magyarországon. In Petercsák–Berecz (szerk.) (1997): i. m. 48–49.

A 16. században nagyon fontos volt az ellenség területén lévő különböző népcsoportok megnyerése, amely közösségek tagjai szükség esetén információval, helyismerettel, de ha kellett, akkor lázadásukkal tudták segíteni az ellenséges hírszerzőket. A Habsburgok főként az oszmánok uralma alatt élő balkáni és görög népcsoportokat használhatták hasonló célokra. Nemcsak információt lehetett szerezni tőlük, hanem esetleges felkelésükkel ellenséges csapatokat vonhattak el a határról, és segíthették kémek bejuttatását az Oszmán Birodalomba. Erre nagy szükség is volt, tekintve, hogy a határ mindkét oldalán jelentős járőrtevékenység folyt, mivel a kémek bejutását csak így lehetett megakadályozni. Az oszmánok szintén igyekeztek belső népcsoportokat megnyerni maguknak a Habsburgok uralma alatt álló területeken. Az egyik ilyen népcsoport a Spanyolországban leigázott móroké volt. A mórok a 8. századtól kezdve harcoltak a különböző keresztény államok ellen. A spanyol királyságok már hosszú ideje igyekeztek felszabadítani a mórok uralma alól a mai Spanyolországot. Azonban ez csak 1492-ben, Granada elfoglalásával vált teljessé, amit az egyesült Spanyol Királyság ért el Kasztília vezetésével. Ezek után áttérésre kényszerítették őket, bár sokan közülük titokban továbbra is gyakorolták eredeti vallásukat. A mórok fontos információkkal látták el a Portát a Habsburg hadseregről, erődökről, a haditengerészetről. Ezeket az információkat azért osztották meg az Oszmánokkal, mert abban reménykedtek, hogy a tengeren keresztül esetleg katonai segítséget küldenek nekik, és ismét szabadok lehetnek. A mórok felkeléseikkel elvonták a Habsburg erőket, és információkat adtak át Isztambulnak. Ezért cserébe lőfegyvert és hozzá tartozó lőszeret kaptak, valamint bátorítást a további ellenállásra. Az oszmánok végig tartották a kapcsolatot a mórokkal, még azután is, hogy a felkelésüket levertek. Továbbra is hasznosnak bizonyultak a számukra, és jelentős információkkal gyarapították a Porta tudását. Sokan közülük katonává váltak, és várakban szolgáltak, így hasznos információt küldhettek az oszmánoknak. A mórok között akadtak olyanok, akik politikai törekvéseik bukása után nem maradtak hazájukban, hanem Konstantinápolyba menekültek. Első csoportjukat II. Bajezid szultán fogadta be, de a későbbiek folyamán további menekültek érkeztek, akik jelentős ismereteket hoztak magukkal. Belőlük később katonák, hírszerzők váltak.³⁵ A másik hasonló csoport a nápolyi fuoricittik közül került ki. Ők olyan nemesek voltak, akik elégedetlenek lettek a nápolyi Habsburg uralommal. A fuoricittik is azért segítették az oszmánokat, hogy meggyőzzék őket egy nápolyi hadjárat szükségességéről. Azt remélték, hogy az oszmán–francia szövetség harapófogóba kényszeríti a Habsburgokat, és az oszmánok majd elfoglalják a királyságot. Jobbnak tartották az oszmán kormányzást, mint a Habsburgokét. Többeket közülük száműztek, de ők később ügynökként tértek vissza, illetve oszmán kémek bejuttatását segítették az országba. Főleg az Itáliában állomásozó Habsburg erők elhelyezkedéséről és a helyi erődökről adtak át információkat Konstantinápolynak.³⁶

Mindezekeken felül beszélhetünk még a zsidó közösségek hírszerző szerepéről is. A zsidók Európa összes jelentős nagyvárosában megtalálhatók voltak, ahol többen közülük üzleti tevékenységet folytattak. Így kiterjedt kapcsolati hálóval rendelkeztek, előfordult, hogy az uralkodói házakban is kapcsolatot építhettek. Ez pedig az oszmánok

³⁵ Gürkan (2012): i. m. 390–392.

