DOI 10.26521/profuturo/2024/1/15120

Kiss Mátyás*

Az ártó szándékú kiberműveletek nemzetközi jogi értékelése az állam szuverenitásának tükrében

Malicious Cyber Operations in the Light of State Sovereignty

Absztrakt

A szuverenitás a modern nemzetközi jog egyik sarokkő jellegű normája. Az alapelv pontos tartalma és jelentése sokat változott az évszázadok során, gyakran heves vitákat kirobbantva. Napjainkban az egyik legfontosabb kérdés a szuverenitás kapcsán, hogy ez az alapelv miként alkalmazható a kibertérben. Az elmúlt évek során exponenciálisan nőtt az ellenséges célú államközi kiberműveletek száma. Mértékadó nemzetközi szervezetek szerint a 2020-as évekre már évente több száz államok közötti kibertámadás valósult meg. Jelen tanulmány célja, hogy megvizsgálja azt, hogy a nemzetközi jogi szakirodalom miként vélekedik az állami szuverenitás kérdéséről a kibertérben, sor kerül a vonatkozó állami gyakorlatok ismertetésére, továbbá a tanulmány bemutat néhány releváns kiberműveletet a közelmúltból.

Tárgyszavak: *szuverenitás, állami gyakorlat, kiberműveletek, Tallinni Kézikönyv, nemzetközi jog*

Abstract

The principle of sovereignty is one of the cornerstone norms of modern international law. The precise content and meaning of this fundamental principle have changed significantly in historical and political contexts, often sparking intense debates. Today, one of the most critical questions regarding sovereignty is how this principle can be applied in cyberspace. In recent years, the number of hostile cyber operations between states has increased dramatically. By the beginning of the 2020s, various international organizations had already recorded more than a hundred incidents annually. The aim of this study is to examine how international legal literature views the relationship between state sovereignty and cyberspace, to show the current state practice, and to introduce some recent cyber operations that are relevant to the issue.

Keywords: *sovereignty, state practice, cyber operations, Tallinn Manual, international law*

A szuverenitás elve a modern nemzetközi jog egyik sarkalatos elve. A nemzetközi jog legtöbb intézménye és alapelve közvetlenül vagy közvetve az állami szuverenitásra támaszkodik, példaként lehet említeni az államiság ismérveit, a területi és

* Dr. Kiss Mátyás, PhD-hallgató, Pécsi Tudományegyetem Állam- és Jogtudományi Doktori Iskola, e-mail: kiss.matyas@ajk.pte.hu.

személyi joghatóságot, az állami immunitás kérdését vagy a beavatkozás tilalmát.[1] Annak ellenére, vagy talán éppen azért, mert a nemzetközi jog egyik legfontosabb alapelvéről beszélünk, jelentése történelmi és politikai kontextusban sokat változott, időnként heves vitákat kirobbantva.[2]

Az elmúlt évek során exponenciálisan nőtt az ellenséges célú, államközi kiberműveletek száma. Ez azt jelenti, hogy a 2020-as évekre évente már nagyságrendileg több száz, államok közötti kiberakció valósult meg.[3] A kibertér és a nemzetközi jog kapcsolatát számtalan aspektusban lehetne vizsgálni. Kiindulópontként fontos leszögezni ugyanakkor, hogy napjainkig az államok még egyetlen alkalommal sem minősítettek egyetlen kiberműveletet sem fegyveres támadásnak vagy erőszak-alkalmazásnak. A legtöbb kiberakció olyan alacsony intenzitású, hogy fel sem merül a jogellenes erőszak alkalmazásának kérdése. Ugyanakkor ilyen esetekben a műveletek további vizsgálatoknak vethetők alá. Felmerülhet a nemzetközi jog további alapelveinek, például a beavatkozás tilalmának vagy a szuverenitás elvének a megsértése.

Jelen tanulmány célja, hogy megvizsgálja azt, hogy a nemzetközi jogi szakirodalom miként vélekedik az állami szuverenitásról a kibertérben (1. rész), sor kerül a szuverenitással kapcsolatos állami gyakorlat ismertetésére (2. rész), a tanulmány bemutat néhány kiberműveletet a közelmúltból (3. rész), végezetül pedig összegző megállapításokat tesz (4. rész). A tanulmánynak nem célja az úgynevezett „kiberszuverenitás", azaz az államok kibertérbeli főhatalmának vizsgálata. A fókusz sokkal inkább annak a bemutatásán van, hogy a kibertérben zajló műveletek milyen hatással vannak az állami szuverenitásra, illetőleg milyen esetekben állapítható meg a szuverenitás megsértése.

1. Az állami szuverenitás a kibertérben

1.1. A szuverenitásról általában

A szuverenitás fogalmának több különböző meghatározása létezik attól függően, hogy milyen jogterület kapcsán beszélünk róla. Nemzetközi jogi szempontból vizsgálva a kérdést az a megállapítás tehető, hogy nincs egységes, kivétel nélkül

[1] Besson, Samantha: Sovereignty. In: *Max Planck Encyclopedias of International Law.* Oxford University Press, Oxford, 2011, 1–2. bekezdés.

[2] Például ilyen vitás pont a közelmúltból, hogy amíg egyesek azzal érvelnek, hogy az állami szuverenitás koncepciója elavult, helyette új, szupra- vagy transznacionális politikai szerveződések koncepcióit kellene előtérbe helyezni, addig mások úgy vélik, hogy az államon túli új hatalmi formák és integrációk, valamint azok belső korlátai a szuverenitás fogalmának megerősítését vagy fejlesztését jelentik. Besson: i. m., 3. bekezdés.

[3] Vonatkozó statisztikák például a Council on Foreign Relations (CFR) oldalán: https://www.cfr.org/cyber-operations/ (2024. 02. 01.), továbbá a Center For Strategic and International Studies (CSIS) adatbázisában: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (2024. 02. 01.). A két hivatkozott nemzetközi szervezet kapcsán kiemelném, hogy az egyes intézmények más-más metódusok szerint számolnak. A magam részéről megbízhatónak fogadom el a két szervezet statisztikáit, amelyeknek köszönhetően legalább nagyságrendi képet kaphatunk arról, hogy hány művelet történik évente.

mindenki által elfogadott definíciója a szuverenitásnak. A legtöbben a Palmas szigetek-ügyben eljáró bíró, *Max Huber* szavait veszik alapul, hogy meghatározzák a szuverenitást: „az államok közötti kapcsolatban a szuverenitás a függetlenséget jelenti. A függetlenség egy földrajzi terület tekintetében azt jelenti, hogy az adott állam jogosult az állami funkciók gyakorlására, más állam kizárásával."[4]

A hatályos nemzetközi jogban különböző nemzetközi szerződések és dokumentumok gyakran hivatkoznak a szuverén egyenlőség elvére. Az ENSZ Alapokmánya rögzíti: *„[a] Szervezet valamennyi tag szuverén egyenlőségének elvén alapszik".*[5] Az elv szerződéses jellegén túl a nemzetközi jog általános elveinek egyike, amelyet a Nemzetközi Bíróság a Nicaragua-ügy kapcsán is megerősített.[6] Az ENSZ Alapokmánya esetében kiemelendő továbbá, hogy az államok belügyeinek szabályozására vonatkozó hatáskört is rögzíti: *„a jelen Alapokmány egyetlen rendelkezése sem jogosítja fel az Egyesült Nemzeteket arra, hogy olyan ügyekbe avatkozzanak, amelyek lényegileg valamely állam belső joghatóságának körébe tartoznak és nem kötelezi a tagokat arra sem, hogy az ilyen ügyeket a jelen Alapokmánynak megfelelő rendezési eljárás alá bocsássák […]".*[7] Az 1970-es évekből két dokumentumot szükséges megemlíteni, amelyek a szuverén egyenlőség elvének kvázi-autentikus értelmezését adják. Az egyik az 1970-es, a baráti kapcsolatok elveiről szóló közgyűlési deklaráció (az ENSZ Közgyűlés 2625 (XXV.) számú határozata),[8] a másik pedig az 1975-ös helsinki záróokmány.[9]

Az említett közgyűlési határozat tartalmaz egy összefoglalót arra vonatkozóan, mi is a szuverén egyenlőség tartalma. Ennek értelmében az államok jogilag egyenlők, minden állam rendelkezik a szuverenitásból eredő jogok teljességével, minden állam köteles tiszteletben tartani más államok jogalanyiságát, az állam területi épsége és politikai függetlensége sérthetetlen, minden államnak joga van, hogy szabadon válassza meg és fejlessze politikai, társadalmi, gazdasági és kulturális rendszerét, valamint minden állam köteles jóhiszeműen és teljesen eleget tenni nemzetközi kötelezettségeinek és békében élni más államokkal.[10]

Valamennyi állam rendelkezik a szuverenitás teljességével, egy állam tehát mindig szuverén. Főszabályként a szuverén állam lép fel formailag önállóan a nemzetközi kapcsolatokban. Az államok nemzetközi jogalanyisága is egyenlő. A szuverenitásnak része, hogy minden állam maga dönt arról, hogy mely entitással lép kapcsolatba. A szuverenitásból fakad ugyancsak a nemzetközi szervezetek döntés-

[4] Reports of International Arbitral Awards. Island of Palmas case (Netherlands, USA). 4. April 1928. Volume II. 838.

