HADTUDOMÁNYI SZEMLE
12. évfolyam (2019) 3. szám 95–111. • DOI: 10.32563/hsz.2019.3.6

Deák Veronika[1]

Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során

Obtaining Confidential Data in Cyberspace Using Social Engineering for Psychological Operations

Absztrakt

A social engineering olyan módszerek és technikák összessége, amely a befolyásolás és manipuláció segítségével teszi lehetővé bizonyos információk megszerzését. A lélektani műveletek (PSYOPS) célja katonai szempontból a szembenálló fél befolyásolására, manipulálására irányuló tevékenység végrehajtása. Ahogy a definíciók hasonlóságából sejteni lehet, a lélektani műveletek során social engineering technikákat is alkalmazhatnak, többek között információszerzésre is, ami elengedhetetlen feltétele a hatékony befolyásolás megvalósításának.
Jelen tanulmány célja annak bemutatása, hogyan és miért alkalmazhatók a social engineering információszerző technikák a lélektani műveletek során. Továbbá annak feltárása, hogy milyen információk szükségesek a sikeres lélektani műveletek végrehajtásához, valamint mely technikák segítségével érhető el a leghatékonyabban ezen információk megszerzése.

Kulcsszavak: *lélektani műveletek, PSYOPS, social engineering, befolyásolás, információszerzés.*

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorandusz – National University of Public Service, Doctoral School of Military Engineering, PhD student, e-mail: deak.veronika@uni-nke.hu, ORCID: https://orcid.org/0000-0001-9220-2002

Abstract

Social Engineering (SE) uses methods and techniques of manipulation to obtain confidential information. Psychological operations (PSYOPS) is responsible for influencing and manipulating opposing parties. The similarity of the two definitions assumes a correlation as follows. Information obtained by SE techniques can be used during the execution of PSYOPS for manipulation purposes.
In this paper, I classify the information types required for a successful psychological operation in cyberspace and I propose SE techniques for each information type to obtain during PSYOPS.

Keywords: *psychological operations, PSYOPS, social engineering, SE, influence, confidential information*

Bevezetés

A klasszikus hadviselés elemeit már az ókorban is aktívan használták, az idő előrehaladtával és ezzel együtt a technológia, valamint a hadviselési technikák folyamatos fejlődésének köszönhetően a hadviselés újabb tevékenységekkel egészült ki. A lélektani hadviselés alkalmazására számtalan példát találhatunk az ókortól kezdve egészen napjainkig, azonban a tudatos és előre megtervezett kivitelezésére csak a 20. században, az első és a második világháborúban került sor. Ezt követően jelentős fejlődés vette kezdetét, a hidegháborúban még inkább kiforrott a lélektani hadviselés és a lélektani műveletek tevékenységi köre, eszköztára, amelynek következtében egyre kifinomultabb alkalmazási módszerek és eszközök jelentek meg, valamint egyre nagyobb hangsúlyt fektettek a célcsoport kiválasztására és típusának meghatározására is, hiszen ennek segítségével sokkal személyre szabhatóbb műveleteket voltak képesek végrehajtani.

A lélektani hadviselés azt a szervezett és speciális erők által végrehajtott harctevékenységet jelöli, amely a szemben álló fél humán erőforrásait (például vezetés, katonaság, lakosság) célozza, annak érdekében, hogy a morális állapotának és pszichikai felkészültségének megtörésével eltántorítsa a további fegyveres küzdelemtől, illetve annak támogatásától.[2] A lélektani műveletek (Psychological Operations – a továbbiakban: PSYOPS) annyiban különbözik ettől, hogy a végrehajtott tevékenység nemcsak a szemben álló félre irányul, hanem a semleges „közeg"-re is. Ez azt jelenti, hogy nemcsak a háború időszakában, hanem a béke és válság időszakában is aktívan alkalmazandó és alkalmazható. Ebben az esetben pedig nemcsak a szemben álló félre, hanem a baráti erőkre, saját csapatokra és a teljesen semleges érintettekre is kiterjednek a lélektani műveletek.[3]

A 21. századi hadviselés egyik legnagyobb kihívása, hogy a korábban kiforrott haditechnikák egy részét a kibertérben is alkalmazhassuk. Ennek fontosságát mi sem

[2] Pix Gábor: A lélektani műveletek jellemzőinek vizsgálata, Budapest, 2005, 9. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12018/tezis_hun.pdf;jsessionid=D287A4C46B2860409B02EAAF99E6C5A5?sequence=2 (Letöltve: 2019. 08. 26.)
[3] Pix (2005): i. m. 10.

mutatja jobban annál a ténynél, hogy 2016 júliusában az Észak-atlanti Szerződés Szervezete (a továbbiakban: NATO) varsói csúcstalálkozóján hivatalosan is deklarálták, hogy a kibertér önálló hadszíntérnek, műveleti dimenziónak tekinthető, a korábbi fizikai dimenziók mellett (szárazföldi, légi, tengeri, kozmikus).[4] Ez azt jelenti, hogy a különféle kibertámadások komoly kihívásként értelmezhetők, továbbá számtalan – a hagyományos támadásokhoz hasonlóan – káros következményt idézhet elő napjaink társadalmaira nézve. Éppen ezért már a NATO kollektív védelmi feladatai között is megjelenik a kibervédelem.[5]

A fentebb említettek alapján megállapítható, hogy a kibertér a hadviselés minden területén létfontosságú szerepet tölt be. A jelen tanulmányban vizsgált lélektani műveletek hatékony és eredményes kivitelezéséhez is jelentősen hozzájárul a kibertér aktív felhasználása. A kibertérben számtalan új kommunikációs és egyéb eszköz áll a lélektani műveletek végrehajtásáért felelős személyek rendelkezésére, így ezek segítségével jelentősen javítható az e műveletek segítségével megvalósuló befolyásolás hatékonysága.

A lélektani műveletek megvalósítására számtalan eszközt és technikát használtak alkalmazásának kezdetétől fogva egészen napjainkig, a technológia és a rendelkezésre álló eszközök fejlettségétől függően. Míg korábban többek között a szórólapok, a hangosbeszélők, illetve a személyközi kommunikáció használata volt a legjellemzőbb, addig napjainkban, az új hálózatos infokommunikációs technológiák megjelenésének köszönhetően, számtalan új technika áll a rendelkezésre. Fontos megjegyezni, hogy a régebben elterjedt eszközök továbbra is alkalmazandók, a kibertér nyújtotta PSYOPS-módszerek csupán kiegészítik azokat. Abban az esetben, ha a kiberinfrastruktúra nem elérhető, a korábban alkalmazott technikák használandók.

