Matuz Gábor

A kiberhadviselés és az ukrán–orosz konfliktus

Nikita a gép előtt ülve várta egy újabb eseménytelen nap végét. Az unalom számára kikapcsolódás volt, a Prykarpattyaoblenergo energiaszolgáltató operátori állása megnyugtató és biztonságos, hiszen biztos lehetett benne, hogy nem fogják a frontra vezényelni. Immár két éve, hogy a Majdan téri tüntetésekkel kezdődő orosz–ukrán feszültség valódi háborúvá fajult, az elmúlt pár hónapban azonban mintha csitultak volna a csatározások a szakadár régiókban, mégis, a hadkötelezettség 2014. áprilisi bevezetése szorongást keltő fejlemény volt. A háború első zavaros heteit követően Nikita és kollégái több megbeszélésen is részt vettek, hogy orosz szabotázzsal kapcsolatos vészhelyzeti terveket készítsenek. Végül nem történt semmi említésre méltó, pedig a Prykarpattyaoblenergónal mindenki tudta, hogy nem lenne nehéz dolguk a szabotőröknek, az évtizedes elhanyagoltság és korrupció hatására az infrastruktúra még külső beavatkozás nélkül is rozoga volt. Ráadásul az oroszok pontosan tudhatták, hol csapjanak le: az eszközök nagy része még a szovjet időkből származott, és a kevés felújítás is orosz beszállítók segítségével történt. Nikita számára azonban ez már csak kellemetlenség, legfeljebb háttérzaj volt: hosszas sorban állás a beengedőkapuknál, kitartó keresgélés a pótalkatrészekkel telerakott raktárban, bonyodalmas havi jelszócserék. Kevéssel a műszak vége előtt jobban foglalkoztatta a kiléptetés, és az szerencsére továbbra is hatékony volt. Az utolsó, rutinszerű ellenőrzés alatt, amikor az állomások ellenőrző pultjain az adatokat kérte le, a kijelző hirtelen nem reagált. Ebben semmi meglepő nem volt, tudta, hogy már akkor elavultnak számítottak, amikor a Prykarpattyaoblenergónál kezdett dolgozni, és még jó pár év, mire lecserélik a számítógépeket. A szokásos újraindítási kísérletek során alkalmazott billentyűkombinációk végigpróbálása közben a gép egyszer csak saját életre kelt. Minden látható beavatkozás nélkül a kurzor szaporán mozogni kezdett, és különböző szabályzórendszereket vezérlő programokat nyitott meg. Ahogy megzavarodva egy pillanatra felnézett, azt látta, hogy a vele szemben ülő Andrii zavarodott arckifejezéssel gépel, vagyis inkább veri a billentyűzetet.

Ebben a pillanatban megszólalt mindkettőjük telefonja. Nikita felvette a telefont, és egy pillanatra már előre megkönnyebbült, talán az informatikai részlegen szórakozik valaki. Senki nem volt a vonalban. Mikor lecsapta a kagylót, hogy ő hívja az informatikusokat, a telefon újra megszólalt.

Ekkor vette csak észre a folyosóról beszűrődő folyamatos telefoncsörgést. Az egész épületben az összes telefon megállás nélkül csörgött.

Valahogy így kezdődhetett 2015. december 23-án az ukrán–orosz háború első jelentősebb kibertámadása.

Az államilag támogatott hackertámadások azonban sokkal hosszabb múltra tekintenek vissza. A nagyhatalmak előszeretettel nyúltak ehhez az eszközhöz, hiszen a kibertámadás nehezen észrevehető és könnyen letagadható módja a szabotázsnak, ráadásul nincs nemzetközi konszenzus arról, hogy mi az elfogadható válaszcsapás kibertámadás esetén. A NATO például elsőként egy 2014-ben publikált memorandumban rögzíti, hogy egy esetleges kibertámadás a kollektív védelmet jelentő 5. cikk hatálya alá tartozó támadásnak tekinthető, azonban a megítélés szempontjait nem részletezi. Az izraeli hadsereg 2019-ben elsőként, valós időben reagálva, fizikai csapással válaszolt a Hamasz hackereinek tervezett akciójára, a hasonló esetek száma azonban elenyésző. Az esetleges válaszcsapás célpontja már önmagában is kérdéses, a legtöbb esetben hónapok telnek el, míg kialakul valamilyen konszenzus az elkövető kilétével kapcsolatban, és a bizonyítékok szinte mindig közvetettek: a támadáshoz használt szoftverek struktúrája, az alkalmazott hackermódszerek kombinációja, a forráskódokban található megjegyzések és azok filológiai jellemzői.

