Petrovits Roberto

joghallgató, Pécsi Tudományegyetem Állam- és Jogtudományi Kar

Az Egyesült Államok 2016. évi elnökválasztása és az orosz befolyás az erőszak tilalmának tükrében

I. Bevezetés

Az Egyesült Államok legutóbbi elnökválasztásának sajtóvisszhangja a korábbiakhoz viszonyítva páratlan volt, és még most is sok tisztázatlan kérdés maradt körülötte. A közösségi média felületek felhasználásával és az internet biztosította gyors információáramlás kihasználásával – részben már bizonyítottan, részben feltételezetten – orosz felhasználók próbálták befolyásolni az elnökválasztást.

A befolyás mértéke, illetve forrása máig is tisztázatlan, így e tanulmány csupán a feltételezett befolyást kívánja elsősorban az erőszak tilalmának *ius cogens* természetű nemzetközi jogi követelményével szembe állítani.

A feltételezett választási befolyás, amelynek egyes elemeit már az amerikai szövetségi hatóságok bizonyítottnak nyilvánítottak,[1] több frontról érkezett az Egyesült Államok területére. A közösségi média felületeken (*Facebook, Twitter*, stb.) elhelyezett ún. „*fake-news*", azaz álhíreket tartalmazó hirdetések mellett, amelyeknek célzott közönsége volt, és nagymértékű kattintást, így olvasást vont maga után, több, a demokratákhoz köthető (vagy azok szövetségi szintű szervezetének) elektronikus levelezés látott napvilágot egy olyan weboldalon, amelyen kiszivárogtatott (sokszor személyesebb, titkosított vagy egyszerűen jogellenesen szerzett) információkat tesznek közzé (*WikiLeaks*).[2] Az egyes befolyásolást célzó tevékenységek mögött feltételezhetően Oroszország áll, amely egyes esetekben bizonyítást is nyert.[3]

---

[1] 2016 Presidential Election Investigation – Fast Facts. https://edition.cnn.com/2017/10/12/us/2016-presidential-election-investigation-fast-facts/index.html (2019.04.16.)

[2] A kiszivárogtatott levelezések elérhetőek a WikiLeaks oldalán, kereshető adatbázis formájában: https://wikileaks.org//dnc-emails/?q=&mfrom=&mto=&title=&notitle=&date_from=&date_to=&nofrom=&noto=&count=50&sort=0#searchresult (2019.04.16.)

[3] Az Amerikai Egyesült Államok Nemzetbiztonságért felelős állami szerve, illetve a választások biztonságáért felelős hírszerzési igazgató 2016. október 7-én közölt közös nyilatkozata egyike a leghitelesebb dokumentumoknak, amelyek alátámasztják a *doxing*-műveletek mögött álló orosz befolyás tényét. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national (2019.04.16.)

II. Tipológia – támadások és befolyásoló tevékenységek a *cyber*-térben

Ahhoz, hogy minősíteni lehessen ezeket a cselekményeket, célszerű több fogalmat tisztázni, illetve rendszerbe foglalni az egyes tevékenységeket. A *cyber*-térben történő, választásokkal kapcsolatba hozható, ártó szándékú külső behatásokat két fő csoportra bonthatjuk: támadásokra és befolyásolásra. A támadások körébe soroljuk az elektronikus rendszerek feltörését, a szavazatok számának megváltoztatását, a választói névjegyzékben történő jogtalan módosításokat és az ehhez hasonló cselekményeket, lényegében az elektronikus rendszerekben tárolt adatok megsemmisítését, megváltoztatását, kiegészítését.

A befolyásolás azonban nem a létező adatok, rendszerek megmásítására törekszik, hanem az egyes személyek, szavazópolgárok viselkedésének megváltoztatására és a befogadó közeg kognitív funkcióira hatnak. Alapvetően a befolyásolással járó tevékenységek az emberi kapcsolatok velejárói, és sok esetben nem problémás jelenségek, azonban – e határvonal meghatározásában a jog és más tudományok is nehézségekbe ütköznek – több esetben aggályosak, esetleg etikátlanok vagy akár jogellenesek is.[4] A nem egyszerűen az emberi kapcsolatok velejárójaként definiált, ebben az esetben a választók viselkedésének befolyásolását célzó *cyber*-tevékenységek további csoportokra oszthatók; elsőként *doxing*-ra, amely azt a tevékenységet takarja, amelyek nem nyilvános információkat, adatokat – a 2016. évi amerikai elnökválasztás esetében elektronikus levelezéseket – a nyilvánosság számára hozzáférhetővé tesznek, amelyet feltételezhetően egy elektronikus rendszerbe való jogellenes behatolás előz meg (*hacking*).[5]

E tevékenységek másik csoportja pedig újonnan kreált vagy már elérhető információ fenyegetésre, összezavarásra, félrevezetésre történő szándékos alkalmazása célzott közönségen. Ezek között meg kell különböztetni a rosszindulatú információt, amelynek célja egyes személyek, szervezetek vagy államok „lejáratása", rossz színben való feltüntetése (ezek általában fenyegető, abuzív, diszkriminatív, zaklató vagy felkavaró hangvételűek), illetve a félretájékoztatást, amely a köznyelvben is elterjedt *„fake news"* jelenséget jelenti.[6]

Az Európai Bizottság közleménye az alábbiak szerint definiálja a félretájékoztatást: „*A félretájékoztatás olyan, igazolhatóan hamis vagy félrevezető információ, amelyet gazdasági*

---

[4] *Sander, Barrie*: Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections. Chinese Journal of International Law 2019. Megjelenés alatt. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341681 (2019.04.16.) 5-6.o.