A lélektani műveletek alapvető célja a másik fél befolyásolása, amely eléréséhez számtalan, a kibertér felhasználásán alapuló módszer vehető igénybe, egyik jellemző formájuk az emberi tényező és az infokommunikációs eszközök gyengeségeit, illetve sérülékenységeit együttesen kihasználó támadási módszer a social engineering (a továbbiakban: SE). A social engineering módszerek alkalmazásával jelentősen növelhető a lélektani műveletek kivitelezéséhez szükséges információk megszerzésének mennyisége és minősége, továbbá ezen műveletek során végrehajtott befolyásolás minősége és hatékonysága.

Jelen tanulmány célja annak feltárása, milyen információk szükségesek a lélektani műveletek végrehajtásához, valamint hogyan és miért alkalmazhatók a social engineering információszerző technikái a PSYOPS során. További cél annak meghatározása, hogy mely – a kibertér felhasználásán alapuló – technikák segítségével érhető el a leghatékonyabban az információszerzés a lélektani műveletek során. Fontos kiemelni, hogy jelen tanulmányban kizárólag a civil környezetben megvalósuló lélektani műveletek során végrehajtott információszerzés alapjait határozom meg.

Az első pontban egy motivációs példán keresztül szemléltetem jelen tanulmány célját, a lehetséges kihívásokat, ezt követően az elméleti felvezetésben bemutatom a téma mélyebb vizsgálatához és megértéséhez szükséges alapvető definíciókat,

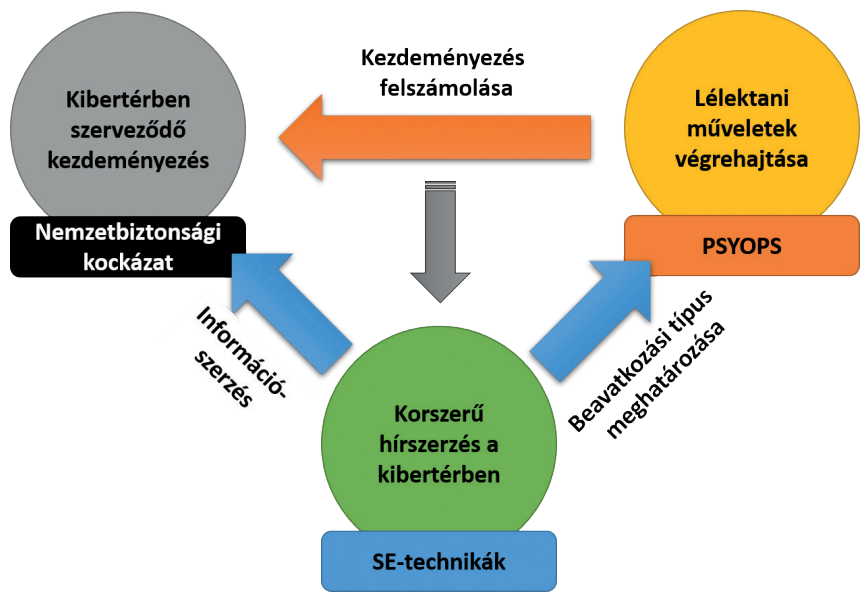
[4] Warsaw Summit Communiqué, 2016. www.nato.int/cps/en/natohq/official_texts_133169.htm (Letöltve: 2019. 08. 26.)
[5] Uo.

háttérismereteket. Ezt követi a civil környezetben megvalósuló PSYOPS-hoz szükséges információszerzés alapjainak ismertetése, a kibertérben alkalmazható információszerző social engineering technikák bemutatása, majd pedig a motivációs példában említett célok és kihívások egy lehetséges feloldása, bővebb ismertetése.

Ahhoz, hogy a témával összefüggően a lélektani műveletekben és a social engineering információszerző lehetőségeinek minden részletre kiterjedő elemzése megvalósulhasson, nélkülözhetetlen a releváns hazai és nemzetközi szakirodalom mélyebb vizsgálata. A PSYOPS és az információszerző social enineering technikák kapcsolatát vizsgáló hazai szakirodalom igencsak hiányos, ezért jelen tanulmányban kísérletet teszek a két terület összefüggéseinek megállapítására. Néhány nemzetközi tanulmány kísérletet tesz a lélektani műveletek során alkalmazott social engineering módszerek vizsgálatára, ám az információszerzés szerepéről és az ehhez alkalmazandó technikákról kevés szó esik.

Motivációs példa

Jelen pontban egy motivációs példát mutatok be a témával kapcsolatos célok, illetve az esetleges kihívások könnyebb és átláthatóbb szemléltetése érdekében. E példa során felvázolt eseményeket, célokat, problémákat és kihívásokat az 1. ábra mutatja be.



1. ábra: *Motivációs példa – SE-technikák felhasználása egy kezdeményezés felszámolására irányuló PSYOPS-tevékenységek során*

Forrás: a szerző szerkesztése

Tegyük fel, hogy valamilyen kibertérben szerveződő kezdeményezés van kialakulóban, amely a hírszerzés jelentései szerint komoly aggályokat vet fel, és akár nemzetbiztonsági kockázatot is jelenthet az országra nézve. A nemzetbiztonság célja még a szerveződés korai fázisában felszámolni a kezdeményezést.

Elsődleges cél e kezdeményezések lélektani műveletekkel való megszüntetése. Ezen belül a pártolók lélektani eszközökkel történő bomlasztása, a tagok egymás ellen fordítása és a kezdeményezés felszámolása.

Problémát jelent, hogy a kezdeményezésben részt vevők száma rendkívül magas lehet, illetve a részvétel mögött álló szándék és az elszántság mértéke eltérő lehet. Kihívás ezen személyek, körök azonosítása és osztályozása. Ezt követően minél részletesebb információk megszerzése, egyfajta profil készítése a résztvevőkről. Továbbá nemcsak azokat érdemes megismerni, akik a kezdeményezés mellett állnak, hanem azokat is, akik bármilyen mértékben ellene vannak, hiszen ők hatékonyan felhasználhatók a kezdeményezés megszüntetése érdekében. Erre azonban nem nyújt megfelelő eszközkészletet a klasszikus hírszerzés.

Cél, hogy a klasszikus hírszerzési technikákat social engineering technikákkal kiegészítve alkalmazzuk, hogy a lélektani műveleteket haladéktalanul végrehajthassuk.

Elméleti felvezetés

Ahhoz, hogy értelmezni tudjuk a social engineering technikákkal megvalósítható kibertérben zajló lélektani műveletek végrehajtásához szükséges információszerzés lehetőségeit, illetve ennek fontosságát, mindenképpen ismernünk kell a releváns fogalmakat, jelenségeket. A különféle fogalmaknak számtalan meghatározása létezik, jelen fejezetben a tanulmány szempontjából általam legkifejezőbbnek ítélt és jelen cikkben alkalmazott definíciókat mutatom be.