A kezdetekben a hackelés gyakorlatilag egy speciális szabotázsakció volt.

Az egyik leghíresebb eset valószínűleg a CIA Deception Program fedőnevű 1982-es akciója, amely egy beépített szoftverhiba segítségével egy szibériai gázvezeték felrobbanásához vezetett. A Szovjetunió technológiai megoldást keresett arra, hogy a kegyetlen időjárási körülmények között a lehető legkevesebb emberi beavatkozással tudja működtetni szibériai gázvezetékeit. Saját technológia hiányában a megoldás a KGB ügynökeire maradt, akik egy kanadai fejlesztőcég szabályozórendszerét tervezték ellopni. Amint ez a nyugati hírszerző szolgálatok tudomására jutott, a céghez beépülve különböző, előre megtervezett hibákat helyeztek el a programban. A három kilotonnás gázrobbanás tényét senki nem vitatja, de orosz források napjainkig építési hibákat említenek, a CIA pedig sohasem erősítette meg az akció tényét.

Hasonlóan monumentális, azonban bizonyított és a kiberhadviselést köztudatba hozó akció volt a 2005-ben kezdődő és több éven át tartó izraeli–amerikai Operation Olympic Games támadás, amelynek az iráni atomprogram megbénítása volt a célja. A titkosszolgálati eszközökkel célba juttatott szoftver önállóan fedezte fel hálózati környezetét, és több százezer számítógépet megfertőzve terjedt el. A vírus célpontok hiányában kivárt, ám ha megfelelő típusú ipari szabályozórendszer jelenlétét észlelte, akkor támadásba lendült, és az uránium dúsításához használt, extrém magas fordulatszámon dolgozó, rendkívül precíz centrifugák átkává vált. A hasonlat pontos, mert úgy tette használhatatlanná az eszközök húsz százalékát, hogy a mérnökök mindvégig nem figyeltek fel a jelenlétére. Mint a 90-es évek kémfilmjeiben az előre felvett üres folyosóról bevágott videó, a program az operátorok számára folyamatosan normálisnak látszó adatokat közölt, miközben a fordulatszám radikális változtatásaival

tönkretette a centrifugák motorját. Az így felgyülemlett meghibásodások miatt éveket csúszott Irán nukleáris programja. Az akció technológiai fejlettsége és sikere miatt a kiberhadviselés egyik pillanatról a másikra minden jelentősebb hatalom prioritásai közé került.

A 2010-es években különböző országok hírszerző szervezetei és katonasága által finanszírozott hackercsapatok egymás után váltak hírhedté nagyszabású támadásaikkal. Eleinte a különböző hatalmak aktuális céljaira fókuszáltak: az észak-koreai hackerek online rablással kezdték, míg a kínaiak a legnagyobb hangsúlyt az ipari kémkedésre fektették. Az Operation Aurora néven ismert 2009–10-es akciójukban amerikai technológiai cégeket támadtak meg, majd 2011-ben japán védelmi beszállítóktól loptak katonai és kutatási titkokat. A Google az Operation Aurora egyik célpontja, a támadás hatására megszüntette együttműködését a kínai állammal, ami később a cég kivonulásához vezetett. Az akció másik célja a politikai irányultságú hírszerzés volt, a Gmail levelezőprogramot feltörve kínai emberi jogi aktivisták e-mailjeihez fértek hozzá. A személyre szabott hírszerzés ilyen módja mára mindennapossá vált, gondoljunk csak a hongkongi tüntetések szervezőit célzó támadásokra vagy az elmúlt évben hírhedté vált Pegasus kémprogramra. A folyamatos kiberháborús fenyegetés hatására mára a legtöbb kibernagyhatalom különálló egységeket hozott létre, hogy azok a különböző célú támadásokra fókuszáljanak.

