HADMÉRNÖK

VIII. Évfolyam 2. szám - 2013. június

Mészáros Gergely
meszaros.gergely@ybl.szie.hu

SZUN-CE ELVEI A DIGITÁLIS VILÁGBAN

Absztrakt

Szun-ce több ezer éves műve a mai napig helyet kap a világ katonai képzésében. Katonai elveinek jó része napjainkig sem vesztette el aktualitását. Ma, a változó katonai kihívások világában felmerül a kérdés, vajon megállják-e ezek az ókori elvek a helyüket, felhasználhatóak-e a digitális hadviselés területén. Írásunkban sorra vesszük Szun-ce néhány elvét, és megvizsgáljuk, hogy ha a valós világ erőforrásait a digitális világ virtuális erőforrásaival helyettesítjük be, mennyire válik ma is érvényessé, akár felhasználhatóvá az ókori stratéga útmutatása a digitális világban.

Thousands of years old work of Tsun-zu has place in the World military strategy training up to the present day. Most of its military principles are remained relevant and up-to-date. In the world of changing military challenges a question emerges: could these ancient principles cope with or are applicable in the field of digital warfare. In this paper we are listing some principles of Tsun-zu, investigating that in what extent are the antique general's guidance feasible or even usable in the modern digital world.

Kulcsszavak: *ókori hadművészet, stratégia, informatikai biztonság, kiberháború ~ antique warfare, strategy, information security, cyberwar*

BEVEZETÉS

Szun-ce az ókori világ kiemelkedő stratégája volt. Művében megfogalmazott elveket több ezer éven keresztül használták fel hadvezérek generációi. Mi lehet az ókori író titka, hogy művének aktualitása ilyen hosszú időn keresztül sem veszített erejéből?

Könnyen lehet, hogy a válasz magában az emberi viselkedésben rejlik. A háború nagyjából egyidős az emberiséggel. A felhasznált eszközök ugyan folyamatosan fejlődtek, az emberi agy néhány ezer év alatt nem sokat változik. A hadviselés taktikai szinten az idők során nagymértékben átalakult, az alapvető hadvezetési elvek viszont lényegesen közelebb állnak az időben nagyjából állandónak tekinthető emberi viselkedéshez és természeti törvényszerűségekhez, így hosszú időn keresztül is képesek megőrizni frissességüket. Talán ebben rejlik Szun-ce titka is.

Felmerül a kérdés, vajon ezek az időtálló elvek képesek-e megőrizni értékeiket egy teljesen más környezetben: a digitális világ „virtuális valóságában". E cikk szerzője úgy gondolja, hogy igen, még ilyen eltérő feltételrendszer esetén is felhasználhatók az ősi elvek. Természetesen csak bizonyos keretek között, korlátozottan és megfelelő fogalom-transzformációt követően.

Szun-ce műve a mai olvasó számára nem egyszerű olvasmány. Részben, mert az európai olvasó – kevés kivételtől eltekintve – csak fordításokon keresztül ismerheti meg az eredeti művet, másrészt, át kell tudnunk hidalni a több ezer éves időtáv fogalmi és kulturális különbségeit.

Írásunkban azt szeretnénk bemutatni, hogy minden nehézség és távolság ellenére az ókori hadtudós művének egyes elvei még a modern idők teljesen eltérő, információs hadszínterén is alkalmazhatóak lehetnek.

MIÉRT (NE) HALLGASSUNK SZUN-CE TANÁCSAIRA?

Manapság meglehetősen sok írás foglalkozik az ókori hadtudós művének digitális vonatkozásaival. Az elmúlt évek szakcikkeit olvasva újra és újra felbukkan Szun-ce neve: a TechWorld nemrégiben megjelent írása információbiztonsági tanácsokkal lát el bennünket a hadvezér útmutatása alapján [1]; Keith Price, az Australian information Security Association igazgatója, a számítógépkalózok elleni küzdelemhez készített hasonló útmutatót [2]; a Cyberwarzone a kiberhadseregek megjelenése kapcsán említi [3]; David Gewirtz komputerspecialista pedig Szun-ce szavait használja a kínai-amerikai kiberháborús feszültség viszonyának illusztrálására [4]. Mondhatni, divatos lett Szun-ce elveit idézni az információbiztonság területén. Adódik a kérdés, van-e egyáltalán értelme egy számítógépről hírből sem halló ókori szerző, teljesen más környezetben született művét nehézkes analógiákkal saját korunk „virtuális világára" erőltetni?

Bizonyos esetekben egészen biztosan, hiszen nem véletlenül találkozunk annyiszor az ókori mester nevével; a hadtudományban jól csengő, ismert név pusztán a figyelem felkeltése szempontjából sem utolsó. Ugyanakkor Szun-ce egy-egy törvénye az ismertetni kívánt modern elv színes kiegészítője, illusztrációja is lehet, amely segíthet a megértésben, illetve hangsúlyozhatja az adott elv univerzális alkalmazhatóságát. Ilyen értelemben az interpretáció tehát mindenképpen előnyös. Mint láthattuk, nem ritka, hogy modern, IT szakembereknek szóló biztonsági útmutatók használják vázlatként ezt az ókori művet.

Semmiképpen sem szerencsés azonban Szun-ce törvényeit látszólag hasonló virtuális objektumoknak megfeleltetve, azokból vakon következtetéseket levonni. Az analógiák is csak akkor hasznosak, ha a helyükön kezeljük őket. Vannak szakemberek, akik emiatt keményen bírálják az ilyesfajta idézeteket [5]. Továbbá nem árt szem előtt tartani, hogy Szun-ce művét a háborúról írta, napjainkban pedig a hálózati hadviselésénél jóval tágabb értelmű

információs műveletek is csak a hagyományos háború egyik, és nem egyetlen eszköze . Önálló, a hagyományos háború ismérveit felvonultató kiberháborút még senki sem vívott, sőt, az is vitatott, hogy egyáltalán lehetséges-e ilyesmi a jövőben [6]. Az USA Nemzeti Katonai Stratégia a Cybertéri Műveletekhez (National Military Strategy for Cyberspace Operations) meghatározása szerint a kibertér olyan tartomány, ahol hálózatos rendszerekben működő elektronikai eszközöket és az elektromágneses spektrumot használják fel az adatok tárolására, cseréjére és módosítására. A kiberhadviselés alatt a kibertérben megvalósuló műveletek összességét értjük [7]. A valódi kiberháború tehát olyan háború lenne, amelyet döntő részben vagy kizárólagosan a kiberhadviselés módszereivel a kibertérben vívnak meg.