[5] *Sander:* i.m. 7-15. o.

[6] *Sander*: i.m. 7-15.o.

haszonszerzés vagy szándékos megtévesztés céljából hoznak létre, hoznak nyilvánosságra és terjesztenek, és amely kárt okozhat a közérdeknek. A közérdeknek okozott károk magukban foglalják azokat a veszélyeket, amelyek a demokratikus politikai és szakpolitikai döntéshozatali folyamatokat, valamint a közjavakat – például az uniós polgárok egészségének, a környezetnek vagy a biztonságnak a védelmét – fenyegetik."[7]

Az elnökválasztás során elsősorban az ún. *doxing*, illetve a félretájékoztatás jelentek meg nagy számban,[8] így legfőképpen ezeket érdemes vizsgálni. Fontos kiemelni azonban, hogy a nemzetközi jog jelenlegi formájában nem áll teljesen készen ilyen, és ehhez hasonló, a XXI. század technológiai újításait kihasználó tevékenységek kategorizálásra, az azok ellen való hatékony fellépésre, tekintettel arra, hogy a technika által biztosított lehetőségek már nem napról napra, hanem szinte óráról órára változnak.

III. A *cyber*-tér a nemzetközi jogban

Az elektronikus tér (*cyber-space*) a jog szempontjából egy nehezen szabályozható terület, hiszen a klasszikus értelemben vett határokkal nem rendelkezik, így abban az egyes államok nehezen elhatárolhatók. Különböző elméletek léteznek arra vonatkozóan, hogy a *cyber*-teret milyen formában lehet összekapcsolni az egyes államok szuverenitásával, illetve az abban végzett tevékenységeket milyen formában lehet egyes államokhoz kötni. Azonban az információs rendszerek, és hálózatok jogellenes *hack*elése, az azokba történő jogellenes külső behatások természetükben hordozzák e kritériumok megállapításának nehézségét, hiszen a professzionális *hacker*ek esetében a legtöbbször vagy nehezen, vagy egyáltalán nem nyomozható vissza a rendszereket érő külső behatás forrása, tekintettel arra, hogy túlnyomó részt céljuk kilétüknek titokban tartása, azokban az esetekben is, amikor motivációik egyértelműen meghatározhatók.[9]

Az úgynevezett Tallin „kézikönyv" (*Tallin Manual)*, amelyet a NATO Kibervédelmi Kiválósági Központjának (*Cooperative Cyber Defence Centre of Excellene – CCDCOE)*

---

[7] Európai Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Európai megközelítés az online félretájékoztatás kezelésére. Brüsszel, 2018.04.26. COM(2018) 236. A magyar fordításból idézett definíció. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52018DC0236&from=EN (2019.04.16.)

[8] 2016 Presidential Campaign – Hacking Fast Facts. https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html (2019.04.16.)

[9] *Yousef*, Ahmed Y. ElGohary: "Cyber Operations below the Threshold of the Use of Force. Principle of State Sovereignty." https://www.academia.edu/38521943/Cyber_operations_below_the_threshold_of_the_use_of_force._Principle_of_state_sovereignty (2019.04.16.)

felkérésére szakértők készítettek el, és a Cambridge Egyetem publikált arról értekezik, hogy a nemzetközi jog miképpen ültethető át a *cyber* konfliktusok és hadviselés eseteire. A *Tallin Manual* 2.0 (a továbbiakban: Kézikönyv) az eredeti mű kiegészített újragondolása. E kézikönyv nemzetközi jog által elismert kötőerővel nem bír, az inkább egy jogirodalmi értelmezésnek vagy szokásjogi analízisnek tekinthető, így számos szerző ezekben a kérdésekben e kézikönyv tartalmára, és jogtudósok általi értelmezésére hivatkozik.[10] A CCDCOE állásfoglalása alapján, amely elismeri e művet és saját fórumain hivatkozik is rá, a Kézikönyv nem képviseli sem a NATO, sem a CCDCOE, sem a tagállamok álláspontját.[11] E mű létezéséből, illetve már egyszeri kibővítéséből mindazonáltal kitűnik, hogy a nemzetközi jogot művelő jogtudósok és szakértők is fontosnak látják a *cyber* folyamatok és tevékenységek megfelelő szabályozását, azoknak a nemzetközi jog szabályaival történő összhangba hozatalát.