Az első ilyen fogalom a *kibertér*, hisz ez jelenti azt a közeget, ahol jelen esetben a lélektani műveletek megvalósulhatnak. A kibertér meghatározására számtalan definíció létezik, a következőkben ismertetek belőlük néhányat.

A kibertérrel kapcsolatban általában az a vélemény, hogy az egész világra kiterjedő, globalizáló közeg, bárhonnan el lehet érni, ha rendelkezésre áll a technikai apparátus és annak működtetéséhez szükséges pénz. A kibertér használatával együtt járó társadalmi, politikai és gazdasági előnyök a hagyományos térbeli és társadalmi megoszlások mentén helyezkednek el, hiszen az internetes hozzáférés nagy területi és társadalmi egyenlőtlenségeket eredményez.[6]

Egy másik megfogalmazás szerint az elektronikus információs rendszerek és infrastruktúrák, valamint az e rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét nevezzük kibertérnek.[7]

A napjainkban elterjedt általános nézet alapján a kibertér egy olyan sajátos közeg, környezet, amely a számítógép-hálózatokkal, az internettel, az ezeken keresztül továbbított információkkal, valamint a felhasználókkal van összefüggésben. Azt azonban

[6] Mészáros Rezső: A kibertér társadalomföldrajzi megközelítése, *Magyar Tudomány,* 48 (2001/7), 769–779.
[7] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 1. § (1) bek.

fontos kiemelni, hogy a vezeték nélküli kommunikációs technológiák rohamos fejlődésének köszönhetően ez a fogalom kibővült, megjelenik benne az elektromágneses tartomány, hiszen a felhasználók nagy része a hálózathoz és így az internethez való csatlakozásra jelentős mértékben a vezeték nélküli rádiófrekvenciás kapcsolatot használja.[8]

A lélektani műveletek lehetséges információszerző eszközeinek mélyebb vizsgálatához mindenképp szükséges megemlíteni a kibertér katonai értelmezését is, hiszen egyrészt ezek sokkal tágabb meghatározást foglalnak magukban, másrészt pedig ez az a közeg, amelyben a lélektani műveleteket végrehajtják.

A NATO értelmezése szerint a kibertér egy komplex dinamikus környezet, a működési környezet (operating environment) egyik összetevője, amely az elektromágneses spektrummal függ össze és kulcsfontosságú minden szárazföldi, tengeri, légi és kozmikus katonai művelet szempontjából. A kibertér sokkal többet jelent az internetnél.

A kibertér három (fizikai, logikai, kiberszemélyiség) rétegre tagolható. A fizikai réteget a különféle fizikailag megfogható eszközök, infrastruktúrák, rendszerek és rendszerelemek alkotják, míg a logikai réteg a hálózat virtuális tere, amely alapvetően a kibertér nem megfogható elemeit tartalmazza (például szoftveralkalmazások). A kiberszemélyiség réteg a social engineering és a PSYOPS szempontjából különösen hangsúlyozandó, hiszen e tevékenységek végrehajtása során a középpontban az e réteget alkotó tényezők állnak, voltaképpen megszemélyesíti magát a kiberteret, a hálózat felhasználóinak digitális reprezentációjaként is értelmezhető. Ebben a rétegben jelenik meg a kibertér egyes szereplőinek ama személyazonossága, amelyet például manipulálásra, információszerzésre is felhasználnak. Mindezt úgy, hogy eközben a valós személyazonosságuk, hovatartozásuk rejtve marad. A kiberszemélyiség-rétegbe sorolhatók a hálózaton lévő személyek, a felhasználók hálózathoz kapcsolódó saját, személyi infokommunikációs eszközei, és a hálózaton lévő személyek kapcsolati hálója, interakciói.[9]

Az *információ* szerepének felértékelődése megkérdőjelezhetetlen, a mindennapi életben és a hadviselésben egyaránt kiemelt jelentőséggel bír. Az információ értelmezésére számtalan meghatározás létezik, nincs egységes meghatározása. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény szerint az információ bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott tapasztalat, megfigyelés, vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét átalakítja, megváltoztatja, illetve befolyásolja, továbbá bizonytalanságát csökkenti vagy megszünteti.[10]

A megfelelő mennyiségű és minőségű releváns információ megszerzésével számtalan előnyhöz juthat annak birtoklója, hisz nemcsak a döntéshozatal során felmerülő bizonytalanságok csökkentését eredményezi, hanem jelentősen hozzájárul a különféle problémák megoldásához is. Ezek alapján megállapítható, hogy a megfelelő információk megszerzése egyfajta előnyt biztosít a katonai műveletek során is. Ezt *információs fölénynek* hívjuk, amelynek kialakítása lehetővé teszi birtoklója számára, hogy

[8] Haig Zsolt: Információs műveletek a kibertérben, Dialóg Campus Kiadó, Budapest, 2018, 219–228.
[9] Haig (2018): i. m. 229–232.
[10] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. 1. § (1) bek.

a különféle infokommunikációs rendszereit és azok képességeit kihasználva a társadalmi élet különböző területein előnyre tegyen szert, illetve az éppen kialakult helyzetet úgy alakítsa és irányítsa, hogy mindemellett a másik fele megfossza ezen képességeitől.[11]

A kibertér és az információ definícióinak tisztázását követően az információs műveletekkel kapcsolatos alapvető fogalmak kerülnek ismertetésre.

Az *információs műveletek* azon koordinált, összehangolt tevékenységeket jelentik, amelyek a szembenálló fél információinak, információs folyamatainak és információs rendszerei működésének korlátozására, befolyásolására irányulnak, politikai és katonai célok elérése érdekében. Mindezt úgy, hogy eközben a saját hasonló folyamatokat, rendszereket hatékonyan kihasználják és megóvják.[12]

A következő fontos fogalom a *lélektani műveletek*. Ezen fogalom meghatározására számos definíció ismert, a NATO-doktrínában található meghatározása szerint „*olyan tervezett tevékenységek, amelyek a célközönség felé irányított kommunikációs módszereket és egyéb eszközöket alkalmaznak annak érdekében, hogy befolyásolják a politikai és katonai célok elérésére hatással lévő észlelési, megértési folyamatot, az attitűdöt és magatartást.*"[13] Ezek alapján a lélektani műveletek elsődleges célja, hogy hatást gyakoroljon és befolyásolja a tevékenység célcsoportjának szándékát, jövőbeli terveit, továbbá viselkedését, magatartását politikai, illetve katonai célok megvalósítása érdekében. Ezek elérésére számtalan kommunikációs és egyéb eszköz alkalmazható, amely kiválasztása nagy mértékben függ attól, hogy milyen típusú célcsoporttal szemben kívánják alkalmazni, illetve, hogy milyen cél elérése érdekében.

