

**PÉCSI TUDOMÁNYEGYETEM ÁLLAM- ÉS JOGTUDOMÁNYI KARÁNAK  
DOKTORI ISKOLÁJA**

---

DR. SERBAKOV MÁRTON TIBOR

**A SZÉLSŐSÉGES TERRORISTA CSOPORTOK  
INTERNETHASZNÁLATÁNAK ELEMZÉSE**

PHD ÉRTEKEZÉS TÉZISEI



Témavezető:

**PROF. DR. GÁL ISTVÁN LÁSZLÓ**

tanszékvezető egyetemi tanár

PÉCS, 2022

# Tartalomjegyzék

<b>I.</b>	<b>BEVEZETÉS.....</b>	<b>3</b>
1.	A TÉMAVÁLASZTÁS INDOKOLÁSA .....	3
2.	A KITŰZÖTT KUTATÁSI FELADAT CÉLKITŰZÉSE, RÖVID ÖSSZEFOGLALÁSA .....	4
3.	AZ ÉRTEKEZÉS SZERKEZETE .....	5
4.	A KUTATÁS NEHÉZSÉGEI ÉS KORLÁTAI .....	6
5.	A KUTATÁS MÓDSZEREI .....	7
6.	A KUTATÁS HIPOTÉZISEI.....	7
<b>II.</b>	<b>ÖSSZEFOGLALÓ: A TUDOMÁNYOS EREDMÉNYEK RÖVID ÖSSZEFOGLALÁSA, AZOK HASZNOSÍTÁSA, ILLETVE A HASZNOSÍTÁS LEHETŐSÉGEI .....</b>	<b>9</b>
<b>III.</b>	<b>SUMMARY.....</b>	<b>17</b>
<b>IV.</b>	<b>A MUNKA TÉMAKÖRÉBŐL KÉSZÜLT SAJÁT PUBLIKÁCIÓK JEGYZÉKE .....</b>	<b>24</b>

# I. BEVEZETÉS

## 1. A témaválasztás indokolása

Schmid 2004-es megállapítása, hogy valószínűleg a terrorizmus a legfontosabb szó a politikai szótárban<sup>1</sup>, napjainkban is igaz, esetleg a koronavírus vagy a migráció előzheti meg. A globalizáció legfőbb biztonsági, rendészeti kihívásai a migráció és a terrorizmus.<sup>2</sup>

Az internet az életünk már megkerülhetetlen, elengedhetetlen része. Sajnos az már a terrorizmusnak is szinte állandó elemévé vált.

A koronavírus (COVID-19) világjárvány felgyorsította a digitális világ felé való elmozdulást.<sup>3</sup> A járvány megfékezésére bevezetett zárlatok idején az online radikalizációnak fokozottan magas a kockázata. A távolságtartási szabályok fokozzák az extrémizmus terjedését. Zárlatok idején otthonrekedt milliók fordulnak az internet és a közösségi média felé.<sup>4</sup> Ezen tényezők miatt is a terroristák internethasználatának kutatása fontosabb, mint valaha.

Természetesen a „(...) terrorcselekmények megakadályozása komplex tevékenységet, és szervezetrendszer igényel,”<sup>5</sup> és úgy vélem, a mai digitalizált világunkban a terrorizmus és a terrorizmus finanszírozása elleni harcban, főleg a terrorcselekmények megelőzésében az internetnek kulcsszerepet kell játszania. Véleményem szerint a legtöbb terrorista akciónak, az azokhoz vezető radikalizáció folyamatának, a szervezésnek etc. van előjele az interneten, de tudni szükséges azt, hogy mit, hol és hogyan kell figyelni. A hatékonyabb terrorizmus és terrorizmusfinanszírozás elleni harc, a terrorcselekmények nagyobb sikerrel történő megakadályozása és a radikalizáció megelőzése szempontjából elengedhetetlen az egyes terrorszervezetek internetes

---

<sup>1</sup> SCHMID, A.: Terrorism - The Definitional Problem. Case Western Reserve Journal of International Law, 2004. Vol. 36. No. 2. 376. o.

<sup>2</sup> RITECZ Gy.: a terrorizmus és a migráció viszonya a számok alapján. Acta Humana, 2016/5. 103. o.

<sup>3</sup> Covid 19 and E-commerce: Findings from a survey of online consumers in 9 Countries. United Nations UNCTAD, 2020. 4. o. [https://unctad.org/system/files/official-document/dtlstictinf2020d1\\_en.pdf](https://unctad.org/system/files/official-document/dtlstictinf2020d1_en.pdf) (2021.06.14.)

<sup>4</sup> MALIK, N.: Self-Isolation Might Stop Coronavirus, but It Will Speed the Spread of Extremism. Foreign Policy. (2020, March 26). <https://foreignpolicy.com/2020/03/26/self-isolation-might-stop-coronavirus-but-spread-extremism/> (2021.06.21.)

<sup>5</sup> KOVÁCS I.: Rendvédelmi ismeretek I. Magyar Rendészettudományi Társaság, Budapest, 2021. 32. o.

aktivitásának beható és naprakész ismerete. Értekezéssel ehhez az ismeretanyaghoz kívánok hozzájárulni.

## **2. A kitűzött kutatási feladat célkitűzése, rövid összefoglalása**

Disszertációmban átfogó képet kívánok nyújtani korunk terroristáinak, különös figyelemmel a szélsőséges iszlám által motivált és a szélsőjobboldali terroristák internethasználatáról, mely méretét tekintve hatalmas léptékű, és kihívást jelentő vállalkozás, számos akadállyal, nehézséggel és kérdéssel.

Bemutatom a terroristák internethasználatának alapvetéseit, hogy általánosságban az egyes terrorszervezetek, terrorista csoportok, magányos terroristák milyen tevékenységek végzésére használják a világhálót. Röviden rávilágítok a terroristák okostelefonos alkalmazás használatára is.

A magyar szakirodalmat vizsgálva látható, hogy dolgozatom hiánypótló területet célzott meg.<sup>6</sup> Jelenleg nem létezik a terroristák internethasználatát mélységeiben tárgyaló monográfia. Értekezésem ezt az űrt kívánja betölteni.