A Kézikönyv kiemeli, hogy a szuverenitás elve a *cyber* térben is alkalmazandó. Értekezik arról, hogy az államoknak tartózkodniuk kell minden olyan *cyber* művelettől, amely más állam szuverenitását sértené. Fontos azonban kiemelni, hogy e megközelítésből az következik, hogy a szuverenitás normaként kezelendő, és annak megsértése jogellenes cselekmény, azonban e meglátás nem univerzálisan elfogadott. Több, e témával foglalkozó szerző szerint a szuverenitás sokkal inkább elvként érvényesül a nemzetközi jogban, amely más normákból, így különösen az erőszak és a beavatkozás tilalmából áll, azonban önmagában az nem bír kikényszeríthető jelleggel.[12]

Az egyes, az információs rendszereket érő, a *cyber*-térben történő külső, legtöbbször jogellenes behatások vizsgálata és tipologizálása után ahhoz, hogy mindez összeköthető legyen az erőszak tilalmának általános követelményével, célszerű e feltétlen alkalmazást igénylő nemzetközi szabály fogalmi elemeit részletesebben megvizsgálni, és bemutatni az eddig megszilárdult gyakorlatot, majd ezt követően levonni azokat a következtetéseket, amelyek mentén megállapíthatjuk, hogy minősülhet-e erőszaknak egy, a *cyber*-világban egy állam által más állam hátrányára elkövetett cselekmény.

---

[10] Tallin Manual 2.0 – NATO CCD COE. https://ccdcoe.org/research/tallinn-manual/ (2019.04.16.)

[11] The Tallin Manual – NATO CCD COE. https://web.archive.org/web/20130424162717/http://ccdcoe.org/249.html (2019.04.16.)

[12] *Schmitt*, Michael N. (szerk.): Tallinn Manual 2.0. on the international law applicable to cyber operations – Prepared by the International Group of Experrts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2017. https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf 741-742. o. (2019.04.16.)

IV. Az erőszak tilalmának fogalmi elemei

Az ENSZ Alapokmánya mint nemzetközi szerződés rendelkezik az erőszak tilalmáról mint a nemzetközi jog feltétlen alkalmazást igénylő szabályáról, amely eltérést nem enged, csak azonos szintű, tehát *ius cogens* jellegű normával módosítható, és mindezt a nemzetközi közösség ekként fogadja el.[13]

„A Szervezet összes tagjainak nemzetközi érintkezéseik során más állam területi épsége vagy politikai függetlensége ellen irányuló vagy az Egyesült Nemzetek céljaival össze nem férő bármely más módon megnyilvánuló erőszakkal való fenyegetéstől vagy erőszak alkalmazásától tartózkodniuk kell".[14]

E tilalom alól két kivételt ismer a nemzetközi jog, így az önvédelmet, illetve a Biztonsági Tanács által foganatosított fegyveres rendszabályokat.[15] A kivételek részletezése e tanulmány szempontjából irreleváns, bár megjegyzendő, hogy az államon belüli erőszak, amely egyes szerzők szerint[16] a fogalomból adódóan az erőszak tilalma alól kivett esetek közé sorolandó, megjelenhet ezekben az esetekben, elsősorban a *hacker* tevékenységek közvetett következményeként.[17]

Az Alapokmányból fentebb idézett tilalom nem rendelkezik arról, hogy mi sorolható az erőszak fogalma alá, így az ENSZ Közgyűlése 1974. évi 3314. sz. határozatában megalkotta az agresszió fogalmát, amelyet irányadónak jelölt meg a Biztonsági Tanács számára annak eldöntésére, hogy egyes cselekmények támadó cselekménynek számítanak-e.[18] Az agresszió egyike az erőszak legsúlyosabb megjelenési formáinak, amelyet az említett határozatában a Közgyűlés fogalmilag körülhatárolt.[19] E határozat alapján az agresszió fegyveres erő elsőként való alkalmazása valamely állam részéről egy másik állam szuverenitása, területi épsége vagy politikai függetlensége ellen, vagy az ENSZ Alapokmányával össze nem férő bármely más módon, amint azt ez a meghatározás kifejti. A határozat exemplifikatíve felsorolja azokat a tényállásokat, amelyek agressziós cselekménynek minősülhetnek. Ebből adódóan e lista nem