A háború erőszakos eszközökkel vívott küzdelem, amely Clausewitz értelmezésének megfelelően mindig politikai célzatú, illetve a politikára visszaható, dinamikusan változó, összetett jelenség. A Szun-ce idézeteket bírálóknak tehát igazat kell adnunk abban a tekintetben, hogy sok szerző informatikai biztonság területén született írásokban alkalmazza azokat, holott az ott jelentkező támadások jelen formájukban aligha nevezhetőek háborúnak. Egy vállalati intranet vagy kritikus információs infrastruktúra védelme sokban hasonlít egy terület vagy erőd védelméhez, de az ellene intézett elektronikus támadás még közel sem háború. A mai informatikai támadások megfelelői taktikai szinten maradnak, inkább állítható párhuzamba velük a rablótámadás, kémtevékenység vagy a gerillaharc harc mint a hagyományos háború.

Mindamellett a valós, összetett és kiterjedt kiberháború gondolata sem vethető el teljesen. Könnyen elképzelhető, hogy azokat nem is államok, hanem cégek vagy ideológiai csoportosulások vívják majd meg. Az informatikai rendszerek egyre bonyolultabbá válnak és egyre jobban áthatják a modern élet minden területét. Az információ felértékelődik, ezzel párhuzamosan az egyes szervezetek által értéknek tekintett erőforrások is „virtualizálódnak" így támadhatóvá válnak. Elég csak arra gondolni, hogy manapság egyre gyakrabban találkozunk a papírmentes iroda fogalmával. Ennek megfelelően az információs infrastruktúra ellen intézett összetett támadássorozat komoly (politikai, társadalmi) következményekkel járhat [8], így kimerítvén a hagyományos háború fogalmát. Szun-ce törvényeivel keresett analógiák is csak ebben a kontextusban válhatnak igazán hitelessé.

Akár egy feltételezett összetett kiberháború, akár egyszerűen csak az információbiztonság összefüggésében vizsgáljuk Szun-ce művét, mindenképpen figyelemre méltó, hogy mennyire sok párhuzamot lehet felfedezni az ókori mű törvényei és a modern technológia által létrehozott információs hadszíntér műveleti elvei között. Ebből a szempontból ismét csak nem érdektelen az összehasonlítás, hiszen felhívja a figyelmet arra, hogy ezek az elvek mélyebbek annál, mint amit a felszínen látunk, olyan alapvető tényezőkből erednek, mint a külső (természeti) hatások vagy maga az emberi természet.

SZUN-CE ALAPELVEI AZ INFORMÁCIÓS HADSZÍNTÉREN

Az öt tényező

Ha értelmezni szeretnénk Szun-ce művét az információs társadalom eltérő környezetében, akkor első lépésként meg kell keresnünk alapvető elveinek informatikai megfelelőit. Szun-ce szerint a háborút öt tényező határozza meg: az út, ég, föld, hadvezér, törvény[1] [9].

Az „út" tulajdonképpen az emberi tényezőt jelenti, a népet, amelynek viszonylag jól megfeleltethető a mai értelemben vett közvélemény. Mai világunkban talán még nagyobb hangsúlyt kap ez az elv mint valaha. Amíg emberek vívják a háborúkat a Földön, addig ez a tényező mindig érvényes marad. A digitális „Út" tehát alapjaiban nem tér el Szun-ce eredeti megfogalmazásától. Tekintve, hogy a valódi háború mindig politikai célokat valósít meg, a

1 Szun-ce: A Hadviselés Törvényei, p. 13

jelenlegi társadalmi berendezkedésünk pedig különösen érzékeny a közvélemény hatásaira ez talán az egyik legfontosabb tényező az öt közül.

Az „ég" Szun-ce értelmezésében a homály, a fény a hőség és az évszakok változásának felel meg[1], tehát a külső, természeti körülményeket érthetjük alatta. A digitális világ talán kevéssé függ a természeti hatásoktól, mindent meg is teszünk annak érdekében, hogy így legyen, ám teljesen kizárni azokat mégsem lehetséges. A hálózati rendszerek igen sérülékenyek lehetnek például a naptevékenységből származó mágneses jelenségekre, de akár az óvatlan mozdulat okozta kábelszakadásra is. Az áramszünetek pedig éppoly egyformán sújthatják mindkét felet, mint a természeti csapások. A kört kicsit kibővítve, ide sorolhatunk minden – nem a digitális világból származó – hatást, amely a szemben álló felektől független és egyformán hatással van az általuk végzett műveletekre.

A „föld" jelentése Szun-ce értelmezésében: „járhatatlan, járható, közeli vagy távoli, tágas vagy szűk"[1]. Vagyis, a fizikai környezet változatos adottságai. A digitális világban ennek a rajtunk kívül álló hálózati és hardver feltételek felelnek meg. A digitális térben végzett műveletek hálózatokon, számítógépeken, elektronikus adatszerző, -tároló, -feldolgozó és -továbbító eszközökön, rendszereken zajlanak. Az idő, mint minden háborús helyzetben itt is kulcsfontosságú, legfeljebb itt napok helyett esetleg milliszekundumokról van szó. Az idő, a sávszélesség, a kapacitás pedig attól függ, hogy mennyi és milyen hardvert tudunk felhasználni és milyen hálózatokon keresztül hajtjuk majd végre a műveleteket. Ez tehát a digitális föld.