³⁶ Gürkan (2020): i. m. 107–108.

számára jelentős információkat biztosíthatott. Mint korábban már volt róla szó, a zsidók Isztambulban is magas pozíciókat tölthettek be. Néhányuk az uralkodó mellé kerülhetett, belőlük a szultán orvosai, kémei válhattak. Példaként említhető József Nászi, aki az egyik legjelentősebb kémfőnök lett. A zsidók fontos információkat küldözgettek Velencéből, ahol jelentős zsidó közösség élt. Itt főleg üzleti tevékenységben vettek részt, így sok hasznos információhoz hozzáférhettek. Az oszmánok számára nagy előny volt, hogy nagyobb zsidó közösségek a Földközi-tenger több nagyvárosában éltek, így majdnem mindenhol információkat szerezhettek. A főváros zsidó közössége pedig megkönnyíthette magát az információ átadását is, tekintve, hogy nekik rokonaik voltak ezekben a városokban, akikkel rendszeresen érintkeztek.³⁷

Természetesen a külföldi nagykövetek által szolgáltatott hírekről sem feledkezhetünk meg. Ezek a nagykövetek személyesen is adhattak át információkat oszmán hivatalnokoknak. Erre példa velencei *baillo*, aki az Isztambulban székelő velencei kereskedelmi érdekeltségek vezetője, és ebből kifolyólag nagykövet is volt. Velencének ugyanis információátadási kötelezettsége volt a Porta felé, amit készségesen teljesítettek, mert nem akartak oszmán támadást magukra vonni. Így a baillon keresztül információval látták el a Dívánt.³⁸ De más európai nagykövetek is adtak át információkat a szultánnak, például a francia nagykövet is, mivel az oszmánokkal szövetségben álltak a Habsburgokkal szemben.³⁹ A követségeken dolgozó helyiek is lehettek ügynökök. Őket az oszmánok ellenőrizték, és mivel a helyből származó dolgozóknak nem járt diplomáciai védelem, gyakran érték őket támadások az oszmán állam részéről. Volt, hogy börtönbe vetették őket, vagy éppen az oszmánoknak kémkedtek. A követségek ráadásul a főváros lakosai közül fogadtak fel futárokat, akiket szintén elfoghattak, és tömlöcbe vethettek az oszmán hatóságok. Így a követségek postáját is megszerezhették. Ez ellen főleg a titkosírás alkalmazásával védekeztek a diplomáciai testületek. Az így sifírozott leveleket az oszmánok nem tudták elolvasni, mivel maguk csak ritkán alkalmazták. E módszerek bevetése ellen emelt szót Szokollu Mehmed nagyvezír Velencében, sikertelenül.⁴⁰

Még egy fontos tényezőről kell beszélnünk a hírszerző tevékenységek áttekin-
tésekor, elemzésekor, ez pedig a vazallus államok szerepe. Az oszmánok határaik mentén vazallus államok egész sorával rendelkeztek, amelyeket még nem tagoltak be teljes mértékben a birodalmi közigazgatásba. Mint a határ menti szandzsákbégeknek, ezek vezetőinek, lakosainak szintén fontos feladatuk volt az információszerezés. Gyakran küldtek különféle híreket a Portának, általában a helyi csapatmozgásokról, erődítményekről vagy nemzetközi politikai hírekről. Ezeket a központi kormányzat fogadta, elemezte, és újabb információkat követelt tőlük. Az egyik leglényegesebb információforrásnak Raguza városállama számított. A külföldi nagykövetek itt lépték át az államhatárt, így jelentős kémtevékenység zajlott a városban.⁴¹

³⁷ Gürkan (2012): i. m. 394–395.

³⁸ Emrah S. Gürkan: *Fonds of The Sultan. How to use Venetian Sources for Studying Ottoman History? News on the Rialto*, 32. (2013), 26–27.

³⁹ Gürkan (2020): i. m. 114.

⁴⁰ Gürkan (2012): i. m. 85–86.