[13] *Kovács Péter:* Nemzetközi közjog. Osiris Kiadó, Budapest 2011. 41-76. o.
[14] Az Egyesült Nemzetek Szervezetének Alapokmánya. 2. cikk 4. bekezdés
[15] *Bruhács János:* Nemzetközi jog I. Dialóg Campus kiadó, Budapest 2014. 178.o.
[16] Bruhács János korábban hivatkozott könyvében például kiemeli az államon belüli erőszakot mint kivételt, azzal a megjegyzéssel, hogy ez magából a normaszövegből adódik. *Bruhács*: i.m. 178. o.
[17] ld. a 6. oldalon bemutatott hipotetikus példában
[18] Ennek elsősorban a nemzetközi béke és biztonság fenntartásával kapcsolatos Biztonsági Tanácsi hatáskörök kapcsán van jelentősége. ENSZ Alapokmány 39. cikk.
[19] *Bruhács: i.m. 178.o.*

tekinthető véglegesnek, pusztán példálózónak, azonban a felsorolt tényállásokban a fegyveres erő – mint fogalmi elem – szerepel, vagy szükséges a tényállás megvalósításához.[20]

A határozat tartalmából kitűnik, hogy az agresszió tényének megállapításához a fegyveres erő mint fogalmi elem főszabályként (kivétel például: terület átengedése) szorosan hozzátartozik és a Biztonsági Tanács számára is e határozat az irányadó azokban az esetekben, amikor az erőszak tilalmának súlyos megsértését készül megállapítani. A fegyveres erő fogalmát (eredeti megfogalmazásban: *armed forces*) a nemzetközi szerződések közül az 1949. évi Genfi Egyezmények 1977-es I. kiegészítő jegyzőkönyve határozza meg, az alábbiak szerint – és habár fontos elkülöníteni a *jus in bello* és a *jus ad bellum* szabályait, e fogalom mindkét jogterületben azonos módon alkalmazandó:

„Valamely összeütköző Fél fegyveres erői olyan szervezett fegyveres erőkből, csapatokból és alakulatokból állnak, amelyek az alárendeltjeik magatartásáért az adott Félnek felelős parancsnokság alá tartoznak, abban az esetben is, ha a Felet a szembenálló Fél által el nem ismert kormány, vagy a hatóság képviseli. Az ilyen fegyveres erők egy belső fegyelmi rendszerbe tartoznak, amely többek között érvényesíteni tartozik a fegyveres összeütközésre vonatkozó nemzetközi jogi szabályok betartását”[21]

A témával kapcsolatban a legfontosabb kérdés az, hogy az egyes *cyber*-térben zajló magatartások számíthatnak-e ez alapján olyan cselekményeknek, amelyek az erőszak tilalmába ütköznek. A fenti meghatározások alapján elsődlegesen arra kell választ keresni, hogy lehet-e erőszak alkalmazása az adott *cyber* tevékenység, és amennyiben igen, az számíthat-e fegyveres támadásnak, ugyanis ebben az esetben aktiválódik az államok egyéni vagy kollektív önvédelemhez való joga.

A különböző értelmezések szerint az erőszak fogalmának létezik egy tágabb értelmezése, amely magába foglalja a politikai és gazdasági erőszakot is, azonban e nézőpont sem a san franciscoi konferencián – és így később a bécsi konferencián sem nyert teret a szerződő felek körében. Az előkészítő anyagokból (*travaux prépraratoires*), illetve a tárgyalásokból is kitűnik, hogy az erőszak szót elsősorban a fizikai erőszakra szűkíti az Alapokmány, és habár a politikai és gazdasági erőszak nem kívánatos, és bizonyos kinyilvánított célokkal, valamint elvekkel ellentétes, az Alapokmány 2. cikkének 4. bekezdése

[20] Az ENSZ Közgyűlésének 1974. évi 3314. számú határozata http://hrlibrary.umn.edu/instree/GAres3314.html (2019.04.16.)

[21] 1989. évi 20. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben 1949. augusztus 12-én kötött Egyezmények I. és II. kiegészítő Jegyzőkönyvének kihirdetéséről. I. jegyzőkönyv. 43. cikk 1.)

nem tiltja az ilyen cselekményeket.[22] A szűkebb és tágabb értelmezési lehetőségek tekintetében McNair gondolata jól érzékelteti azt, hogy miért fogadható be nehezen a nemzetközi jog gyakorlatába a gazdasági *„erőszak"* tilalma. Law of Treaties művében úgy fogalmazott, hogy „*közel minden szerződés tartalmaz olyan rendelkezéseket, amelyek komoly alkudozás eredményei, és amelyeket a felek egyike nagyon is el szeretett volna kerülni"*[23]

Az önmagában megvalósuló politikai és gazdasági nyomásgyakorlás ezek alapján nem ítélhető meg egyértelműen aszerint, hogy jogellenes-e a nemzetközi jog alapján vagy sem. Az 1968-69-es bécsi konferencián elfogadott nyilatkozat szövege – amely csak a zárójegyzőkönyv részét képezi és szerződéses erővel nem bír[24] – tovább szűkíti a tényállási kritériumokat azzal, hogy a nyomásgyakorlás céljának a nemzetközi szerződés megkötését nevezi meg, és azokat a szerződéseket ítéli el, azonban nem érvényteleníti, amelyek ily módon jönnek létre. A szerződések jogáról szóló 1969. évi bécsi egyezmény szövegét megvizsgálva – amely hivatkozik az erőszak tilalmáról szóló Alapokmányban található cikkre – láthatjuk, hogy a teljes Alapokmány szövegére hivatkozással teszi meg a szerződés esetleges érvénytelenségére vonatkozó megállapítást. Az utalás ellenére a témával foglalkozó nemzetközi irodalom is azt a következtetést vonta le, hogy főszabály szerint önmagában nem érvényteleníti az egyes szerződéseket az a tény, hogy azok politikai vagy gazdasági nyomásgyakorlás következményeként jöttek létre.[25]

