Kovács László

Információs hadviselés kínai módra

Az ZMNE Információs Műveletek és Elektronikai Hadviselés Tanszékének docense jelen írásában Kínának az információs hadviselés terén tapasztalható törekvéseit, módszereit, illetve az e területen elért eredményeit foglalja össze.

Egy évtizede még nem keltett nagy feltűnést a volt amerikai elnöki nemzetbiztonsági tanácsadó, Zbigniew Brzezinski figyelmeztetése, amely szerint az Egyesült Államok legnagyobb vetélytársa Kína lesz, mégpedig belátható időn belül.

Az elmúlt években Kína nagy iramú gazdasági fejlődésének felemlegetése mármár általánossá és megszokottá vált. A világméretű gazdasági válság természetesen Kínát sem kerülte el, de gazdaságának növekedése 2009-ben várhatóan 7-8 százalék lesz, ami ugyan kínai szemmel nem túl jó eredmény, de még mindig jóval magasabb a világ többi részére prognosztizálhatónál.

Brzezinski jóslata ugyanakkor ma már nemcsak gazdasági téren látszik igazolódni, hanem a katonai potenciál különböző szegmenseiben is. Ennek igen szembetűnő jelét adják azok a kínai törekvések, amelyek az információs technológiának a polgári felhasználás mellett egyre több katonai alkalmazásában figyelhetők meg.

Mindezek alapján joggal feltételezhetjük, hogy Kína az információs hadszíntéren különösen gyorsan fejlődik, így meghatározó és megkerülhetetlen szereplővé válhat a közeljövőben, sőt egyes vélemények szerint a nem túl távoli jövőben behozhatatlan előnyre tehet szert az információs hadviselés terén.

Kína e téren egyre fokozódó (és tegyük hozzá: egyre sikeresebb) tevékenységét jól jellemzi egy – igencsak megdöbbentő – példa, amely egy, az Egyesült Államok kongresszusa számára 2008 őszén készült jelentésben is szerepel. 2002-től kezdve a számítógépes biztonsággal foglalkozó amerikai hatóságok számos Kínának tulajdonítható informatikai behatolássorozatot észleltek – elsősorban nem titkos – amerikai katonai, kormányzati és a kormánnyal szerződésben lévő közepes és nagyvállalatok számítógépes rendszerei-

Az **információs hadviselés** fogalma az 1980-as években jelent meg, legelőször az Egyesült Államok légierejénél. Azóta maga a fogalom és az a tevékenység, amit takar, az az információért folyó küzdelem hatalmas változáson ment keresztül. Ma az információs hadviselés leginkább a civil szóhasználatban jelenik meg, amely az információ megszerzését, feldolgozását, majd az információ jelentette előnyök gazdasági és politikai eredményekké való konvertálását jelenti. A katonai terminológia ma már az információs műveletek fogalmat használja az információs hadviselés helyett. Az információs műveletek olyan összehangolt és koordinált tevékenységeket takarnak, amelyek a műveleti biztonság, a katonai megtévesztés, a pszichológiai műveletek, az elektronikai hadviselés és a számítógép-hálózati műveletek különböző akcióival támogatják a harc sikeres megvívását.

be és hálózataiba. A később *Titan Rainnek* (Titánesőnek) elkeresztelt, igen szisztematikus és jól felépített támadások során a kínai hackerek 10–20 terabájtnyi adatot töltöttek le a megtámadott számítógépekről. Csak összehasonlításképpen: a Kongresszusi Könyvtár (nem mellesleg a világ legnagyobb könyvtára) összes könyve körülbelül 10 terabájtnyi adatot tárol.

Az említett kongresszusi jelentés, amely az Egyesült Államok és Kína gazdasági, valamint biztonsági kapcsolatait értékeli, az említett példán kívül számos más figyelemre méltó tényt is felsorol. A jelentés külön figyelmet szentel azoknak a kínai törekvéseknek, amelyek egyrészt az űrben, másrészt a cybertérben mutatnak egyre növekvő kínai aktivitást.

Kínaiak az űrben, avagy információs hadviselés műholdakkal

Az űr „meghódítására” tett kínai lépések számos alkalommal az információs hadviselés céljait is magukban foglalják, hiszen abban komoly jelentősége van az információszerzésnek, ezen belül is a műholdakkal végzett felderítésnek. Ebből a szempontból különös figyelmet érdemelnek azok a lépesek, amelyeket Kína saját műholdas rendszereinek kifejlesztése érdekében tesz. Elemzések szerint a különböző kínai űrprogramokon – például nukleáris energia alkalmazása, multispektrális szenzorrendszerek, űrben használható anyagok, robotok stb. – több mint 200 ezer ember dolgozik. Természetesen már az is jelzésértékű, hogy Kína képes volt önállóan embert juttatni a világűrbe, ráadásul nem is egy alkalommal. 2003-ban egy, majd 2005-ben már két kínai asztronauta hajtott végre sikeres űrutazást. 2008 szeptemberében a harmadik ilyen alkalom során a három tajkonauta (az angolszász asztronauta, illetve az orosz kozmonauta kínai megfelelője) egyike már űrsétát is végrehajtott.