A választott téma (maga a terrorizmus jelensége is) interdiszciplináris megközelítést igényel, ezért a bűnügyi tudományok<sup>7</sup> közül elsősorban a kriminológiai irányából közelítő értekezésem óhatatlanul és szükségesen is átlépi annak határait, és többek között rendészettannal, akár hadtudománnyal is színeződik. A vizsgált tárgyból adódóan informatikai kérdéseket is szükséges érintenem, melyekben olyan mélységekben szándékozom csak elmerülni, amennyire a mű tárgyának megértéséhez feltétlenül szükséges.

Végző célkitűzésem az, hogy a művem a terrorizmus elleni harc szereplői számára a gyakorlatban is hasznosítható tudásanyagot nyújtson, de ha értekezésem az ehhez szükséges színvonalat a legnagyobb igyekezetem ellenére sem éri el, bízom benne, hogy legalább képes lesz a tárgyalt témát illetően termékeny diszkussziót, vitát generálni és a jelen munkánál jobb, további műveket inspirálni.

---

<sup>6</sup> Ugyan az állítás alátámasztásához a magyar szakirodalom felsorolása indokolt lenne, de azt a jelen értekezés terjedelmi korlátai nem teszik lehetővé. A releváns és felhasznált irodalmat az irodalomjegyzékben feltüntettem.

<sup>7</sup> HORNYÁK Sz.: A büntetőjog-tudomány és a bűnügyi tudományok rendszere. In: BALOGH Á. – TÓTH M. (szerk.): Magyar Büntetőjog. Általános Rész. Osiris Kiadó, Budapest, 2015. 31-34. o.

### 3. Az értekezés szerkezete

A téma kontextusba helyezéséhez és megértéséhez elengedhetetlen a terrorizmus definíciójának, típusainak, történetének, és napjainkban történt változásainak bemutatása.

A terrorizmus témáját bármilyen irányban megközelítve az első problémával már akkor szembesülünk, mikor azt szeretnénk eldönteni, hogy egyáltalán mit is nevezünk annak. A terrorizmusnak számtalan definíciója létezik. Még ha el is döntjük, hogy a szakirodalom és különféle szervezetek, kormányok mit tekint terrorizmusnak, akkor sem lehetséges általánosságban a terroristák internethasználatáról írni, mivel a terrorizmusnak sokféle tipizálása is létezik. Az II. fejezetben röviden felvázolom a terrorizmus definíciójának kérdését és a terrorizmus típusait.

Csak a meghatározások és a tipizálás alapvetéseinek tisztázása után érdemes a III. fejezetben a nemzetközi terrorizmus történetét dióhéjban felvázolni, és korunkban a jelenségét illető változásokat bemutatni.

A IV. fejezet a média és terrorizmus kapcsolatának vázlatos történetét és elméletét tárgyalja, és rávilágít arra, milyen változásokat hozott a média és terrorizmus kapcsolatába az internet és a közösségi média megjelenése.

Az V. fejezet a terroristák internethasználatának alapvetéseit mutatja be, hogy a szakirodalom szerint mire használják a terroristák a világhálót, továbbá ebben a fejezetben tisztázom, hogy jelen értekezésben mit értek terroristák internethasználatával, és mit nem.

Úgy vélem, komplexitásuk miatt külön fejezetet érdemel a terroristák dark webes jelenlétének kérdése és a méltatlanul alulkutatott terroristák okostelefonos alkalmazás használatát, melyek a VI. és VII. fejezetben kerülnek bemutatásra.

A VIII. fejezet a terrorizmus finanszírozásának internethez köthető technikáit és forrásait mutatja be.

A IX. fejezet az online történő radikalizáció kérdését tárgyalja, és a terrorcselekményeket előrejelző internetes magatartásokat.

A X. fejezet három szélsőséges iszlám által motivált terrorszervezet, az al-Kaida, az Iszlám Állam (továbbiakban IS) és a Boko Haram internethasználatát illetően próbál átfogó képet nyújtani.

A XI. fejezet a szélsőjobboldali terroristák online jelenlétét tárgyalja.

A XII. fejezet az online terjedő összeesküvés-elméleteket, és az azokhoz fűződő terror-kockázatot tárgyalja, fő fókuszában a The Great Replacement és a QAnon elméletekkel.

Vitatható lehet, hogy az incelek melyik fejezetbe illenek. Érvelni lehetne amellett, hogy a XI. fejezetben lenne a helyük, mint alt-jobb szereplők, de sajátos nézeteik miatt külön, a XIII. fejezetben kerülnek tárgyalásra.

A XIV. fejezetben a 3D nyomtatott lőfegyverek, online elérhető tervrajzaik és ezek terrorista célokra való felhasználhatóságát mutatom be.

A XV. fejezet a koronavírus (COVID-19) pandémia hatását vizsgálja a terroristák internethasználatára.

A XVI. fejezet tárgya a terrorizmus elleni küzdelem és a terrorcselekmények megelőzésének egyes elméleti kérdései, különös tekintettel az internethez kötődő megelőzési módszerek.

#### **4. A kutatás nehézségei és korlátai**

Fontos volt számomra, hogy a munkám a gyakorlat, a terrorizmus elleni harc szereplői számára is felhasználható legyen, ezért a magyar nyelvű és idegen nyelvű szakirodalom mellett kutatásom során kifejezetten sok internetes forrásra is kellett támaszkodnom, melynek okai a következők: Internethez kötődő témám nagyon modern, napról napra formálódik. Számos ahhoz kötődő forrás (még) csak az interneten lelhető fel, és a legtöbb esetben csak idegen nyelven. Számos kérdést, amit dolgozatomban vizsgálok, nem is dolgoz még fel tudományos munka, amire támaszkodhatnék. Témám nem minden aspektusával foglalkozik magyar szerző, annak erősen nemzetközi, globalizált természete miatt sok külföldi forrásból kellett dolgoznom. Az internetes források különösen kritikus értékelést igényeltek.

Jelen dolgozatnak nem tárgya a terroristák által elkövetett kibertámadás, a kiberterrorizmus. Jelen disszertáció fókusza a terroristák internethasználatának egyes aspektusai, nem pedig az ehhez fűződő elhárítási, eltávolítási módok, technikák, kérdések, melyeket csak röviden tárgyal.