⁴¹ Ágoston (2014): i. m. 106.

Raguza kiterjedt kereskedelmi kapcsolatokkal rendelkezett a Földközi-tenger egész medencéjében, ezért tökéletes információs központnak bizonyult. Azonban Raguza kényes helyzetben volt, mivel a Habsburg- és az Oszmán Birodalom határán helyezkedett el. Így mindkét félnek juttatott információkat. Raguza a Porta megbízásából is küldött ki hírszerzőket, például Málta ostromakor raguzai kémek tartották a kapcsolatot a megszálló erők és a központ között.⁴² A másik ilyen vazallus állam az Erdélyi Fejedelemség volt, amely igyekezett hasznos információkkal szolgálni az oszmánoknak. Sőt, gyakran bízták meg embereiket kifejezetten határon túli feladatokkal. Ebben megkönnyítette a dolgukat, hogy magyarul beszélő ügynököket sokkal egyszerűbb volt átküldeni, mivel a Királyi Magyarországon jobban el tudott vegyülni. De a fejedelem külföldi ügynököket is fizethetett. Például I. Rákóczi György is fogadott fel német zsoldosokat, akik a környező várak német zsoldosai között feltűnésmentesebben mozoghattak, és az erősségeket szemügyre vehették.⁴³

Az oszmán hírszerzésnek dolgozni nagy haszonnal járt. Egy-egy kiváló hírszerzőművelet után busás jutalmat oszthattak ki, sőt akár birtokhoz is lehetett jutni. Általában a hírszerzőket tímárbirtokkal fizették. Ez így volt mind a nyugati, mind a keleti határterületeken. Ahol nem alkalmazták a tímárrendszert, ott a vilajet kincstárából vettek ki meghatározott összeget, és ezt kapta az ügynök. Ha valaki sikeres volt, és kiváló „nyelvet” fogott, akkor akár a korábbi, elveszett birtokait, pozícióját is visszakaphatta. De nemcsak a jó hírek, hanem a rossz hírek hozóit is igyekeztek megjutalmazni. Ezzel általában serkentették a kémek információszerző tevékenységét. A jutalom természetesen a támadó hadjáratok alatt is szerepet kaphatott. Ostromoknál a benti lakosságnak gyakran ígértek adómentességet, cserébe a vár feladásáért, ezzel pedig gyakran több sikert értek el, mint a több hónapos ostrommal.

2.3. A postai hálózat szerepe

Az Oszmán Birodalom számára nagyon fontos volt, hogy a hírek gyorsan érkezenek be a központba. A hírek továbbítását a korabeli államok postaállomások és -útvonalak alkalmazásával hajtották végre. Azonban az európai országok inkább vállalkozók által üzemeltetett útvonalakat használták a központiak helyett, amelyek lassúak voltak.⁴⁴ Az oszmánok állama ezen a téren is kivételt jelentett. Ők a birodalom területén belül saját postahálózatot tartottak fenn, a menzil-rendszert alkalmazták.

A menzil-szisztéma hasonló volt, mint mondjuk a mongol póniexpressz- vagy a mamelukok által alkalmazott *barrid*-rendszer.⁴⁵ A lényeg minden esetben az volt, hogy a birodalmi útvonalakon egymástól bizonyos, meghatározott távolságokra postaállomásokat helyeztek el, ahol friss lovak és pihent futárok tartózkodtak. Egy futár két állomás között vitte az üzenetet, amit másik futárnak adott át az állomáson. Ezt a fajta postát a 16. században szervezték meg. Előtte a futár szultáni engedély

⁴² Gürkan (2020): i. m. 189–204.

⁴³ Pálffy (1997): i. m. 47.

⁴⁴ Gürkan (2012): i. m. 193–195.

