Kerti András

ÁTVITELI ÚT BIZTONSÁG

Absztrakt

Az információbiztonság egyik részterülete az átvitelbiztonság, melynek feladata az információink, adataink védendő tulajdonságainak megőrzése, az infokommunikációs csatornákon. Az átvitelbiztonság az információbiztonság egyik legrégebbi szakterülete, de napjainkban bekövetkezett változások miatt egyre kevesebb szó esik róla.

The one of the partial area of the information security is transmission security. The task of this is the protection of the main character of information and data in the infocommunications channels. The transmission security is one of the oldest special areas of the information security but because of the current changes it is lost importance itself.

Kulcsszavak: *információbiztonság, információvédelem, átviteli út biztonság, híradó biztonság, transmission security,*

Az információbiztonsággal foglakozó szakirodalmak valamilyen formában egyetértenek abban, hogy az információ biztonság, azon belül is az elektronikus információbiztonság egyik alappillére az átvitel biztonság. Ennek ellenére az átvitel biztonság a többi információbiztonsági területhez képest teljesen hátérbe szorult az utóbbi időkben megjelent szakirodalomban, aminek több oka is van:

Az első ok, hogy az utóbbi időkben végbe ment az informatikai és távközlési rendszerek konvergenciája eredményeképpen a civil vállalatvezetésben az adatfeldolgozást, továbbítást gyakorlatilag csak az informatikai hálózatokon biztosítják. Ezzel összefüggésben az információbiztonság szinte teljes egészében csak az informatikai biztonság szakterülete. Dr. Haig Zsolt így ír erről[1]:

„… a szakmai közvélemény az információbiztonságot kizárólag csak az informatikai rendszerekre, számítógép-hálózatokra értelmezi, ami e problémakör jelentős leszűkítését jelenti.”

A második ok, amiért az átviteli út biztonság a polgári életben nem kap nagy figyelmet, hogy a vállalkozások az átviteli utakat gyakorlatilag bérlik, az átviteli problémákkal így a szolgáltatónak kell foglalkoznia. És ez sok esetben a honvédségi felhasználókra is igaz.

A harmadik ok a véleményem szerint, hogy az átvitel biztonság nem egy jól körülhatárolható terület, feladatait sokan a hálózatbiztonsághoz sorolják, illetve az átvitel biztonságot megoldottnak látják az adatok rejtjelzéssel történő védelmével. Például az ITB 8-s ajánlásában ezt olvashatjuk:”A fizikai rétegben az alapvető biztonsági mechanizmus a teljes adatfolyam rejtjelezése. A rejtjelezésnek egy speciális formája csak a fizikai rétegben alkalmazható: az átvitel-biztonság, ami széles spektrumú védelmet biztosít.”

Átvitel biztonság

Mi tehát az átvitel biztonság? Mindazon védelmi rendszabályok összességének az eredménye, amelyek végrehajtásával biztosítjuk a híradó adatátviteli utakon, csatornákon az

[1] Dr. Haig Zsolt: Az információbiztonság komplex értelmezése

információk sértetlenségének, rendelkezésre állásának, bizalmasságának meglétét,[2] valamint adott esetekben a hitelességét illetve letagadhatatlanságát.

A sértetlenség, rendelkezésre állás, és a bizalmasság megóvása nem kíván különösebb magyarázatot, a másik három funkciót viszont érdemes kicsit jobban szemügyre vennünk.

Az információ átvitelt biztosító utak és csatornák azokon a területeken mennek, mehetnek keresztül, amelyek nem teljesen egészen, illetve egyáltalán nincsenek az ellenőrzésünk alatt. Ez alapján viszont az ellenérdekelt félnek lehetősége van az ellenállomás megszemélyesítésére, ezért mindenképpen szükséges az információk, valamint az információ szolgáltatók hitelesítésére, ami annak a bizonyítása, hogy az ellenállomás az aminek, akinek állítja magát.

Nagyon fontos az is hogy tudjuk azt az általunk elküldött információról, hogy azt a címzett megkapta, a kézbesítettség tényét később ne tudja letagadni.

Az átvitel biztonság feladatai, lehetőségei

Ahhoz, hogy meg tudjuk állapítani az átvitelbiztonság feladatait, vázlatosan át kell tekinteni az MH infokommunikációs rendszerét. Ehhez a legjobb, mint egy állatorvosi ló, ha egy elképzelt missziós feladatot végrehajtó szervezet infokommunikációs kapcsolatait vizsgáljuk meg.

Ebben az esetben a következő összeköttetéseket kell megszervezni:

- Az elöljáró parancsnoksággal
- A Magyarországon levő elöljáró parancsnoksággal,
- Az alárendelt szervezetekkel
- Az együttműködő illetve szomszédos alakulatokkal, szervezetekkel
- A helyi polgári szervekkel
- A különböző fegyverirányítási és felderítési rendszerekkel.