Egy még érdekesebb, és még kevésbé meghatározott képet kapunk abban az esetben, ha e tevékenységeket, valamint a politikai nyomásgyakorlást, illetve a belföldi politika bármilyen formában történő, külső állam területéről, képviselőitől érkező befolyást, illetve behatásokat a *cyber-térbe* helyezzük át.

V. Az egyes befolyásoló cselekmények és esetleges megítélésük

Az elektronikus hírközlés és a számítógépek világában az államok fegyverarzenáljainak nagy része elektronikusan, informatikai eszközökön keresztül, adott esetekben hálózatokról üzemeltethetők. E hálózatok vélhetően rendkívül védettek, de az internet világának eddig rövidnek mondható története során is számos példát láthattunk arra, hogy rendkívül magas

[22] *Patridge, Charles E.*: Political and Economic Coercion: Within the Ambit of Article 52 of the Vienna Convention ont he Law of Treaties? The International Lawyer, 5. évfolyam/4. sz. 1971. 764. o. www.jstor.org/stable/40704716. (2019.04.16.)

[23] *McNair, Arnold*: Law of Treaties.Clarendon Press, Oxford 1961. 207. o. Idézi: Patridge, Charles E.: Political and Economic Coercion: Within the Ambit of Article 52 of the Vienna Convention ont he Law of Treaties? The International Lawyer, 5. évfolyam/4. sz. 1971. 769. o. (szerző fordításában)

[24] *Bruhács*: i.m. 63.o.

[25] *Partridge:* i.m. *755*–769. o.

védettségű rendszerek *hacker* támadások áldozatává váltak (ilyen történt például az Egyesült Államokban 2008-ban[26], a párizsi G20 találkozón[27], és számos, kevésbé elhíresült esetben). Értelmezésem szerint önmagában egy információs rendszer ellen elkövetett – adott esetben külföldről érkező – támadás nem minősül az erőszak tilalmával szembe helyezkedő tevékenységnek. Habár fontos lenne e tevékenységeket célok és motivációk alapján differenciálni, – tekintettel arra, hogy az egyes behatások természetét ezek nagyban befolyásolják – a fentiek alapján e tevékenységek jelenleg nem ellentétesek az erőszak tilalmának követelményével.

Előbbi gondolatomra – a választásokkal kapcsolatos eset előtt – egy hipotetikus példát mutatok be, amelyen keresztül jól érzékelhető a nemzetközi jog fogalmaival kapcsolatos probléma. Ebben az esetben feltételezzük, hogy a támadó magatartása betudható egy ENSZ tagállamnak – a Tallin kézikönyv alapján például az állami szervek *cyber*-tevékenységei ilyennek minősülnek[28] –, és a támadás egy, a megtámadott ország államigazgatással kapcsolatos információs rendszerét érinti, méghozzá oly módon, hogy az informatikai rendszert ún. elektronikus kártevőkkel fertőzik meg, amely a számítógépek túlmelegedését okozza, és a hardverekben (a számítógépek fizikai egységeiben) okoz maradandó kárt. Szélsőségesebb esetben ilyenkor ezek a számítógépek ki is gyulladhatnak, teljesen meg is semmisülhetnek. Az államigazgatás támadással érintett területe összeomlik, amely az adott országon belül káoszhoz, balesetekhez, zavargásokhoz is vezethet. Érdemes megvizsgálni, hogy ebben az esetben beszélhetünk-e fegyverről, fegyveres erőről, tágabban tehát agresszióról, hiszen egy állam a másik állam területén fizikailag észlelhető kár keletkezhet. E cselekmény ebben az esetben a megtámadott állam szuverenitását sérti (amennyiben a fentiekre hivatkozva pedig a szuverenitást elvként kezeljük, abban az esetben az erőszak és a beavatkozás tilalma kerül előtérbe), kárt okoz, és mindez egyértelműen nem fér össze az Egyesül Nemzetek céljaival. Ebben az esetben véleményem szerint, erőszakos cselekményről van szó, amely szembeállítható az Alapokmány 2. cikkének 4. bekezdésével.