[5] ENSZ Alapokmány, 2. cikk 1. bekezdés.

[6] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Jurisdiction and Admissibility, Judgment, ICJ Reports 1984, p. 392. (a továbbiakban: Nicaragua-ügy) 73.

[7] ENSZ Alapokmány, 2. cikk 7. bekezdés.

[8] GA Res. 2625 (XXV), 24 October 1970.

[9] *„A részt vevő államok tiszteletben tartják egymás szuverén egyenlőségét és egyéniségét, valamint a szuverenitásukban rejlő és általuk lefedett valamennyi jogot, beleértve különösen minden állam jogát a jogi egyenlőséghez, területi integritáshoz, valamint a szabadsághoz és politikai függetlenséghez. Tiszteletben tartják egymásnak azt a jogát is, hogy szabadon megválasszák és fejlesszék politikai, társadalmi, gazdasági és kulturális rendszereiket, valamint azt a jogot, hogy meghatározzák törvényeiket és szabályaikat."* (saját fordítás) Forrás: Conference on Security and Co-operation in Europe Final Act. Helsinki, 1975. 4.

[10] GA Res. 2625 (XXV), 24 October 1970. 124.

hozatalában főszabályként érvényesülő 'egy állam egy szavazat' elv, valamint ebből fakad az államimmunitás is, amelynek lényege, hogy az állam közhatalmi aktusai mentességet élveznek más államok bíróságainak joghatóságától.[11]

A szuverén egyenlőség fogalma befolyásolta a szerződések jogát, valamint a diplomáciai és a konzuli jogot egyaránt. Érdemes megemlíteni az államelismerés kérdését. A nemzetközi jog szerint a szuverenitás csak államokhoz kapcsolható, ezért fontos annak a megállapítása, hogy az adott területi egység állam-e. E tekintetben az el nem ismert államok vagy a korlátozott elismeréssel rendelkező államok helyzete problematikus. Annak eldöntése, hogy egy entitás rendelkezik-e az államiság ismérveivel (terület, lakosság, kormányzat), az elismerő állam előjoga. Ennek eredményeként adódhatnak olyan helyzetek, amikor egy adott államot nem egyenlően ismernek el, még egy adott régión belüli országok sem (ez a helyzet például Koszovó esetében is).[12]

A szuverenitásból következően az állam úgynevezett területi és személyi főhatalommal rendelkezik. A területi főhatalom azt jelenti, hogy az állam a saját területe felett kizárólagos ellenőrzést gyakorolhat, azaz egyedül ő végezhet közhatalmi cselekményeket. A nemzetközi jog megsértését jelentené, ha egy állam a saját területén kívüli cselekvésekre nézve alkotna jogot, vagy próbálná meg azt kikényszeríteni. A személyi főhatalom azt jelenti, hogy az állam szuverenitása kiterjed a területén tartózkodó személyekre, ideértve más államok polgárait és azokat a hontalanokat is, akik alá vannak vetve az állam közhatalmának.[13] Amíg az állampolgár saját államában él, addig a személyi főhatalom kérdésének nincsen valódi jelentősége. Más a helyzet akkor, ha az állampolgár ideiglenesen vagy tartósan elhagyja saját országának területét, és egy másik országban van: ilyenkor merül fel az a kérdés, hogy a személyi főhatalom elve alapján milyen jogok illetik, illetve kötelezettségek terhelik az állampolgárság szerinti államot. Nem sérti a másik állam szuverenitását, ha az állam a másik országban tartózkodó saját állampolgáraira nézve ír elő bizonyos, rendszerint korlátozó jellegű szabályokat.[14] Megemlítendő még az egyetemes joghatóság kérdése is. Az állam ebben az esetben attól függetlenül jogosult a feltételezett elkövetők elleni büntetőeljárás megindítására, hogy létezik-e területi vagy állampolgársági, illetve a nemzetközi jog által elismert egyéb joghatósági kapcsolat. Az egyetemes joghatóság gyakorlásának lehetősége elsősorban nemzetközi szokásjogon alapul, de bizonyos esetekben multilaterális szerződés is létrehozhatja.[15]

[11] Kardos Gábor: Az államok szuverén egyenlősége. „Az államok szuverén egyenlősége". In: Jakab András–Fekete Balázs (szerk.): *Internetes Jogtudományi Enciklopédia* (Nemzetközi jog rovat, rovatszerkesztő: Sulyok Gábor). http://ijoten.hu/szocikk/az-allamok-szuveren-egyenlosege (2018). [15]–[16] bekezdés. (2024. 02. 01.)

[12] Czubik, Paweł: Sovereignty in International Law. In: Raisz Anikó (szerk.): *International Law from a Central European Perspective.* Central European Academic Publishing, Miskolc–Budapest, 2022, 100. (DOI: 10.54171/2022.ar.ilfcec_5).

[13] Kende Tamás–Nagy Boldizsár–Sonnevend Pál–Valki László: *Nemzetközi jog.* Wolters Kluwer, Budapest, 2018, 98.

[14] Kovács Péter: *Nemzetközi közjog.* Osiris, Budapest, 2016, 225–226.

[15] Kende–Nagy–Sonnevend–Valki: i. m., 593–594.

1.2. A szuverenitás és a kibertér kapcsolata

Napjaink nemzetközi jogában nincs olyan nemzetközi szerződés, amely a kibertér és a nemzetközi jog kapcsolatát szabályozná.[16] Ennek következtében nincs olyan konkrét szerződés sem, amely kifejezetten a szuverenitás kérdését boncolgatná a kibertér vonatkozásában. Vonatkozó szerződés hiányában különösen felértékelődik a különböző magánkodifikációs művek szerepe, illetve az állami gyakorlat is.

Az ENSZ Közgyűlése 2011-ben immár harmadik alkalommal hívta életre a Kormányzati Szakértők Csoportját,[17] amely kétévnyi munkát követően 2013-ban fogadott el egy jelentést, amelyben a kibertér nemzetközi biztonságra gyakorolt hatásait vizsgálta.[18] Ebben a jelentésben úgy fogalmaznak a szakértők, hogy *„[a]z állami szuverenitás és a szuverenitásból fakadó nemzetközi normák és elvek vonatkoznak az információs és kommunikációs technológiával kapcsolatos tevékenységek állami lefolytatására, valamint a területükön belüli infrastruktúra feletti joghatóságukra”.*[19] Ezt lényegében szó szerint megismétli a két évvel későbbi, 2015-ös jelentés[20] is, kiegészítve azzal, hogy *„az információs és kommunikációs technológia alkalmazása során az államoknak tiszteletben kell tartaniuk a nemzetközi jog egyéb elvei mellett az állami szuverenitást, a szuverén egyenlőséget, a viták békés úton történő rendezését és a más államok belügyeibe való beavatkozás tilalmának elvét”.*[21] Az eddigi utolsó, 2021-es jelentésben a szuverenitás tekintetében kifejezetten utalnak a korábbi jelentések tartalmára, és megerősítik a korábbi jelentésekben meghatározottakat.[22]

A téma kapcsán megkerülhetetlen a jelenleg második kiadását megélő Tallinni Kézikönyv, teljes nevén *„Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations”.*[23] A Kézikönyv nem tükrözi az egyes államok álláspontját, a szer-

[16] Említést érdemel ugyanakkor az Európa Tanács égisze alatt létrejött, számítógépes bűnözésről szóló Budapesti Egyezmény, amely lehetővé teszi a részes felek számára, hogy megosszák egymással tapasztalataikat, és olyan kapcsolatokat hozzanak létre, amelyek elősegítik az együttműködést a kiberbűnözés területén. Forrás: The Budapest Convention (ETS No. 185) and its Protocols. *Council of Europe,* https://www.coe.int/en/web/cybercrime/the-budapest-convention (2024. 05. 27.). Szintén megemlítendő az Afrikai Unió kiberbiztonságról és a személyes adatok védelméről szóló egyezménye, más néven Malaboi Egyezmény. Az egyezmény kilenc évvel az elfogadását követően lépett hatályba, és az egyetlen kötelező érvényű regionális adatvédelmi szerződés lett Európán kívül. Forrás: Ayalew, Yohannes Eneyew: The African Union's Malabo Convention on Cyber Security and Personal Data protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond? *EJIL:TALK!,* https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/ (2024. 05. 27.). Mindkét egyezményben közös azonban, hogy nem kifejezetten a kibertér és a nemzetközi jog kapcsolata áll a középpontjukban, a szuverenitás kérdését pedig érintőlegesen sem említik.