Egy másik meghatározás szerint a lélektani műveletek fogalma olyan előre megtervezett tevékenységeket jelöl, amelyek béke, válság és háború időszakában egyaránt az ellenséges, a semleges, a baráti és a saját közegekre irányulnak. Eme tevékenységek politikai és katonai célok elérése érdekében hatást gyakoroljanak az érintett célcsoportok pszichikumára, cselekvésére, magatartására és viselkedésére.[14]

Jelen tanulmány célja annak vizsgálata, hogyan használhatók a social engineering információszerző technikák a lélektani műveletek során, éppen ezért mindenképp szükséges kitérni a social engineering fogalmára is.

Az emberi tényező és az infokommunikációs eszközök gyengeségeit, illetve sérülékenységeit együttesen kihasználó támadási módszer a *social engineering.* Ez a technika az ember megtévesztésével, kihasználásával és manipulálásával teszi lehetővé belső és bizalmas információk megszerzését.

Kevin D. Mitnick, az egyik leghíresebb hacker, a social engineering nagymestere *A legendás hacker* című könyvében így határozza meg a social engineering fogalmát:

„A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek

[11] Haig Zsolt – Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák, 2012, 108. http://hdl.handle.net/11410/285 (Letöltve: 2019. 01. 19.)

[12] Haig Zsolt: Az információs műveletek, a SIGINT és az elektronikai hadviselés kapcsolatrendszere, *Felderítő Szemle*, Különszám, 6 (2007) 32. http://knbsz.gov.hu/hu/letoltes/fsz/2007-konferencia.pdf (Letöltve: 2019. 01. 19.)

[13] Haig (2018): i. m. 262–263.

[14] Pix (2005): i. m. 10.

mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni."[15]

A következő fejezetben kifejtem, hogy miért és hogyan alkalmazhatók eredményesen a social engineering információszerző technikái a lélektani műveletek előkészítése és végrehajtása során.

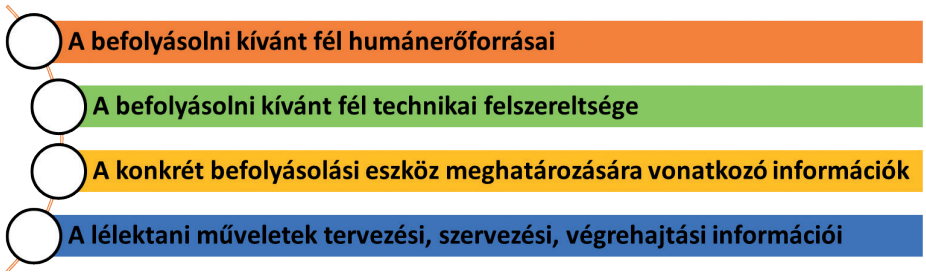
A lélektani műveletek végrehajtásához szükséges információszerzés alapjai

Felmerül a kérdés, hogy napjainkban, amikor már a technológia robbanásszerűen fejlődik, naponta jelennek meg új és új fejlesztések, eszközök, akkor mégis miért éppen egy állandóan változó, sokszor kiszámíthatatlan támadási módszert kívánunk alkalmazni a lélektani műveletek során? A social engineering fontossága abban rejlik, hogy az e támadási technikák által nyújtott előnyök tökéletesen felhasználhatók a lélektani műveletek során. A social engineering a manipuláció segítségével képes információt szerezni, amely a lélektani műveletek megtervezése és kivitelezése során egyaránt elengedhetetlen. A social engineering általi információszerzés célja a megfelelő célcsoport és befolyásoló-eszköz kiválasztása, illetve, hogy ez az eszköz képes-e megvalósítani a célszemélyek manipulálását. Tehát maga a social engineering arra a kérdésre is választ ad, hogy egyáltalán végrehajtható-e.

A lélektani műveletek végrehajtásához szükséges információk típusai

Ahhoz, hogy a civil környezetben megvalósuló lélektani műveletek eredményesen végrehajthatók legyenek, első lépésként meg kell szerezni azokat a releváns információkat, amelyek a kivitelezéshez feltétlenül szükségesek. A lélektani műveletek megtervezése időigényes feladat, sok feltételt és szempontot kell megvizsgálni. Annak érdekében, hogy a terv minden részletre kiterjedjen, és biztosítsa a befolyásoló tevékenység eredményes végrehajtását, minél teljesebb, pontosabb, hitelesebb, továbbá naprakész és releváns információk megszerzése a cél. Ahhoz, hogy ez megvalósulhasson, elengedhetetlen a megszerzendő információk konkrét meghatározása és csoportosítása, így a következőkben egy általam javasolt kategorizálást ismertetek a 2. ábra segítségével.

[15] Kevin D. Mitnick – William L. Simon: A legendás hacker, A megtévesztés művészete, Perfact-Pro, Budapest, 2003, borító.



2. ábra: *A lélektani műveletek végrehajtásához szükséges információk csoportosítása*

Forrás: A szerző saját szerkesztése

A befolyásolni kívánt fél alatt érthetjük a szemben álló ellenséges csapatokat, a semleges közeget, a baráti erőket és a saját csapatokat egyaránt.[16] A lélektani műveletek végrehajtása előtt elengedhetetlen a célcsoport pontos meghatározása, hiszen ennek segítségével lehet személyre szabott befolyásoló tevékenységet végrehajtani. Nem mindegy, hogy ellenséges erőket vagy saját csapatainkat kívánjuk saját céljaink szerint irányítani, továbbá a befolyásolás módja jelentősen függ attól, hogy az milyen célcsoportra irányul.

A *befolyásolni kívánt fél humánerőforrására vonatkozó információk* sokrétűek lehetnek. Ide tartozik többek között az emberek morális állapota, az általuk követendő erkölcsi, viselkedési normák, valamint a különféle rutinhelyzetekben általuk tanúsított magatartás is. Ezen kívül ide sorolható még, hogy az adott célcsoportnak milyen szándékai vannak cselekményei hátterében (például ellenállás, együttműködés), továbbá milyen jövőbeli terveik vannak.

A *technikai felszereltségre vonatkozó információk* magukba foglalják a befolyásolni kívánt fél számára fizikailag rendelkezésre álló infokommunikációs eszközöket, információs rendszereket és infrastruktúrákat, amelyek hasznos információt nyújthatnak számunkra arra vonatkozóan, hogy milyen eszközökön, felületeken keresztül lehet megvalósítani a legeredményesebben a befolyásolást. Ezen kívül fontos az adott rendszer felépítésére, működésére vonatkozó adatok, és a rendszerhez csatlakozó eszközök jellemzőinek megszerzése is. Abban az esetben, ha sikerül azonosítani az informatikai rendszer vagy az infokommunikációs eszközök sebezhetőségeit, akkor ezen információk segítségével meghatározható, hogy a rendszer mely pontján lehet megvalósítani például egy esetleges social engineering támadást további bizalmas és belső információk megszerzése, illetve a befolyásolás sikeres végrehajtása érdekében, vagy akár magát a befolyásolást is. Azt azonban mindenképp érdemes kiemelni, hogy a technikai felszereltségre vonatkozó információk rendkívül fontos szerepet töltenek be a sikeres befolyásolás megvalósításában, ennek ellenére a social engineering nem képes ezen

[16] Pix (2005): i. m. 10.

információk teljes körű megszerzésére, csupán egyes aspektusai tárhatók fel annak segítségével.