Minden típusú terrorista internethasználatának minden egyes aspektusát a területi korlátok miatt nem tudom tárgyalni, a vizsgált témát illetően szelektálni kényszerültem. Számos, a dolgozattól a területi korlátok miatt kimaradt aspektus külön műben való feldolgozást, vizsgálatot érdemelne. Külön vizsgálatot és bemutatást érdemelnének még, a teljesség igénye nélkül: a terrorista tartalmak internetről való eltávolítása, a terroristák online aktivitásának visszaszorítására hozott jogszabályok, egyezmények, irányelvek, a szabályozás lehetőségei, az erre szolgáló gépi eszközök, az egyes felületek felhasználási

feltételei és irányelvei, a terrorista tartalmak tekintetében, az EU válaszai a terroristák internethasználatára, a téma magyar vonatkozásai, a magyar és további külföldi esetek elemzése a terroristák internethasználata szempontjából, más típusú terroristák, más terrrorszervezetek, magányos terroristák internetes aktivitása is. Valamennyi fejezet által taglalt kérdés további vizsgálatra, kifejtésre volna érdemes.

## **5. A kutatás módszerei**

Szekunder kutatást végeztem, mely során a témához fűződő terjedelmes mennyiségű magyar és idegen nyelvű szakirodalmat – monográfiákat, tankönyveket, tanulmányköteteket, szaktanulmányokat, továbbá számos terrorizmussal foglalkozó szervezet dokumentumait, jelentéseit, bírósági határozatokat és jogszabályokat, számos magyar és idegen nyelvű internetes forrást tekintettem át, elemeztem, értékeltem és vetettem össze.

Elsődleges adatra épülő vizsgálatot a téma specifikumai miatt nem végeztem. Az interjú lehetőségétől azért kellett eltekintennem, mert terrorista vélhetően nem adna, terrorelhárító pedig nem adhat ki adatokat, információt a témát illetően.

## **6. A kutatás hipotézisei**

A kutatásom során a következő hipotéziseket fogalmaztam meg:

1. A terrorcselekmények gyakori elkövetési módjai és közvetlen céljai 9/11 óta változáson mentek át.
2. Az internet és a közösségi média elterjedése drasztikus változást hozott a terrorizmus jelenségébe.
3. A dark web napjaink terroristáinak fontos eszköze.
4. A terroristák kihasználják az okostelefonos alkalmazások előnyeit.
5. Az internethez kötődő terrorizmus finanszírozási források és technikák, főleg a kriptovaluták használata egyre nagyobb fenyegetést jelentenek.
6. A radikalizáció folyamatában korunkban kulcsszerepet játszik az internet.
7. Az interneten a terrorcselekményének többségének vannak előjelei.
8. Nem csak a muszlim elkövetők képviselik az egyedüli komoly terrorveszélyt.
9. Több online terjedő összeesküvés-elmélet terror-kockázatot képvisel.
10. Az incel elkövetők terroristák, és a főként online táplált és inspirált nőgyűlölő

terrorizmusuk valós fenyegetést képvisel.

11. Az utóbbi évekbeli szélsőjobbaldali terrorhullámba tartozó támadások között online kapcsolat állhat fenn.

12. Az online terjedő 3D lőfegyver tervrajzok komoly (terror-) veszélyt képviselnek.

13. A koronavírus (COVID-19) világjárvány hatott a terrorizmusra, és megnövelte a terroristák internethasználatának fenyegetését is.

14. A terroristák internethasználatának behatóbb ismerete hozzájárulhat a terrorcselekmények hatékonyabb megelőzéséhez.



## **II. ÖSSZEFOGLALÓ: A TUDOMÁNYOS EREDMÉNYEK RÖVID ÖSSZEFOGLALÁSA, AZOK HASZNOSÍTÁSA, ILLETVE A HASZNOSÍTÁS LEHETŐSÉGEI**

Jelen doktori értekezés tárgya a szélsőséges iszlám által motivált és a szélsőjobboldali terroristák internethasználatának egyes aspektusai.

A téma kontextusba helyezéséhez és megértéséhez elengedhetetlen a terrorizmus definíciójának, típusainak, történetének, és napjainkban történt változásainak bemutatása.

A terrorizmus témáját bármilyen irányban megközelítve az első problémával már akkor szembesülünk, mikor azt szeretnénk eldönteni, hogy egyáltalán mit is nevezünk annak. A terrorizmusnak számtalan definíciója létezik. Még ha el is döntjük, hogy a szakirodalom és különféle szervezetek, kormányok kiket tekintenek terroristáknak, akkor sem lehetséges általánosságban „a terroristák” internethasználatáról írni, mivel a terrorizmusnak sokféle tipizálása is létezik. Röviden felvázoltam a terrorizmus definíciójának kérdését és a terrorizmus típusait.

A meghatározások és a tipizálás alapvetéseinek tisztázása után dióhéjban felvázoltam a nemzetközi terrorizmus történetét, és rávilágítottam korunkban a jelenségét illető fő változásokra.

Tárgyaltam a média és terrorizmus kapcsolatának vázlatos történetét és elméletét, és rámutattam arra, milyen változásokat hozott a média és terrorizmus kapcsolatába az internet és a közösségi média megjelenése.

Ezt követően felvázoltam a terroristák internethasználatának alapvetéseit, hogy a szakirodalom szerint mire használják a terroristák a világhálót, továbbá tisztáztam, hogy jelen értekezésben mit értek terroristák internethasználatával, és mit nem.

Tárgyaltam a terroristák dark webes jelenlétének kérdését és a méltatlanul alulvizsgált terroristák okostelefonos alkalmazás használatát.

Bemutattam a terrorizmus finanszírozásának internethez köthető technikáit és forrásait.

Tárgyaltam az online történő radikalizáció kérdését, és a terrorcselekményeket előrejelző internetes magatartásokat.

Három szélsőséges iszlám által motivált terrorszervezet, az al-Kaida, az Iszlám Állam (továbbiakban IS) és a Boko Haram internethasználatát illetően próbáltam átfogó képet

nyújtani.