A „hadvezér" tulajdonságai: „a bölcsesség, a megbízhatóság, az emberség, a bátorság és a szigorúság"[2], azaz az vezetői emberi értékek. Akárcsak az Út esetében, ez az elv is az emberhez kötődik, aki a háborút vívja és nem az eszközhöz, amellyel a konkrét tetteket végrehajtják. Ezért az ide vonatkozó elveket is szinte változtatás nélkül elfogadhatjuk. A bátorság fogalmát talán érdemes kicsit jobban körüljárni. A virtuális világban nem teszi kockára testi épségét egyik fél sem, nyilvánvalóan egészen másfajta bátorság kell egy rendszer feltöréséhez mint a tűzvonalban való élethalálharchoz. Igaz, korunk hagyományos háborúiban is könnyen előfordulhat, hogy a parancsok igen távolról, teljes biztonságból érkeznek, közvetlen életveszélynek csak a harcoló kötelékek vannak kitéve. Szun-ce korában azonban mindez nem így volt. A tisztek éppúgy életükkel fizethettek a kudarcért mint a közkatonák, még ha túlélési esélyeik a jobb felszerelés, informáltság és védelem miatt valamivel nagyobbak is voltak. A digitális hadszíntér „tisztjei" programozók, „harcoló katonái" pedig jobbára programok. Ebben az esetben a bátorság kérdése is kicsit más megvilágításba kerül. Ennek ellenére mint tényező továbbra is létezik, a kudarccal vagy felfedéssel járó konzekvenciáktól való félelem minden bizonnyal a digitális kor „harcosát" is éppen úgy befolyásolják mint ókori megfelelőit.

A „törvény", „a katonai szabályok és a rend, a helyes úton való vezetés, valamint a szükségletekről való gondoskodás."[2] Amit Szun-ce e tényezőben megfogalmaz, az nagyjából megfelel a modern hadviselés szervezési és háttértámogatási feladatainak. Akárcsak az ókorban, ma is lényeges elem, hogy mennyire hatékonyan sikerül felépíteni egy olyan összetett struktúra működési szabályait mint a haderő. A digitális világ kihívásainak megfelelni igyekvő haderő tekintetében sincs ez másként. A struktúra kialakítása nagymértékben kihat a reakcióidőre és a pontosságra, ami kritikus paraméter lehet egy esetleges konfliktus során. A digitális haderő esetében a szervezeti felépítésen túl a megfelelő reakciótervek és protokollok kidolgozását is jelenti. Különös figyelmet érdemel, hogy a virtuális tér műveleti sebessége lényegesen meghaladja az ókori, illetve akár a modern hadviselés feladat-végrehajtási idejét. Ezért különösen fontos, hogy a lehető legtöbb elképzelhető helyzetre megfelelő akcióterv álljon rendelkezésre. Szun-ce törvénye tehát a

2 Szun-ce: A Hadviselés Törvényei, p. 13

digitális világban a rendszabályoknak, előzetes felkészülés során összeállított megelőzési, reakció és helyreállítási terveknek felel meg.

A hét alapelv

A hadi helyzet megállapítása Szun-ce szerint a hét alapelv alapján történhet. Ha ezekbe a korábban tett megállapításaink alapján behelyettesítjük a modern információs hadszíntér megfelelőit, értelmezhető és aktuális megállapításokat kapunk:

1. „Melyik uralkodó van birtokában a helyes útnak?”[3] Azaz, melyik fél vezetői képesek a közvéleményt maguk mellé állítani. A politika és a háború összefonódása, egymásra hatása a nyugati hadtudományban Clausewitz óta ismert tényező. Még az egyébként sikeres kibertámadás sem érheti el valódi célját, ha annak társadalmi interpretálása nem „kívánatos úton” történik, sőt, adott esetben éppen ellenkező hatást válthatja ki, mint a támadó eredeti célja volt.
2. „Melyik hadvezér tehetségesebb?”[3] A tehetség kérdését napjainkban kicsit másként kell értékelnünk, hiszen Szun-ce korában sokkal több múlt a hadvezéren, aki alatt mindenki más lényegében katona volt. Helyesebb, ha a hadvezér alatt itt a vezetők csoportját értjük. Nyilvánvalónak látszik, hogy a helyzetértékelés során érdemes figyelembe vennünk, hogy melyik fél vezetői rendelkeznek jobb képességekkel és kaptak megfelelőbb képzést.
3. „Az eget és a földet [a természeti feltételeket] melyik tudja a maga számára hasznosítani?”[4] A virtuális hadviselésben egyedülálló lehetőségeket teremthetnek a külső körülmények (természeti jelenség, áramkimaradás vagy akár a kulcsemberek megbetegedése), ahogy nagy előnyt jelent az is, ki képes maga javára kiaknázni a hálózati és hardver erőforrásokat. Gondolhatunk itt egy botnet[5] feletti uralom megszerezésére éppúgy, mint a DDoS támadással blokkolandó teljes sávszélesség és redundáns rendszer kialakításának ismeretére, amely nélkül a támadás tervezése lényegesen nehezebb lenne.
4. „A törvényeket és rendeleteket melyik valósítja meg jobban?”[4] Korábban már kiemeltük az akciótervek különös fontosságát. Nyilvánvaló, hogy az a szervezet van előnyben, amely jobb, pontosabb és szélesebb körű tervekkel rendelkezik és ahol az irányítási struktúra kevésbé sérülékeny. A felkészültebb felet lényegesen nehezebb lehet meglepni, és a sikeres támadás negatív hatásait is hamarabb képes semlegesíteni. A virtuális térben vívott háború esetén a kérdés még nagyobb hangsúlyt kap, hiszen az informatika világában hetek helyett órák, percek helyett milliszekundumok alatt történnek az események. A rögtönzés lehetősége jelentősen lecsökken, esetenként olyan gyorsan kell döntést hozni, amelyre az emberi agy fizikailag képtelen. A részletesen kidolgozott akciótervek, protokollok, biztonsági szabályzatok megléte vagy éppen hiánya könnyen eldöntheti az összecsapás végkimenetelét.
5. „Melyik hadsereg az erősebb?”[4] A kiberhadviselés területén nem egyszerű dolog definiálni az erő fogalmát, de ha a harcoló katonák helyére hálózati erőforrásokat (számítógépeket) képzelünk valamelyest világosabb képet kapunk. A nagyobb méretű hálózat (botnet, közösségi, vállalati hálózat) és a routerek feletti kontroll és a nagyobb számítási kapacitás egyértelmű előnyt biztosít az azt birtokló félnek. Gondoljunk csak a túlterheléses támadásokra vagy egy kulcs vagy jelszó teljes visszafejtésen (brute force) alapuló feltörésére. Mindamellett, a szakképzett emberi