E helyzetekben a Biztonsági Tanács nyilváníthat adott államokat agresszorrá, mint azt korábban is tette már a koreai-háború[29], illetve az öbölháború[30] esetében, azonban ekkor

[26] *Prince,* Bryan: Defense Department Confirms Critical Cyber-attack. https://www.eweek.com/security/defense-department-confirms-critical-cyber-attack (2019.04.16.)
[27] *Hollinger,* Peggy: Cyber attackers target G20 documents. https://www.ft.com/content/83dc8ce4-48f4-11e0-af8c-00144feab49a#axzz2Kw48Onjf (2019.04.16.)
[28] *Schmitt:* i.m. 750-751. o.
[29] Az ENSZ Biztonsági Tanácsának 82. sz. határozata
[30] Az ENSZ Biztonsági Tanácsának 660/661/662/664/665/666/667/669/670/674/677/678. sz. határozatai

előtérbe kerül a nemzetközi jog egy fontos problémája, hiszen az államok nehezen ismerik el nemzetközi felelősségüket, az eseményeket úgy alakítják, illetve a nemzetközi jogot úgy értelmezik, hogy elkerüljék a nemzetközi felelősségre vonásukat, és így a Biztonsági Tanács ilyen tárgyú döntései megfontoltak és ritkák.[31]

A fenti példából látszik, hogy az információs társadalom és az internet korában az elektronikus, *cyber*-térben történő kriminalizált cselekmények növekvő száma mellet – amelyre az államok belső joga igyekszik gyorsan és hatékonyan reagálni – más jogterületeken, így a nemzetközi jog világában is releváns kérdés lett a jog és a *cyber*-világ viszonya, amelyre többek között a Tallin kézikönyv is bizonyítékként szolgál. Az alapvető fogalmak, amelyek alkalmazása az eddigi gyakorlat során megszilárdult, megértek arra, hogy a kor változó viszonyaihoz mérten, konszenzus mentén újra legyenek definiálva. Az elektronikus hírközlés világában ilyenek különösen az államterület, az agresszió, a fegyveres erők, az erőszak, és ehhez hasonló, a feltétlen érvényesülést igénylő szabályok alkalmazását legfőképpen érintő, kialakított definíciók.

Az imént ismertetett eset elsősorban *cyber*-támadásnak minősíthető, azonban az orosz befolyás az Egyesült Államok 2016. évi elnökválasztásán nem, hiszen fegyveres erőket nem vetettek be, az állam területi egységét nem sértették meg, és közvetlenül nem is hatottak az állami működésre, hiszen nem hatoltak be államigazgatási hálózatokba, ott nem okoztak kárt, így ezekben az esetekben, befolyásolásról, azon belül is *doxing*-ról, és félretájékoztatásról beszélhetünk a fenti tipológia alapján. A behatás jelentőségét, veszélyességét és kockázatait a fogalmi megkülönböztetés (támadás-befolyásolás) nem kicsinyíti le, azonban fontos kiemelni, hogy a korábban vizsgált definíciók alapján a befolyásoló cselekmények esetében nem is beszélhetünk nemzetközi jogi értelemben vett erőszak alkalmazásáról, míg a támadások esetén ez felmerülhet.

Ezek a befolyásoló tevékenységek szintén más megközelítést igényelnek az eddigiekhez képest, hiszen közvetlenül nem beszélhetünk megtámadott államról, sőt még csak támadásról sem. Nemzeti jogban is nehezen szabályozható kérdésről van szó akkor, amikor álhírek terjesztésével vagy megbotránkoztató állítások célzott hirdetések formájában történő „támadásával" próbálnak választói akaratot befolyásolni. Ilyenkor ütköztetni kell az állampolgárok választáshoz (államirányításban való részvétel) jogát, azon belül is a választások befolyásoltságtól mentességét az információs szabadsággal, véleménynyilvánítás

[31] *Bruhács*: i.m. 131-163. o.

szabadságával és egyéb szabadságjogokkal.[32] Nemzetközi színtéren e cselekmények még kevésbé szabályozhatók a jog segítségével, hiszen az, hogy egy másik állam állampolgára egy, a *befolyásolt* államot értinő álhírt elkészít, terjeszt, esetleg fizetett hirdetés formájában megosztja az egyes közösségi média felületeken, amely hirdetésben célközönségnek a *befolyásolni kívánt* ország állampolgárainak egy részét jelöli meg, nem szabályozható két állam viszonyára szűkítve.

Ugyancsak ez a probléma áll fenn akkor, amikor egy, a *befolyásolt* állam politikai pártjának levelezőrendszerét támadják meg egy másik ország területéről, akár bizonyítottan a támadás forrás országának állami vezetőinek utasítására, hiszen itt nem az állam ellen indítanak *cyber* támadást, fizikai kárt nem okoznak, azonban ezekkel a tevékenységekkel a választói akarat szabad érvényesülését részben gátolják az adott állam belföldi viszonyait tekintve.[33]