A *konkrét befolyásolási eszköz meghatározására vonatkozó információk* ölelik fel a konkrét befolyásolási tevékenység lehetséges eszközeit, vagyis azokat a módszereket, amelyek a célcsoport manipulálására alkalmasak. Ezen információk nemcsak a konkrét eszközök meghatározását foglalják magukba (például televízió, rádió, vagy közösségi oldalak), hanem a célcsoportra jellemző azon ismereteket, jellemvonásokat is, amelyek arra utalnak, hogy milyen módon, milyen technikával lehet befolyásolni őket. Például milyen infokommunikációs eszközöket alkalmaznak, milyen eszközhasználati szokásaik vannak, a befolyásolni kívánt fél csapataiban milyen generációs megoszlás figyelhető meg, milyen hajlandósággal rendelkeznek az ismeretek befogadására és számtalan további, a célcsoportra jellemző információ gyűjthető. Ezen információkból hasznos következtetések vonhatók le arra vonatkozóan, hogy mely eszköz a legalkalmasabb a hatékony befolyásolás elérése érdekében.

A *lélektani műveletek tervezési, szervezési, végrehajtási információi* alatt a konkrét lélektani művelet kivitelezéséhez szükséges technikai, személyi, tárgyi és pénzügyi feltételeire vonatkozó ismereteket értjük. Ezek egy része külön információszerző tevékenységet igényel, míg másik részét a már korábban megszerzett három célinformáció-csoport alapján határozzák meg. A befolyásolás végrehajtásához szükséges technikai feltételek tartalmazzák az infrastruktúra meglétét, többek között a különféle infokommunikációs eszközöket, hálózati eszközöket, vezeték nélküli hálózatokat és az energiát is. A személyi feltétel magába foglalja a befolyásolás megvalósításának egyik elengedhetetlen feltételét, vagyis azokat a személyeket, akik a befolyásoló tevékenységet végrehajtják. A tárgyi feltételek a lélektani műveletek kivitelezéséhez szükséges eszközöket, berendezéseket, szervereket és szoftvereket jelentik. A pénzügyi feltételek az előbb említettek beszerzéséhez, megszervezéséhez szükséges anyagi forrásokat jelölik.

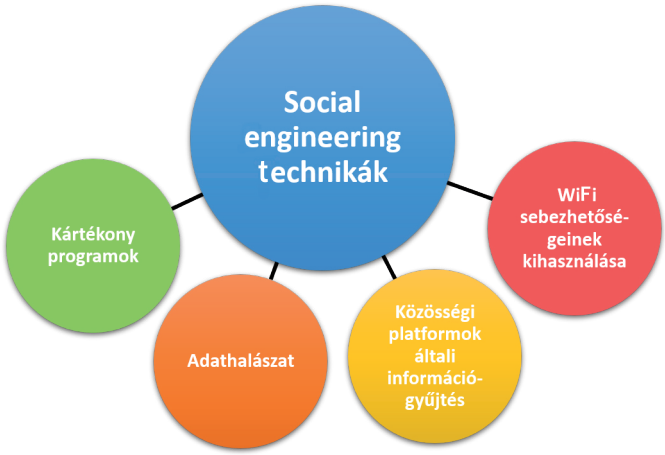
Ezen információk megszerzését követően lehet összeállítani a lélektani műveletek konkrét és végleges végrehajtási tervét, amely az előbbiek alapján tartalmazza a kivitelezők körét, az ehhez szükséges technikai, infrastrukturális, tárgyi, pénzügyi feltételeket, a támadás konkrét időpontját, helyét, cselekvési tervét és a támadás konkrét célját. A fentebb említett információk megszerzésére tökéletesen alkalmazhatók a social engineering egyes információszerző technikái.

Információszerzésre alkalmas social engineering technikák

A következőkben a kibertér nyújtotta lehetőségek segítségével működő social engineering általi információszerzést fejtem ki, a teljesség igénye nélkül.

Az alábbi, 3. ábra szemlélteti az információszerzésre alkalmas, kibertérben megvalósuló lehetséges social engineering technikákat, amelyek a következők lehetnek:

- adathalászat,
- kártékony programok,
- WiFi sebezehetőségei, és a
- közösségi platformok általi információgyűjtés.



3. ábra: *A kibertérben alkalmazható információszerző social enineering technikák*

Forrás: A szerző saját szerkesztése

Adathalászat

Az adathalászat, más néven phishing, lényege abban rejlik, hogy az adathalászok a felhasználókat, valamilyen elektronikus csatornán keresztül, – például e-mailben, azonnali üzenetben, vagy éppen szalagcím-hirdetésekben – egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kérik, hogy adja meg bizalmas adatait. Az adathalászatnak számos válfaja van, aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis web-oldalra.[17] Létezik hamis üzenetek és weboldalak általi, sms alapú, telefonos, valamint eltérítéses adathalászat, a cél minden esetben bizonyos információk megszerzése különféle platformok segítségével. Ezek rendkívül hasznosak lehetnek a lélektani műveletek szempontjából, hiszen számtalan hasznos információ megszerezhető e technikák segítségével.

Kártékony programok

A kártékony programnak vagy másnéven rosszindulatú szoftvernek (malware – Malicious Software) tekinthetők azok a szoftverek, amelyek célja bizonyos információk megszerzése, módosítása, törlése, megsemmisítése, valamint engedély nélküli tevékenységek

[17] Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, NKE, Budapest, 2014, 51.

végzése. Az esetek jelentős hányadában ezek a programok a felhasználó engedélye és tudta nélkül kerülnek az eszközeire. A malware-ek csoportjába sorolhatók a vírusok, férgek, trójai programok, kémprogramok, zsarolóprogramok, flooderek, dropperek, ál vírusírtók, rootkitek, keyloggerek, backdoor programok és számos további rosszindulatú program.[18]

A kibertérben folytatott lélektani műveletek során megvalósuló információszerzésre számtalan kártékony program alkalmazható. Ilyenek például a keylogger programok, amelyek billentyűzet naplózására alkalmas programok, amelyek segítségével számtalan hasznos információ megszerezhető, mint a különféle azonosítók, felhasználónevek, jelszavak, tulajdonképpen szinte bármi, amit leütnek az adott infokommunikációs eszköz billentyűzetén. De ide sorolhatók még többek között a vírusok, trójai programok, férgek, zsarolóvírusok, kémprogramok, amelyek károsíthatják, illetve törölhetik és módosíthatják a számítógépek vagy egyéb infokommunikációs eszközök, illetve a merevlemezek adatait. Ezenkívül nemcsak távoli elérést biztosíthatnak idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé tehetik, ezáltal számtalan bizalmas információ megszerzésére is alkalmasak.