[17] United Nations Group of Governmental Experts (UN GGE).

[18] United Nations Group of Governmental Experts Achieve a 'Landmark Consensus'. *CCDCOE*, https://ccdcoe.org/incyder-articles/united-nations-group-of-governmental-experts-achieve-a-landmark-consensus/ (2024. 05. 27.).

[19] UNGA, A/68/98, 24 June 2013. 20. bekezdés.

[20] UNGA, A/70/174, 22 July 2015. 20. bekezdés.

[21] UNGA, A/70/124, 22 July 2015. 28. (b) bekezdés.

[22] UNGA, A/76/135, 14 July 2021. 71. (b) bekezdés.

[23] Schmitt, Michael N.: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press, New York, 2017 [a továbbiakban: Schmitt (2017)].

zők nem valamely állam felkérésére jártak el, hanem kizárólag személyes minőségükben vettek részt a szerkesztési folyamatban. A projekt igazgatója azt nyilatkozta, hogy a dokumentum célja az volt, hogy az államok számára eszközül szolgáljon saját jogértelmezésük kialakítása során, és nem az, hogy egy normatív hatállyal rendelkező dokumentumot hozzanak létre.[24]

A Tallinni Kézikönyv rögtön az első fekete betűs szabályai között rögzíti, hogy *„az állami szuverenitás elve érvényesül a kibertérben”.*[25] A dokumentum külön vizsgálja az államok belső és külső szuverenitását. A belső szuverenitás tekintetében a kézikönyv úgy fogalmaz: *„az állam szuverén hatalmat gyakorol a területén található kiberinfrastruktúra, személyek, és kibertevékenységek tekintetében, figyelemmel nemzetközi jogi kötelezettségeire”.*[26] Ebből következően egy állam szabadon meghozhat minden olyan intézkedést, amelyet szükségesnek vagy helyénvalónak tart a területén belül a kiberinfrastruktúrával, kibertevékenységeket folytató személyekkel, vagy magukkal a tevékenységekkel kapcsolatban, kivéve ha ezt egy, az államra nézve kötelező nemzetközi jogi szabály nem tiltja meg. Ennek következménye, hogy a kibertevékenységek az állam jogi ellenőrzése alá tartoznak. Az állam kihirdeti és végrehajtja a rájuk vonatkozó törvényeket és rendelkezéseket, másodszor pedig az állam területe feletti szuverenitása feljogosítja a kiberinfrastruktúra és a kibertevékenységek védelmére.[27] Ez azt is jelenti, hogy az államok felhatalmazással rendelkeznek például arra vonatkozóan, hogy szabályozzák a területükön az internethasználatot, valamint arra, hogy lépéseket tegyenek az állampolgáraik jogainak és érdekeinek online védelme érdekében.[28] Az államok külső szuverenitása kapcsán a Kézikönyv elvi éllel szögezi le, hogy az államok szabadon folytathatnak kibertevékenységet nemzetközi kapcsolataikban, tekintettel a rájuk vonatkozó nemzetközi jogi szabályokra.[29] Ez azt jelenti, hogy egy állam külkapcsolataiban független más államoktól, és szabadon folytathat kibertevékenységet a területén kívül, a nemzetközi jog szabályainak betartása mellett.

A területi szuverenitás teljes és kizárólagos hatalmat biztosít az államoknak a területük felett, amely magában foglalja a belvizeket, a parti tengeri területeket, valamint a felettük lévő légteret is.[30] Ahogy fentebb már szóltam róla, az állam szuverén hatalommal rendelkezik a területén található kiberinfrastruktúra, valamint a kibertevékenységet és azokat megvalósító személyek tekintetében. Fontos megvizsgálni, hogy vajon sor kerülhet-e a szuverenitás megsértésére a kibertéren keresztül. A Tallinni Kézikönyv deklarálta azt a szabályt, hogy az államok nem hajthatnak végre olyan kiberműveleteket, amelyek sértik egy másik állam szuverenitását.[31]

[24] Schmitt, Michael N.: International Cyber Norms: Reflections on the Path Ahead. *Militair Rechtelijk Tijdschrift,* 2018, 1–12.

[25] Schmitt (2017): i. m., 11.

[26] Schmitt (2017): i. m., 13.

[27] Schmitt (2017): i. m., 13.

[28] Chatinakrob, Thanapat: Interplay of International Law and Cyberspace: State Sovereignity Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignity. *Chinese Journal of International Law,* 2024/1, 42. (DOI: 10.1093/chinesejil/jmae006).

[29] Schmitt (2017): i. m., 16.

[30] Nicaragua-ügy, 212. bekezdés.

[31] Schmitt (2017): i. m., 17.

Megjegyzendő, hogy a területi szuverenitás megsértése csak olyan cselekményből eredhet, amelyet egy állam hajt végre, vagy amely betudható valamely államnak.[32] Ezzel szemben az egyének önmagukban nem sérthetik meg a területi szuverenitást. Továbbá, az államok nem engedhetik meg más államok számára, hogy területüket jogsértő cselekmény elkövetésére használják. Egy állam, amely lehetővé teszi, hogy területét nem állami szereplők vagy harmadik államok használják egy másik állam elleni jogsértő cselekmény elkövetésére, a sértett állam részéről felelősségre vonható lehet a kellő gondosság *(due diligence)* elve alapján.[33] Ez azt jelenti tehát, hogy az államoknak kötelességük megakadályozni, hogy területükről rosszindulatú kibertevékenységek induljanak el, ideértve például a rosszindulatú szoftvereket, valamint DDoS, azaz elosztott szolgáltatásmegtagadásos támadásokat.[34]

A Tallinni Kézikönyv alapján két nagy esetkört tudunk megkülönböztetni a szuverenitásnak a kibertérben történő megsértése esetére. Az első, az állam területének épségét vagy sérthetetlenségének megsértését jelenti, a második pedig, amikor a kiberművelettel az állam beavatkozik egy eredendően kormányzati funkcióba, vagy elbitorolja azt.[35] Ez a kettősség lényegében a Palmas szigetek-ügy, szuverenitásról adott fogalma kapcsán is megjelenik. A Kézikönyv rendszerének ismertetése azért is fontos, mert egyfelől széles körben elfogadott a szakirodalomban,[36] másfelől pedig az állami állásfoglalások, nyilatkozatok gyakran használják az itt kidolgozott fogalomrendszert.

Ami az első okcsoportot illeti, a szakértői gárda három szinten vizsgálta a kérdést. A legtöbb szakértő egyetértett abban, hogy a kiberműveletek a szuverenitás megsértését jelentik abban az esetben, ha fizikai kárt vagy sérülést okoznak. Példaként azt a helyzetet említik, amikor a kiberművelet egy berendezés hűtőelemeinek meghibásodását eredményezi, amely túlmelegedéshez, és ezáltal az alkatrészek megolvadásához vezet. Egyetértettek abban is, hogy a fizikai károsodáson túl a kiberinfrastruktúra funkcionalitásának elvesztése is a szuverenitás megsértésének minősül. Noha a pontos küszöbértékben nem tudtak megállapodni, abban egyetértettek, hogy az infrastruktúra működéséhez szükséges berendezések vagy a fizikai elemek működőképességének elvesztése a funkcionalitás elvesztését jelenti.[37] Nyilvánvaló azonban a szakirodalom szerint, hogy nem minden kiberművelet sérti a szuverenitást, akkor sem, ha részben vagy egészben más állam kiberinfrastruktúráján keresztül valósul meg. Erre példaként említhető a propaganda továbbítása egyik állam területéről a másik állam területére valamilyen műholdon keresztül,[38] valamint az a kiberakció amely kizárólag terroristák vagy terrorista szervezetek felhasználói fiókjai vagy eszközei ellen irányul, és csupán csekély hatást gyakorol a területi állam infrastruktúrájára.[39]

[32] Delerue, Francois: *Cyber Operations and International Law.* Cambridge University Press, Cambridge, 2020, 210; Schmitt (2017): i. m., 17–18.
[33] Delerue: i. m., 210–211.
[34] Chatinakrob: i. m., 42.
[35] Schmitt (2017): i. m., 20–22.
[36] Schmitt, Michael N.–Vihul, Liis: Respect for Sovereignty in Cyberspace. *Texas Law Review,* 95/7, 1648.
[37] Schmitt (2017): i. m., 20–21.
[38] Schmitt–Vihul: i. m., 1648.
[39] Corn, Gary–Taylor, Robert: Sovereignty in the Age of Cyber. *AJIL Unbound,* 2017, 211.