Tárgyaltam a szélsőjobboldali terroristák online jelenlétét, és a 2019-2020-as szélsőjobboldali terrorhullámot és azok elkövetőinek internethasználatát.

Vizsgáltam az online terjedő összeesküvés-elméleteket terror-kockázat szempontjából, fő fókuszban a The Great Replacement és a QAnon elméletekkel.

Bemutattam a különösen internet-orientált, nőgyűlölő inceket és a hozzájuk fűződő fő elkövetéseket.

Elemeztem a 3D nyomtatott lőfegyverek, online elérhető tervrajzaik és ezek terrorista célokra való felhasználhatóságát.

Vizsgáltam a (COVID-19) pandémia hatását a terrorizmus jelenségére és a terroristák internethasználatára.

Tárgyaltam a terrorizmus elleni küzdelem és a terrorcselekmények megelőzésének egyes elméleti kérdéseit, különös tekintettel az internethez kötődő megelőzési módszereket.

Végül a témát illetően javaslatokat fogalmaztam meg.

Hipotéziseimet illetően a következő eredményekre jutottam:

1. A terrorcselekmények gyakori elkövetési módjai és közvetlen céljai 9/11 óta változáson mentek át.

Az utóbbi évtized, főleg körülbelül az utóbbi 5-6 év során elterjedtek az olcsó és egyszerű, puha célpontok elleni terrortámadások, például gázolások, késelések, lövöldözések, és majdnem eltűntek a gépeltérítések és az olyan elkövetések, melyek során a terroristák követelést terjesztenek elő. Az elkövetések fókuszában az áldozatok számának maximalizálása, az ölés áll.

Az olcsó, egyszerű, szinte semmi szervezést és anyagi forrást nem igénylő terrorcselekmények rendkívül nehezen előzhetőek meg.

2. Az internet és a közösségi média elterjedése drasztikus változást hozott a terrorizmus jelenségébe, megkönnyítve azt.

A terrorizmus jelenségébe hatalmas változást hoztak a modern technológia lehetőségei, köztük az internet, a közösségi média, az okostelefonok és az azokhoz kötődő alkalmazások és a 3D nyomtatás elterjedése és fejlődése.

Az internet és a közösségi média elterjedése gyökeresen megváltoztatta a terrorizmus

„játékszabályait”, nagyban megkönnyítve azt. Az internetet a terroristák számos tevékenység végzésére használhatják, többek között propagandájuk terjesztésére, elkövetéseik élő közvetítésére, kommunikációra, koordinálásra, támadások elkövetésére való felszólításra, oktatásra, adományok gyűjtésére, célpontokról információ gyűjtésére etc. Ezek az internet nyújtotta előnyök hatalmas segítséget jelentenek a terroristák számára, számtalan módon és nagyban megkönnyítve korunk terrorizmusát: Terroristák nemzeteken átívelően tudják egymással valós időben, ingyen tartani a kapcsolatot, a terrorizmus elméleti alapjait, a „know how-jait” az otthonuk kényelméből, az interneten keresztül már el tudják sajátítani, támogatóiktól adományokat kérhetnek és kaphatnak a világ minden részéről, akik akár nem is feltétlenül vannak tudatában annak, hogy terrorizmust finanszíroznak etc.

A közösségi média széleskörű használatának elterjedését kihasználták a terroristák is. Ezek a felületek számtalan emberhez juthatnak el a szűretlen tartalmaikkal.

Mielőtt a közösségi média felületek elkezdtek koordináltan és erélyesen fellépni ellenük, ezeket a platformokat el tudták lepni a terroristák, melyre jó példa az IS Twitteren végzett tevékenysége 2014-2015-ben. Az ilyen tevékenységeik elleni fellépés rendkívül nehéz, azokhoz gépi módszerek is szükségesek, melyek megkerülésére a terroristák is fejlesztettek ki módszereket, melyre példa az IS Facebookon használt eltávolítást megkerülő taktikái.

### 3. A dark web napjaink terroristáinak fontos eszköze.

Az internet deep web rétegéhez tartozó, számos illegális tevékenységnek helyt adó dark web használatával a terroristák kiegészítik a felszíni weben végzett tevékenységeiket.

2015 után a felszíni webről való „elüldözésük” után a dark webet fokozottabban használják, ahol nehezebben megfigyelhetőek, de annak a felszíni webhez képest nehezkesebb és nehezebben elérhető felülete miatt a terroristák is nehezebben tudják elérni egymást és a közönségüket. Több szerző szerint hiba volt a dark webig száműzni őket, mivel ott könnyen szem elől téveszthetőek. A dark webről számos illegális szolgáltatás, és akár fegyverek is vásárolhatók.

### 4. A terroristák kihasználják az okostelefonos alkalmazások előnyeit.

A terroristák élnek az okostelefonos alkalmazások nyújtotta előnyökkel, azokkal végzett tevékenységeik szinte megegyeznek az interneten végzettekkel. Számos alkalmazást

tevékenységeik biztonságosabb végzéséhez, titkos kommunikációjukhoz, adományok kéréséhez, másokat propagandájuk terjesztésére használnak. Hamis alkalmazások fejlesztése, vagy ezek feltörése lehetőséget biztosít a terroristák megfigyelésére.

5. Az internethez kötődő terrorizmus finanszírozási források és technikák, főleg a kriptovaluták használata egyre nagyobb fenyegetést jelentenek.

A terrorizmus finanszírozásában a hagyományos technikák mellett már megjelentek a modern technológiához kötődők is. Az internet kiváló eszközt nyújt ahhoz, hogy terroristák adományokat akár virtuális fizetőeszközökben, immár nemzetközi szinten, akár fedett vagy explicit módon kérjenek és kapjanak támogatóiktól és mit sem sejtő donoroktól.

A szerzők egyetérteni látszanak abban, hogy a terrorizmus finanszírozás internethez fűződő technikai és módszerei jelentőségük tekintetében még a hagyományos technikák és módszerek mögött helyezkednek el, de a jövőben relevanciájuk nőhet. A terrorizmus elleni küzdelem szereplői általi figyelemmel kísérésük épp ezért elengedhetetlen fontosságú.