3 Szun-ce: A Hadviselés Törvényei, p. 15

4 Szun-ce: A Hadviselés Törvényei, p. 15

5 Robot-network, legálisan vagy illegálisan telepített, valamilyen cél érdekében automatikusan kommunikáló programok hálózata.

erőforrás létszáma is hatással van az erőre, bár koránt sem olyan mértékben mint az ókori hadseregek esetén.

6. „A tisztek és a gyalogosok melyik seregben gyakorlottabbak?”[4] Azaz, a programozók hol képzettebbek, a programokat hol tesztelték megfelelőbben? A digitális hadviselés elsődleges fegyverei vagy ha úgy tetszik „harcosai” a kémprogramok, férgek, vírusok csak addig igazán hatékonyak amíg észrevétlenek tudnak maradni. Ennek elsődleges kritériuma a lehető legszélesebb körű tesztelés. A nemkívánatos rendszerkomponens jelenlétére az esetek nagy részében a komponens hibás működése derít fényt (nem tervezett szoftverkörnyezet miatti leállás, túlzott memóriahasználat, lassulás stb.) A programozók gyakorlata és a gyakorlatnak megfeleltethető tesztelés tehát a digitális világban is meghatározó jelentőségű a helyes helyzetmegítélés során.
7. „A jutalmazás és büntetés melyik seregben világosabb?”[4] Vagyis, a felelősségek rendszere hol van világosan és egyértelműen kidolgozva. Melyik fél fog egy nem várt esemény bekövetkezésekor időt veszíteni a felelőskereséssel, ahelyett, hogy a problémával foglalkoznának? Akár csak az ókorban, napjainkban is előnyt jelent, ha szervezet tagjai számára világos és átlátható meddig terjed a hatáskörük és kitől fogadhatnak el utasításokat, legyen szó erősen strukturált katonai hierarchiáról vagy laza megoszló felépítésű terrorista szervezetről. Személyi számítógépek és webkiszolgálók feltörését könnyen elvégezheti akár egyetlen ember is, de a kiberháború összetett műveleteit és időzítését aligha lehet jól felépített szervezeti struktúra nélkül végrehajtani. A magasan szervezett struktúrák közül pedig az fog hatékonyabban működni, amelynél a jogok és felelősségek rendszere világosabb.

Szun-ce hét alapelve mind a mai napig nem sokat vesztett érvényességéből. Különösen figyelemre méltó, hogy kis átalakításokkal és behelyettesítéssel az eredetitől jelentősen eltérő virtuális környezetben, a kiberháború vonatkozásában is értelmezhetőek. Igaz ugyan, hogy néhány elv olyan általános értékeket fogalmaz meg, amelyek magára az emberi viselkedésre jellemzőek és bármely versenyhelyzetben értelmezhetőek lennének, ugyanakkor külön figyelmet érdemel Szun-ce első és negyedik alapelve, amelyek a kibertérben talán erősebben érvényesülnek mint korábban bármikor.

SZUN-CE ÚTMUTATÁSAI

Az alapelvek értelmezése után az alábbiakban megpróbálunk olyan hasonlatokat és azonosságokat keresni, amelyek segítenek feltárni és megérteni a kiberhadviselés és a Szun-ce által megfogalmazott hagyományos háború esetleges összefüggéseit.

Behatolás és visszatérés

Szu-ce szerint „ha idegenek vagyunk valahol, akkor mindig alapelvünk legyen, hogy mély behatolás esetén jól összpontosítsuk erőnket, s akkor az odavalósiak nem győzhetnek le bennünket”[6] Az ellenséges területre történő behatolás, betörés fogalma könnyen értelmezhető a digitális világban is. Az ellenséges informatikai rendszer védelme feltörhető, megkerülhető, az ott felhalmozott erőforrások és értékek (információk) megszerezhetők, akár csak az anyagi világban. Az informatikai védelem sokban hasonlít a hagyományos védekezéshez. Ha a külső megerősített vonalakat sikerül áttörni, a belső jóval kevésbé védett (és általában rosszabbul tesztelt) belső rendszerekben már sokkal könnyebb dolga van a támadónak.

A visszatérés fogalma viszont már nem ennyire egyértelmű. Mivel valós fizikai mozgás kibertámadás esetében többnyire sincs, eredeti megfogalmazásban a visszatérés sem

6 Szun-ce: A Hadviselés Törvényei, p. 87

értelmezhető. Ugyanakkor a behatolás értékét nagyban csökkentheti, ha a behatolás ténye és módszere idő előtt nyilvánosságra kerül. Ezért a támadó saját jól felfogott érdekében megkísérli eltüntetni a nyomait, elrejteni a hátrahagyott rendszereit (rootkit, logger, backdoor). A nyomok eltüntetése történhet egyszerű, erőből történő megoldással, például a naplófájlok törlésével, fájlrendszer és másolatok megsemmisítésével, de akár egészen szofisztikált eljárással is (lopakodó módszerek, rendszeranalízis eszközök megtévesztése, védelmi rendszerek, vírusirtók célzott támadása).