A második esetkör, amelyet a szerkesztői gárda megvizsgált, az az, amikor egy állam egy kiberműveleten keresztül beavatkozik egy másik állam kormányzati funkcióiba, vagy bitorolja azokat. Ez azért minősül szuverenitás-sértésnek, mert a megcélzott állam kizárólagos jogot élvez e funkciók kapcsán. Nem számít, hogy történt-e fizikai kár, sérülés, vagy hogy a funkcionalitás elvesztése bekövetkezett-e. A szakértők egyetértettek abban, hogy tilos olyan kiberműveletet végrehajtani, amely az eredendően a kormányzati funkciók ellátásához szükséges adatokat vagy szolgáltatásokat zavarja meg. Ilyen lehet például olyan adatok törlése vagy megváltoztatása, amely akadályozza a választások lebonyolítását, vagy az adók beszedését.[40]

Kiemelendő, hogy a szuverenitás megsértését mindig eseti alapon, műveletről műveletre szükséges vizsgálni, figyelembe véve mennyiségi és minőségi kritériumokat, valamint az eset összes körülményét.[41]

Végezetül a szuverenitás kapcsán meg kell említeni azt a szakirodalmi vitát, amelynek mozgatórugója az a kérdés, hogy a szuverenitás a nemzetközi jog elsődleges szabálya-e, amelynek megsértése államfelelősséget keletkeztet, avagy sem. Ahogy már említettem, a Kézikönyv a 4. szabályában úgy rendelkezik, hogy az államok nem hajthatnak végre olyan kiberműveletet, amely sérti egy másik állam szuverenitását.[42] Ebből kétségkívül az következik, hogy a szerkesztők a nemzetközi jog elsődleges szabályaként tekintenek a szuverenitásra. Egyes szerzők ugyanakkor ellenzik azt, hogy ez a tilalom ebben a formában érvényesüljön. Corn és Taylor például amellett érvel, hogy nem megalapozott azoknak a kiberműveleteknek a tilalma, amelyek nem érik el a jogellenes beavatkozás szintjét. A szerzőpáros egyfelől azt mondja, hogy az államok megértik, hogy a kémkedés csak akkor sértheti a nemzetközi jogot, ha az alkalmazott módszerek egyébként megsértik a nemzetközi jog egyéb rendelkezéseit, például a beavatkozás tilalmát vagy az erőszak alkalmazását, ez az analógia pedig alkalmazható a kiberműveletekre is. Továbbá úgy vélik, hogy eltérések vannak abban a tekintetben, hogy a szuverenitás hogyan jelenik meg a nemzetközi jog egyes területein, például a légijogban, a tengerek jogában vagy az űrjogban. Szerintük ez erősíti azt a nézetet, hogy a szuverenitás egy elv, amely az adott területtől és az államok gyakorlati szükségleteitől függően módosítható, nem pedig egy szigorúan meghatározott szabály.[43]

A *Corn és Taylor* által felvetettekre *Michael N. Schmitt,* a Tallinni Kézikönyvet megalkotó szerkesztőgárda vezetője szerzőtársával reagált, és védte meg a Kézikönyv által képviselt álláspontot. Szerintük a kritika nem veszi figyelembe, hogy az említett jogi rendszerek mindegyike a területi integritáson és a sérthetetlenségen alapszik.[44] A szerzők véleménye szerint egyfelől az állami gyakorlat és az *opinio iuris* azt támasztja alá, hogy a szuverenitás a nemzetközi jog elsődleges szabálya. Másfelől pedig a Nemzetközi Bíróság statútumára hivatkoznak, amely a jogszabályok megállapításának segédeszközeiként sorolja fel a bírói döntéseket, illetve a nemzetek legkiválóbb tudósainak tanítását. Előbbi kapcsán a Nemzetközi Bíróság (és elődje) ítéleteiből kö-

[40] Schmitt (2017): i. m., 21–22.

[41] Tsagourias, Nicolas: The legal status of cyberspace: sovereignty redux? In: Nicolas Tsagourias–Russell Buchan (szerk.) *International Law and Cyberspace.* Edward Elgar Publishing, Cheltenham, 2021, 23.

[42] Schmitt (2017): i. m., 22.

[43] Corn–Taylor: i. m., 209–210.

[44] Schmitt–Vihul: i. m., 1644.

vetkeztetnek a szuverenitás elsődlegességére, a Tallinni Kézikönyvre pedig olyan műként tekintenek, amit a legmagasabban kvalifikált szerzők hoztak létre.[45]

2. Az állami gyakorlat

Az elmúlt években érzékelhetően megnőtt azoknak az államoknak a száma, amelyek valamilyen hivatalos állásfoglalást, nyilatkozatot tettek a kibertér és a nemzetközi jog kapcsolatára vonatkozóan. E nyilatkozatok jelentős hányada foglalkozik a szuverenitás kérdésével is. Az alábbiakban ezeket az álláspontokat ismertetem.

Összevetve a különböző állami állásfoglalásokat, leszögezhető, hogy az államok elfogadják, hogy a nemzetközi jogi értelemben vett szuverenitás a kibertérben is alkalmazható. Ugyanakkor az államok között sincs teljes összhang abban a tekintetben, hogy a szuverenitás a nemzetközi jog önálló szabálya-e, vagy pusztán csak elv, amelynek megsértéséhez nem kapcsolódik állami felelősség.

Az államok döntő többsége szerint más állam szuverenitásának megsértése a nemzetközi jog elsődleges, anyagi normái közé tartozik, amelynek megsértése nemzetközi jogellenes cselekmény. Ez a nézet tűnik ki a brazil,[46] a Costa Rica-i,[47] a cseh,[48] a dán,[49] az észt,[50] a finn,[51] a holland,[52] az iráni,[53]

[45] Schmitt–Vihul: i. m., 1650–1651.

[46] *„It is applicable as a standalone rule, including to the use of ICTs by States…"* UNGA, A/76/136, 13 July 2021. 18.

[47] *„Sovereignty is a fundamental principle of international law, underpinning the entire international legal order and firmly grounding the position of States therein." Costa Rica's Position on the Application of International Law in Cyberspace.* Ministry of Foreign Affairs of Costa Rica, 2023, 5. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf (2024. 07. 16.).

[48] *„At the same time, sovereignty is a rule in its own right which is capable of being violated. Thus, cyber activities that do not amount to a prohibited intervention or a prohibited use of force may nevertheless amount to a violation of a State's sovereignty under international law."* Position paper on the application of international law in cyberspace. *Ministry of Foreign Affairs of the Czech Republic,* 2024 (a továbbiakban: Csehország állásfoglalása), 3. https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf (2024. 07. 16.).

[49] *„Denmark is of the view that sovereignty is not only a principle but a primary rule of international law a breach of which amounts to an internationally wrongful act and if attributable to a State it may give rise to State responsibility."* Kjelgaard, Jeppe Mejer–Melgaard, Ulf: Denmark's Position Paper on the Application of International Law in Cyberspace. *Nordic Journal of International Law,* 2023/3, 448. (DOI: 10.1163/15718107-20230001).

[50] *„Sovereignty as a fundamental principle of international law applies in cyberspace."* UNGA, A/76/136, 13 July 2021, 24.

[51] *„Finland sees sovereignty as a primary rule of international law, a breach of which amounts to an internationally wrongful act and triggers State responsibility."* Lehto, Marja: Finland's view on International Law and Cyberspace. *Nordic Journal of International Law,* 2023/3, 463. (DOI: 10.1163/15718107-20230002).

[52] *„It believes that respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act." Appendix: International law in cyberspace.* Government of the Kingdom of the Netherlands (a továbbiakban: Hollandia állásfoglalása), 2019, 2. https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace (2024. 07. 16.).