Továbbá természetesen ki kell alakítani a vezetési pontok belső kommunikációs rendszerét is.

Milyen eszközökkel valósítható meg mindez? Ez minden esetben külön elemzést igényel, függ magától a terület földrajzi elhelyezkedésétől, az ország politikai viszonyaitól, a technikai fejlettségétől, a meglévő kommunikációs infrastruktúrától, annak épségétől, a feladattól, amelyet a missziónak végre kell hajtani.

Átviteli utak felosztása

Az átviteli utakat sokféleképpen lehet csoportosítani, de a jelen cikk szempontjából kétfajta csoportosítás a legcélszerűbb:

Az átviteli út létrehozója alapján, lehetnek általunk létesítendő átviteli utak, illetve más szervezet, szolgáltató által biztosítottak. Ebben az utóbbi esetben a biztosító szervezet lehet az elöljáró vagy együttműködő szervezet, illetve az adott területen szolgáltatást nyújtó polgári cég. Ebben az esetben az átvitel biztonságért a szolgáltató felel, nekünk a feladatunk a hálózat biztonságra, illetve rejtjelzés biztonságra terjed ki az információk átvitele esetén.

Az átviteli út technikai megvalósítása szerint szintén két csoportot különböztethetünk meg: vezetékes illetve nem vezetékes (vezeték nélküli), sugárzó eszközökkel megvalósított összeköttetések. A vezetékes rendszerek lehetnek modern üvegszálas, valamint hagyományos fémes kábelek, amely kategóriába a tábori nehéz- és könnyűvezetékek, többeres kábelek sorolhatók. A sugárzó eszközök kategóriájába a különböző rövid-, és ultrarövid hullámú rádiók, mikrohullámú relék, troposzféra állomások, műholdas és cellás rendszerű telefonok.

[2] Ezeknek fogalmaknak a magyarázata szinte minden információvédelemmel foglalkozó cikkben, szakirodalomban megtalálható ezért itt nem részletezem.

Fenyegetettségek

A fent felsorolt különböző technikai megvalósítású átviteli utak, szinte mindegyike más és más fenyegetettségnek van kitéve információvédelmi szempontból.

Ezek a fenyegetettségek a vezetékes átviteli utak esetében a következők lehetnek: a kábel fizikai szakadása, szakítása, az információ lehallgatása. A lehallgatás szempontjából különbség van a két fajta vezeték típus között, mert a fémes vezetékek az információk átvitele során nem kívánt kisugárzást bocsáthatnak ki és ezt a sugárzást a vezetéktől távolabb is érzékelni lehet, vagyis a lehallgatáshoz nem feltétlenül szükséges a fizikai kapcsolat. Az optikai kábeles átviteli utak esetében sokan azt gondolják, hogy a lehallgatás nem lehetséges, de ez nem megoldhatatlan, viszont ebben az esetben közvetlen fizikai kapcsolat szükséges a lehallgató berendezés és a kábel között, vagyis a lehallgató berendezést közvetlenül a kábelre kell csatlakoztatni.

Vezeték nélküli eszközök használatakor a következő fenyegetettségekkel kell számolnunk: zavarás, lehallgatás, lefogás, megtévesztés (megszemélyesítés), fizikai pusztítás. A sugárzó eszközök felderítése sokkal egyszerűbb, sokkal nagyobb távolságról lehetséges, mint a vezetékes eszközök esetében, a hullám terjedési sajátosságokat figyelembe véve ez akár több tíz-száz kilométer is lehet (pl.: rövidhullámú rádiók esetében). Azt is könnyű belátni, hogy a felderített átviteli utak előbb-utóbb az ellenérdekelt fél támadásainak középpontjába kerülnek.

Fenyegetők

Ahhoz azonban, hogy meg tudjuk vizsgálni milyen ellenintézkedéseket tehetünk a fenyegetettségekkel szemben, meg kell vizsgálnunk kik azok illetve milyen körülmények azok, amelyek negatívan befolyásolják az információbiztonságot az átviteli út során. Az átvitelt biztosító csatornák kialakulásában, kialakításában, három egymáshoz kapcsolódó elem különböztethető meg: az adóberendezés, a terjedését biztosító közeg, és a vevőberendezés. Ezek közül negatívan lehet befolyásolni a vevőberendezés vételi körülményeit, amely befolyásolást végrehajthatja az ellenség is, de mi magunk is. A természeti jelenségek befolyásolják a terjedését biztosító közeg tulajdonságait. Az adóberendezések fizikai pusztításán kívül más ellenséges szándékú befolyásolása, véleményem szerint gyakorlatilag nem lehetséges, elképzelhető ugyan egy teljesen árnyékolt terület kialakítása az adó körül, de ez gyakorlatban a jelen ismereteink birtokában kivitelezhetetlen.