A visszatérésnek közelítőleg megfeleltethető a megtámadott rendszerből való nyom nélküli visszatérés, vagyis a támadás célját szolgáló rendszerek elegendő ideig történő elrejtése. A támadó kötelék ugyan elérheti a támadási célját, de ha visszavonulási útját elvágják és végső soron a megsemmisülés fenyegeti, összességében pürrhoszi győzelmet arat, esetleg nagyobb veszteséget szenved mint amit az amúgy sikeres támadással okozott. Hasonlóképpen, ha a digitális támadás ugyan sikeres, de a nyomok alapján a támadó rendszerek egyértelműen beazonosíthatóak, esetleg az irányítók kiléte is felderíthető, az adott esetben a vereséggel érhet fel.

A felfedett sérülékenységeket, az azokra építő szoftvereket másodszor már nem fogjuk tudni használni, ugyanúgy, ahogy a betörés során csapdába esett vagy megsemmisített erőket sem. A visszatérés helyét a digitális háborúban tehát a rejtett működés, a felderíthetetlenség veszi át.

Szun-ce azt tanácsolja, ha ellenséges területen járunk, összpontosítsuk erőinket, fosztogassunk (azaz használjunk helyi erőforrásokat) és lehetőleg pontos tervek alapján dolgozzunk, amelyeket más nem képes áttekinteni[7]. Az ellenséges rendszer feltörése (a behatolás) során a támadást ezek szerint lehetőleg egyetlen gyenge pontra, ismert sérülékenységre kell irányítani. Racionálisan hangzik, hiszen több sérülékenység szisztematikus végigpróbálása növeli a felderítés kockázatát. Nagyszámú, rosszul védett rendszer támadása (botnet kiépítése polgári gépeken) esetén járható út lehet a lehető legtöbb sérülékenység végigpróbálása, de fejlett védelmi és monitoring rendszerrel rendelkező célpontok elleni támadás során nem bölcs dolog a szükségesnél nagyobb „zajt csapni”.

Ha elérhetőek, akkor a helyi rendszer erőforrásait érdemes felhasználni, kisebb részben azért, hogy saját erőforrásainkat kíméljük, nagyobb részben pedig, mert saját belső rendszereikről érkező forgalommal szemben értelemszerűen sokkal elnézőbbek a megfigyelő rendszerek, lényegesen kisebb a valószínűsége, hogy a gyanús tevékenység riasztást generál.

A hadvezetés és az erőforrások

Szun-ce felhívja a figyelmet az erőforrások fontosságára, az utánpótlás kimerülésének veszélyeire. Azt javasolja, használjunk fel minél többet az ellenfél erőforrásaiból, ha nem szükséges ne semmisítsük meg őket. „Aki ért a hadvezetéshez, az katonákat nem soroztat másodszor, élelmet nem szállíttat harmadszor. […] Az ellenséget megölni: dühöngés, ám az ellenségtől elvenni: javaink gyarapítása.”[8] Nem kétséges, hogy a digitális hadviselés során is hasonló a helyzet. Ha az ellenség által használt botnet felett sikerül átvenni az uralmat, nem csak meggyengítettük, de meg is erősödünk általa.

Ugyanakkor látni kell, hogy az ami Szun-ce korában elképzelhető volt, nevezetesen, hogy egy teljes (legyőzött) hadsereg átáll az oldalunkra, a digitális harctéren nehezebben elképzelhető. Egy-egy kisebb csoport talán megvásárolható vagy kényszeríthető, de egy komplett védelmi/támadó infrastruktúra átállása már kevéssé valószínű. Nyilvánvalóan a kényszerítő erő is kisebb, hiszen az irányító személyzetet nem fenyegeti a fizikai megsemmisülés. Cégcsoportok közötti összecsapás során mégis elképzelhetőnek tartom, hogy

7 Szun-ce: A Hadviselés Törvényei, p. 83
8 Szun-ce: A Hadviselés Törvényei, p. 23

a lelepleződéstől való félelem és a nagy ráfordítással kiépített támadó infrastruktúra megtartásának ígérete elegendő az átálláshoz.

Szun-ce azt mondja: „...a legjobb hadsereg az, amelyik meghiúsítja az ellenség terveit; csak ezután következik az, amelyik szétzúzza az ellenség szövetségeseit, majd utána az, amelyik harcot vív az ellenséges sereggel, s végül az a legrosszabb, amelyik városfalakat kezd ostromolni."[9]

Amennyiben a kiberháború és a hagyományos háború között valóban létezik párhuzam, ez a törvény érdekes kérdést vet fel. Vajon tényleg a leginkább védett, legfejlettebb elhárító rendszerekkel felvértezett kritikus informatikai rendszereket érdemes „kiberhadseregünkkel" megtámadni?

Szun-ce véleménye szerint az a legjobb, ha harc nélkül vagyunk képesek akaratunknak alávetni az ellenséges hadsereget. Véleménye szerint az ellenséges sereg szétverése sem tartozik az igazán jó megoldások közé. A digitális háború legalább annyira az emberi fejekben megy végbe, mint a „digitális harcmezőn". Nem lehetetlen, hogy az ilyen háborút a közösségi hálózatok és jóval kevésbé hatékonyan védett személyi számítógépek (okostelefonok, táblagépek) világában kell majd megvívni. Ebben a környezetben Szun-ce elve is értelmezhetővé válik, hiszen ha a végső, politikai cél elérhető a közvélemény direkt manipulálásával, aligha van értelme a jól védett központi rendszerek (várak) ostromának.

Üresség és teltség elve

Az üresség az ellenfél gyengeségét, a teltség saját hatékony csapásmérő erőnket jelképezi. Szun-ce szerint az erőnket az ellenfél ürességére kell irányítanunk, amit úgy érünk el, hogy előnyöket felkínálva, cselvetéssel pozíciójából kimozdítjuk. Saját ürességünket csökkenthetjük más forma mutatásával, pozíciónk titokban tartásával, az ellenfél bizonytalanságban tartásával. „Jól támadni annyit jelent, hogy az ellenség nem tudja, hol védekezzék jól, védekezni pedig annyit, hogy az ellenség nem tudja hol támadjon." [10]

A fenti elvek tulajdonképpen az információs fölény modern fogalmával kapcsolhatók leginkább össze. Az információs hadviselés korunkban egyre hangsúlyosabb szerepet játszik, az Öbölháború óta a hagyományos háborúk egyik legfontosabb célkitűzése is az információs fölény biztosítása.