⁴⁵ Reuven A. Preiss: *Mongols and Mamluks. The Mamluk–Ilkhanid War 1260–1281*. Cambridge, Cambridge University Press, 1995. 74–75.

birtokában bárki lovát lefoglalhatta, ami azonban ellenérzéseket váltott ki a helyi lakosság körében, illetve a központi kincstárnak kellett megtérítenie a keletkezett károkat. Így I. Szelim a fent bemutatott módon szervezte újra a postahálózatot. Azt remélte ettől, hogy a futárok majd nem fogják mások lovait kölcsönvenni, ez azonban nem valósult meg a gyakorlatban. A központi posta másik jellegzetessége, hogy civilek nem vehették igénybe a szolgáltatásait, sem pedig más tisztviselők. Csak a szultáni páténessel rendelkezők használhatták az infrastruktúrát. A Porta igyekezett csökkenteni annak leterheltségét, ezzel pedig növelni szerették volna a küldemények célba jutásának gyorsaságát. A posta működését a kádi ellenőrizte, és nem a központi kincstárból finanszírozták, hanem egy ideiglenes adóból (*menzilkes*). Ám ez a rendszer csak belföldön működött. Külföldön több módszert is alkalmazhattak. Az egyik az volt, hogy egy birodalmi tisztviselő vitte a levelet (csausz, janicsár, müteferrika). Másik megoldás lehetett, hogy egy külföldi nagykövet vitte el a küldeményt. De az oszmánok gyakran alkalmazták a velencei postát is leveleik kézbesítésére. A velenceiek gyakran visszaéltek ezzel, és elolvasták a küldeményeket. Az oszmánok ennek megakadályozására igyekeztek szóban megállapodásokat kötni, illetve a leveleket kevésbé releváns témában megírni, hogy azok esetleges illetéktelen elolvasása esetén se derüljön fény az igazi tartalmukra. A haditengerészet egységei közti információáramlást is futárok tartották fenn. Ha a kötelék közel volt, akkor általában egy futárhajót küldtek ki az információval. Ha viszont a kötelék távol volt, úgy közvetítőkön keresztül tartották a kapcsolatot, például a velenceiek útján, akik például a máltai ostrom alatt is hozták-vitték a híreket a flotta és a központ között.⁴⁶

3. Elhárítás

Az elhárítással kapcsolatos aktivitásokról, erőfeszítésekről lényegesen kevesebb információval rendelkezünk az Oszmán Birodalom vonatkozásában, mint a hírszerző tevékenységről. Ennek oka egyrészt az, hogy a hírszerzésről több forrás áll rendelkezésre a külföldi államok elhárítása által készített dokumentumokban. Az oszmán elhárításról általában nem készült hivatalos feljegyzés, mivel titokban tartották a besúgók és tartótisztjeik nevét. Másrészt véleményem szerint az elhárítás nem volt igazán megszervezve és kiépítve a Portán, bizonyos szinten a hírszerzéssel együttműködésben dolgozott. De Európa más uralkodói udvaraiban sem működött túlságosan megszervezett elhárítás, vagy annak funkcióit nem állami intézmények látták el (pl. az Inkvizíció). Így ebből a kevés forrásból kell megkísérelnünk képet alkotni.⁴⁷

Vélhetően az oszmán elhárítás is decentralizált volt, és szintén a helyi igazgatás végezte. Természetesen Isztambulban is működtek elhárítók. Bár számukról nem rendelkezünk biztos információkkal, annyi mindenesetre megállapítható, hogy kevesen voltak. Az elhárítás főleg a politikai rendőrséghez hasonló feladatkört jelentett. Általában álruhás janicsárok járták éjszaka a várost, akik találkoztak a besúgóikkal. Tőlük igyekeztek információkat szerezni a közhangulatról, a janicsárok között uralkodó

⁴⁶ Gürkan (2020): i. m. 154–157.