[53] *„Any utilization of cyberspace if and when involves unlawful intrusion to the cyber structures which is under the control of another state, maybe constituted as the violation of the sovereignty of the targeted state."* General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat. *NourNews,* 2020 (a továbbiakban: Irán állásfoglalása) 4. bekezdés.

az ír,[54] a japán,[55] a kanadai,[56] a kínai,[57] a német,[58] a norvég,[59] az olasz,[60] az osztrák,[61] a román[62] és a svéd[63] állásfoglalásokból.

Ezzel ellentétes nézetet leginkább az Egyesült Királyság képvisel. 2018-ban *Jeremy Wright,* akkori brit főügyész volt az első, aki a szigetországnak a kibertér és a nemzetközi jog kapcsolatát illető álláspontját ismertette. Ebben a beszédében *Wright* úgy fogalmazott: *„[…] nem vagyok meggyőződve arról, hogy ebből az általános elvből jelenleg a tiltott beavatkozáson túlmenően konkrét szabályt vagy további*

[54] *„A violation of a state's sovereignty may arise where a cyber operation attributable to another state causes physical damage to ICT or other infrastructure, functional impairment to such infrastructure, interference with data, and/or secondary effects." Position Paper on the Application of International Law in Cyberspace.* Department of Foreign Affairs, 2023, 6. bekezdés. https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf (2024. 07. 17.).

[55] *„An internationally wrongful act occurs when the conduct of a State consisting of an action or omission violates an obligation prescribed by primary rules of international law. In the case of cyber operations as well, there is an internationally wrongful act when a State violates primary rules, including the principles of sovereignty, non-intervention…" Basic Position of the Government of Japan on International Law Applicable to Cyber Operations.* Ministry of Foreign Affairs of Japan, 2021, 3. https://www.mofa.go.jp/files/100200935.pdf (2024. 07. 17.).

[56] *„Territorial sovereignty is a rule under international law. An infringement upon the affected State's territorial integrity, or an interference with or usurpation of inherently governmental functions of the affected State, would be a violation of territorial sovereignty." International Law applicable in cyberspace*. Government of Canada, 2022 (a továbbiakban: Kanada állásfoglalása), 13. bekezdés. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng (2024. 07. 17.).

[57] *„State sovereignty in cyberspace is a legally binding principle under international law."* Forrás: China's Views on the Application of the Principle of Sovereignty in Cyberspace. *Ministry of Foreign Affairs of the People's Republic of China,* 2021, 3. https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf (2024. 07. 17.).

[58] *„Germany agrees with the view that cyber operations attributable to States which may violate the sovereignty of another State are contrary to international law."* Forrás: On the Application of International Law in Cyberspace. *The Federal Government,* 2021 (a továbbiakban: Németország állásfoglalása), 3. https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf (2024. 07. 17.).

[59] *„Norway is of the view that sovereignty constitutes both an international law principle from which various rules derive, such as the prohibition of intervention and the prohibition of the use of force, and a primary rule in its own right capable of being violated."* Musæus, Vibeke: Norway's Position Paper on International Law and Cyberspace. *Nordic Journal of International Law,* 2023/3, 477. (DOI: 10.1163/15718107-20230003).

[60] *„The principle of sovereignty is a primary rule of international law, the violation of which amounts to an international wrongful act." Italian Position Paper on International Law and Cyberspace.* Italian Ministry for Foreign Affairs and International Cooperation*,* 2021 (a továbbiakban: Olaszország állásfoglalása), 4. https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf (2024. 07. 17.).

[61] *„Respect for the sovereignty of other states is a binding rule of customary international law that also applies to cyber activities."* Forrás: Position Paper of the Republic of Austria: Cyber Activities and International Law. *Government of Austria,* 2024 (a továbbiakban: Ausztria állásfoglalása), 4. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Austrian_Position_Paper_-_Cyber_Activities_and_International_Law_(Final_23.04.2024).pdf (2024. 07. 17.).

[62] *„Romania considers that respect for the state sovereignty is an international obligation per se, the breach of which constitutes an internationally wrongful act."* UNGA, A/76/136, 13 July 2021. 76.

[63] *„However, States also have an obligation to respect the sovereignty of other States, and a breach of this obligation would amount to a wrongful act and give rise to State responsibility."* Engdahl, Ola: Sweden's Position Paper on the Application of International Law in Cyberspace. *Nordic Journal of International Law,* 2023/3, 492. (DOI: 10.1163/15718107-20230004).

tilalmat lehet kivetni a kibertevékenységre. Az Egyesült Királyság kormányának álláspontja ezért az, hogy nincs ilyen szabály jelenleg a nemzetközi jogban."[64]

Ezt a különutas álláspontot először 2021-ben erősítették meg: *„[a]z Egyesült Királyság emlékeztet arra, hogy az államok tevékenységére vonatkozó minden tilalmat, akár a kibertérrel, akár más ügyekkel kapcsolatban egyértelműen rögzíteni kell a nemzetközi szokásjogban, vagy egy szerződésben. Az Egyesült Királyság úgy véli, hogy a szuverenitás általános fogalma önmagában nem nyújt elegendő vagy egyértelmű alapot egy konkrét szabály vagy magatartásra vonatkozó további tilalom extrapolálásához."*[65] Majd 2022-ben ismét: *„[a]z államok eltérő véleményt fogalmaztak meg a szuverenitás pontos jelentőségéről a kibertérben. Az Egyesült Királyság még 2021 júniusában megismételte saját álláspontját a kérdésben. Nevezetesen, hogy az államok tevékenységének bármilyen tilalmát, akár a kibertérrel, akár más ügyekkel kapcsolatban a nemzetközi jogban egyértelműen rögzíteni kell. A szuverenitás általános fogalma önmagában nem ad elengedő vagy egyértelmű alapot egy konkrét szuverenitási szabály vagy a kibermagatartás további tilalmának extrapolálásához."*[66] Az Egyesült Államok részben szintén osztja az Egyesült Királyság álláspontját.[67]

A szakirodalom szerint minden államnak tiszteletben kell tartani a többi állam szuverenitását, tehát nem végezhetnek olyan kiberműveletet, amely egy másik állam szuverenitását sértené. Az állami gyakorlatokat összevetve azt láthatjuk, hogy e tekintetben konszenzus alakult ki az államok között is. Azonban továbbra sincs egyöntetű szabály arra vonatkozóan, hogy milyen kritériumok vagy milyen küszöb elérése szükséges ahhoz, hogy a szuverenitás megsértéséről lehessen beszélni. Fontos megemlíteni azt is, hogy a különböző állami állásfoglalások eltérő mennyiségben és minőségben foglalkoznak a szuverenitás kérdésével.

Elsőként megemlítendő, hogy több állam nyilatkozatában is említésre kerül, hogy az „elhanyagolható" hatású, vagyis a *„de minimis"* küszöböt el nem érő kiberműveletek nem minősülnek a szuverenitás megsértésének. A kanadai nyilatkozat szerint *„[a]z elhanyagolható, vagy de minimis hatásokat okozó tevékenységek nem minősülnek a területi szuverenitás megsértésének, függetlenül attól, hogy kiber- vagy nem kiberkontextusban végzik őket".* Egyúttal egy példát is hoz a nyilatkozat, amely értelmében az újraindítást, vagy az operációs rendszer újratelepítését igénylő kibertevékenység valószínűleg nem sérti a területi szuverenitást.[68] A csehek legújabb

[64] Cyber and International Law in the 21st Century. Speech of Jeremy Wright. Government of the UK, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (2024. 06. 08.).

[65] Application of international law to states' conduct in cyberspace: UK statement. Policy Paper. *Government of The UK,* 10. bekezdés. https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement (2024. 07. 17.).

[66] International Law in Future Frontiers. Speech of Rt. Hon Suella Braverman. *Government of The UK,* https://www.gov.uk/government/speeches/international-law-in-future-frontiers (2024. 06. 08.).

[67] *„For cyber operations that would not constitute a prohibited intervention or use-of-force, the Department believes there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's. territory."* DOD General Counsel Remarks at. U.S. Cyber Command Legal Conference. Speech. US. Department of Defense, https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/ (2024. 06. 08.).

