Előszó

Kibertámadás. Egyre többször hallani a kifejezést a médiában, de kevesen tudják, mit is jelent tulajdonképpen. Az incidensek mögött ugyanis több különböző motivációt találhatunk. A legtöbb esetben anyagi haszonszerzés hajtja az elkövetőket, amivel leggyakrabban találkozunk tehát, az a kiberbűnözés. Megítélése egyértelműen a kiberbűnözésről szóló budapesti egyezmény körébe tartozik, és alapvetően nincsen vita arról az államok között, hogy üldözendő cselekmény, bár az akarat nyugatról keletre, a képesség pedig északról délre csökken ezen bűncselekményág megfékezésére.

Szintén gyakran lehet hallani információszerzési célzattal véghez vitt támadásokról, az úgynevezett kiberkémkedésről. Amennyiben ezt állami szereplő hajtja végre, a cselekmény nemzetközi jogi megítélése szürke zónába tartozik, de gyakran kötődik valamilyen katonai szervezethez. Ritkán, de találkozhatunk hacktivista-, illetve kiberterrorista-cselekedetekkel is, amikor a csoport célja valamilyen politikai ideológia terjesztése, esetleg ennek az ideológiának a támogatására valamilyen kiberfizikai rendszeren keresztül pusztítás végrehajtása. Ezeket a nemzeti jog kezeli, az eddig ismert esetekben ugyanis államoktól független csoportosulások, például az Anonymous csoport, vagy államokhoz nem egyértelműen, inkább patrióta alapon kapcsolódó csoportok tevékenységét lehetett megfigyelni.

Végül idetartoznak az egyértelműen katonai műveletek, azaz a nyilvánosság számára is ismert kiberhadviselés, amely egyre gyakrabban része, támogatója a hagyományos, kinetikus műveleteknek. Összességében viszont azt lehet érzékelni, hogy az államok katonai műveleteik során akár leplezetten, akár nyíltan, de mind a négy motivációt előszeretettel használják fel. Könyvünk célja éppen ezért az, hogy áttekintsük a kiberhadviselés ismert történetét, és a nyilvánosság számára is megismerhető, mérvadó források segítségével, kritikus elemzéssel bemutassuk az olvasónak az államok által használt kiberműveleti eszköztárat.

Ez már csak azért is fontos terület, mert a legtöbb kibertámadás nem éri el azt a szintet, hogy állam elleni támadásnak nevezhessük – habár az a határ sem egyértelmű, ahonnan már az egész államot érintő tevékenységről beszélhetünk. Általánosságban a tulajdon megsemmisülése vagy az ember sérülése lehet az a kulcsmomentum, amely a fizikai világban kinetikus vagy a kibertérben informatikai jellegű erő alkalmazását válthatja ki egy viszontválaszban. De ez még mindig nem háború a szó jogi értelmében. Michael Schmitt

és Liis Vihul, a téma két elismert kutatója éppen ezért felhívja a figyelmet arra, hogy a „háború", így a „kiberháború" fogalma is meghaladott a nemzetközi jog fogalmi keretei között, mert a 20. század közepétől a „fegyveres konfliktus" szóhasználat terjedt el a négy genfi egyezménnyel párhuzamosan. A humanitárius jog szempontjából ugyanis nem számít, hogy a hadviselő felek betartották-e a hadüzenet formai követelményeit, vagy sem. A katonai jellegű kibertámadások megítélése abban az esetben egyértelmű, amikor egy hagyományos fegyveres konfliktus kísérőjeként jelennek meg, ahogy történt az 2008-ban, a grúz–orosz konfliktusban vagy a szíriai polgárháborúban. Ezekben az esetekben minden hadviselő félnek be kell tartania a humanitárius jog szabályait. A kiberháborút tehát szerencsésebb „kibertérben történő fegyveres konfliktusnak" nevezni, így megkülönböztetve azt a békeidőben végrehajtott kibertéri műveletektől a nemzetközi jog szempontjából. Márpedig napjainkban éppen ezt a szabályozatlan, „se nem béke, se nem háború" állapotot érzékelhetjük, ami sokkal kevésbé korlátozza az államokat, mint ha a „hagyományos háború" forgatókönyve szerint kellene eljárniuk.