2007-ben Kína egy holdszondát is útnak indított, amely a Csang-o ji-hao, azaz Holdistennő–1 nevet viselte. A szondát egy Hosszú Menetelés–3A hordozórakéta állította Föld körüli pályára. A hordozó egy közel tizenöt rakétából álló család tagja, amelyek közül több is alkalmas műholdak Föld körüli pályára állítására. Ez lehetővé teszi, hogy Kína szolgáltatásként is árulja ezt a képességet, így például Brazília, Venezuela, illetve Nigéria számára lőttek fel műholdakat e rakétákkal.

A különböző feladatokra, például a már említett információszerzésre vagy meteorológiai célokra alkalmazott kínai műholdak mellett megjelentek a saját navigációs rendszer alapjait jelentő első kínai szatellitek is. A Beidou (Nagymedve) névre keresztelt kínai navigációs rendszer első műholdját 2000-ben állították Föld körüli pályára, amelyet még öt további követett. A rendszer jelenleg öt műholdat használ az elviekben 0,5 méter pontosságú navigáció biztosítására. Azonban a Beidou igen nagy hátránya, hogy ma még csak Kína területén használható. Ezért a távlati tervek 2015-re Compass néven egy 30-35 műholdból álló globális navigációs rendszer kiépítését célozzák meg.

Információszerzésre alkalmas műholdak fedélzetén különböző felderítő eszközök lehetnek. A képi felderítésre *(Imagery Intelligence – IMINT)* alkalmas műholdak multispektrális eszközöket, videokamerákat, infrakamerákat hordozhatnak. Ezekkel ma már akár a 30 cm-es felbontásnál is jobb képek készíthetők. A felderítő műholdak egy másik csoportja rádióelektronikai felderítő *(Signal Intelligence – SIGINT)* eszközöket hordozhat. Ezekkel a földi, vagy akár a műholdas kommunikációs vonalak is lehallgathatók, ellenőrizhetők.

A saját navigációs rendszer gyors tempóban történő fejlesztése és rendszerbe állítása mellett Kína belépett az Európai Unió Galileo navigációs rendszerének projektjébe is. Ez a pénzügyi részvétel mellett (amely nem mellesleg igen nagy segítséget jelent az állandó pénzügyi gondokkal küszködő projektnek) technikai és technológiai fejlesztéseket is jelent az európai program számára.

Az új, saját navigációs rendszer kiépítése egyrészt nyilvánvalóan az amerikai GPS-től való függőség csökkentését szolgálja, másrészt lehetőséget teremt arra is, hogy a már említett rakétákat igen pontosan célba lehessen juttatni.

Mindezek mellett a Galilelo-programba való belépés is felvet számos biztonsági kérdést, hiszen ezzel Kína is rendelkezhet mindazokkal az információkkal, amelyek a rendszer üzemeltetését teszik lehetővé, nem beszélve arról a tényről, hogy sok alrendszert Kína tervez és gyárt.

A kémműholdak kapcsán is kijelenthető, hogy komoly kockázattal kell számolni, hiszen ezeknek köszönhetően a kínai alkalmazók birtokában lehetnek akár ez európai, akár a tengerentúli csapásmérő arzenál pillanatnyi helyzetéről, elhelyezkedéséről szóló információknak. Bár a műholdak ma még nem mindenhatóak a felderítésben, de nyilvánvaló, hogy egyre kevesebb tény marad titokban az előtt, aki rendelkezik ilyen felderítő-információszerző eszközzel.

További veszélyt jelenthet, hogy mind az Egyesült Államok, mind a NATO-tagországok jelentős mértékben függnek saját műholdas kommunikációs, felderítő vagy éppen navigációs rendszereiktől. Abban az esetben ugyanis, ha Kínának sikerül áttörést elérnie az olyan fegyverek kifejlesztésében, amelyek alkalmasak a különböző űreszközök elpusztítására, akkor a korábban említett erős függőség hatalmas fenyegetettséget jelent majd.

Galileo. Az elsősorban polgári feladatok ellátására szánt Galileo fejlesztéséért az Európai Űrügynökség (ESA) felel. Az eredeti tervek szerint a rendszer már 2009-ben üzemképes lett volna, azonban pénzügyi és egyéb koordinációs problémák miatt várhatóan csak 2012-ben lesz használható. Ugyanakkor az alkalmazott új technológiáknak köszönhetően (például új típusú atomórák alkalmazása a műholdak fedélzetén, vagy az új jelfeldolgozó algoritmusok) a rendszer pontosabb lesz, mint a jelenleg legelterjedtebb és civil alkalmazásokban is legnépszerűbb amerikai NAVSTAR GPS. A várakozások szerint az új európai fejlesztésű navigációs rendszer a szállításban, a mezőgazdaságban, a polgári közlekedésben és a halászat területén hozhat komoly előrelépést.