[68] Kanada állásfoglalása, 17. bekezdés.

nyilatkozatában is megjelenik a küszöb kérdése, amikor úgy fogalmaznak, hogy az elhanyagolható vagy *de minimis* küszöböt meghaladó kibertevékenységek, amelyek jelentős káros hatásokat okoznak egy másik állam területén az adott állam beleegyezése nélkül, a szuverenitás megsértését jelenthetik.[69] A német nyilatkozat pedig csupán egy mondatot szentel a kérdésnek, amikor azt mondja, hogy *„az elhanyagolható fizikai hatások, és bizonyos hatásküszöb alatti funkcionális károsodások – önmagukban véve – nem tekinthetők a területi szuverenitás megsértésének”.*[70] Végezetül pedig a dán nyilatkozat annyit jegyez meg, hogy az elhanyagolható fizikai hatást vagy a funkcionalitás elvesztését okozó kibertevékenységek általában nem tekinthetők a szuverenitás megsértésének.[71]

A Tallinni Kézikönyv által felvázolt rendszerben a szuverenitás megsértése kétféle módon következhet be a kibertér esetén: az első esetkör, amikor az állam területi épsége kerül megsértésre, a másik pedig, amikor a kiberművelet a kormányzati funkciók ellátásába avatkozik be.

Az állásfoglalásokból kiderül, hogy az államok egy csoportja kifejezetten egyetért a Tallinni Kézikönyvben meghatározottakkal. Ebbe a csoportba tartozik például Németország is, amelynek nyilatkozata rögzíti, hogy ha egy kiberművelet betudható egy államnak, és ez a művelet egy másik állam területén fizikai hatásokat és károkat eredményez, akkor sérti az adott állam területi szuverenitását. Ugyanez igaz a jelentős funkcionális károsodásra akkor is, ha nincs fizikai kár, csupán a szoftverrel kapcsolatos működési probléma lép fel.[72] Ehelyütt szeretnék utalni arra, hogy az állásfoglalás e része összhangban van a humanitárius nemzetközi jog és a kibertér kapcsolatát vizsgáló bekezdésekkel. Németország néhány más állammal egyetemben elismeri, hogy – humanitárius nemzetközi jog értelmében – az adatok katonai célponttá válhatnak.[73] Szintén *expressis verbis* jelenik meg a Kézikönyv a holland nyilatkozatban is: *„[á]ltalánosságban a kormány támogatja a Tallinni Kézikönyv szakértői által javasolt 4. szabályt, amely a szuverenitás határainak megállapításáról szól a kibertérben. E szabály értelmében a szuverenitás megsértésének minősül, ha a célállam területi integritása sérül meg, illetve, ha beavatkozás történik egy másik állam kormányzati funkcióiba vagy azok elbitorlása történt. E tényezők pontos értelmezése vita tárgya.”*[74] Részletesen taglalja a Kézikönyv által felállított rendszert a kanadai nyilatkozat is, amely először a területi integritás megsértéséről, majd a következő bekezdésekben a kormányzati funkciók megzavarásáról szól.[75] Finnország nyilatkozata is visszautal a szakértői gárda által összeállított dokumentumra, amikor kinyilvánítja, hogy a szuverenitás tekintetében az állásfoglalás összhangban van a Kézikönyvben megállapított szabállyal.[76]

Bizonyos mértékig Csehország 2024-es állásfoglalásában is megjelenik a fentebb említett rendszer, külön kiemelve a halált vagy fizikai kárt okozó kiberműveletet,

[69] Csehország állásfoglalása, 5. bekezdés.
[70] Németország állásfoglalása, 4.
[71] Kjelgaard–Melgaard: i. m., 449.
[72] Németország állásfoglalása, 4.
[73] Kis Kelemen Bence: Protection of (Personal) Data in Armed Conflicts. *Baltic Journal of Law & Politics,* 2024/1, 13. (DOI: 10.2478/bjlp-2024-0001).
[74] Hollandia állásfoglalása, 3.
[75] Kanada állásfoglalása, 15–18. bekezdés.
[76] Lehto: i. m., 462.

valamint a kormányzati funkciók ellátását megzavaró kiberműveleteket, amelyek adott esetben sérthetik a területi állam szuverenitását.[77] A skandináv államok nyilatkozatai is hasonló logikát követnek, ugyanakkor a Kézikönyvet kifejezetten nem említik a szuverenitással kapcsolatosan. A norvég nyilatkozatban szerepel, hogy egy másik állam területén, kibereszközökkel történő fizikai károkozás könnyen a területi szuverenitás megsértésének minősülhet. A fizikai károk mellett a funkcionalitás elveszítését nevesítik, illetve a kormányzati funkciók elbitorlása vagy megzavarása is megjelenik. A nyilatkozat különlegessége, hogy egy fiktív példát is hoz: Norvégia szerint egy petrolkémiai üzem ipari vezérlőrendszere ellen végrehajtott kiberművelet az állam területi szuverenitásának megsértését jelenti, ha az az üzem meghibásodásához és tűzhöz vezet.[78] A svéd nyilatkozat csupán röviden foglalkozik a kérdéssel, amikor megjegyzi: *„a szuverenitás megsértése adódhat olyan kiberműveletből, amely a funkcionalitás károsodását vagy elvesztését eredményezi. Az adatok fizikai sérülés nélküli megváltoztatása szintén sértheti a szuverenitást. Az állam alapvető kormányzati funkcióiba való beavatkozás az állam szuverenitásának megsértését is jelentheti, ideértve a kibereszközökkel történő beavatkozást is."*[79] Dánia a Kézikönyv kifejezett említése nélkül veszi át annak terminológiáját, amikor nyilatkozatában rögzíti, hogy *„a kiberművelet jogszerűségét két különböző alapon kell értékelni: a célállam területi integritása megsértésének mértéke, valamint az alapján, hogy történt-e beavatkozás a kormányzati funkciókba".*[80] Külön kiemelném Ausztria nyilatkozatát, amely a legfrissebb a nyilatkozó államok egyre növekvő sorában. Ebben a nyilatkozatban is megjelenik a kettős rendszer, amely szerint akkor sérti egy kibertevékenység egy másik állam szuverenitását, ha a művelet megsérti az állam területi integritását, vagy amikor lényeges kormányzati funkciókba történő beavatkozást vagy bitorlást jelent. Rögzítik az állásfoglalásban, hogy a fizikai károkat okozó kibertevékenységek biztosan sértik az állami szuverenitást. A nyilatkozat példát is hoz, amelyben 'A állam' a kibertérben folytat kémtevékenységet 'B állam' külügyminisztériuma ellen, hogy hozzáférést szerezzen az állam belső információs rendszeréhez. 'B állam' felfedezi, hogy rendszere kompromittálódott, ezért teljes leállítást kell végrehajtania, valamint ideiglenes rendszert kell kialakítania, amíg a rendszer helyreállítását elvégzik. Ausztria szerint az ilyen jellegű kibertevékenység 'B állam' szuverenitásának megsértését jelentené.[81]

Franciaország némileg alternatív tesztet javasol, amikor úgy fogalmaz, hogy *„bármely, az ország digitális rendszerei elleni kibertámadás, vagy bármely olyan hatás, amelyet egy állami szerv, kormányzati hatáskörrel rendelkező személy vagy entitás, illetve egy vagy több személy az állam utasítására, vagy irányítása alatt fejt ki kibereszközökkel francia területen, a szuverenitás megsértését fogja jelenteni".*[82]

[77] Csehország állásfoglalása, 6. bekezdés.

[78] Musæus: i. m., 477–478.

[79] Engdahl: i. m., 492. Svédország ugyanakkor nem foglalt állást arra vonatkozóan, hogy katonai célpontnak tekinthetők-e az adatok a humanitárius nemzetközi jog alapján. Kis Kelemen: i. m., 13.

[80] Kjelgaard–Melgaard: i. m., 449.

[81] Ausztria állásfoglalása, 4–5.

[82] International Law Applied to Operations in Cyberspace. Paper shared by France with the Open-ended working group established by resolution 75/240. Government of France, 2021 (a továbbiakban: Franciaország

Hasonlóképpen az iráni nyilatkozat is úgy szól, hogy *„a kibertér bármely felhasználása ha és amikor az egy másik állam ellenőrzése alatt álló kiberinfrastruktúrába való jogellenes behatolást von maga után, a célzott állam szuverenitása megsértésének minősülhet”*.[83]

Az új-zélandi dokumentumban pedig a kiberművelet hatásának mértéke és jelentősége, valamint a művelet célja mellett a célpont természetét is megemlítik mint releváns faktort, ami egyedüliként ebben az állásfoglalásban szerepel.[84]

Számos állam nyilatkozatában megjelenik tehát a kiberműveletek esetről esetre történő vizsgálatának követelménye annak megállapítására, hogy a művelet sérti-e más állam szuverenitását. A skandináv államok nyilatkozatain kívül[85] előkerül többek között a francia,[86] kanadai,[87] az olasz[88] és az új-zélandi[89] állásfoglalásban is.