⁴⁷ Gürkan (2020): i. m. 86–97.

véleményekről. Így tudták fenntartani a rendet a fővárosban. Őket a „szalma csukadár” névvel illették. A tőlük származó információkat jelentés formájában közölték a nagyvezírrrel.⁴⁸

A vidéki elhárítás a *derbenteken* alapult. Ezek stratégiai helyeken lévő falvak voltak, amelyekből folyamatosan a határt vagy tengerek mellett a partszakaszt kémlelték. Ha ellenséget láttak, akkor füstjelekkel kommunikáltak. Ezt a többi falu is továbbadta, így a jel végül eljutott az illetékes szandzsákbégekhez, akik megtehették a szükséges intézkedéseket. Egyébként a határon jelentős erőket tartottak fent, amelyek őrizték az utakat és igyekeztek kiszűrni az illetéktelen behatolókat.⁴⁹ A külföldi követek Raguzán keresztül léphettek be a birodalomba, és őket a csasz kísérte. Igyekeztek megakadályozni a követek kapcsolattartását a helyiekkel, ezért meghatározott útvonalakon mentek, és a követ minden lépését figyelte a csasz. A követet természetesen Isztambulban is megfigyelték, és igyekeztek megszerezni a leveleit, a beosztottjain és a tolmácsán keresztül pedig információkat gyűjtöttek róla.⁵⁰ Ha bármi szabálytalanságot találtak vagy kémkedést fedeztek fel, az illetőt kiutasíthatták az országból. Gyakran Raguzának is küldtek fenyegető üzenetet, amelyben bizonyos kémek kiutasítását követelték. Ennek Raguzá eleget is tett félve az esetleges retorziótól.⁵¹

Az Oszmán Birodalomban kedvelt módszer volt a hírek terjedésének megakadályozására a le- vagy elzárás. Ekkor nemcsak a falvak, bizonyos térségek közti közlekedést fagyaszthatták be, hanem – főleg háború esetén – az ellenséges fél nagykövetét szintén őrizetbe vehették. A Hódoltságban a nagyobb portyák során zárhattak le falvakat a helyi katonai erők segítségével. Attól tartottak, hogy a helyi lakosság a portya irányát közölheti a legközelebbi várkapitánnyal. Ez a félelmük nem volt alaptalan, tekintve, hogy az Udvari Haditanács a végvárakból hírszerző szolgálatot hozott létre, amelynek élén a várkapitányok álltak. Nekik volt egy éves pénzügyi keretük, amit hírszerzésre fordíthattak. Így főleg kereskedőket, helyi jobbágyokat, esetleg bizonyos oszmán tisztviselőket is fizethettek. A helyi falvakat nemcsak fizetség útján, hanem fenyegetés alkalmazásával ugyancsak igyekeztek rábírní az együttműködésre. Az oszmánok szintén alkalmaztak fenyegetéseket, így a falvak gyakran két malomkő között őrlődtek. A falvak a nagyobb portyák észlelésekor futárt küldhettek a várakba, így figyelmeztetve azokat. Ezt az oszmánoknak nem mindig sikerült megakadályozniuk. A dolog ellensúlyozására jelentős portyázó csapatokat állomásoztattak a határon, aminek következtében a várkapitányok sokszor a sötétben tapogatóztak a támadás várható helyéről, köszönhetően az egymásnak ellentmondó ellenséges tevékenységeknek.⁵²

Az oszmánok a keleti határon is a teljes lezárást alkalmazták. Itt a Porta folyamatos háborúban állt a szafavida uralom alatt álló Perzsiával, amely a határ túloldalán jelentős támogatói bázissal rendelkezett. Sőt, az oszmánok az elfoglalt területek

⁴⁸ Ágoston (2014): i. m. 96.

⁴⁹ Gürkan (2020): i. m. 361.

⁵⁰ Ágoston (1997): i. m. 149–151.

⁵¹ Gürkan (2012): i. m. 402–403.

⁵² Kelenik József: Kémek, hírek, rémhírek. Hírszerzés és hadviselés a dél-dunántúli végeken a 17. század első felében. In Petercsák–Berecz (szerk.) (1997): i. m. 169–173.

lakosságában sem bízhattak meg, mivel ők is a szafavidáknak kémkedhettek. Így igyekeztek kémeket küldeni a határon át, illetve megfelelően ellenőrizni a határszakaszt. Perzsia urainak kedvelt módszere volt, hogy papokkal vitettek át a határon adományok álcázott, valójában az informátoraiknak szánt kempénzt. Ezért a Porta parancsba adta, hogy akinél ilyen pénzt találnak, azt azonnal végezzék ki. Így igyekeztek elejét venni a sítizmus terjedésének, s az újabb és újabb *kizilbas*-felkeléseknek. Háború kitörése esetén az ellenséges ország nagykövetét is bezárták, hogy elvágják a fő információforrásaitól, sikertelenül.⁵³