Kínaiak a cybertérben: akciók külföldön

Nagy visszhangot váltott ki a német sajtóban és később a német politikai életben is, hogy Németországban több kormányzati számítógépen is találtak kínai kémprogramokat. Mindez annak fényében vált különösen izgalmassá, hogy az ügy 2007 augusztusában, néhány nappal Angela Merkel német kancellár hivatalos kínai útja előtt pattant ki.

A német kormány szóvivője a *Der Spiegel*nek később cáfolta, hogy a kémprogramok károkat okoztak volna. Elmondása szerint a felfedezett rosszindulatú programokat főleg gazdasági hírszerzési célokra használták. Mindezt megerősítette a Német Szövetségi Alkotmányvédelmi Hivatal egyik korábbi bizalmas jelentése, amely szerint Németország kedvelt célpontja a kínai gazdasági kémkedésnek. A jelentésben szerepel az is, hogy a német számítógépes rendszerek elleni támadások szinte mindennaposak, és elsősorban Északnyu-

Rosszindulatú programok. Az angol *malicious software (malware)* összefoglaló névvel illetett számítógépes programok anélkül jutnak a felhasználó számítógépére, hogy arra a felhasználó engedélyt adott volna, vagy arról tudomása lenne. A rosszindulatú programok napjainkban igen elterjedt fajtái a trójai programok. Látszólag, vagy akár valóságosan is hasznos funkciókat látnak el, de emellett olyan programrészeket is tartalmaznak, amelyek nem kívánt műveleteket is végrehajtanak. Ezek adatokat módosítanak, könyvtárakat, adatállományokat törölnek, vagy egyszerűen felkészítik a gépet egy következő támadásra, azaz észrevétlenül „kaput" nyitnak egy újabb behatolásra. Az említett németországi kínai kémprogramokat is trójai programokkal juttatták többek között a kancellária, a külügyminisztérium és a gazdasági minisztérium egyes gépeire.

gat-Kínából, Lancsouból és Pekingből indulnak ki. Ugyanakkor a Der Spiegel szakértőkre hivatkozva azt állította, hogy német információvédelmi szakemberek egyenként vizsgálták át a minisztériumok számítógépeit, és miközben folyamatosan ellenőrizték az adatforgalmat, sikerült blokkolniuk egy a Távol-Keletre indítandó, összesen 160 gigabájtos adatcsomagot. Ennek megfelelően nehezen hihető, hogy a kínai trójai programok nem okoztak károkat.

Természetesen az incidens szóba került Angela Merkel és Ven Csia-pao kínai miniszterelnök találkozóján is. A vendéglátó cáfolta, hogy a kínai kormánynak bármilyen köze lenne a hackertámadásokhoz, ugyanakkor hangsúlyozta, hogy Kína szorosan együtt fog működni Németországgal a nemzetközi hackertevékenységek ellen, amely során Kína „határozott és erőteljes" lépéseket fog tenni.

Az IT-szakembereket egyáltalán nem lepték meg a kínai kémprogramok, hiszen nem első alkalommal fordult elő ilyen eset. 2005-ben hasonló programokat találtak többek között elektronikai eszközöket gyártó vállalatok számítógépein. Ezzel kapcsolatosan fontos hangsúlyozni, hogy a kis- és közepes vállalatok sokkal nagyobb veszélynek vannak kitéve ezen a téren, mint a nagyvállalatok, hiszen nincs még meg az a teljes körű és átfogó informatikai védelmi rendszerük, amely ki tudná védeni a hasonló támadásokat. Az elektronikai ipar mellett a gyógyszergyárakat, az autóalkatrész-gyártókat, de akár az élelmiszeripar különböző cégeit is fenyegeti ez az elsősorban az ipari kémkedésben, illetve a know-how eltulajdonításában jelentkező veszély. Az e cégektől a hackerek által ellopott információk, illetve azok későbbi felhasználása csak Németország esetében több milliárd dollár kárt okoz évente.

Ahogy Németország, úgy az Egyesült Államok esetében sem szokatlan és meglepő a kínaiak cybertevékenysége. A már említett Titan Rain támadássorozat 2002-ben kezdődött, de szakértők még 2005-ben is találtak arra utaló nyomokat, hogy elsősorban kínai területről érkeztek illegális számítógépes behatolások olyan nagyvállalatok és kutatóintézetek rendszereibe, mint például a SANS Institute, a Lockheed Martin, a Sandia National Laboratories, a Redstone Arsenal, vagy a NASA. Természetesen a Pentagon különböző rendszereit is érintették a támadások. Ugyanakkor itt is megfigyelhető volt, hogy a hackerek elsősorban a nem titkos rendszerekből töltöttek le adatokat.