Különösen aggályos, hogy az utóbbi években elterjedt olcsó, egyszerű terrortámadásokhoz szinte semmilyen finanszírozásra nincsen szükség, tehát ezeket nem lehet a terrorizmus finanszírozás elleni harc eszközeivel megelőzni.

6. A radikalizáció folyamatában korunkban kulcsszerepet játszik az internet.

Az interneten a terroristák számtalan felületen és módon terjeszthetik ideológiájukat, propagandájukat, különféle anyagaikat, szabadon kommunikálhatnak mely valószínűleg komoly szerepet játszik korunkban a terrorizmusra való radikalizáció folyamatában. Számos terrorcselekményt elkövető személy online radikalizálódott. Megjelent az online egymást inspiráló elkövetők terrorhullámának jelensége, mely során az elkövetők egymást láncreakció-szerűen inspirálhatják, melyet illusztrál a 2019-2020-as szélsőjobboldali terrorhullám. Az internet miatt a terrorszervezetekhez tartozás akár már egyéni megítélés kérdése is lehet.

A terrorcselekmények megelőzése szempontjából kritikus fontosságú a különböző online található radikalizáló anyagok eltávolítása, az ellenük oktatással, felvilágosítással történő küzdelem.

7. Az interneten a terrorcselekményének többségének vannak előjelei.

„Az internet sosem felejt”, minden interneten végzett tevékenységnek digitális nyoma van. Egy személy radikalizációs folyamatának, egy terrorcselekmény megszervezésének, az arról való kommunikációnak, a szükséges eszközök beszerzésének, az online végzett terrorizmus finanszírozásnak sokszor vannak online jelei. Az olcsó, egyszerű, szinte semmi szervezést és anyagi forrást nem igénylő terrorcselekmények nehezen megelőzhetők, esetleg az elkövető online radikalizációjának és egyéb terrorcselekményt előrejelző magatartásainak, például szándéka szivárogtatásának lehetnek nyomai.

A nehézséget ezeknek az időben történő felfedezése, felismerése, valós fenyegetésüknek kritikus felmérése jelenti. Problematikus annak a pontos ismerete, hogy milyen formát öltenek, és hol történnek a terrorcselekmény elkövetésére utaló előjelek, például a szándék harmadik személy irányába történő szivárogtatása, egy személy radikalizációs folyamatának online jelei etc. Nehézkes a valódi és a nem komoly online szándéknyilatkozatok elhatárolása, és a radikalizáció sem feltétlenül vezet terrorcselekmények elkövetéséhez.

Elengedhetetlen a terroristák internethasználatának részletes, pontos, és naprakész ismerete, továbbá az információk/adatok felfedezéshez és értékeléséhez emberi és gépi módszerek és szakértők alkalmazása szükséges.

8. Nem csak a muszlim elkövetők képviselik az egyedüli komoly terrorveszélyt.

Az utóbbi évek során globális szinten fokozódott a szélsőjobboldalhoz köthető erőszak. Egyre gyakrabban történnek szélsőjobboldali nézeteket által motivált terrorcselekmények. 2019-2020-ban egy egymás által online inspirált terrorhullámot hajtottak végre egymástól látszólag független elkövetők.

A szélsőjobboldali terrorizmust nem szabad kevésbé fenyegetőként kezelni, mint a szélsőséges iszlám által motiváltat, ugyanis az komoly és fokozódó fenyegetést képvisel, ezért fokozott figyelmet és kutatást igényel meg.

A szélsőjobboldali terror „játékosítása”<sup>8</sup> és az ahhoz kapcsolódó versengés, fokozódási kényszer az online fórumokban egy rendkívül aggasztó jelenség, melyet nem szabad

---

<sup>8</sup> EVANS, Robert: The El Paso Shooting and the Gamification of Terror. Bellingcat. (2019, August 4). <https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/> (2022.02.09.)

szem elöl téveszteni. A terrorizmus témájának elemzése során hiba azt csupán a muszlim elkövetőkre leszűkíteni, mivel a terrorizmus jelensége ennél sokkal tágabb kategória. Úgy vélem szakirodalomban több szónak kellene esnie a szélsőséges iszlám terrorizmuson kívüli más terrorizmus típusokról is.

9. Több online terjedő összeesküvés-elmélet terror-kockázatot képvisel.

Radikalizáló ereje miatt különösen nagy terror-veszélyt képvisel a „The Great Replacement elmélet”, mely a 2019-2020-as szélsőjobb oldali terrorhullám elkövetőinek manifesztumaiban is visszaköszön.

A QAnon összeesküvés-elméletéhez számos erőszakos cselekmény köthető. 2021. január 6-án is számos hívője jelen volt az Egyesült Államok Capitoliumának ostrománál, melyet többen terrorizmusnak tituláltak, köztük Joe Biden is.

A pandémia alatti bizonytalan időkben sok, egyre elszigeteltebb ember összeesküvés-elméletekkel próbál választ adni a korunkat illető nehéz kérdésekre, bizonytalanságokra. Különösen aggasztóak a koronavírushoz kapcsolódó összeesküvés-elméletek.

10. Az incel elkövetők terroristák, és a főként online táplált és inspirált nőgyűlölő terrorizmusuk valós fenyegetést képvisel.

Az incelek rendkívül internet-orientáltak, maga a mozgalom is az interneten született, és egymást is ott ideologizálják, radikalizálják, kergetik egymást egyre mélyebb kétségbeesésbe, melyből többük úgy érzi, hogy végül csak a terrorizmus jelenthet kiutat. Elméletileg létezhet az incel és a dzsihád közötti átjárás, az ún. „jihadpill” magukéva tételével, mely annyit jelent, hogy néhányuk úgy véli, dzsihadistává válással nőkhöz juthatnak.

11. Az utóbbi évekbeli szélsőjobb oldali terrorhullámba tartozó támadások között online kapcsolat állhat fenn.

Rendkívül veszélyes jelenség a terrorhullám. A jövőben egy ilyen hullám felismerése kritikus fontosságú, figyelni kell az elkövetők által közzétett manifesztumokra, és az ezekben fellelhető közös elemekre. Kutatást igényel, hogy egy ilyen hullámot hogyan lehet megakadályozni, azt megtörni.