4. Következtetések

Tanulmányomban az oszmán hírszerzés átfogó jellemzését végeztem el, az eddigi kutatások fényében. Természetesen ez nem a teljes kép, mivel még sok kérdés vár válaszra. Az oszmánok igyekeztek a hírszerzésüket a saját lehetőségeikhez és képességeikhez igazítani, és így egy rendkívül hatékony szervezetet felépíteni. Ez a szervezet, ellentétben a korabeli „modern” szolgálatokkal, nem volt centralizált. Ennek ellenére jól működött, mert például nem kellett a központnak a sok információt elemeznie és összehasonlítani, lényegében csak a végső döntést kellett meghoznia. Továbbá nem kellett nagy információ-tömegből kihalászni a megfelelő adatokat, hanem csak az igazán fontos híreket kapta meg. Így nem volt leterhelt, kisebb adminisztrációra volt szüksége, és a postai hálózata is megfelelőképpen üzemelhetett. Hátránya viszont az volt ennek a rendszernek, hogy a hírszerzést alapvetően kézben tartó nagyúri udvarok gyakran befolyásolták az uralkodói döntéseket, és céljaik elérése érdekében hamis információkat is átadhattak a központnak.

Az oszmán hírszerzés Európa minden udvarában és országában jelen volt, a hírek azonnal eljutottak a birodalmi központba. Ez köszönhető volt a hatékony postának, amely behálózta a Porta által irányított teljes területet. Az oszmánoknak több kémlet sikerült beépíteniük kulcsfontosságú udvarokba, így a Tudorokhoz is. Sőt, ügynökeik mindenhol jelen voltak, a városokban és a stratégiaileg fontos pontokon egyaránt. Ez a kiterjedt hálózat pedig biztosította a gyors reagálóképességet is. Hátrányt talán az jelentett, hogy a legfontosabb posztokon az érintett államokban élő kisebbségeket alkalmaztak (mórok, zsidók), akik gyakran a keresztény hírszerzőknek is jelentettek.

Jelentős hátrányt hordozott az is, hogy az oszmánok vallási okokból nem tartottak fenn állandó követségeket a keresztény országokban. Ez ugyanis az állandó hírszerzői szervezet kialakításának lehetőségétől fosztotta meg őket, ami viszont a keresztényeknek folyamatos információszerezést biztosított a Porta döntéseiről. Így ehelyett csak az ideiglenes követekre vagy a dragománokra, áttértekre támaszkodhattak. Fontos azt is megjegyezni, hogy az oszmánok a titkosírás terén is le voltak maradva Európa többi részétől. Így az ellenfél képviselői rejtjelezni tudták üzeneteiket, amelyeket a Porta ügynökei nem tudtak megfejteni. A kódokat csak a követségeken dolgozó külföldi ügynökök bevonásával tudták feltörni. Az információáramlást az is gátolta,

⁵³ Gürkan (2020): i. m. 174–175.

hogy az Oszmán Birodalomban nem volt újságkiadás, így a hírek sem terjedhettek olyan gyorsan, mint nyugaton.⁵⁴ Azonban ez nem jelentette azt, hogy az oszmánok ne befolyásolták volna ezek hasábjain a róluk kialakított képet, így hatva ezzel a helyi lakosságra is.