2008 áprilisában kínai hackerek összehangolt támadást terveztek a CNN televíziós hírcsatorna ellen. A támadás azokat a kritikus hangvételű riportokat lett volna hivatott megbosszulni, amelyek az olimpiai láng és a körülötte kialakult tiltakozó megmozdulások hivatalos kínai kezelését mutatták be. A CNN közleményben számolt be arról, hogy a csatorna weboldalának érezhetően lassúbbá vált az elérése, ami nagy valószínűséggel egy támadás következménye, így

egy forgalomszűrőt volt kénytelen alkalmazni. Az összehangolt, nagy – vélhetően DDoS – támadás terve azonban elég gyorsan napvilágra került, és ennek következményeként, mivel a meglepetés ereje már elmúlt, csak kisebb támadások következtek be nemcsak a CNN, hanem egyéb amerikai online médiumok ellen.

2009 áprilisában kínai (és orosz) hackerek behatoltak az Egyesült Államok villamosenergia-rendszerébe. A támadások több pontot vagy rendszerelemet is értek, az egész országban számos helyen észlelték őket. A támadók nem okoztak kárt, de nyilvánvaló, hogy sok gyenge vagy sebezhető pontot feltérképeztek. Nem ez volt az első ilyen – az energiarendszert érintő – támadás, hiszen 2001-ben a kaliforniai elektromos rendszerbe hatoltak be hackerek. Akkor is egyértelműen bizonyítható volt, hogy a támadás kínai kommunikációs hálózatról érkezett. Persze ebben az esetben is nagyon nehéz megmondani – és ami még nehezebb: bizonyítani –, hogy valójában ki is követte el a támadásokat.

Ezekből a támadásokból levonható az a következtetés, hogy a külföldre irányuló kínai cybertevékenységek elsődleges célja nem a legszigorúbban őrzött titkok ellopása vagy megszerzése. Ennél sokkal fontosabb, hogy akcióik során a támadók olyan tapasztalatokra tesznek szert, amelyek a különböző rendszerek gyenge pontjaira derítenek fényt. Mindezek alapján egyelőre egyes infrastruktúrák, akár kritikus információs infrastruktúrák elemzése és analizálása tűnik a fő célnak. Az ma még kérdéses, hogy ezeket az információkat maga a kínai állam vagy egyes hackercsoportok fogják-e használni.

Mindamellett, hogy Kínában megközelítőleg 250 „államilag megtűrt” hackercsoport van, egyes hírek szerint a kínai hadsereg is komoly erővel rendelkező számítógép-hálózati műveletekre alkalmas egységet tart fent. Az egység létezéséről természetesen nincs hivatalos információ, de gyaníthatóan sok olyan hackert fog össze, illetve alkalmaz, akik magasan képzettek, hatalmas informatikai tudással és tapasztalattal rendelkeznek, amelyek egy részét kínai katonai akadémiákon szerezték.

Az amerikai hadsereg is megkülönböztetett figyelmet szentel ezeknek a csoportoknak és „szakértőknek”. Egyrészt az amerikai infrastruktúra – kiemelten az információs infrastruktúra – védelme, másrészt az olyan sérülékeny katonai információs rendszerek védelme a fő feladat, mint amilyen a *Nonsecure Internet Protocol Router Network*, a NIPRNet. Ezzel párhuzamosan működik a SIPRNet *(Secret Internet Protocol Router Network),* amelynek fő feladata a minősített információk szétosztása teljesen különválasztott, titkosított hálózaton. Ez a

A **kritikus információs infrastruktúrák** azok a mindennapi élethez ma már nélkülözhetetlen rendszerek, amelyek kiesése vagy teljes működésképtelensége komoly anyagi és közvetve akár humán károkat is okozhat. Ilyen rendszerek például az energiaellátó rendszerek rendszerirányító számítógép-hálózatai; a vezetékes, mobil, műholdas kommunikációs hálózatok; a közlekedésszervezés és -irányítás számítógép-hálózatai; a pénzügyi-gazdasági rendszer számítógép-hálózatai; a védelmi szféra riasztási, távközlési, számítógép-hálózatai; az egészségügyi rendszer számítógép-hálózatai; vagy a kormányzati és önkormányzati számítógép-hálózatok.

Számítógép-hálózati műveletek *(Computer Network Operations – CNO):* az információs műveletek körébe tartozó tevékenység a szemben álló fél információs rendszereibe történő beavatkozást jelent, amely során egyrészt információt szerez azok felépítéséről, támadható gyenge pontjairól, másrészt csökkenti képességeiket, vagy megakadályozza működésüket, miközben a saját számítógép-hálózatok működőképességét védi.

hálózat jelenleg elengedhetetlen a nem titkos, de szenzitív harctámogatási információk szétosztására mind békében, mind háborús műveletekben. A létfontosságú rendszer különösen sérülékeny, mert a publikus internethez kapcsolódik. Elemzők szerint gyenge pontjait a kínaiak már feltérképezték, és fennáll a veszélye, hogy adott körülmények között képesek komoly károkat is okozni, ami a működőképességet is veszélyezteti.