12. Az online terjedő 3D lőfegyver tervrajzok komoly (terror-) veszélyt képviselnek.

3D nyomtató és legálisan és könnyen beszerezhető eszközök (nyomtatáshoz szükséges anyag, esetleg fémcső etc.) beszerzése után, egy kis online utánajárással, a hatóságok előtt ismeretlenül már otthonról is gyártható többféle 3D nyomtatott lőfegyver. Ezek terrorcselekmények elkövetése során való használata még nem olyan elterjedt, de a technológia elkerülhetetlen fejlődésével a jövőben fokozódhat a használatuk.

13. A koronavírus (COVID-19) vilájárvány hatott a terrorizmusra, és megnövelte a terroristák internethasználatának fenyegetését is.

A terroristák kihasználhatják az állami szervek a pandémia elleni küzdelem miatti leterheltségét, és a potenciálisan kialakuló biztonsági réseket. Szélsőséges nézeteket vallók maga a vírus fegyverként való használatát is javasolták.

A koronavírus pandémia megfékezése miatt bevezetett zárlatok és távolságtartási előírások miatt drámaian megnőtt az emberek online töltött ideje. A hosszú izoláció alatt sokan elmagányosodnak, kétégbeesettebbek lesznek, a pandémia a mentális egészségükre is hatással van, mely a fokozott online töltött idővel kombinálva azt eredményezi, hogy sebezhetőbbek lesznek általánosságban a szélsőségek, a terroristák online terjesztett ideológiájával szemben, fogékonyabbak lesznek a radikalizációra és az összeesküvés-elméletekre. A terroristák ezeket felismerve megkettőzik az ideológiájuk online terjesztésére tett erőfeszítéseiket.

14. A terroristák internethasználatának behatóbb ismerete hozzájárulhat a terrorcselekmények hatékonyabb megelőzéséhez.

A terroristák internethasználatának bővebb, pontosabb ismerete által ezen internethez kötődő tevékenységeik ellen a terrorizmus elleni harc szereplői is hatékonyabban tudnak fellépni (a kommunikációjuk kifürkészésével, megzavarásával, anyagaik eltávolításával etc. is) mely közvetetten és akár közvetlenül eredményezheti terrorcselekmények megelőzését, vagy hozzájárulhat ahhoz.

Az értekezésemben a terroristák internethasználatának számos vetületére világítottam rá, melyek alapján belátható, hogy az internet korunk terrorizmusát számos módon segíti, a radikalizációs folyamatban is fontos szerepet játszhat, számos terrortámadásnak, azok elkövetőinek vagy azok finanszírozásának vannak közvetve vagy közvetlenül

internethez kötődő elemei.

Az értekezésem tudományos eredményei segítséget nyújthatnak, a terrorizmus elleni harc szereplői, a bűnüldöző szervek, a titkoszolgálatok számára a terrorizmus és a terrorizmus finanszírozása elleni küzdelem terén, de akár a jogalkotást is orientálhatják. Kutatásom a témát és annak egyes aspektusait illető további kutatást, termékeny vitát ösztökélhet, és hozzásegíthet a terrorizmus jelenségének mélyebb megértéséhez.



### **III. SUMMARY**

This dissertation aims to analyse some aspects of the internet usage of radical Islamic and right-wing terrorists.

In order to understand and contextualise the topic at hand, it is essential to examine the definitions, the types, the history and the recent changes of terrorism.

When we approach the topic of terrorism we already meet the first issue when we try to define it. Terrorism has countless definitions.

Even if we decide who is considered a terrorist by the scientific literature and various organizations and governments, it is not possible to write about the internet usage of “terrorists” in general, as there are many different types of terrorism.

I have briefly outlined the questions of the definition and the types of terrorism. After clarifying the definitions and the basics of the types, I have outlined the history of international terrorism in a nutshell and highlighted the main changes in its phenomenon in our time.

I have briefly outlined the history and theory of the relationship between media and terrorism and pointed out the changes that the advent of the internet and social media has brought to their relationship.

After that, I examined the basics of the internet usage of terrorists according to the literature. I clarified what I mean by the internet usage of terrorists in my dissertation.

I discussed the issue of the dark web presence of terrorists and their use of smartphone applications, which is an undeservedly under-researched topic.

I have presented the internet-related techniques and sources of terrorist financing.

I have examined the issue of online radicalisation and the online warning behaviors before acts of terrorism.

I have attempted to give a comprehensive picture of the online activities of three terrorists organisations motivated by radical Islam, namely the Al-Qaeda, the Islamic State, and Boko Haram.

In my dissertation I have examined the online presence of right-wing terrorists and the far-right terror-wave of 2019-2020 and the internet usage of their perpetrators.

I have examined online conspiracy theories in terms of terrorist risk, with giving special attention to The Great Replacement and the QAnon theories.

I have introduced the especially internet-oriented, misogynist incels, and their most relevant attacks.

I have analyzed the usability of 3D printed firearms, and their blueprints available online for terrorist purposes.

I have examined the effect of the COVID-19 pandemic on the phenomenon of terrorism and the internet usage of terrorists.

I have discussed some theoretical issues regarding the fight against terrorism and the prevention of terrorist attacks, in particular the prevention methods associated with the internet.

Finally, I have made suggestions on the subject.

Regarding my hypotheses, I came to the following results:

1. The common modus operandi and the direct goal of terrorist attacks have gone through changes since 9/11.

In the last decade, especially in the last 5-6 years, cheap and simple terrorist attacks against soft targets, such driving into crowds, knife attacks have become widespread, and hijackings and attacks where perpetrators present their demands have almost disappeared. Terrorist attacks now focus on maximising the number of victims, their goal is to kill as many people as possible. Cheap, simple attacks which require almost no financial funding and organising are very difficult to prevent.

2. The internet and the spread of social media has brought a drastic change in the phenomenon of terrorism, making it easier.

The phenomenon of terrorism has been vastly transformed by modern technology, including the internet, social media, smartphones and smartphone applications, and 3D printing.