A részletesen megtervezett és céltudatos akciók gyakran sikeresek, mivel minden kellően bonyolult rendszer feltörhető, hiszen gyakorlatilag átláthatatlanul nagy mennyiségű szoftver és ember interakciójára épül. Ez hozza létre azt az aszimmetrikus helyzetet, hogy a védekező félnek minden lehetséges hibára gondolnia kell, míg a támadónak csak egyet kell megtalálnia. Ha a támadó egyetlen célja, hogy a lehető legnagyobb költséget okozza, akkor hirtelen minden védelem alultervezett lesz. Ezt a dinamikát erősítik és egészítik ki a nagy konfliktusok idején az aktivista hackerek felélénkülő támadásai. Gyakran hivatalos struktúra és vezetők nélküli, fórumok, chatszobák köré szerveződő csoportok egyetlen célja, hogy a pillanatnyi ellenségnek minél nagyobb problémát okozzanak. Főleg egyedi események, ideológiák vagy országok köré szerveződő laza csoportok, idővel akár maradandóbb szervezetekké is átalakulhatnak, mint például az Iranian Cyber Army vagy a közismertebb Anonymous hackerkollektíva. Ezek a hackerközösségek jobbára magánemberekből állnak, és – habár több nemzetközi példa szerint ezekből alakultak ki nem hivatalos, de államokhoz közeli hackercsoportok, mint a kínai Honker Union – legtöbbször az államtól csak passzív támogatást, esetleg koordinációt kapnak. Erre példa az invázióra válaszul létrehozott IT Army of Ukraine.

Az ilyen jellegű támadásoknak a célja a cégek és az állami szervek szokásos üzletmenetének ellehetetlenítése és a tulajdonosi kör vagy a felhasználók megalázása. Mivel nem egy specifikus cél elérése mozgatja a csoportokat, így nem egy célpontnál kell kitartóan hibát keresniük, hanem megtehetik, hogy egyszerű

támadási módszereikhez keresnek sérülékeny áldozatokat. Különösebb koncepció nélkül, ismert sérülékenységek kihasználásával, adathalász e-mailekkel vagy túlterheléses támadásokkal nagyszámú motivált résztvevő esetén látványos eredményeket tudnak elérni.

Ezeknek a támadásoknak szinte mindig jelentősebb hatásuk van, ha a mindennapi kiberbiztonság kockázatairól gondolkozunk, konfliktusok idején velük érdemes foglalkozni, és nem a katonaság és a titkosszolgálatok hackereivel. Ugyanakkor koordináció hiányában stratégiai eredményt ezek a támadások soha nem érnek el, így, amikor katonai elemzők a kiberháború várható lefolyásáról beszélnek, főleg állami szereplők lépéseit veszik figyelembe.

A Nikita kurzorát mozgató láthatatlan, távoli, de igencsak valóságos kezek az orosz hírszerzés (GRU – Felderítő Főcsoportfőnökség) Sandworm nevű hackercsapatához tartoztak. Három áramszolgáltatót megcélzó 2015. december 23-i támadásukban a számítógépes rendszereket távolról elérve, villamos ellátó alállomásokat és transzformátorokat kapcsoltak le, többórás, kétszázezer embert érintő áramkimaradást okozva ezzel. A káosz növelésére – és hogy megnehezítsék a visszaállítást – a szolgáltatók telefonszámait megállás nélkül automatizáltan hívták, és igyekeztek minden rendszerüket túlterhelni. Ez a látványos siker csak a kezdetét jelentette a beavatkozásoknak. Egy évvel később Kijiv áramellátását megcélozva immár előre programozott automatizált módszerekkel értek el áramszünetet. A terv része volt maradandó károk okozása is, a telepített károkozó több biztonsági rendszert is kikapcsolt, és végül csak szerencse kérdése volt, hogy visszakapcsoláskor a rendszer nem terhelődött túl.

2017 nyarán ugyanez a hackercsapat zsarolóvírusnak álcázott – az adatokat valójában visszaállíthatatlanul törlő – programja egy könyvelőszoftveren keresztül terjesztve támadott meg egyszerre több alapvető fontosságú szektort Ukrajnában. Szokásos esetben a zsarolóvírusok az informatikai rendszerekhez hozzáférést szerezve a számítógépek adatait titkosítják, az esetleges biztonsági mentéseket törlik. Ha az áldozatok a váltságdíjat kifizetik, a támadók a legtöbb esetben átadják a titkosítás feloldásához szükséges kulcsokat. Hogy tovább növeljék a váltságdíj kifizetésének esélyét, gyakran a céges adatokat ellopva és nyilvánosságra hozatalukkal fenyegetve gyakorolnak még nagyobb nyomást a cégekre. Ám ennek a NotPetya akció esetében nyoma se volt, a támadók egyből törölték az adatokat. Minden valószínűség szerint a mai napig is ez világ legpusztítóbb kibertámadása, amely a többi között leállította a csernobili erőmű sugárzásmonitorozó rendszereit, és egy időre papíralapú működésre kényszerítette az Ukrán Nemzeti Bankot. Az Ukrajnából véletlenül kiszabaduló és külföldön az ukrán áldozatok számának töredékét megfertőző vírus több nemzetközi cégnek, mint a DHL, a FedEx és a Maersk Line szállítmányozóknak vagy a Merck & Co. amerikai gyógyszeripari cégnek, több milliárd dolláros kiesést okozott. A vírussal okozott teljes kárt 10 milliárd dollárra becsülik.