Az Egyesült Államok elmúlt évekbeli katonai akciói – az Öböl-háborúk, a délszláv háború, Afganisztán – óriási nyilvánosságot kaptak. Az így megjelent információk, illetve a NIPRNet-hez való hozzáférés lehetővé tette Kína számára, hogy a logisztikai rendszertől kezdve a harctámogatás különböző elemein át kielemezze az Egyesült Államok számos rendszerét. Ez felveti annak a veszélyét, hogy ha akár Kínát, akár egy Kínával baráti országot érne amerikai támadás, akkor a kínaiak a lehető legkorábban be tudnak avatkozni ezekbe a rendszerekbe, jó esélyt teremtve arra, hogy az akciók eleve kudarcba fulladjanak.

Mindazonáltal a 2007-es orosz–észt konfliktus is bizonyítja, hogy egy fejlett információs infrastruktúrával rendelkező ország különösen sebezhető abban az esetben, ha a támadások azon kulcsfontosságú rendszerek vagy rendszerelemek ellen irányulnak, amelyek feltérképezése éppen a fent említett támadásokkal viszonylag egyszerűen megvalósítható.

2007 áprilisában és májusában DDoS-támadások érték Észtország számítógépes hálózatait. Az egyébként igen fejlett információs infrastruktúrával rendelkező, az e-kormányzat területén komoly sikereket elért Észtország a több mint kéthetes támadás során komoly anyagi károkat szenvedett, mert számos kormányzati, minisztériumi és több banki internetes oldal vált elérhetetlenné. A támadások a tallinni orosz emlékmű elmozdítása után kezdődtek, és nagy részük többé-kevésbé beazonosíthatóan Oroszországban működtetett szerverekről indult. Az észt miniszterelnök az orosz kormányt tette felelőssé az akciókért. Oroszországot korábban Ukrajna és az Egyesült Államok is megvádolta hasonló támadások végrehajtásával, de Moszkva minden alkalommal határozottan tagadta részvételét. Észtország esetében az ország nemzetközi internetforgalmát irányító szervereket, valamint a hírportálokat érték támadások. Az online támadások alatt összesen 128 túlterheléses támadás történt. A legkomolyabbak öt-tíz órán át, több száz megabitnyi sávszélességen bombázták folyamatos adatlekérésekkel a megtámadott szervereket mindaddig, amíg azok össze nem omlottak. Az észt hálózaton az adatforgalom esetenként órákon át a normális ezerszerese volt. Ehhez egyes források szerint valószínűleg az internetes alvilágtól kellett erőforrásokat bérelnie a támadóknak. A támadások következtében azonban – eltekintve a komoly pénzügyi károktól – Észtország gazdasága nem roppant össze.

Grúzia és Oroszország között is hasonló konfliktus alakult ki 2008-ban. A Dél-Oszétia miatt kirobbant orosz–grúz konfliktus nagyon gyorsan megjelent az interneten is. Az első, orosz eredetűnek tűnő túlterheléses támadások grúz kormányzati szerverek és a grúz elnök weboldala ellen történtek. Az orosz csapatok Dél-Oszétiába történő bevonulása után az egész grúz internetet támadás alatt tartották. Elsődlegesen az állami szervezetek weboldalait, a Grúzia nemzetközi internetforgalmát irányító szervereket, valamint a hírportálokat érték támadások.

Fontos hangsúlyozni ugyanakkor, hogy egy az Észtországihoz hasonló nagyságrendű támadás esetében korántsem biztos, hogy például az Egyesült Államok is ilyen, re-

latíve kis károkkal megúszná. Sokak szerint ennek oka egyrészt abban keresendő, hogy az Egyesült Államok (sok más országhoz hasonlóan) nincs felkészülve egy ilyen összehangolt támadásra. Nincsenek meg az együttműködésnek azok a gyakorlati keretfeltételei a védelemben részt vevő különböző ügynökségek, kormányszervek stb. között, amelyek egy támadás esetén koordinált és összehangolt választ tudnának adni. Természetesen már megkezdődött azoknak a terveknek és programoknak a kidolgozása, amelyek a kritikus információs infrastruktúrák védelmét szolgálják majd, de ezek hatékonysága ma még erősen megkérdőjelezhető.