Végezetül el kell mondani: az oszmán elhárítás is remekül dolgozott, annak ellenére, hogy főleg katonai eszközöket használt, és archaikus felépítésű volt. Felhasználták a stratégiai falvak által küldött híreket, illetve időnként nagyobb mértékben eszközöltek lezárásokat, amelyekkel bizonyos információk kiadását, terjedését igyekeztek meggátolni. De természetesen koruk diplomáciai eszközeit is bevetették, amilyen például az idegen ügynökök kiutasítása volt. Bár az oszmán elhárítás főleg katonai volt, de ez semmit nem von le a teljesítményéből. Ennek oka, hogy a határterületek ellenőrzése céljából főleg hagyományos módszereket alkalmaztak (ellenséges csapatok, kémek katonai felderítése). Azonban sem a Habsburg, sem az Oszmán Birodalomnak nem állt rendelkezésre fejlettebb eszköz a határőrizetre. Az pedig külön előnyt jelentett utóbbi számára, hogy míg Európában az elhárító tevékenységet gyakran nem állami szereplők végezték (például Inkvizíció), addig ez náluk mindig a Porta kezében összpontosult. Véleményem szerint így volt képes hatékonysága megőrzésére.

Felhasznált irodalom

- Ágoston Gábor: Információszerzés és kémkedés az Oszmán Birodalomban a 15–17. században. In Petercsák Tivadar – Berecz Mátyás (szerk.): *Információáramlás a magyar és a török végvári rendszerben*. Eger, 1997. 129–156.
- Ágoston Gábor: Európa és az oszmán hódítás. Budapest, Hadtörténelmi Intézet – Európa Könyvkiadó, 2014.
- Gürkan, Emrah S.: *Espionage in the 16th Century Mediterranean. Secret Diplomacy, Mediterranean Go-Betweens and the Ottoman–Habsburg Rivalry*. Doktori értekezés. Washington D.C., Georgetown University, 2012.
- Gürkan, Emrah S.: Fonds of The Sultan. How to use Venetian Sources for Studying Ottoman History? *News on the Rialto*, 32. (2013), 22–28.
- Gürkan, Emrah S.: L'Idra del sultano. Lo spionaggio ottomano nel cinquecento. *Mediterranea*, 13. (2016), 12. 447–476.
- Gürkan, Emrah S.: *A szultán kémei. Oszmán hírszerzési módszerek és ügynökhálózatok a 16. században*. Budapest, Gondolat, 2020.
- Hahner Péter: A velencei hírszerző és biztonsági szolgálatok. In Boda József – Regényi Kund (szerk.): *A hírszerzés története az ókortól napjainkig*. Budapest, Dialóg Campus, 2019. 66–67.
- Ivanics Mária: Tatár kémszolgálat az 1663-as magyarországi hadjáraton. In Petercsák Tivadar – Berecz Mátyás (szerk.): *Információáramlás a magyar és a török végvári rendszerben*. Eger, 1997. 207–227.

⁵⁴ Ágoston (2014): i. m. 111–112.

- Kelenik József: Kémek, hírek, rémhírek. Hírszerzés és hadviselés a dél-dunántúli végeken a 17. század első felében, In Petercsák Tivadar – Berecz Mátyás (szerk.): *Információáramlás a magyar és a török végvári rendszerben*. Eger, 1997. 169–182.
- Pálffy Géza: Hírszerzés és hírközlés a törökkori Magyarországon. In Petercsák Tivadar – Berecz Mátyás (szerk.): *Információáramlás a magyar és a török végvári rendszerben*. Eger, 1997. 33–64.
- Preiss, Reuven A.: *Mongols and Mamluks. The Mamluk-Ilkhanid War 1260–1281*. Cambridge, Cambridge University Press, 1995.

Tartalom

LENDVAI TÜNDE – KRASZNAY CSABA: <i>A SARS-CoV-2-vírus okozta fertőzés terjedését nyomon követő és karanténellenőrző applikációk</i>	3
ERDÉLYI ÁKOS: <i>Az online térben bekövetkező zaklatások lehetséges okai, dinamikai jellegzetességei és megoldási lehetőségei</i>	18
ZOLTÁN LECHNER: <i>Opposing Discourses of Terror: The Use of the Terrorist Label by the Turkish and Russian Governments in the Northern Syrian Conflict</i>	33
ECK GÁBOR: <i>A terrorizmus és az információs tér kapcsolódási pontjai</i>	54
MAJOROSI ÁDÁM: <i>Az Oszmán Birodalom hírszerzése</i>	65