A félretájékoztatás esetében, éppen azért, mivel a nemzetközi jog jelenleg nem tud megfelelően és hatékonyan reagálni ilyen eseményekre, az egyes, e híreknek és információknak felületet adó szolgáltatók, tanulva a 2016-os elnökválasztás alatt történtekből, megkezdték a tartalmak szűrését annak érdekében, hogy az egyes álhíreket kiszűrjék, és azokat eltávolítsák, tekintettel arra, hogy a legtöbb belföldi joganyag szabályozza a valótlan hírek terjesztését, és azok tudatosan valósnak való feltüntetését.[34] E felületek nem csak teret és lehetőséget adnak az esetleges befolyásolásoknak, hanem ahhoz megfelelő adatot is tudnak szolgáltatni. A közösségi média felületeken, illetve az interneten a választópolgárokról tárolt adatok is veszélyforrása lehet a választói akarat esetleges befolyásolásának. A *Facebook* esetében például annak vezérigazgatója és alapítója az Egyesült Államok Szenátusa előtt is meghallgatáson vett részt, miután kiderült, hogy a felhasználók személyes adatait továbbította többek között politikai szervezeteknek is.[35] E felületek a klasszikus felfogás szerint nem ismernek államhatárokat, azok a világ legtöbb pontján[36] elérhetőek, így ezeken keresztül egy adott államból bármely más állam lakosságát kijelölhetik a felhasználók célközönségnek adott tartalom tekintetében.

Az orosz befolyásolás esetén figyelemmel kell lennünk arra is, hogy a közösségi média adta lehetőségek kiaknázásával történő befolyásolási cselekmények tekintetében több kapcsolatot is

---

[32] *Sander:* i.m. 36-46. o.

[33] *Sander*: i.m. 9-11. o.

[34] Matter of fact-checkers: Is Facebook winning the fake news war? https://www.bbc.com/news/technology-47779782 (2019.04.16.)

[35] US senators demand answers from Facebook and Mark Zuckerberg after data sharing report. CNBC News. https://www.cnbc.com/2018/06/05/us-senators-demand-answers-from-facebook-and-mark-zuckerberg.html (2019.04.16.)

[36] Egyes államok korlátozzák a hozzáférést a közösségi médiaszolgáltatókhoz, például a Kínai Népköztársaság területén a Facebook felülete nem érhető el.

szükséges lenne vizsgálnia a nemzetközi jognak is, ami további akadályokat állíthat a hatékony és a változó viszonyokra adekvát választ adó szabályozás lehetősége elé.

VI. További megközelítési lehetőségek

Az Egyesült Államok választásait befolyásoló, államhatárokon átnyúló és az elektronikus, hálózati térben zajló tevékenységek és eseménysorozatok feltétlenül bizonyíték arra, hogy a nemzetközi jog hatályos szabályai és gyakorlata alapján nem tud kiváltképp adekvát választ adni az ilyen cselekményekre. A témában kutatók évtizedek óta értekeznek a *cyber*-világ mibenlétéről, jogi szabályozhatóságáról, illetve arról, hogy milyen módon befolyásolják az eddigi fogalmi- és viszonyrendszereket a technológiai újdonságok. Az ENSZ gyakorlatából és a kutatók közötti konszenzusból is kitűnik, hogy az itt felsorolt, megtörtént cselekmények nem sértik a jelenlegi értelmezés szerint az erőszak tilalmának általános követelményét.

Az erőszak tilalma mellett feltétlenül érdemes szólni a beavatkozás tilalmának szabályáról, amely egy másik, releváns megközelítése lehet az elnökválasztáson történt eseményeknek. A beavatkozás tilalmának megszegésére az egyik legismertebb példa az ún. *Nicaragua*-ügy. A Nemzetközi Bíróság ítéletében megállapította, hogy az Egyesült Államok azzal, hogy az ún. *contrákat* felfegyverezte, felszerelte, támogatta és segítette a katonai és nemkatonai tevékenységüket, megszegte a nemzetközi szokásjogon alapuló kötelezettségét, amely tiltja a más állam ügyeibe történő beavatkozást.[37] Fontos kitétel azonban, hogy a bíróság ítéletében azt is kinyilatkoztatta, hogy a beavatkozás abban az esetben jogellenes, amennyiben kényszert (*coercion*) mint eszközt alkalmaznak, így ez a beavatkozás tilalmának megszegéséhez minden esetben szükséges feltétel (*sine qua non*).[38]

A beavatkozás tilalmának egyik legjelentősebb dokumentuma a Közgyűlés 1883. plenáris ülésén elfogadott 1970. évi nyilatkozata a nemzetközi jog elveiről, tekintettel az államok közötti baráti kapcsolatokra és együttműködésre összhangban az Alapokmánnyal. E nyilatkozatban olvasható, hogy semelyik államnak vagy államcsoportnak sincs joga ahhoz, hogy beavatkozzon – közvetve vagy közvetlenül, bármely oknál fogva – más állam belső vagy külső ügyeibe. E nyilatkozat rendelkezik arról is, hogy e tilalom alá nem csak fegyveres erőszak, hanem a beavatkozás valamennyi formája értendő, és e cselekmények a nemzetközi jog szabályaiba ütköznek. Mindemellett tartalmaz még egy, a téma szempontjából rendkívül

[37] Militarv and Puramilitary Activities in und aguinst Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986. 136. o. https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf (2019.04.16.)