Ezekkel az előzményekkel és öt év technológiai fejlődését szem előtt

tartva nem meglepő a hibrid háborút vizionálók álláspontja: széles körben kialakult konszenzus volt, hogy a 2022-es ukrán–orosz konfliktus lehet az első hibrid háború, amelyben a kibertérnek a fizikaihoz hasonló súlya lehet. Az elmúlt évek konfliktusai alapján ez nem tűnt túlzásnak.

Egyelőre azonban nem nekik lett igazuk. A 2022. február 25-én kezdődött háborúnak nagyon kevés látható hatású kibertérbeli eleme van, és úgy tűnik, inkább kommunikációs szempontból hoz újdonságot, mert az öbölháború óta megszokott televizionált háborút felváltotta a web2-es, interaktív, közösségi médiatérben elhelyezett tájékoztatási és ezzel együtt járó félretájékoztatási propagandakampány. Ebben a pillanatban egyetlen komolyabb következményű hackertámadás köthető a konfliktushoz. Az invázió megkezdése előtt egy órával célzott támadás ért több ukrán céget, állami szervet és a Viasat nevű amerikai műholdas kommunikációval foglalkozó céget. A támadók törölték az ukrán hadsereg és a bevethető katonai eszközök által használt műholdas modemek programját, ezzel gyakorlatilag gyári javításig használhatatlanná tették őket. Az ukrán védelmi minisztérium is elismerte, hogy a támadás komoly problémákhoz vezetett a hadsereg irányításában az invázió kezdeti fázisában. Jellemző azonban, hogy maga a hatás még ekkor se volt annyira jelentős, hogy erről a szélesebb közvélemény tudomást szerezzen, és a hadsereg napokon belül át tudott állni alternatív módszerekre, később a Starlink műholdas kommunikációs eszközeire.

Ezt az egy esetet leszámítva semmi nem utal arra, hogy akár stratégiai, akár taktikai szinten jelentős hatása lenne a kibertérnek az invázióra. A laikusok és a katonai megfigyelők is azt várták, hogy a szankciókra Oroszország kibertámadásokkal fog válaszolni, de ezek eddig teljesen elmaradtak.

Megoszlanak a vélemények arról, hogy miért tévedtek ekkorát a szakértők. Egyesek szerint valójában a színfalak mögött igenis komoly szerep jut a kiberhadviselésnek. Számos nyugati ország és technológiai cég aktívan támogatja az ukrán kibervédelmet. Az elmúlt években a nemzetközi kiberbiztonsági piac egyik legfontosabb szolgáltatójává vált Microsoft több gyakorlati támadás vizsgálata alapján kiadott elemzésében például kimutatta, hogy az orosz hadsereg összehangolja hagyományos és technológiai hadviselését. Egyértelműen látható, hogy a fizikai célpontok változását (katonai, helyi adminisztráció, telekommunikáció, energetika) közvetlenül követik a hackertámadások és a propagandakampányok. Továbbá egyértelműen megnőtt a nyugati cégeket és állami szerveket célzó támadások száma is. Megint más szakértők úgy gondolják, hogy az orosz vezetés saját szolgálatai előtt is titokban tartotta a támadást, így azoknak nem volt idejük érdemben felkészülni. Egyik lehetőséget sem lehet kizárni, lehetséges, hogy néhány sikeres hackertámadás miatt a szakértők túlbecsülték az eszköz hatékonyságát, és még inkább azt, hogy háborúban mennyire lehet hasznos az alternatívákhoz képest. A kiberhadviselés legnagyobb előnye a letagadhatóság, illetve hogy amúgy nehezen elérhető célpontok is támadhatók, és mindezt úgy lehet végrehajtani, hogy a célpont csak ké-

sőbb vagy éppen egyáltalán nem szerez tudomást a támadásról. Kérdéses, hogy egy nyílt háborúban ezek mennyire fontos szempontok egy olyan katonai képességekkel rendelkező országnak, mint Oroszország. Ebben a pillanatban vitatható, hogy propagandacélokból nem jobb-e, ha egyértelmű, hogy konvencionális eszközökkel tetszésük szerint bármit megtehetnek, valamint kérdéses, hogy ha például a cél az áramellátás leállítása, megéri-e hónapokon át készülni egy akcióra, amely siker esetén néhány órás áramszünethez vezet. Kézenfekvő alternatíva egy ötszáz kilós robbanófejjel ellátott cirkálórakéta, amely biztosan hosszú időre használhatatlanná tesz egy transzformátorállomást. A fizikai támadások erejét mutatja, hogy az orosz hadsereg az invázió korai szakaszában tüzérséggel mért csapást ukrán adatközpontokra, és nem informatikai módszerekkel bénította meg őket.