Természetes következtetésnek látszik, hogy egy lehetséges információs háborúban az információs fölény kivívása van a legnagyobb hatással az végkimenetelre, de ez jelenti egyúttal a legnagyobb kihívást is. Szun-ce erősen érvel a kiszámíthatatlanság és a információhiányban tartás mellett, oly mértékben, hogy szerinte saját erőinket sem hasznos beavatni terveinkbe. Ezáltal tulajdonképpen eljutunk a nyíltság kerülésén alapuló biztonság (security through obscurity) elvéhez, amely ellentétben áll a gyakran hangoztatott Kerckhoffs elvvel, miszerint kizárólag a kulcsok titkosságának megőrzése célravezető, a módszerek titkosítása nem vezethet eredményre.

Több szakértő vitatja azonban, hogy a rendszer (program, hálózat) működési elvének vagy jelenlétének eltitkolása valóban hiábavaló próbálkozás lenne. [10] Az ismeretlen vagy nehezen kiismerhető rendszer elriaszthatja a kevésbé eltökélt támadót, aki esetleg más, könnyebb célpontot keres, a kitartóbbakat pedig lelassíthatja. A információs rendszerek védelem-támadás mérlege egyenlőtlen: a védekező félnek minden fronton hibátlan védelmet kell alkotnia, a támadónak ellenben az is elegendő ha egyetlen-egy biztonsági rést felfedez. Ha élünk a rejtés módszerével, tulajdonképpen Szun-ce útmutatását követve elérhetjük, hogy a támadó ne tudja hol érdemes támadnia.

Fordítva vizsgálva a dolgokat: az ellenfél motivációinak, gyengeségeinek, sőt, kilétének felfedése úgyszintén kritikus lehet. A digitális hadszíntéren sem egyszerű pontosan

9 Szun-ce: A Hadviselés Törvényei, p. 25
10 Szun-ce: A Hadviselés Törvényei, p. 45

megállapítani, hogy ki-kicsoda. A rendszer támadója éppúgy lehet unatkozó diák, „munkáját végző” megélhetési un. fekete-sapkás cracker, szervezett terroristacsoport tagja vagy éppen professzionális hírszerző-hálózat. Szun-ce szerint igen fontos, hogy pontosan tudjuk mikor és mire kell támadnunk. A digitális hadviselés esetén talán helyesebb úgy fogalmazni: „kire kell támadnunk”. Hiszen nyilvánvaló erőforrás pazarlás lenne (valós vagy virtuális) ellencsapást mérni egy diákcsíny elkövetőire, nem beszélve arról, hogy ez esetben védelmi képességeink és módszereink egy része óhatatlanul napvilágra kerül.

Területformák

Szun-ce szerint: „A hadvezetés törvényei szerint van laza terület, van könnyű terület, van harcra ingerlő terület, van nyílt terület, van kulcsfontosságú terület, van súlyos terület, van nehezen járható terület, van körülzárással fenyegető terület és van halálos terület.”[11]

Nem tűnik különösebben hasznosnak a digitális hadszíntérre vonatkoztatva vizsgálni ezeket a valós területviszonyokra íródott elveket. Különös módon a fizikai tényezőknek digitális fogalmakat megfeleltetve mégis kapunk néhány használhatónak tűnő elvet. Először is azt kell tisztázni, mit érthetünk terület alatt a digitális világában. Véleményem szerint a terület fogalma jól megfeleltethető a hálózatoknak, a hálózati jelenlétnek. Olyan hálózatba kapcsolt, kevéssé védett rendszerek együttesét érthetjük alatta, amelyek irányítása (uralása) valamilyen előnyt jelent.

Súlyos területen (mély behatolás esetén) az erőket összpontosítani kell, vagyis kis számú, de jól kihasználható sérülékenységre kell koncentrálni. Az ilyen területen a behatoló még működőképes védelmi rendszerek mögött tevékenykedik, vagyis „erődöket” – azaz esetünkben felderítő rendszereket, nem kompromittált tűzfalakat és naplózó rendszereket – hagy maga mögött. Valóban racionális elvnek hangzik, hogy ilyen esetben lehető legkevesebb felderíthető abnormális tevékenység elvét alkalmazzuk. Ilyen helyzetben Szun-ce a fosztogatást részesíti előnyben. Hálózati hadviselés esetén is az adatforgalom figyelés, esetleg egyetlen rendszer gyors és lehetőleg hibajelenségnek álcázott kiiktatása lehet hatásos, hiszen számos ismeretlen tényezővel és rendszerrel a hátunk mögött direkt konfliktust fölvállalni (belső rendszer túlterheléses támadása, férgek opportunista bevetése a belső rendszerek ellen, stb.) merőben kockázatos és kevés hosszú távú sikerrel kecsegtető vállalkozás.

Könnyű területen (kis mértékben behatolva), azaz amikor külső, rosszabbul védett „határmenti” rendszereket támadunk, a lehető legtöbb sérülékenységet végigpróbálva megoszló támadást indíthatunk. Ez tehát a IP-szkenneléses eljárások, férgek és trójai programok lehetséges alkalmazási területe.