Civil és katonai védelmi megoldások is születtek az Egyesült Államok kritikus infrastruktúráinak védelmére. Ilyen civil megoldás például az úgynevezett Einstein-rendszer, amely a szövetségi hivatalok informatikai rendszereinek védelmét hivatott ellátni. Az Einstein erősen kötődik az NSA-hez, így alkalmas az e-mailek olvasására, illetve egyéb elektronikus kommunikációs csatornák ellenőrzésére is. Katonai védelmi megvalósítás az Air Force alárendeltségébe utalt Cyber Command. A 2008 októberére tervezett – a kritikus információs infrastruktúrák védelmét is feladatul kapó – szervezet működése azonban egyelőre nem teljesen világos okok miatt nem indult el. Meglehetősen érdekes fejlemény azonban az ügyben, hogy Robert Gates 2009. június végén bejelentette az Egyesült Államok Cyber Command (USCYBERCOM) megalakulását, amelyet az NSA alárendeltségében indítanak 2009 szeptemberétől. Az új parancsokság támadó cybertevékenységeket is fog végezni a civil információs rendszerek védelmében való közreműködés mellett.

Kínaiak a cybertérben: akciók hazai pályán

Kína külföld felé irányuló cyberakciói mellett érdemes megvizsgálni azokat a tevékenységeket, amelyeket elsősorban a kínai internetezők ellenőrzése végett folytat.

A kínai internethasználók száma az elmúlt években dinamikusan – a világ más területeihez mérve sokkal gyorsabban – növekedett. 2008-ban 42 százalékkal nőtt a felhasználók száma, amely 2009-ben elérte a 298 milliót. A közel 300 millió felhasználóval Kína megelőzte az Egyesült Államokat, ahol ez a szám 227 millió. Természetesen önmagában csak az internethasználók számából kiindulva még nem jelenthető ki a kínai világelsőség, hiszen a népesség arányához viszonyítva Kínában 22,4 százalék internetet naponta használók aránya, míg az Egyesült Államokban ez az arány több mint 74 százalék.

Ugyanakkor ez a 300 millió internetező óriási problémákat is jelent a kínai állami vezetésnek. Az állam a gyorsan növekvő felhasználói kör ellenére (vagy éppen emiatt) megpróbálja korlátozni az egyszerű internethasználó számára elérhető információkat. Kína a webes cenzúra biztosítására a nyugati országokban csak Kínai Nagy Tűzfalnak nevezett rendszert fejlesztett ki, amelyet a 2003-as indulástól kezdve folyamatosan használ. A hivatalos nevén Aranypajzsnak (Jindun gongcheng) hívott hardver- és szoftverrendszert a közbiztonsági minisztérium tartja fent. Egyes szakértői vélemények szerint a 300 millió felhasználót ötvenezer „netrendőr” ellenőrzi folyamatosan, azaz ennyi ember működik közre a Kínai Nagy Tűzfal üzemeltetésében.

A rendszer által a leggyakrabban cenzúrázott tartalmak közé tartoznak az olyan betiltott csoportok, mint a Falun Gong, a tajvani kormány hivatalos oldalai, a pornográf internetoldalak, a Tibet függetlenségével, vagy például az 1989-es Tienanmen téri eseményekkel foglalkozó weboldalak. (Érdemes kipróbálni, hogy a google.cn keresőbe akár magyar IP-címről beírva a Tienanmen szót, milyen találatokat kapunk, össze-

hasonlítva mondjuk a google.hu által erre a szóra adott találatokkal.)

Az internetes tartalmak cenzúrázására számos kifinomult informatikai technikát alkalmaznak. Ezek közé tartozik például az IP-cím blokkolása. Gyanús vagy nemkívánatos IP-címek esetében blokkolják a HTTP, az FTP és akár a POP3 protokollokat is. Több website-ot kiszolgáló szerver esetében, ha akár csak egyikükön is van olyan tartalom, amely tiltott, akkor egyik hosztolt site sem érhető el. További technika a DNS-szűrés és átirányítás. Olyan tartományneveket, amelyeken tiltott tartalom van, a DNS-szerver egyáltalán nem old fel vagy hibás IP-címet küld vissza a felhasználónak. Gyakran alkalmazott szűrési megoldás a kulcsszavak alapján történő csomagszűrés, amely már természetesen URL esetében is működik. Ez azt jelenti, hogy az előre meghatározott szavakra vagy fogalmakra történő keresés esetén a rendszer blokkolja a kapcsolatot. Ez már keresőprogramok esetében is működik, azaz ha egy keresőprogram olyan oldalakat ad fel találatként, amelyeken tiltott szavak találhatók, akkor a rendszer blokkolja ezeket az oldalakat is. Ha valamilyen szűrőmechanizmus bontja a TCP-kapcsolatot, a rendszer egy bizonyos ideig (általában 1–30 percig) a további kapcsolódási kísérleteket is blokkolja, azaz bünteti a felhasználót, amiért rossz helyen és rossz tartalmat keresett.

Természetesen a cenzúráról túl sok hivatalos állami információ nincs, de sokatmondó az a tény, hogy 2007-ben több internetes tartalomszolgáltató és blogfelületet biztosító céggel közösen a Yahoo! és a Microsoft is elfogadta a kínai állami feltételeket. Ezek a feltételek többek között előírják, hogy a blogok használata regisztrációhoz kötött, a felhasználók adatait pedig a szolgáltatók kérésre kötelesek átadni a rendőrségnek. A hivatalos megfogalmazás szerint minderre a felhasználók védelme érdekében volt szükség, azaz így kívánják megvédeni az állampolgárokat a cyberbűnözéstől, valamint más olyan veszélyektől, amelyek a felhasználók biztonságát fenyegethetik.