E kártékony programok social engineering technikákkal könnyedén eljuttathatók a célszemélyhez vagy célcsoporthoz. Érkezhetnek levelek csatolmányaként, amikor a támadó valamilyen figyelemfelkeltő, érdekes tárgyat (szexuális tartalom, akciós ajánlatok, játék, sport) ír az üzenetbe, hogy a felhasználó biztosan megnyissa az üzenetet és a mellékletet egyaránt. Eljuthatnak a célszemélyhez különböző kétes eredetű letöltőoldalakon keresztül is. Ezek az oldalak általában ingyenesen kínálnak vonzó tartalmat (videókat, képeket, zenét, filmet) a felhasználó számára, amelynek letöltésével a kártékony program is feltelepül.[19] Ezen kívül könnyen terjeszthetők a rosszindulatú programok a baiting technika segítségével is. A baiting magyarul odacsalogatást jelent, különféle csalikkal, amikor is valamilyen adathordozót (pendrive, CD, DVD, okostelefon) „véletlenül" szétszórnak, elhagynak.[20] Amikor a gyanútlan felhasználó csatlakoztatja a számítógépéhez az eszközt, hogy kiderítse, kié lehet vagy mi található rajta, az adathordozó-eszközön található fájl megnyitásával már települ is a kártékony program, amelynek segítségével számtalan bizalmas információ megszerezhető. Ezen kívül a WiFi-hálózat gyengeségeit és az okostelefon-alkalmazások jogosultságkezelését kihasználva is megvalósulhat a kártékony program terjesztése.

A WiFi-hálózat sebezhetőségeinek kihasználása

A WiFi-hálózat gyengeségeinek kihasználása nemcsak a rosszindulatú szoftverek terjesztésére alkalmas, hanem további információk megszerzésére is. Ez megvalósítható többek között úgy, hogy azzal tévesztik meg a célszemélyt, hogy egy az eredetivel (a hálózat nevével is) szinte teljesen megegyező, nagy jelerősségű csatlakozási pontot

[18] Haig Zsolt: Számítógép-hálózati hadviselés rendszere az információs műveletekben, *Bolyai Szemle*, 15 (2006/1) 54–73. http://hdl.handle.net/11410/1931 (Letöltve: 2018. 10. 19.)

[19] Oroszi Eszter: Social Engineering, 2008, 50. http://docplayer.hu/3827943-Social-engineering-az-emberi-eroforras-mint-az-informaciobiztonsag-kritikus-tenyezoje.html (Letöltve: 2019. 09. 23.)

[20] Muha–Krasznay (2014): i. m. 52.

hoznak létre, ezáltal a felhasználó nem biztos, hogy meg tudja különböztetni a két hálózat közötti különbséget, így automatikusan a nagyobb jelerősségű hotspothoz fog kapcsolódni a kényelmesebb internetelérés érdekében.[21] Amint a gyanútlan felhasználó rácsatlakozik erre a csatlakozási pontra, már könnyedén megfigyelhetők és naplózhatók az általa küldött és fogadott adatok. Ez nemcsak azért rendkívül veszélyes, mert ennek segítségével számtalan bizalmas információ megszerezhető, hanem azért is, mert tökéletes alapként szolgálhat a profilozáshoz is. A hatékony lélektani műveletek megvalósítását elősegíti a befolyásolni kívánt félről alkotott profil, hiszen ennek segítségével következtetéseket és előrejelzéseket is le lehet vonni nemcsak a személyükről, tulajdonságaikról, hanem a lehetséges jövőbeli cselekvéseikről is.

A WiFi-hálózatok veszélyei közé sorolható a közbeékelődéses támadás is vagy más néven man in the middle támadás. A módszer lényege, hogy a támadó annak érdekében, hogy elfoghassa, lehallgathassa, esetleg módosíthassa a célszemélyek közötti kommunikációt, megszakítja vagy átirányítja, majd beékeli magát a kommunikációs csatornába, és mindkét fél irányába azt mutatja, hogy ő a másik fél, vele kommunikálnak.[22] Ennek segítségével nemcsak bizalmas információk megszerzésére van lehetőség, hanem akár a befolyásolás megvalósítására is, hiszen a másik fél nem sejti, hogy valójában valaki mással kommunikál, így könnyedén átadhatók hamis információk a szemben álló fél számára.

Ezen kívül érdemes még megemlíteni azt az esetet is, amikor a célszemély nem tiltja le a fájlmegosztást. Ez nemcsak a korábban említett rosszindulatú programok terjesztésére alkalmas, hanem a fájlok ellopására is, hiszen mások számára is elérhetővé válnak a hálózaton. Ezáltal a támadó nemcsak lemásolhatja az eszközön lévő fájlokat, de fel is tölthet fertőzött fájlokat vagy kártékony programokat az eszközre, illetve hozzáfér minden információhoz, amit a felhasználó elküld az interneten, így nevezetesen az e-mailekhez, bankkártyaadatokhoz, azonosítókhoz, felhasználónevekhez vagy jelszavakhoz.[23]

A fentebb említetteken kívül számtalan további olyan nem legális WiFi-n keresztüli információszerző, megfigyelő módszer létezik, amelyek segítséget nyújthatnak a szemben álló félnek és szándékainak előrejelzését szolgáló információk megszerzésében.

Közösségi platformok általi információgyűjtés

A népszerűbb közösségi oldalak kitűnő kiindulópontot jelenthetnek, hiszen a befolyásolni kívánt célcsoport tagjairól számos személyes információ begyűjthető.[24] A közösségi hálózatok általi információszerzés különösképp kedvező a befolyásoló fél számára, hisz ezek segítségével kis költséggel nagy mennyiségű információ szerezhető meg. Éppen ezért és az egyre növekvő alkalmazási kör miatt tökéletes kiindulási alapként szolgálnak

[21] Steve Watts: Secure authentication is the only solution for vulnerable public wifi, *Computer Fraud & Security*, (2016/1) 18–20. (Letöltve: 2019. 01. 22.)

[22] Stacy Prowell – Rob Kraus – Mike Borkin: Man-in-the-Middle. Seven Deadliest Network Attacks, 2010, 101–120.

[23] Kovács Marcell: A nyílt Wi-Fi hálózatok veszélyei, 2016, https://blog.crosssec.com/a-nyilvanos-wi-fi-halozatok-veszelyei (Letöltve: 2019. 01. 24.)