3. Példák a közelmúltból

2010 jelentős mérföldkőnek tekinthető a kiberműveletek egyébként meglehetősen rövid történelmében. A *Stuxnet* névre hallgató, vélhetően az Egyesült Államok és Izrael titkosszolgálatai által fejlesztett kártevő bejutott az iráni Natanz városában található urándúsító üzem rendszerébe. Annak ellenére, hogy a létesítményt üzemeltető operátorok hosszú időn keresztül a helyes értékeket kapták az irányítóközpontban, a kártevő észrevétlenül a centrifugák meghibásodását okozta. Mire az akció kiderült, a károsodás már visszafordíthatatlan volt. Ez volt az első alkalom, hogy egy kiberművelet tesztüzemen kívül fizikai károkat okozott.[90] Az eset kapcsán véleményem szerint Irán szuverenitásának megsértése kétségkívül megállapítható, a szakirodalom ráadásul akként vélekedik, hogy ez a művelet potenciálisan akár erőszak alkalmazásának is minősülhet.[91]

2017-ben két, meglehetősen hasonló zsarolóvírus támadás zajlott le a kibertérben. A *WannaCry* nevű kártevő – amellyel kapcsolatban leggyakrabban észak-koreai kötődést emlegetnek – világszerte végzett pusztítást. A legismertebb áldozata kétségtelenül a brit egészségügyi rendszer (NHS) volt. A vírus elszabadulását követően több egészségügyi intézményben vissza kellett térni a papíralapú ügyintézésre,

állásfoglalása) 3. https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf (2024. 07. 17.).

[83] Irán állásfoglalása.

[84] The Application of International Law to State Activity in Cyberspace. Government of New Zealand, 2020 (a továbbiakban: Új-Zéland állásfoglalása), 15. bekezdés. https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf (2024. 05. 17.).

[85] Kjelgaard–Melgaard: i. m., 449; Lehto: i. m., 463; Musæus: i. m., 476; Engdahl: i. m., 492.

[86] Franciaország állásfoglalása, 3.

[87] Kanada állásfoglalása, 21. bekezdés.

[88] Olaszország állásfoglalása, 4.

[89] Új-Zéland állásfoglalása, 15. bekezdés.

[90] A Stuxnet-ügyről szóló összefoglaló dokumentum a Council on Foreign Relations adatbázisában érhető el. https://www.cfr.org/cyber-operations/Stuxnet (2024. 05. 09.).

[91] Schmitt (2017): i. m., 342.

legalább 20 000 előjegyzett időpontot kellett törölni, és öt kórházban teljesen leállt a sürgősségi ellátás.[92] Nem sokkal később egy másik vírus, a *NotPetya* is utat tört magának, célpontja főként Ukrajna volt. Ennek tükrében nem meglepő, amikor ukrán politikusok és az Ukrán Biztonsági Szolgálat (SZBU) Oroszországot vádolták a zsarolóvírus létrehozásával és elterjesztésével. Úgy vélték, hogy *„a vírus fő célja fontos adatok megsemmisítése, megzavarva ezzel a köz- és magánintézmények munkáját, pánikot terjesztve az emberek között"* – állt az SZBU közleményében. Az orosz állami szervek nem reagáltak érdemben a vádakra. Érdekesség, hogy kis számban ugyan, de orosz vállalatok is érintettek voltak a támadásban.[93]

A fentebb említett rosszindulatú programok gyorsan elterjedtek a világ számos országában. Hatásuk főként a számítógépes rendszerekbe való behatolásból, az adatok lezárásból, illetve megsemmisítéséből állt. A kiberakciók nem voltak kényszerítő jellegűek az érintett államokra nézve, így nem tekinthetők jogellenes beavatkozásnak. Nem okoztak továbbá fizikai sérüléseket vagy halált, így a jelenlegi nemzetközi jogi szabályozás szerint nem merül fel az erőszak alkalmazásának kérdése sem. A zsarolóvírusok esetében az adatokhoz való hozzáférés megakadályozása, valamint törlése, illetve a kiberinfrastruktúra nem kívánt működésének előidézése arra enged következtetni, hogy ezek a műveletek sérthették a területi állam szuverenitását.[94]

2020 talán túlzás nélkül legnagyobb kibertámadása a SolarWinds vállalat rendszerének feltörése volt. Az eset kapcsán nem csupán a cég volt érintett, hanem egy sokkal nagyobb ellátási lánc, amelybe több ezer szervezet tartozik. A sértettek között volt az Egyesült Államok kormánya is. A SolarWinds egy jelentős, szoftverekkel foglalkozó vállalat az Egyesült Államokban, amely rendszerfelügyeleti eszközöket biztosít hálózat- és infrastruktúra-felügyelethez, valamint egyéb műszaki szolgálatásokat is végez szervezetek százezrei számára, szerte a világon. A cég termékei között szerepel az Orion nevű informatikai teljesítményfigyelő rendszer. Felügyeleti rendszerként az Orionnak hozzáférése van a számítógépes rendszerekhez, valamint napló- és rendszeradatokkal rendelkezik. A támadás során a – vélhetően orosz – hackerek több ezer olyan hálózathoz és rendszerhez, valamint az ezekhez kapcsolódó adatokhoz jutottak hozzá, amelyek a SolarWinds üzleti körébe tartoztak. A művelet példátlanul széles körű volt, és az egyik legnagyobb, amit valaha is rögzítettek.[95]

Ha a SolarWinds feltörését valóban egy állami szereplő – jelen esetben Oroszország – hajtotta végre, az az állami szuverenitás megsértésének minősülhet. Le kell szögezni, hogy a vállalatot ért támadás nem okozott sérülést, halált vagy fizikai

[92] Hern, Alex: WannaCry, Petya, NotPetya: how the ransomware hit the big time in 2017. *Guardian,* https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware (2024. 06. 09.).

[93] Polityuk, Pavel: Ukraine points finger at Russian security services in recent cyber attack. *Reuters,* https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19M39P/ (2024. 06. 09.).

[94] Schmitt, Michael N.–Biller, Jeffrey: The NotPetya Cyber Operation as a Case Study of International Law. *EJIL:Talk!,* https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/ (2024. 06. 09.); Delerue: i. m., 230–231.

[95] Oladimeji, Saheed–Kerner, Sean Michael: SolarWinds hack explained: Everything you need to know. *TechTarget,* https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (2024. 06. 09.); Temple-Raston, Dina: A 'Worst Nightmare' Cyberattack: The Untold Story of The SolarWinds hack. *NPR,* https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (2024. 06. 09.).

károkat. Ugyanakkor, a Tallinni Kézikönyv egyes szerkesztői arra az álláspontra helyezkedtek, hogy a szuverenitás megsértését jelentené – a funkcionalitás elvesztése miatt – ha *„az operációs rendszert vagy más adatbázist, amelyre a megcélzott kiberinfrastruktúra támaszkodik, rendeltetésének teljesítéséhez újra kell telepíteni”.*[96] Itt szükséges megjegyezni, hogy az Amerikai Kiberbiztonsági és Infrastruktúra-biztonsági Ügynöksége (CISA) az események felderítését követően utasította valamennyi érintett felhasználót az újratelepítésre.[97] A szuverenitás megsértése származhat egy állam kormányzati funkcióiba történő beavatkozásból, legyen szó akár a fizikai, akár a kibertérről. Az Egyesült Államok pénzügyminisztériuma, illetőleg a Pentagon is érintett volt a támadásban, így legalább annyiban, amennyiben e kormányzati rendszerek felett megszerezték az irányítást, megsértették az Egyesült Államok szuverenitását.[98] Egyes szerzők azonban ezzel ellentétesen érvelnek. Szerintük a SolarWinds feltörése pusztán kémkedés, és 'nagyon távol áll' a kormányzati funkciókba történő beavatkozástól, például az adatok módosításától, a digitális kommunikáció blokkolásától vagy a választások megzavarásától.[99]