[38] Nicaragua v. USA ügyben hozott ítélet. 107-108. o.

releváns kijelentést, mely szerint minden államnak elidegeníthetetlen joga van politikai, gazdasági, szociális és kulturális rendszerének megválasztásához anélkül, hogy ebbe bármely más állam bármilyen formában beavatkozzon.[39]

Mindezek ellenére azonban fontos kiemelni, hogy a nemzetközi jogot kutatók körében is vita tárgyát képezi, hogy a Közgyűlés határozatai szolgálhatnak-e a nemzetközi jog *szabályaiként*. Az elterjedtebb és elfogadottabb nézet szerint e határozatok és nyilatkozatok nem válnak a nemzetközi jog közvetlen forrásává, egyfajta értelmező szerepet azonban betöltenek, és emellett a fent említett nyilatkozatnak vitathatatlanul van jogi jelentősége.[40] A Közgyűlés részéről számos további nyilatkozat született a beavatkozás tilalmáról, illetve a Nemzetközi Bíróság is több ügyben foglalt állást ítéleteiben amellett, hogy egy más állam belügyeibe történő beavatkozás nem feleltethető meg a nemzetközi jog elveinek.[41]

VII. Konklúzió

A politikai beavatkozás – így egy nemzeti választás befolyásolása – mint jelenség azonban nehezebb kérdés. Tekintettel arra, hogy nem általánosan elfogadott, hogy a Közgyűlés határozatai és nyilatkozatai kötőerővel bírnak, a politikai befolyás esetén az egyetlen forgatókönyv, amely tisztán a nemzetközi jog tilalmaiba ütközik, az a rezsimváltás harmadik állam beavatkozásának következményeként, amelyre kísérletet a fent említett *Nicaragua*-ügyben láthatunk. Véleményem szerint a 2016-os elnökválasztás esetében hasonló megítélés alá kerülhetnek a megvalósított magatartások a más államok által történő, egyes politikai pártokat célzó pénzbeli és egyéb támogatásokkal (*funding),* amelyek gyakoriak, azonban a nemzetközi jog jelenlegi szabályai alapján nem ellentétesek a beavatkozás tilalmával, tekintettel arra, hogy hiányzik a kényszer (*coercion*) mint kötelező elem.[42]

A különböző események és cselekmények külön-külön vizsgálandók, minden körülményt figyelembe véve, és azok alapján állapíthatók meg egyes, a nemzetközi jog szabályaival ellentétes magatartások, azonban a bemutatott nézőpontok és gyakorlat alapján – álláspontom szerint – kijelenthető, hogy az erőszak tilalmát, valamint a beavatkozás tilalmát – kényszer hiányában – e cselekmények nem szegik meg.

---

[39] *Jamnejad, M.; Wood, M.:* The Principle of Non-Intervention. Leidin Journal of International Law. 2009/22 353-355. o. https://doi.org/10.1017/S0922156509005858 (2019.04.16.)
[40] *Kerwin, Gregory J.*: The Role of United Nations General Assembly Resolutions in Determing Principles of International Law in United States Courts. Duke Law Journal, 1983/4 898-899. o. https://www.jstor.org/stable/1372469 (2019.04.16.) és *Jamenjad, M.:* i.m. 354. o.
[41] *Jamenjad, M.:* i.m. 356-368. o.
[42] *Jamenjad, M.:* i.m. 368. o.

E két nemzetközi jogi tilalom megszegésének hiányában az elnökválasztás körüli események megítélése a szuverenitás megsértésének kérdéskörébe utalandó, ekkor azonban az e köré szerveződött tudományos vitával találjuk magunkat szemben, amely arra keresi a választ, hogy a szuverenitás normaként kezelendő-e, és így kikényszeríthető, megsértéséhez jogkövetkezmények fűződhetnek, vagy elvként, amelyet több, másik nemzetközi jogi norma alkot.[43] Amennyiben azt az álláspontot fogadjuk el, hogy csak elv, amelynek fő alkotóelemei az erőszak és a beavatkozás tilalma, abban az esetben az előbb felsorokoztatott indokok alapján nem vonható felelősségre az orosz állam – amennyiben elfogadjuk, hogy e cselekmények az föderációnak betudhatók voltak. A másik nézőpont elfogadása esetén, ha külön normaként tekintünk a szuverenitásra, abban az esetben Oroszország magatartása megalapozhatja nemzetközi felelősségét, és ellenintézkedésre is lehetőséget adhat. Az az állítás kétségkívül igaz, hogy az Egyesült Államok szuverenitása sérült, azonban az orosz állam felelősségre vonhatósága attól függ, miképpen tekintünk a szuverenitásra a nemzetközi jogban.

[43] *Sander*: i.m. 18-21. o.