A mindkét félnek előnyöket kínáló terület a „harcra ingerlő terület”. Szun-ce szerint: „harcra ingerő területen csak az ellenség után szabad cselekednünk”[12], vagyis az ellenfél lépéseire reagáljunk. Az ilyen területen a világos szándék hátrányt jelenthet. Tegyük fel, hogy egy szervezetnek valamely 0-day sérülékenység[13] folytán lehetősége van nagy számú rendszer fölött átvenni az irányítást, ugyanakkor a rendelkezésre álló információk alapján nagy az esélye, hogy a sérülékenységet ellenfelei is ismerik. A helyzet megfelel a harcra ingerlő terület fogalmának, hiszen mindkét fél előnyt kovácsolhat magának. Ha a szervezet átadja az ellenfélnek a kezdeményezést, megmarad a döntési pozícióban. Amennyiben az ellenfelek elkezdik kiaknázni a sérülékenységet, megpróbálhat bizonyítékokat gyűjteni, majd a sérülékenységet bejelentve (ezzel hatékonyságát drasztikusan csökkentve) a közvéleményt jelentős mértékben a sérülékenységet kihasználó ellenséges csoportok ellen hangolni. Ugyanakkor dönthet úgy is, hogy a sérülékenységet saját céljaira maga is felhasználja.

11 Szun-ce: A Hadviselés Törvényei, p. 83

12 Szun-ce: A Hadviselés Törvényei, p. 93

13 Zero-day exploit: olyan publikálatlan sérülékenységet kihasználó kód, amelyről a fejlesztő nem tud, nincs elérhető biztonsági javítás az elhárítására.

Amennyiben viszont a kezdeményezést magához ragadja, nincs többé döntési lehetősége és az ellenfelet juttatja hasonló döntési szituációba.

Halálos az a terület ahol teljes megsemmisülés fenyeget, „nincs számunkra kiút" és csak gyors csatával nyerhetünk. Esetünkben megsemmisülés alatt a támadó infrastruktúra teljes harcképtelenségét vagy a szervezet emberi irányítóinak nagy arányú morálcsökkenését érthetjük, ami a további harcot elképzelhetetlenné teszi. Szu-ce szerint ilyen területen katonáinknak meg kell mutatnunk milyen veszély fenyeget, hogy azok szorult helyzetüket felfogva maximális hatékonysággal végezzék feladatukat. Ez ellentétben áll Szun-ce általános kiismerhetetlenségi elvével miszerint a vezér „legyen képes ostobaságban tartani katonáinak fülét és szemét, s érje el, hogy senki ne tudjon semmit; változtassa meg intézkedéseit ..."[14] Tehát általánosságban érdemes a lehető legnagyobb titokban tartani a terveket, a szervezet minden tagjának a lehető legkevesebb, éppen csak szükséges információt elérhetővé tenni. Ugyanakkor, ha végveszély fenyeget, érdemes lehet a személyi állományt szembesíteni a konkrét veszélyekkel. Természetesen számolni kell azzal, hogy az egzisztencia esetleges elvesztése azért lényegesen kisebb motivációt jelent, mint a fizikai megsemmisüléstől való félelem, ami kiberhadviselés esetén azért elég ritkán kerül szóba.

Kémek

A kémek alkalmazása minden korban minden hadviselő félnek nagy előnyt jelentett, ez alól a „kiberháború" sem lehet kivétel. Tulajdonképpen jelenlegi formájában a kiberhadviselés szinte kizárólag erre az egy területre koncentrálódik.

Tekintve, hogy a számítógépes rendszereket egyenlőre emberek működtetik, egy lehetséges kiberháborúban az emberi kémek pontosan úgy használhatók mint bármely más háborús helyzetben, azaz Szun-ce ide vonatkozó megállapításai változtatás nélkül érvényesek lehetnek. A minket elsősorban érdeklő terület a hagyományostól eltérő gépi kémkedés, azaz a kémprogramok világa.

Milyen kémrendszereket, adatforrásokat használhatunk fel információgyűjtésre, azaz mi felel meg Szun-ce által meghatározott öt kémtípusnak? Az első csoportot az adatgyűjtő és feldolgozó rendszerek jelentik. Ezek a rendszerek nyilvános (vagy kvázi-nyilvános) adatforrásokból származó információkkal dolgoznak, emberi közreműködéssel vagy anélkül állítanak elő stratégiai információt. Közelítőleg megfeleltethetők Szun-ce, az ellenséges vidéken „megtelepedett kém" fogalmának.

A második csoportba már konkrét kémprogramok tartoznak, amelyek az ellenséges rendszerbe épülve belső információkat képesek megszerezni (keyloggerek, spyware). Ezek Szun-ce belső kémeinek felelnek meg. Ebben az esetben a kémprogram észrevétlen működésén túl a megszerzett információ észrevétlen kijuttatása is igen hangsúlyos kérdés, sőt talán ez a legnehezebb feladat.

A harmadik csoportba olyan ellenséges kémrendszereket soroljuk, amelyeket sikeresen beazonosítottunk, így lehetőség nyílik hamis információk továbbítására. Kiváló lehetőség arra, hogy a támadók figyelmét a megfelelő (pl. honeypot[15]) célpontra irányítsuk. Szun-ce a „visszatérő kém" nevet adta ennek a csoportnak, igaz, esetünkben használatuk valamivel nehezebb, hiszen a felderített kémprogram önmagában csak erősen korlátozott információkat szállít alkalmazójáról, sőt, a pontos azonosításra még jól megtervezett csapdarendszerrel is csekély lehet az esély.

A negyedik kémcsoportot kifejezetten dezinformáló célokra használunk fel. Ilyen lehet egy szándékosan gyengén megírt malware, amely más csoportokra utaló információkat tartalmaz, illetve információ-mérgezéses támadások, ahol algoritmikusan generált, szintaktikailag helyes, de hibás vagy értelmetlen információt helyezünk el az ellenséges adatbázisokban.

14 Szun-ce: A Hadviselés Törvényei, p. 91

15 Szándékosan, csalétekként kihelyezett rendszer, a támadás észlelése és szándékainak elemzése céljából

Jelenkori példaként felhozhatjuk a BitTorrent hálózatokat adatmérgező eljárásokkal[16] (decoy insertation, index poisoning, swarming támadó jogtulajdonosokat, akik ilyen módszerekkel próbálják elejét venni az illegális másolatok terjedésének [11]. Ezt a kémcsoportot Szun-ce a „halál kémeinek”[17] nevezi.