A Colonial Pipeline nevű olajvezeték az egyik legfontosabb és legnagyobb csővezeték az Egyesült Államokban. A több mint 5500 mérföldön átívelő létesítménynek 1962-ben indult a működése, feladata pedig az volt, hogy segítse az olaj szállítását a Mexikói-öbölből a keleti part államaiba. Az elmúlt években a vezeték azért került be a hírekbe, mert 2021 májusában zsarolóvírus-támadás áldozata lett. A kiberművelet több szakaszból állt a vezeték informatikai rendszerei ellen. A művelet akkor kezdődött, amikor a DarkSide néven azonosított hackercsoport hozzáfért a Colonial Pipeline hálózathoz. A támadók 100 gigabájtnyi adatot loptak el, ezt követően zsarolóvírussal fertőzték meg az informatikai hálózatot, amely számos számítógépes rendszert érintett. A vállalat fizetett a hackereknek, hogy visszaszerezzék az irányítást a rendszerek felett. A támadás következtében a csővezeték néhány napra leállt, ami széles körben érintette a fogyasztókat és a légitársaságokat a keleti parton. Emiatt Joe Biden elnök szükségállapotot hirdetett.[100]

A támadás kapcsán véleményem szerint felmerülhet a szuverenitás megsértése, hiszen az adatokhoz való hozzáférés korlátozása, valamint az, hogy napokra leállt a csővezeték elegendő alapot szolgáltat ehhez. Ugyanakkor a DarkSide csoport, amely elkövette a támadást, vélhetően nem áll túl közeli kapcsolatban a Kremllel. 2022 elején az orosz belföldi hírszerző ügynökség letartóztatta a fél évvel korábbi zsarolóvírus-támadásért felelős hackereket. A szuverenitás megsértéséhez szükséges, hogy a támadás betudható legyen egy államnak, a nem állami szereplők, magánszemélyek nem tudják megsérteni egy másik állam szuverenitását.

---

[96] A puszta újraindítás itt nem elégséges, kifejezett újratelepítésről van szó. Schmitt (2017): i. m., 20–21.

[97] ED 21-01: Mitigate SolarWinds Orion Code Compromise. *Cybersecurity and Infrastructure Security Agency,* https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise (2024. 06. 09.).

[98] Coco, Antonio–Dias, Talita–van Bentham, Tsvetelina: Illegal: The SolarWinds Hack under International Law. *European Journal of International Law,* 2022/4, 1280. (DOI: 10.1093/ejil/chac063).

[99] Eichensehr, Kristen: Not Illegal: The SolarWinds Incident and International Law. *European Journal of International Law,* 2022/4, 1270. (DOI: 10.1093/ejil/ehac060).

[100] Kerner, Sean Michael: Colonial Pipeline hack explained: Everything you need to know. *Techtarget,* https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know (2024. 06. 13.).

2022. február 24. napján Oroszország teljes körű inváziót indított Ukrajna ellen. Ugyanezen a napon a hajnali órákban kibertámadás érte a Viasat vállalat műholdas rendszereit. A támadás jelentős kommunikációs kiesést okozott Ukrajnában, ideértve a katonai és kormányzati ügynökségek között zajló információáramlást is. Az akció hatása több tízezer felhasználót érintett Európa-szerte, köztük műholdas internetfelhasználókat Lengyelországban, Németországban és az Egyesült Királyságban. A támadás mellékhatása volt, hogy Németországban a több mint 5000 szélturbinát működtető Enercon vállalat felügyeleti és vezérlési rendszere is leállt, a turbinák hetekig nem működtek. Fontos megjegyezni azonban, hogy a támadás következtében fizikai károk nem keletkeztek sem műholdakban, sem egyéb hálózati infrastruktúrában. Több nyilatkozat is arra utal, hogy a támadás célja az ukrajnai műholdas kommunikáció megszakítása lehetett, különösen azért, mert ugyanezen a napon az orosz szárazföldi haderő fegyveres támadást indított nyugati szomszédja ellen. Szakértők szerint a Viasat hálózata kommunikációs szolgáltatásokat biztosított az ukrajnai katonai parancsnokságoknak.[101] Ha csupán önmagában vizsgáljuk ezt a kiberműveletet, és eltekintünk attól, hogy Oroszország inváziója Ukrajna ellen fegyveres támadásnak minősül, akkor véleményem szerint azt a következtetést lehet levonni, hogy ez a kiberművelet önmagában is megsértette Ukrajna szuverenitását, tekintettel arra, hogy akadályozta az információk áramlását a kormányzati szervek és a katonai alakulatok között. Ugyanakkor az eset összes körülményét figyelembe véve azt gondolom, hogy az erőszak alkalmazásának szintjét a művelet nem érte el.

4. Összegzés

A szuverenitás az egyik legfontosabb alapelv a nemzetközi jogban és az államok közötti kapcsolatokban. A Tallinni Kézikönyv, amely talán a legjelentősebb magánkodifikációs műnek tekinthető a nemzetközi jog és a kibertér kapcsolatát illetően, szintén kiemelten foglalkozik a szuverenitás kérdésével. A szerkesztői gárda kivétel nélkül egyetértett abban, hogy az állami szuverenitásra vonatkozó nemzetközi jogi szabályok a kibertérben is alkalmazandók. Az állam szuverén hatalmat gyakorol a területén található kiberinfrastruktúra, a személyek és a kibertevékenységek felett. Ez azt jelenti, hogy meghozhat minden olyan intézkedést, amelyet szükségesnek tart a kiberinfrastruktúrával, kibertevékenységgel és a tevékenységet végző személyekkel kapcsolatban mindaddig, amíg ezt nemzetközi jogi kötelezettségeivel összhangban teszi.

A Kézikönyv által felállított rendszer értelmében a szuverenitás megsértése két fő módon lehetséges. Az első eset az állam területének épségét vagy sérthetetlenségének megsértését jelenti. A legtöbb szakértő egyetértett abban, hogy egy kiberművelet abban az esetben sértheti a területi állam szuverenitását, ha fizikai kárt vagy sérülést okoz. A fizikai károkon túl pedig a működőképesség (funkcionalitás)

[101] Az akció összefoglalója, például: https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat-#overview (2024. 06. 14.).

elvesztése is releváns szempont lehet. A pontos küszöbértékek meghatározására nem került sor. A második esetkör, amelyet a szerkesztői gárda megvizsgált, az az, amikor egy állam egy kiberműveleten keresztül beleavatkozik egy másik állam kormányzati funkcióiba vagy elbitorolja azokat. Ebben az esetben nem számít az, hogy történt-e fizikai kár, sérülés, sem az, hogy a funkcionalitás elvesztése bekövetkezett-e.

Az elmúlt években jelentősen megnőtt azon államok száma, amelyek valamilyen hivatalos állásfoglalást, nyilatkozatot tettek a kibertér és a nemzetközi jog viszonyáról. E dokumentumok szinte kivétel nélkül érintik a szuverenitás kérdését. A nyilatkozó államok elfogadják, hogy a szuverenitás, mint nemzetközi jogi alapelv a kibertérre is érvényes. Ugyanakkor – főként az Egyesült Királyságnak köszönhetően – nincs teljes konszenzus az államok között a tekintetben, hogy a szuverenitás a nemzetközi jog önálló szabálya-e, amelynek megsértése nemzetközi felelősséget keletkeztet. Ez a vita egyébként a szakirodalomban is megjelenik.

Az államok egyetértenek abban, hogy nem hajtható végre olyan kiberművelet, amely sérti más államok szuverenitását. Vannak államok, amelyek kifejezetten elismerik nyilatkozataikban a szuverenitás megsértésének a Tallinni Kézikönyvben meghatározott esetköreit. Ebbe a csoportba tartozik Németország, Hollandia és Kanada. Más államok, mint Franciaország vagy Új-Zéland, további kritériumokat is meghatároznak. A legtöbb állam egyetért abban is, hogy esetről esetre, műveletről műveletre kell vizsgálni, hogy az adott művelet sérti-e a területi állam szuverenitását.

Végezetül fontosnak tartom megjegyezni, hogy bár számos környező állam, például Németország, Ausztria, Csehország, Lengyelország vagy Románia is állást foglalt a kibertér és a nemzetközi jog kapcsolatát illetően, hazánk részéről egyelőre ez nem történt meg. Úgy gondolom, Magyarország számára is fontos lenne egy mélységében és terjedelmében hasonló állásfoglalás elfogadása. E dokumentumnak véleményem szerint mindenképp tartalmaznia kellene az állami szuverenitásnak a kibertérben történő alkalmazásával kapcsolatos álláspontot. Egy ilyen jellegű nyilatkozat nemcsak tudományos, de nemzetstratégiai és külpolitikai szempontból is hasznos lehet.