Tóth Eszter[1]

AZ USA KIBERBIZTONSÁGI FEJLESZTÉSEI VISSZAFELÉ SÜLHETNEK EL

Néhány hónappal ezelőtt az Egyesült Államok legnagyobb üzemanyagszállító vezetéke leállásra kényszerült. A Colonial Pipelinet, mely a keleti államokat látja el benzinnel, gázolajjal és repülőgépüzemanyaggal, egy zsarolóvírus támadta meg. Amennyiben ez az állapot sokáig állt volna fent, az hatalmas károkat okozott volna az USA több iparágának. A történelem során először az Egyesült Államokban egy kibertámadás következtében kellett szükségállapotot elrendelni.

Vagy hogy egy másik esetet említsek, még egy év sem telt el egy rendkívül jelentős az USA ellen irányuló kibertámadás óta. Hackerek feltörték a SolarWinds amerikai szoftvercég által kifejlesztett rendszerek kiskapuit és ezt arra használták fel, hogy megtámadjanak főbb amerikai kormányzati intézményeket; érintettek volt többek között a belbiztonság, védelmi és kereskedelmi területek.

Mindezek az események arra mutatnak rá számunkra, hogy még az Egyesült Államok, az az ország, amely a világ legkiterjedtebb és leginkább kidolgozott kiberbiztonsági rendszerével rendelkezik, sem immunis a kibertámadásokra. Mindez pedig arra enged következtetni, hogy globális szinten is hagy még kívánnivalót maga után ez a terület.

Az Egyesült Államok egyértelmű fölénnyel rendelkezik a kibertérben, ennek következtében effektív kiberbiztonsági stratégiák kidolgozása, illetve további támadó kiberfegyverek fejlesztése központi kérdés számára. Azt azonban alábecsülte, hogy mennyire nehéz ezeket az eszközöket kontrollálni, illetve a fejlesztéseket ténylegesen titokban végezni. Míg az USA célja ezekkel elsősorban az, hogy erőteljesebben tudjon fellépni többek között Kína vagy Oroszország ellen, addig nem fordított elég figyelmet a nem állami szereplőkre. Felülbecsülte a nagyon komplex támadó kiberfegyverek kifejlesztésének számára releváns előnyeit, de nem foglalkozott azzal, hogy egyidejűleg mekkora káoszt okozhatnak a globális kibertérben, amennyiben ezen fejlesztések rossz kezekbe kerülnek.

A nyitottság jegyében az amerikaiak, miután létrehozták az internetet, globálisan is elterjesztették azt. Azonban a 21. századra az internethasználatra és a kibertérre is átterjedt az éppen aktuális geopolitikai gondolkodás, az Egyesült Államok részéről a világ még a hidegháborús viszonyokhoz hasonló megosztása. 2017 májusában a WannaCry zsarolóvírus egyszerre a világ közel 100 országában

[1] Budapesti Corvinus Egyetem nemzetközi tanulmányok szakos hallgatója

okozott problémákat. Az EternalBlue, az eszköz, amit a hackerek ehhez használtak, mint kiderült, az USA Nemzetbiztonsági Ügynökségének kiberfegyverekkel foglalkozó osztályáról szivárgott ki. Ez is egy bizonyíték a sok közül, hogy az USA támadó kiberbiztonsági stratégiája gyakorlatilag bármely országot veszélybe sodorhatja. Egy felmérés alapján 2020-ban világszerte a szervezetek 61%-át érte támadás valamilyen zsarolóvírus által.

A Colonial Pipelinet ért kibertámadás esete, ami kapcsán szükségállapot állt be az Egyesült Államokban, nagy port kavart. Egyre több aggodalom merült fel annak kapcsán, hogy a kibertér további fejlesztése mennyire kockázatossá és veszélyessé vált. Egyre inkább realitássá válik, hogy nemzetgazdaságokat és átlagos emberek mindennapjait érintő területet ér kibertámadás. A hagyományos kiberbiztonsági rendszerek és technológiák is egyre inkább elavulnak, sőt még az Egyesült Államok kiberbiztonsági támadó és védekező modellje is nehézségekkel néz szembe. Mióta az internetet használók száma meghaladta az 5 milliárdot, egy sokkal inkább összekapcsolt és hatékonyabb globális kiberbiztonsági kormányzás kidolgozása sürgető kérdés.

A kibertérben jelen pillanatban is uralkodó káosz sokak szerinti elsődleges felelőse az Egyesült Államok támadóstratégiája. Az USA továbbra is riválisaiként festi le többek között Kínát és Oroszországot, ezáltal megosztottságot kreál a kibertérben is. Ez azért probléma, mert azáltal, hogy egyre jelentősebbé válnak nemzetközi nem állami aktorok, mint például internetes szuperplatformok vagy nemzetközi hacker szervezetek, a globális kiberbiztonságot már nem tudja az USA önmagában fenntartani.

Emellett a közhatalom és a közjavak birtokában a kormányoknak feladatuk lenne őrködni a hálózatbiztonság felett. Ennek ellenére azonban az Egyesült Államok olyannyira dominálja a kiberteret, hogy számos állam labdába se rúghat mellette, olyankor sem, amikor saját kiberbiztonságukról van szó. Ezen felül az ENSZ globális szinten kormányzó és koordináló szerepvállalását is visszautasítja ezen a területen. Ez, párosulva azzal, hogy számos a hackerek által alkalmazott eszköz is az amerikai fejlesztések révén szivárgott ki, összességében elmondható, hogy az USA több aspektusból is inkább ront, mint segít a globális kiberbiztonság helyzetén.

Már az eddigiekből is következik, hogy bármely, akár hivatalos szervek által végzett kiberbiztonsági fejlesztés globális szinten fokozza kibertámadások valószínűségét. Ezt csak akkor tudjuk meggátolni, ha kevésbé átpolitizált és megosztott a kibertér. Ha az egyes államok elköteleződnek a kibertér biztosítása mellett, akkor alakulhat csak ki egy olyan keret, ami globális szinten hatékonyabbá teszi a kiberbűnözés elleni fellépést. Ennek pedig első lépése lehet az Egyesült Államok attitűdjének megváltozása, ugyanis csak kooperációval lehet globális eredményeket elérni.