[24] Leitold Ferenc: Sebezhetőségvizsgálatok a gyakorlatban, NKE, Budapest, 2014, 12.

a lélektani műveletek előkészítéséhez vagy akár megvalósításához is. A támadó nemcsak a célszemély személyes adatait és elérhetőségeit (e-mail cím, esetleg telefonszám, lakhely), hanem számos egyéb információt is megszerezhet. Gondoljunk csak arra, hogy első kézből láthatja az ismerőinek, családtagjainak, barátainak nevét, akik nevében egy kártékony programmal megfertőzött üzenetet is küldhet. Sokan megjelenítik a születési dátumukat, és gyakran posztolnak a családtagjaikról, kedvenc háziállatukról, amelyek akár az áldozat jelszavára is utalhatnak. A jelszó megszerzésével pedig nemcsak a célszemély profilja, hanem a közvetlen üzenetváltások, a különféle fórumokon, esetleg bizalmas csoportokban közétett bejegyzései is hozzáférhetővé válnak, amely rendkívül hasznos lehet a konkrét befolyás megvalósítására és a célszemélyek szándékainak meghatározására nézve. Fontos megemlíteni azt is, hogy a közösségi portálok nemcsak az információgyűjtésre alkalmasak, hanem kártékony program csatolására, például egy üzenetben elküldött link vagy fájl formájában, amire, ha rákattint a felhasználó, már aktiválódik is a kártékony program. Ezen kívül számos további social engineering információszerző technika létezik, amelyek felhasználásával jelentősen növelhető a lélektani műveletek során végrehajtott befolyásolás hatékonysága, de terjedelmi okok miatt jelen tanulmánynak nem célja ezek bemutatása.

Fontos, hogy e technikák a civil környezetben használhatók, a katonai műveletekben nem alkalmazhatók, mert a katonai vezetési, irányítási rendszerek nem erre épülnek.

Social engineering technikák alkalmazása motivációs példán

A korábbiakban ismertettem egy motivációs példát, a téma mélyebb vizsgálatához szükséges alapvető fogalmakat és a lélektani műveletek végrehajtásához szükséges információk körét, valamint az ezek megszerzésére alkalmas social engineering technikákat. Jelen pontban bemutatom, hogy a motivációs példában felvázolt esetben a fentebb ismertetett social engineering technikák hogyan alkalmazhatók.

A motivációs példa szerint egy a kibertérben szerveződő kezdeményezés van kialakulóban, amelynek felszámolásához lélektani műveletek megvalósítására van szükség. Ahhoz, hogy tudjuk milyen célcsoportra irányuljon a PSYOPS-művelet, mindenképp szükséges a kezdeményezés résztvevőinek meghatározása, osztályozása és profil készítése, annak érdekében, hogy minél személyre szabottabban valósulhasson meg a befolyásolás. A klasszikus hírszerzés mellett a social engineering technikák hatékonyan alkalmazhatók a releváns információk megszerzésére.

Az *első lépés* a kezdeményezés lehetséges résztvevőinek azonosítása. Ennek megvalósítására alkalmazható social engineering módszer a közösségi portálok általi információgyűjtés, aminek több típusa létezik. A különféle közösségi oldalak segítségével információ szerezhető egy adott téma iránt érdeklődő személyek köréről, többek között az ilyen témával kapcsolatos személyes adatlapok, oldalak, csoportok és fórumok vizsgálatával. Ezáltal nemcsak a személyek azonosítására, hanem osztályozására is lehetőség nyílik. Priorizálható, hogy az adott személy mennyire komolyan érdeklődik, mennyire elhivatott a téma iránt vagy esetleg mennyire ellenzi e normákat és ideológiát, esetleg semleges-e. Ennek segítségével osztályozhatók az emberek aszerint, hogy befolyásolhatók-e vagy sem. Ez azért fontos, mert ez alapján választható ki a pontos célcsoport és a befolyásolásra

alkalmas módszer. A közösségi oldalak segítségével információ szerezhető meg az esetleges résztvevők jelleméről, személyes tulajdonságairól, ami elengedhetetlen a hatékony befolyásoláshoz. Mindezek meghatározásához segítséget nyújthat a célszemély adatlapja, hozzászólásai, csoporttagságai, bejegyzései, továbbá, hogy milyen oldalak kedvelője. Ezek segítségével profil készíthető a célcsoport tagjairól, amely egyfajta előrejelzésként szolgálhat az emberek viselkedését és magatartását illetően, továbbá következtetések vonhatók le szándékaik, jövőbeli tevékenységeik vonatkozásában.

A *második lépés* az így meghatározott célcsoport határozottan érdeklődő személyeinek további profilozása, például álprofil létrehozásával, illetve a hamis weboldalak és üzenetek útján megvalósuló adathalászat segítségével. Ezen adathalászat végrehajtásával megállapítható, hogy az adott személy mennyire megtéveszthető vagy befolyásolható, ami azért rendkívül fontos, mert az ilyen típusú személyek könnyebben manipulálhatók. A cél olyan emberek kiszűrése, akik mohók, pénzéhesek, bedőlnek a megtévesztő ajánlatoknak. Ennek érdekében nyereményjáték meghirdetésére kerül sor, amelyet célzott hirdetésekkel reklámoznak a különféle weboldalakon, közösségi platformokon. Ez az adathalászat (phishing) konkrét megvalósítása.

Ezen kívül ebben a lépésben kerülhet sor a kezdeményezés irányvonalát támogató álprofil létrehozására, hiszen a privát üzenetváltások segítségével további információk gyűjthetők. Ez alapján kiszűrhető, hogy az adott személy mennyire elkötelezett és milyen az irányvonalhoz kapcsolódó szándékai vannak. E lépés eredményeként a célcsoport olyan szintű leszűkítése valósítható meg, amely segítségével a belső körhöz tartozó tagok kiléte körvonalazódik.

A *harmadik lépésben* valósul meg a belső kör konkrét szándékaival, terveivel kapcsolatos információk megszerzése, amelyre hatékonyan alkalmazhatók a kártékony programok terjesztésén alapuló és a WiFi gyengeségeit kihasználó social engineering technikák. Mindkét módszer segítségével felfedhetők olyan információk, amelyek a közösségi oldalakon rejtve maradnak. Kártékony programok terjesztésével és aktiválásával információ szerezhető a célcsoport elszántságának mértékéről, a belső körhöz tartozó további tagokról, egy esetleges csoportosulás, támadás tényéről, illetve részleteiről. Ezenkívül a technikai felszereltségre vonatkozóan is gyűjthetők adatok, azonban fontos kiemelni, hogy ez nem terjed ki minden részletre, csupán alapinformációk (például milyen eszközt használnak) szerezhetők meg. A WiFi gyengeségeit kihasználó módszer esetében két technikát érdemes megemlíteni. A man in the middle támadás segítségével lehallgatható a két fél közötti kommunikáció, továbbá hamis, téves üzenetek is továbbíthatók, hiszen e támadás előnye, hogy a másik fél még csak nem is sejti, hogy valójában valaki mással kommunikál, így hitelesnek véli a kapott üzenetet. A másik technika a fájlmegosztás letiltásának hiánya, ami hozzájárulhat a fájlok eltulajdonításához vagy akár egy kártékony program terjesztéséhez.