Korábban a Google is arra a következtetésre jutott, hogy ha Kínában jelen akar lenni, akkor engednie kell a kínai államnak, azaz meg kell engednie bizonyos tartalmak cenzúrázását. 2006-ban, a keresőóriás kínai változatának elindításakor Andrew McLaughlin, a Google kormányzati kapcsolatokért is felelős vezetője ezt mondta: „A google.cn meg fog felelni a kínai törvényeknek és rendeleteknek. Abban a döntésben, hogy hogyan jelenünk meg a kínai vagy bármely más piacon, szerepet kap annak az egyensúlynak a kialakítása, amely a kötelezettségvállalásaink, a felhasználók igényei, valamint a helyi követelményeknek való megfelelés területeit érintik."

Mindezek után a Google-t nagyon sok bírálat érte, hogy kvázi lepaktált a kínai kormánnyal, és hozzájárul a cenzúrához. Különösen a francia székhelyű Riporterek határok nélkül *(Reporters Sans Frontieres)* szervezet bírálta élesen mind a Google-t, mind kínai kormányt, de az Európai Unió információs társadalomért és médiáért felelős biztosa, Viviane Reding is tiltakozását fejezte ki.

A cenzúra területén a Nagy Tűzfalnál is komolyabb lépésre szánta el magát a kínai kormány. 2009. július 1-jétől minden Kínában forgalmazott és eladott új számítógépre a gyártóknak kötelező előre feltelepíteniük az úgynevezett Green Dam webszűrő szoftvert. Ez az alkalmazás hivatalosan szintén a fiatalok védelmét szolgálja a pornográf és egyéb káros tartalmakkal szemben. Ugyanakkor a szoftver többek között a személyes adatokat is rögzíti, így a rendőrség gyakorlatilag bármit és bárkit ellenőrizhet az interneten. Mindezek mellett a program már beépítve tartalmazza azokat a kifejezéseket és

szavakat, amelyek keresését a kormány blokkolni akarja.

Mindezek mellett Kína a szofisztikált cenzúrázási megoldásoknál sokkal drasztikusabb eszközöktől sem riad vissza, amennyiben érdekei vagy a helyzet úgy kívánja. A 2009. június végén a Hszincsiang tartomány fővárosában, Urumcsiben kitört ujgur zavargások kapcsán egyszerűen korlátozták a területen az internethozzáférést, a nemzetközi telefonvonalakat pedig lekapcsolták. Ennek oka nagy valószínűséggel az volt, hogy a szeparatista Ujgur Világkongresszus vezetője – a jelenleg az Egyesült Államokban élő Rebija Kadír – az internet segítségével szervezte és irányította a tüntetéseket.

Hasonló lépéseket tett a kormány a Tienanmen téri tüntetések huszadik évfordulója alkalmával is. Több olyan közösségi weboldalt is letiltottak, köztük a kínai fiatalok között is legnépszerűbb Twittert, ahova a megemlékezéssel kapcsolatos beszámolók kerültek fel. De ezenkívül ideiglenesen a Hotmail levelezőrendszert is blokkolták. Azonkívül, hogy a „hagyományos" média képviselőit meglehetősen érdekes módszerekkel akadályozták a téren történő forgatásokban (például civil ruhás rendőrök esernyővel takarták el a kamerák elől a riportereket), zavarták a *BBC*, a *CNN* és a francia *TV5 Monde* kínai adásait is.

Iráni–kínai kapcsolat?

Az iráni vezetés a választásokat követő utcai zavargások miatt elérhetetlenné tette az ezekről az eseményekről – majdhogynem egyetlen forrásként – információval szolgáló Twitter közösségi oldalt, illetve korlátozta számos egyéb weboldal elérhetőségét. Persze túlzás lenne ebben a kínai mintát feltételezni, de mindenesetre ott már hatásosnak bizonyultak ezek a módszerek. Az iráni kormány cyberteret érintő korlátozásaira mintegy válaszként, hackercsoportok e-mailes levelező listákon, illetve weboldalakon nemzetközi felhívásokat tettek közzé, amelyek szerint minden olyan cybereszközre szükség van, amely segíti kikerülni az iráni vezetés által blokkolt rendszereket, és így segítséget nyújthat a „szabadságukért küzdő" iráni embereknek. A magyarországi hackerek közül is sokan kaptak ilyen tartalmú levelet, ami nemzetközi ismertségüket is jelzi. Felhívásukban az iráni kormányzati szerverek és egyéb számítógépes rendszerek támadására buzdítottak a kezdeményezők. Lelkesítő példaként sok olyan linket is közzétettek, amelyeken az Irán ellen már végrehajtott támadásokról lehet beszámolókat olvasni. Talán ennek is köszönhető, hogy több iráni állami híroldal is elérhetetlenné vált a felhívást követő néhány napon.