Nem véletlen az sem, hogy a korábban említett összes nagyszabású és sikeres kibertámadás fontos eleme volt az időzítés. A Prykarpattyaoblenergo és további ukrán energiaszolgáltatókat ért támadás december 23-án történt, a Sandoworm zsarolóvírusát szintén nemzeti ünnepen – június 28-án, az alkotmány napján – vetették be, a műholdas kommunikációt megbénító támadás egy órával az invázió megkezdése előtt kezdődött. Az ilyen típusú támadások alapvető eleme a meglepetés és a lehető legnehezebben kezelhető időzítés. Akinek van tapasztalata informatikai rendszerek fejlesztésében és bevezetésében, az pontosan tudja, hogy ez milyen komoly kihívásokkal jár. A támadók programja tesztelés nélkül, elsőre, hiba nélkül kell hogy lefusson egy olyan környezetben, amelyet csak közvetve ismernek, a működését alapvetően és nem tervezett módon akarják megváltoztatni. Ráadásul azzal is kell számolniuk, hogy amint a támadás tényére fény derül, a rendszert behatóan ismerő szakemberek mindent meg fognak tenni, hogy céljukat megakadályozzák. Ez rendkívül költségessé és kockázatossá teszi a bonyolultabb kibertámadásokat. A pontos és körültekintő tervezés ellenére több akció is apró hibákon bukik el. Az ukrán áramszolgáltatók elleni 2016-os támadás alatt a kezelők más sorrendben kapcsolták vissza az állomásokat, mint arra a támadók számítottak, ezért nem rongálódtak meg maradandóan a rendszerek. Egy másik esetben, egy hónapokon át felépített, feltehetőleg az észak-koreai államnak dolgozó hackerek által végrehajtott, Bangladesh Bank Cyber Heist néven közismertté vált támadás kis híján a világ legnagyobb bankrablása lett. A támadók 851 millió dolláros átutalását a címzett nevének elgépelése miatt állították csak meg. A katonai vezetésnek ezt a teljes kontextust figyelembe kell vennie, amikor a kibertámadást mint esetleges eszközt vizsgálja.

Más a helyzet azonban, ha ukrán szemszögből vizsgáljuk a konfliktust, illetve ezzel összefüggésben a NATO és Oroszország szembenállásának tekintetében. Ukrajna láthatóan el akarja kerülni a 2014 előtt is Oroszországhoz tartozó területek közvetlen támadásával járó potenciális eszkalációt. A NATO és Oroszország esetében mindkét fél érdeke,

hogy a feszültség ne eszkalálódjon nyílt konfliktussá, de egyértelmű, hogy az oroszoknak mind katonai, mind propagandaszempontokból hasznos lenne, ha letagadhatóan el tudnák érni, hogy nyugati műholdak, katonai felderítő gépek váljanak használhatatlanná, esetleg rejtélyes balesetek történjenek európai uniós gáztározókban.

Feltehetőleg korai erről bármit is mondani, de ha hibrid háború nem is lesz az ukrán–orosz konfliktusból, az várható, hogy a mára klasszikusnak számító kibertámadások a konfliktus során nagyobb hangsúlyt kaphatnak. Ahogy azonban a július 31-én felrobbant bolgár vagy a másik oldalon a krími lőszerraktárak és repterek példájából sejthető, erre is alkalmasak klasszikus, hackelést nem igénylő megoldások, gyakran úgy tűnik, jóval hatékonyabban is.

Ha a közeljövő konfliktusaiban fontosabb szerepet tölt is be a kiberhadviselés, a filmekben bemutatott látványos akciók, az autók és repülők vagy katonai eszközök fölött irányítást átvevő hackerek által okozott apokalipszis helyett érdemesebb a legrosszabb pillanatban lefagyott számítógépekre és Nikita megállíthatatlanul csörgő telefonjára gondolnunk.

Tranker Kata: Nagy anyaállat