Hordós Alex[3]

NINCS MÉG A KÜSZÖBÖN A NEMZETKÖZI KIBERVÉDELMI MEGÁLLAPODÁS

Scott Neuman – Greg Myre: Hacks Are Prompting Calls For A Cyber Agreement, But Reaching One Would Be Tough)

2021 nyarán két zsarolóvírusos támadás érte az Amerikai Egyesült Államokat: májusban a Colonial nevű kőolajvezetéket, míg júliusban a JBS húsipari vállalat gyárát támadták meg ismeretlen hátterű hackerek. Az esetek a biztonságpolitikai megfontolásokkal összhangban egy nagyon is aktuális kérdést vetettek fel: miként lehetne szabályozni a nemzetközi kibertechnológia felhasználását?

A jelenleg hatályos nemzetközi jogi instrumentumok közül az Európa Tanács keretében tető alá hozott Budapesti Egyezmény (Egyezmény a Számítástechnikai Bűnözésről) az, ami a kibervédelem és a kiberbűnözés elleni küzdelem nemzetközi rezsimjének elsődleges (és a mai napig egyetlen) multilaterális normája. A szerződésnek tagja az Egyesült Államok, az európai kontinens zöme, valamint néhány másik állam különböző kontinensekről. Hátránya viszont a szerződésnek, hogy a kiberhadviselésben aktív nemzetközi szereplők, így Kína, Irán, Észak-Korea vagy éppen Oroszország nem tagja a megállapodásnak.

Oroszország pedig éppen az az állam, amelyet a nyári támadásokkal összefüggésbe hoztak: a Nemzetbiztonsági Ügynökség (*National Secuity Agency*, *NSA*) állítása szerint Moszkva több ízben támadja kormányzati és magánszemélyek eszközeit. Június közepén Genfben találkozott az év elején beiktatott Joe Biden Vladimir Putin orosz elnökkel, ahol kiemelte, hogy az Egyesült Államok nem fogja válasz nélkül hagyni a kibertámadásokat, különösen akkor, ha azok kritikusan fontos infrastruktúrát érintenek.

Az elsődleges probléma egy tényleg átfogó, nemzetközi kiberbűnözést szankcionáló szerződéssel kapcsolatosan a felek tárgyalóasztalhoz ültetése lesz. Ennek egyik oka, hogy a kibertámadások tipikus „*low-cost*, *high reward*" cselekmények, vagyis alacsony kockázat mellett lehet jelentős eredményt elérni velük. A nemzetközi politikában a geopolitikai-hatalmi pozíciókat javíthatják ezek a kibertámadások, mivel a katonai, hírszerzési és egyéb, az állam védelme szempontjából fontos apparátusok digitális szegmensének meggyengítésére alkalmasak. Az NSA korábbi munkatársa, April Falcon Doss szerint a szerződés betartásának monitorozása is kihívásokat jelentene: míg a nukleáris

[3] Jogászhallgató, ELTE ÁJK, 2020-ban nemzetközi tanulmányok alapszakon végzett a BCE-n.

fegyverzetkorlátozó szerződéseknél a kapacitáscsökkentést, a töltetek megsemmisítését és a gyártási folyamatokat jól lehet ellenőrizni, addig a számítógépes kódok előállítását „nem lehet látható módon ellenőrizni".

Klasszikus problémája a 21. századnak az is, hogy a nem állami szereplők megállítása akkor is próbatétel marad, ha az államok meg tudnak állapodni a kiberbiztonsági rezsim játékszabályaiban. A bevezetőben említett támadásokat is oroszországi bűnszervezetekre fogták, nem pedig az orosz kormányzatra. Ebben az összefüggésben is megjelenik a nemzetközi jog problematikája, nevezetesen a betudhatóság (*attributability*), vagyis az, hogy mennyiben felelős az állam a saját állampolgárai által, saját területén elkövetett nemzetközi jogi jogsértésekért (valamint, hogy az államnak volt-e effektív befolyása az adott tevékenységre). Glenn Altschulter professzor szerint ezen faktorok beazonosítása is hatványozottan nehezebb, mivel a támadók el tudják fedni lokációjukat a valós IP-cím elrejtésével. Altschulter és Robert G. Papp, a Center for Cyber Intelligence at the Central Intelligence Agency volt igazgatója is azon az álláspontón van, hogy legalább bilaterális szinten meg kell próbálni megállapodni Oroszországgal a kiberbűnözés területén.

A kibertérben végzett káros tevékenységek, bár nem kézzelfoghatók, megfelelő mértékben nagyon is valós, fizikai károkat tudnak okozni. A helyzet kezelése ezért is egyre égetőbb, mivel a globalizált, internet-dependens világunkban a digitális hálózatok elleni rosszindulatú támadások emberéletekbe is kerülhetnek. A genfi Biden-Putyin csúcson, bár szerződéses megállapodásról nem esett szó, a két fél ígéretet tett a párbeszédre, amely kapcsán megindulhat azon alapvető normák formálódása, amely keretek közt tartja a (virtuális térben egyébként nehezen értelmezhető) határokon átívelő kiberbűnözést.