Mindezeket követően az internet nyíltságáért harcoló szervezetek olyan proxyhálózat fejlesztésébe kezdtek, amely lehetővé teszi az iráni felhasználóknak a blokkolt oldalak elérését. A Nyílt Forrás Mozgalom társalapítója, Eric S. Raymond – aki élére állt a kezdeményezésnek – szerint: „Célunk, hogy egy védett kommunikációs csatornát biztosítsunk a másképp gondolkodóknak. Hat hacker dolgozik mindennap az állami blokkok kikerülésén, és több mint 1000 ember ajánlott fel szervereken sávszélességet proxy oldalak hosztolására."

Összegzés

A kínai űrbéli, valamint cybertérben tapasztalható aktivitás nagyon jól mutatja, hogy Kína olyan ambíciókkal rendelkezik, amelyek komoly figyelmet érdemelnek a világ vezető hatalmaitól. Ez különösen olyan területeken igaz, ahol akár az Egye-

sült Államok, akár az Európai Unió országai csak korlátozott képességekkel rendelkeznek vagy sebezhetők.

A veszély sokrétű, amely egyrészről abban jelentkezik, hogy mind Európa, mind a tengerentúli, fejlett infrastruktúrával rendelkező országok erősen függnek a kritikus infrastruktúráktól, ezen belül is a kritikus információs infrastruktúráktól. A mindenhol ott lévő kínai figyelő szemek pedig mint alvó cellák hordozzák annak lehetőségét, hogy adott esetben ott csapjanak le, ahol az a legjobban fáj: például korlátozzák katonai információs rendszerek működését, amelyek nélkül ma már igen nehezen képzelhető el bármilyen katonai tevékenység, illetve olyan civil információs rendszerek ellen irányulhat egy adott pillanatban összehangolt támadás, mint például az energiaellátás rendszerének irányítása.

Kína az első olyan állam, amely először alkalmazott és várhatóan továbbra is alkalmazni fog politikai és katonai célokra cybertámadásokat. Jelenleg ezek a támadások inkább a gyenge pontok feltérképezését jelentik, semmint a valódi támadást. Ugyanakkor otthoni cybertevékenységét elemezve láthatjuk, hogy Kína a célok elérése érdekében rendkívül sokféle eszközt használ fel. ■

Irodalom

Zbiegniew Brzezinski: *A nagy sakktábla.* Budapest, 1999, Európa.

2008 Report to Congress of the U.S.–China Economic and Security Review Commission One Hundred Tenth Congress Second Session. U.S. Government Printing Office, Washington, November 2008.

Job van Haaften: China's Beidou Navigation Project. Geoinformatics. 2007. január–február.

Beidou Satellite Navigation System. http://www.bjreview.com.cn/special/node_28605.htm.

EU–Kína megállapodás a Galileo rendszer fejlesztéséről (2003. november 1.), Galileo-honlap, hírarchivum http://galileo.khem.gov.hu.

Innenministerium bestreitet Schäden durch Hackerangriffe. *Der Spiegel,* 25 August, 2007.

Premier Wen: China opposes hacker activity. *China View,* August 27, 2007. http://news.xinhuanet.com/.

Chinesische Hacker spionieren deutschen Mittelstand aus. *Der Spiegel,* 8 Februar, 2007.

CNN Web site targeted. CNN, 2008. április 18. http://edition.cnn.com.

Hackers Attacked California Power. *The New York Times,* June 10, 2001.

Kovács László: Az információs terrorizmus elleni tevékenység kormányzati feladatai. *Hadmérnök,* 2008. június, http://www.zmne.hu/hadmernok/2008_2_kovacsl.php.

Internet Usage in Asia. http://www.internetworldstats.com/stats3.htm.

Gates Creates Cyber-Defense Command. *The Washington Post,* June 24, 2009.

Government gets blog service providers to sign "self-discipline" pact to end anonymous blogging. August 23, 2007. http://www.rsf.org/Government-gets-blog-service.html.

Google to censor China Web searches. *Cnet news,* January 24, 2006. http://news.cnet.com.

Indul a legdrágább internetcenzúra Kínában. *Pcworld.hu,* 2009. június 27.

Experts Say Chinese Filter Would Make PCs Vulnerable. *The New York Times,* June 13, 2009.

China Fears Ethnic Strife Could Agitate Uighur Oasis. *The New York Times,* July 23, 2009.

Kína ideiglenesen letiltotta a Hotmailt, a BBC-t és a CNN-t is. *Origo,* 2009. június 3.

Az utcai tüntetések helyét a hackerek támadásai vették át Iránban. *Hírszerző,* 2009. június 29.