A kibertéri műveletek nemzetközi jogi szempontjait vizsgáló *Tallinni kézikönyv* javaslatot tesz a „kibertámadás" meghatározására, amely merőben eltér a mérnöki *terminus technicusból* levezethető fogalomtól. A Kézikönyv 92. szabálya ekképpen fogalmaz: „Egy kibertámadás olyan kiberművelet, legyen az akár támadó, akár védelmi jellegű, mely alapján személyek sérülése vagy halála, illetve objektumok megrongálódása vagy megsemmisülése megalapozottan várható." Ezen forrás 103. szabálya szerint a kiberhadviselés eszközei a kiberfegyverek és a hozzájuk tartozó kiberrendszerek, módszerei pedig azok a kibertaktikák, technikák és eljárások, amelyekkel az ellenséges tevékenységet végrehajtják. A könyv szerzői azt a célt tűzték ki maguk elé, hogy ezt a témát járják körbe a lehető legalaposabban. Jelenleg ugyanis nincs magyar nyelven elérhető, az offenzív katonai kibertéri műveletek taktikáit és stratégiai szándékait elemző mű. Hasonló munkák idegen nyelven sem gyakoriak, tekintettel a téma érzékenységére és a nyilvánosságra hozott információk mennyiségére, valamint megbízhatóságára. A szerzők mégis úgy gondolják, hogy a kibertéri műveletek közel 30 éves története tartogat már annyi esetet és az ezeket alátámasztó hiteles beszámolót, hogy be lehet mutatni a terület fejlődését, és rá lehet mutatni az egyes taktikai és stratégiai elemek erősségeire, esetleges hibáira, el lehet tehát végezni a kritikai elemzést.

A kiadvány illeszkedik a Nemzeti Közszolgálati Egyetem oktatási és kutatási portfóliójához és intézményközi megállapodásaihoz, így elsősorban tankönyvként

hasznosítható a kiberbiztonsági mesterképzésben, és jegyzetként felhasználható a katonai képzéseken. Kiegészíti a témában korábban megjelent monográfiákat, s kapcsolódik a Honvédelmi Minisztérium és a Nemzeti Közszolgálati Egyetem által megkötött, kiberbiztonsági kutatásokat elősegítő együttműködési megállapodáshoz, illetve támogatja a Magyar Honvédség Parancsnoksága Kibervédelmi Szemlélője által végzett tevékenységet. Nem érinti azonban az orosz–ukrán háborút, amely a kézirat 2021-es lezárása után tört ki.

A szerzők a téma elismert magyarországi szakértői. Prof. dr. Kovács László a Magyar Honvédség Parancsnokságának korábbi kiberszemlélőjeként elsődleges felelőse volt a magyar haderő kiberképességei fejlesztésének. Prof. dr. Molnár Anna az európai védelempolitika szakértője. Prof. dr. Haig Zsolt az NKE Katonai Műszaki Doktori Iskolájában a védelmi elektronika, informatika és kommunikáció kutatási terület vezetője, a kiberhadviseléssel foglalkozó kutatások úttörője Magyarországon. Dr. Krasznay Csaba az NKE Kiberbiztonsági Kutatóintézetének vezetőjeként, a témában legkomolyabbnak számító CyCon konferencia előadójaként több mint egy évtizede foglalkozik a kiberhadviselés kérdésével. Dr. Molnár Dóra az európai kiberbiztonsági stratégiák kutatója. Dr. Nyáry Gábor a kiberdiplomácia, a nemzetközi kiberkapcsolatok szakértője. Rajtuk kívül az NKE három doktori iskolájának kiberbiztonsági témákkal foglalkozó doktoranduszai (Ambrus Éva, Dévai Dóra, Koczka Ferenc, Koller Marco, Legárd Ildikó, Üveges András) vettek részt a könyv megírásában, amely alapvető forrása lehet azon hallgatóknak, akik akár a katonai, akár a nemzetközi kapcsolatok területén végzik tanulmányaikat, és a szakértőknek, akik a honvédelmi vagy külügyi ágazatokban szándékoznak megismerni a kibertéri műveletek valóságát.

Budapest, 2023. június 15.