Az utolsó kémcsoport az „élet kémei”, olyan kémet jelöl, amely az ellenségtől információval tér vissza. Digitális megfelelője olyan kémprogram, amely közvetlenül nem képes alkalmazójával kommunikálni (illetve a felderíthetetlenség érdekében szándékosan nem kommunikál), ezért a hírekkel együtt ki kell hozni, vissza kell térnie az ellenséges területről. Ilyen kémeszköz (program) lehet minden telepített rendszer, azaz amelyet fizikailag az ellenséges hálózat vagy rendszer közelébe kell vinni, esetleg közvetlenül csatlakoztatni[18].

ÖSSZEFOGLALÁS

Szun-ce műve korának legátfogóbb, összefoglaló műve volt a háború témaköréről. Sikere nem véletlen. Nagyon valószínű, hogy több generáció felhalmozott tudását tartalmazza és sok olyan máig érvényes általános háborús törvényszerűséget fogalmaz meg helyesen, melyek nem a kor haditechnikájához hanem magához az emberi viselkedéshez és természeti törvényekhez köthetők. Nem meglepő, hogy ezek a gondolatok időtállónak bizonyultak. Ha a kulturális és fogalmi eltéréseket sikerül áthidalni, lényegében ma is használható elvekhez jutunk.

Természetesen minden információforrást a helyén kell tudni kezelni. Vakon alkalmazni Szun-ce törvényeit egy eltérő környezetre éppoly hiba lenne, mint teljesen figyelmen kívül hagyni. Egy több ezer évvel ezelőtt született műnek nyilvánvalóan vannak részei, amelyeket egyáltalán nem érdemes egy lehetséges kiberháború során az információs hadviselés területén felhasználni. Ilyenek azok az elvek amelyek Szun-ce korának eltérő katonai-taktikai és társadalmi sajátosságaiból erednek. Az adott korban minden bizonnyal jól működtek, de környezetükből kiragadva már aligha használhatóak.

Írásomban bemutattam Szun-ce néhány hadviselési törvényének lehetséges értelmezését. Megpróbáltam párhuzamot vonni az akkori körülmények és a modern információs hadviselés feltételrendszere között, ami által, mint láthattuk, a régi elvek olykor meglepő módon érvényesnek tűnő megállapításokká alakulnak a modern környezetben.

Joggal merül fel a kérdés: érdemes-e tanulnunk egy ókori mestertől, aki számítógépről hírből sem hallott? Érdemes egyáltalán technológiai és társadalmi értelemben ilyen távoli környezetben született írás elemzésével foglalkozni? Véleményem szerint mindenképpen. Szun-ce műve ma is hasznos szerepet tölthet be. Kiváló gondolatébresztő, teljessége folytán segíthet megtalálni azokat a szempontokat, amelyekre esetleg nem is gondoltunk. Akár vázlatként is felhasználható egy specifikusan információs rendszerek támadásával és védelmével foglalkozó mű gondolatvezetéséhez. Végül, a kibertér összetett környezetének megfelelni kívánó szabályozások kialakítása során segíthet felismerni azokat az alapelveket, amelyek általánosabb, magasabb rendű törvényekben gyökereznek.

16 decoy insertation, index poisoning, swarming
17 Szun-ce: A Hadviselés Törvényei, p. 107
18 TEMPEST támadás, network spy devices

Felhasznált irodalom

[1] Angel S. Averia Jr.: Information security: Seeking Sun Tzu's guidance. *TechWorld* [online]. 2012. http://features.techworld.com/security/3413059/information-security-seeking-sun-tzus-guidance/ [2013-05-29]

[2] K. Price: Sun Tzu's 13 lessons to combat hackers. *Secure Business Intelligence* [online]. 2010. http://www.scmagazine.com.au/News/230430,sun-tzus-13-lessons-to-combat-hackers.aspx/1 [2012-12-19]

[3] Reza Rafati: Sun Tzu: The Art of cyber warfare. *cyberwarzone.com* [online]. 2013. http://www.cyberwarzone.com/sun-tzu-art-cyber-warfare [2013-05-29]

[4] David Gewirtz: For China, hacking may be all about Sun Tzu and World War III. *ZDNet* [online]. 2013. http://www.zdnet.com/for-china-hacking-may-be-all-about-sun-tzu-and-world-war-iii-7000015988/ [2013-05-29]

[5] S. Tornio, B. Martin: InfoSec, Sun Tzu and the Art of Whore. *Attrition.org* [online]. http://attrition.org/security/rant/fsck_sun_tzu/ [2012-12-19]

[6] T. Rid: Cyber war will not take place. *Journal of Strategic Studies*. 2012, Vol. 35, no. 1, pp. 5–32. ISSN 0140-2390.

[7] Haig Zs., Várhegyi I.: A cybertér és a cyberhadviselés értelmezése. *Hadtudomány* [online]. Vol. XVIII. évf., no. Elektronikus szám (2008). http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf [2013-03-20]

[8] Kovács L., Krasznay Cs.: Digitális Mohács Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság*. 2010, Vol. 3, no. 1, pp. 44–55. ISSN 1789-5286.

[9] Szun-ce: *A hadviselés törvényei*. 2. S.l.: Balassi kiadó, 1998. ISBN 963 506 194 3.

[10] Alex Armstrong: Security by obscurity - a new theory. *I programmer* [online]. http://www.i-programmer.info/news/149-security/3132-security-by-obscurity-a-new-theory.html [2012-12-29]

[11] R. Cuevas, M. Kryczka, A. Cuevas, S. Kaune, C. Guerrero, R. Rejaie: Is content publishing in BitTorrent altruistic or profit-driven? *Proceedings of the 6th International COnference* [online]. 2010. pp. 11. http://dl.acm.org/citation.cfm?id=1921183 [2012-12-28]