The spread of the internet and social media has radically changed the “rules of the game” of terrorism, making it much easier. The internet can be used by terrorists to carry out a number of activities, including spreading their propaganda, broadcasting their crimes, communicating, coordinating, inciting attacks, educating, collecting donations, gathering information about targets etc. These benefits of the internet are a huge help to terrorists, greatly facilitating the terrorism of our time in many ways: On the internet, terrorists can keep in touch with each other in real time, for free, they can learn the basics and the know-how of terrorism from the comfort of their homes, they

can ask for donations from their supporters, from all over the world, who might not even be aware of the fact that they financing terrorism etc.

Terrorists exploited the increased use of social media. On these platforms their unfiltered contents are able to reach countless people.

Before social media platforms began to act remove their content in a coordinated and vigorous manner, these platforms were swarmed by terrorists. IS's Twitter activity in 2014-2015 is a good example. Combating such activities is extremely difficult, and also requires automated methods, which terrorists have developed tactics to circumvent, for example IS has found ways to avoid automated detection of Facebook.

### 3. The dark web is an important tool in the hands of today's terrorists.

By using the dark web, which belongs to the deep web layer of the internet and hosts many illegal activities, terrorists complement their activities on the surface web.

After 2015, after their "expulsion" from the surface web, their use of the dark web increased, where it is more difficult to observe their activities, but because of its limited usability and because it is more inaccessible compared to the surface web, it is also more difficult for terrorists to reach each other and their audience.

According to several experts, it was a mistake to „banish" them to the dark web, as they much harder to track there. Many illegal services and even weapons can be purchased from the dark web.

### 4. Terrorists exploit the advantages presented by smartphone applications.

Terrorists exploit the benefits of smartphone applications, and their facilitated by these are almost the same as those of the internet. They use many applications to conduct their activities more securely, to communicate secretly, to solicit donations, and to spread their propaganda to others. Developing fake applications or hacking them provides an opportunity to monitor terrorists.

### 5. The threat of the internet-related techniques and sources of terrorist financing, especially the use of cryptocurrencies are a growing threat.

In addition to traditional techniques, those associated with modern technology have also appeared in the financing of terrorism. The internet is an excellent tool for terrorists to

internationally, covertly or explicitly solicit and receive donations from their supporters and unsuspecting donors, even in virtual currencies.

The experts seem to agree that the techniques and methods of terrorist financing on the internet are still behind traditional techniques and methods in terms of their importance, but their relevance may increase in the future. Monitoring by those involved in the fight against terrorism is therefore essential.

It is particularly worrying that the cheap, simple terrorist attacks that have become commonplace in recent years require almost no funding, so they cannot be prevented by the means of combating the financing of terrorism.

#### 6. The internet plays a key role in today's radicalisation.

On the internet, terrorists can spread their ideology, propaganda, various materials and they can communicate freely in countless ways. Terrorists's materials online are likely to play a major role in the the radicalisation process leading to terrorism today. Several people who committed acts of terrorism have been radicalised online.

The phenomenon of the terror wave in which online perpetrators inspire each other like a chain reaction has emerged, illustrated by the far-right terror wave of 2019-2020. Because of the internet, nowadays belonging to a terrorist organization might even be a matter of individual judgment. The removal of various radicalising materials found online and the fight against them through education and information are critical for the prevention of terrorist attacks.

#### 7. Most acts of terrorism have warning signs on the internet.

“The internet never forgets,” every activity on the internet leaves a trace, digital evidence.

There are often online signs of a person's radicalisation process, the organisation of a terrorist act, the communication about it, the acquisition of the necessary tools, and the financing of terrorism online all leave traces, all have online signs.

Inexpensive, simple terrorist acts that require almost no organisation or financial resources are difficult to prevent, but the perpetrators's radicalisation process, or other warning signs before terrorist attacks such as leak of intent might sometimes have early signs online. The difficulty is discovering these signs in time, recognising them, and

critically assessing their real threat.

It is problematic to know exactly what form and where the signs of preparation of a terrorist attack act take place, such as the leak of intent to a third party, the online signs of a person's radicalisation process, etc. It is difficult to distinguish between serious and non-serious online declarations of intent, and radicalisation does not necessarily lead to terrorism.

Detailed, accurate, and up-to-date knowledge of the internet usage of terrorists is essential, as well as the use of human and automated methods and experts to discover and assess the discovered information/data.

#### 8. Not only muslim attackers pose serious terrorist threat.

Violent acts connected to the far right have increased globally in recent years. Terrorist attacks motivated by far-right views are becoming more frequent. In 2019-2020, a wave of terror in which attackers were inspired by each other was carried out by seemingly independent perpetrators.

Far-right terrorism should not be treated as less of a threat than that motivated by radical Islam, as it poses a serious and growing threat and therefore requires increased attention and research. The “gamification”<sup>9</sup> of far-right terror and the associated competition, the compulsion escalate in online forums, is an extremely worrying phenomenon that should not be overlooked. In analyzing the subject of terrorism, it is a mistake to limit it to muslim perpetrators only, as the phenomenon of terrorism is a much broader category.

I believe that more should be said in the literature about other types of terrorism than radical Islamic terrorism.

#### 9. Several consiracy theories which circulate online pose a terrorist risk.

Because of its radicalising potemntial, the „The Great Replacement” theory poses an especially serious terror-threat. This theory was referenced in the manifestos of the perpetrators of the right-wing terror-wave of 2019-2020.

Several violent acts can be connected to the QAnon conspiracy theory. On January 6, 2021, several believers were present at the siege of the U.S. Capitol, which several

---

<sup>9</sup> EVANS, Robert: The El Paso Shooting and the Gamification of Terror. Bellingcat. (2019, August 4). <https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/> (2022.02.09.)

people, including Joe Biden described as terrorism.

In the uncertain times of the pandemic, many increasingly isolated people are trying to answer the difficult questions and uncertainties of our time with conspiracy theories. Conspiracy theories related to the coronavirus are of particular concern.

10. Incel attackers are terrorists, and their primarily online inspired misogynist terrorism poses a real threat.

Incels are extremely internet-oriented, the movement itself was born online, and there they ideologise, radicalise, and drive each other into deeper despair, from which many of them feel that terrorism can be the only way out. Theoretically, there could be a path between incel and jihad, by embracing the so-called “jihadpill,” which means that some incels believe they can only get women by becoming a jihadist.