Ezen információk megszerzését követően kerülhet csak sor a lélektani műveletek végrehajtására irányuló tervek pontosítására, véglegesítésére, a konkrét befolyásoló eszköz kiválasztására és a megvalósítás megszervezésére, hogy a feltételezett kezdeményezést felszámoljuk.

Összefoglalás

A lélektani műveletek rendkívül fontos szerepet játszanak a hadviselésben és a civil környezetben egyaránt, hiszen segítségükkel a háborús, katonai konfliktusok, fegyveres összecsapások elháríthatók és megelőzhetők, illetve a civil és politikai célok megvalósulása elérhető. Éppen ezért a legfőbb cél e műveletek eredményességének biztosítása, aminek megvalósításához elengedhetetlen a végrehajtáshoz szükséges információk megszerzése. Ennek elérésére tökéletesen alkalmazható számos social engineering módszer.

Jelen tanulmány összegezte a kibertérben megvalósuló lélektani műveletek tervezéséhez és végrehajtásához szükséges információk megszerzésére alkalmas lehetséges social engineering technikákat. Ennek célja az volt, hogy feltárja a lélektani műveletek során megvalósítandó befolyásolás eredményes kivitelezéséhez szükséges információk megszerzésének egyes lehetőségeit, és meghatározza ezen információk kategóriáit. Ennek érdekében egy motivációs példa segítségével szemléltettem a téma aktualitását, fontosságát és szükségességét, majd bemutattam azokat a háttérismereteket, amelyek elősegítik a kibertérben zajló lélektani műveletek tervezéséhez és végrehajtásához szükséges információszerzés lehetőségeinek értelmezését. Ezt követően azonosítottam és osztályoztam a lélektani műveletek eredményes végrehajtásához szükséges információkat, illetve meghatároztam az ezen információk megszerzésére alkalmas social engineering módszereket. A továbbiakban a korábban felvázolt motivációs példában meghatározott célok és kihívások mentén mutattam be a példa egy lehetséges megoldását. Ennek keretében a példa segítségével szemléltettem milyen információk megszerzése szükséges a lélektani műveletek tervezése és végrehajtása során, továbbá, hogy ezek milyen konkrét social engineering technikákkal szerezhetők meg.

Összegezve a lélektani műveletek fontossága vitathatatlan, megvalósítása és kimenetele nagymértékben befolyásolja a katonai műveletek további lefolyását. Segítségével elkerülhető a fegyveres konfliktus kialakulása, illetve folytatása, így kulcsfontosságú a végrehajtás eredményessége. A sikeres befolyásolás kivitelezéséhez pedig nélkülözhetetlen a tervezés és a megvalósítás során egyaránt a releváns információk megszerzése. Megállapítható, hogy a kibertéri technikák számtalan új lehetőséget nyújtanak az információszerző képesség bővítésére, hiszen az egyre újabb és újabb technikák, technológiák lehetővé teszik, hogy minél több, pontosabb, teljesebb, illetve hitelesebb információt szerezhessünk meg. E technikák segítségével rövid idő alatt nagy mennyiségű információ gyűjthető kevés erőforrás felhasználásával, költséghatékonyan. Mindemellett kijelenthető, hogy a social engineering széles eszköztárának köszönhetően hatékonyan alkalmazható a lélektani műveletek során.

Felhasznált irodalom

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

Haig Zsolt: Számítógép-hálózati hadviselés rendszere az információs műveletekben, *Bolyai Szemle*, 15 (2006/1), 54–73. http://hdl.handle.net/11410/1931 (Letöltve: 2018. 10. 19.)

Haig Zsolt: Az információs műveletek, a SIGINT és az elektronikai hadviselés kapcsolatrendszere. *Felderítő Szemle*, Különszám (2007) 27–48. http://knbsz.gov.hu/hu/letoltes/fsz/2007-konferencia.pdf (Letöltve: 2019. 01. 19.)
Haig Zsolt: Információs műveletek a kibertérben, Dialóg Campus Kiadó, Budapest, 2018.
Haig Zsolt – Kovács László: Fenyegetések a cybertérből, *Nemzet és Biztonság*, (2008/5) 61–69. www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf (Letöltve: 2019. 01. 24.)
Haig Zsolt – Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák, NKE, Budapest, 2012, http://hdl.handle.net/11410/285 (Letöltve: 2019. 01. 19.)
Kovács Marcell: A nyílt Wi-Fi hálózatok veszélyei, 2016, https://blog.crosssec.com/a-nyilvanos-wi-fi-halozatok-veszelyei (Letöltve: 2019. 01. 24.)
Leitold Ferenc: Sebezhetőségvizsgálatok a gyakorlatban, NKE, Budapest, 2014.
Pix Gábor: A lélektani műveletek jellemzőinek vizsgálata. Budapest, 2005, https://nke-repo.uni-nke.hu/xmlui/bitstream/handle/123456789/12018/tezis_hun.pdf;jsessionid=D287A4C46B2860409B02EAAF99E6C5A5?sequence=2 (Letöltve: 2019. 08. 26.)
Mészáros Rezső: A kibertér társadalomföldrajzi megközelítése, *Magyar Tudomány*, 48 (2001/7) 769–779.
NATO Standard AJP-3.2 Allied Joint Doctrine for Land Operations, NATO Standardization Office, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/624149/doctrine_nato_land_ops_ajp_3_2.pdf (Letöltve: 2019. 01. 14.)
Mitnick, Kevin D. – Simon, William L.: A legendás hacker, A megtévesztés művészete, Perfact-Pro, Budapest, 2003.
Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, NKE, Budapest, 2014.
Oroszi Eszter: Social Engineering, Budapesti Corvinus Egyetem, Budapest, 2008. http://docplayer.hu/3827943-Social-engineering-az-emberi-eroforras-mint-az-informaciobiztonsag-kritikus-tenyezoje.html (Letöltve. 2019. 09. 23.)
Prowell, Stacy – Kraus, Rob – Borkin, Mike: Man-in-the-Middle, Seven Deadliest Network Attacks, 2010, 101–120. DOI: https://doi.org/10.1016/C2009-0-61914-0 (Letöltve: 2019. 01. 24.)
Warsaw Summit Communiqué, 2016, www.nato.int/cps/en/natohq/official_texts_133169.htm (Letöltve: 2019. 08. 26.)
Watts, Steve: Secure authentication is the only solution for vulnerable public wifi, *Computer Fraud & Security*, (2016/1) 18–20. DOI: https://doi.org/10.1016/s1361-3723(16)30009-4