11. There might be common online elements in the attacks of the right-wing terror wave of 2019-2020.

The terror-wave is an extremely dangerous phenomenon. In the future, recognising such a wave is critical. It is essential to study the manifestos posted on the internet by the perpetrators and to discover and assess the common elements found in them. The prevention and breaking such a wave requires research.

12. The 3D printed firearm blueprints available online pose a serious (terror-) threat.

After purchasing a 3D printer and legally and readily available tools (printing material, a metal tube, etc.), with the help of a some online research, several 3D printed firearms can be manufactured from home without the knowledge of the authorities. Their use in terrorist attacks is not yet widespread, but with the inevitable development of technology, their use may increase in the future.

13. The coronavirus (COVID-19) pandemic had an effect on terrorism, and increased the threat posed by terrorists’ internet related activities.

Terrorists may take advantage of potential security vulnerabilities that may arise when the governments are occupied with fighting the pandemic. Several extremists have also

suggested the use of the virus itself as a weapon. Lockdowns and social distancing rules introduced to curb the coronavirus pandemic have dramatically increased people's time spent online.

During long isolation, many people become lonely and desperate, and the pandemic affects their mental health, which, combined with increased time spent on the internet, makes people more vulnerable to the ideology of terrorists spread online, and to extremism, conspiracy theories and radicalisation in general. Terrorists recognizing these effects of the pandemic and they are duplicating their efforts to spread their ideology online.

14. A better understanding of the use of the internet by terrorists can contribute to more effective prevention of terrorist attacks.

In my dissertation I have highlighted many aspects of the use of the internet by terrorists, which show that the internet contributes to terrorism in many ways, plays an important role in the radicalisation process, and many terrorist attacks, their perpetrators or their financing have many direct or indirect elements related to the internet.

By gaining a broader and more accurate knowledge of terrorists' internet related activities, counter-terrorism actors can also take more effective action against these activities (by scouting, disrupting, removing material, etc.), which actions can directly or indirectly contribute to the prevention of terrorist attacks.

The scientific findings of my dissertation can be helpful to the actors in the fight against terrorism, law enforcement agencies, secret services in the fight against terrorism and terrorism financing, but they may also be used to orient legislation. My research might encourage further research on the topic and some aspects of it, or a fruitful debate, and a deeper understanding of the phenomenon of terrorism.

## **IV. A MUNKA TÉMAKÖRÉBŐL KÉSZÜLT SAJÁT PUBLIKÁCIÓK JEGYZÉKE**

GÁL, István László – SERBAKOV, Márton Tibor: How Acts of Terrorism are Financed and Orchestrated in Secrecy Today: Criminal Offenses, Donations, Legal Businesses and Smartphone Applications. *Journal Of Eastern-European Criminal Law*, 2019. Vol. 6. No. 1. 66–76. o.

SERBAKOV Márton Tibor: A Boko Haram internethasználatának evolúciója. In: KÖHALMI László (szerk.): PhD Tanulmányok 15. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2021. 137–153. o.

SERBAKOV Márton Tibor: A Dohány utcai zsinagógánál történt két merénylet a korabeli jogszabályok és antiszemita szervezetek tükrében. *Jogtörténeti Szemle*, 2021/2. 32–40. o.

SERBAKOV Márton Tibor: A koronavírus (COVID-19) pandémia hatása a globális terrorizmus és extrémizmus fenyegetésére. In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XXII.: A Hadtudománytól A Rendészettudományig – Társadalmi Kihívások A Nemzeti Összetartozás Évében. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, 2020. 323–330. o.

SERBAKOV Márton Tibor: A terroristák drónhasználata. *Nemzetbiztonsági Szemle*, 2019/4. 30–43. o.

SERBAKOV Márton Tibor: A terroristák internethasználatára. *Büntetőjogi Szemle*, 2018/2. 85–93. o.

SERBAKOV Márton Tibor: A terrorizmus definíciójának kérdése. *Büntetőjogi Szemle*, 2019/2. 87–100. o.

SERBAKOV Márton Tibor: Az Iszlám Állam finanszírozási forrásai. In: TÓTH Dávid – BENDES Ákos László – DIÓSI Szabolcs – GÁSPÁR Zsolt – PROJICS Nárcisz – SERBAKOV



Márton Tibor – SZÍVÓS Alexander Roland (szerk.): I-II. Konferenciakötet. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2021. 137–149. o.

SERBAKOV Márton Tibor: Az online felületek és okostelefonos alkalmazások mint a terrorcselekmények előrejelző rendszerei. In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.). Pécsi Határőr Tudományos Közlemények XXI.: A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2019. 119–124. o.

SERBAKOV Márton Tibor: Az utóbbi évek jelentős nemzetközi szélsőjobboldali terrorcselekmények elkövetőinek internethasználata és globális összefüggései. Jogelméleti Szemle, 2020/3. 60–69. o.

SERBAKOV Márton Tibor: Gondolatok a terrorizmus elleni küzdelem és a terrorcselekmények megelőzésének elméleti kérdéseiről, különös tekintettel az internethez kötődő megelőzési módszerekről. KRE-DIT: A KRE-DOK ONLINE TUDOMÁNYOS FOLYÓIRATA, 2020/1.

SERBAKOV Márton Tibor: Kriminálitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem. Büntetőjogi Szemle, 2020/1. 91–107. o.

SERBAKOV Márton Tibor: Legújabb tendenciák a terroristák internethasználatát illetően. Büntetőjogi Szemle, 2020/2. 122–139. o.

SERBAKOV Márton Tibor: Okostelefonos alkalmazások a terroristák szolgálatában. JURA, 2020/2. 143–155. o.

SERBAKOV, Márton Tibor: The attack on the U.S. Capitol and the security threat posed by the QAnon conspiracy theory. Jogelméleti Szemle, 2021/2. 106–124. o.

SERBAKOV, Márton Tibor: The latest techniques and sources of terrorist financing. KRE-DIT: A KRE-DOK ONLINE TUDOMÁNYOS FOLYÓIRATA, 2020/2.

SERBAKOV, Márton Tibor: Trends in terrorism in 2021. Büntetőjogi Szemle, 2021. Vol. 10. No. különsz. 68–75. o.