Természeti jelenségek

A vezeték nélküli összeköttetések minőségére a legnagyobb befolyással a természeti jelenségek vannak. A terjedési folyamat során az elektromágneses hullámok gyengülése, torzulása következik be, amelyre hatással vannak a légkör terjedési tulajdonságai, és a terep domborzata. Közismert tény, hogy a különböző frekvencia sávok terjedési tulajdonságai mások, és még a frekvencia sávban is különbözőek.[3] A terjedési tulajdonságra ezenkívül hatással vannak az időjárási körülmények a napszak, de még a naptevékenység is. Amennyiben rosszul választjuk meg a használni kívánt frekvenciát, úgy az összeköttetés minősége romlik, sőt az összeköttetés meg is szakadhat.

A vezetékes összeköttetések nem annyira érzékenyek a természeti jelenségekre, de előfordulhat, hogy a szélsőséges körülmények, mint például a vihar hatására, illetve az időjárás okozta földmozgások (fagyok, csuszamlások) következtében a vezetékek elszakadnak. Mind a két esetben az információink védendő tulajdonságai közül sérül, sérülhet a **sértetlenség** és a **rendelkezésre állás**.

[3] A rádióhullámok terjedési sajátosságaival könyvtári szakirodalom foglalkozik, ezért itt erre nem térek ki bővebben.

Ellenséges szándék

A modern infokommunikációs hálózatokban, a hagyományosnak mondható ellenséges szándékú tevékenységek, mint például a kémkedés, hírszerzés a harcmezőn, az ellenséges rádió elektronikai tevékenységek stb…, egyre inkább számolni kell az Internetet rossz szándékkal felhasználók széles táborával. Véleményem szerint azonban ez a nem csekély probléma a hálózat biztonsági szakemberek feladatai között jelenik meg. Addig, amíg hálózatokon végrehajtott támadásokhoz egyre kisebb és kisebb szakértelem szükséges, az átviteli utak támadása szakértelmet kíván, és bár ezen a területen is csökken a felhasználható eszközök ára, a mindennapi életben az információs támadásokat „hobbyként" űző cracker-ek, hacker-ek számára ez nem „kifizetődő". Ezek alapján az átvitel biztonság területén az ellenséges erők fenyegetéseinél az ellenérdekelt fél, az ellenség rádióelektronikai harc tevékenységével kell számolnunk, amelyek lehetnek: az elektronikai felderítés, a megszemélyesítés és az elektronikai támadás.

Az ellenség az elektronikai felderítés során lehallgathatja a különböző átviteli utakon -és ezekbe bele kell érteni természetesen a vezetékes átviteli utakat is - történő kommunikációt. A nem kellőképpen védett és a nyílt információk felhasználásával, a védett csatornákon történő forgalom analizálásával következtetéseket vonhat le a saját csapataink helyzetéről és a szándékainkról. Ugyan ezen adatok felhasználásával segítséget nyújthat a saját kriptográfia szakembereinek a rejtjelzett adataink feltöréséhez. A különböző rádió irányímérő állomások alkalmazásával meghatározhatja magának a sugárzó eszköznek a helyét, és ebből következtetésre juthat a vezetési pontok helyére is. Amikor a védendő információkról beszélünk, általában mindig a valamilyen formában rögzített (papíron, mágneses adathordozón, stb…) adatokra gondolunk, és nagyon sokszor elfeledkezünk arról, hogy a védendő információt egy objektum is hordozhatja.[4] Ez kifejezetten igaz egy harcfeladatot ellátó alakulat vezetési pontjára, amelynek a felderítése az ellenség számára elsődleges. Könnyen belátható az is, hogy a csapatok elhelyezkedéséből, mozgásából, az ellenség következtethet a szándékainkra, tevékenységeinkre. Ezeket az információkat is megszerezheti az elektronikai felderítés segítségével, és ezáltal az információink **bizalmassága** sérül.

A megszerzett információk birtokában az ellenség beléphet az átviteli csatornába, ott az egyik saját állomásunknak adhatja ki magát, ezzel az információnkat elfoghatja, illetve számunkra megtévesztő információkat szolgáltat. Ilyen tevékenység lehet, ha az ellenség egy rádióhálóba belép, ott az egyik tagállomásnak adja ki magát, valamint ha egy átjátszó állomást elfoglal és azt tovább üzemelteti a saját céljai szerint. Ezekben az esetekben sérül az információk **hitelesége, rendelkezésre állása, bizalmassága, sértetlensége**.

Szintén a felderítéssel megszerzett információk birtokában az ellenség támadhatja is az információs rendszerünket. A támadás lehet rádióelektronikai zavarás, rádióelektronikai lefogás, illetve fizikai pusztítás. A rádióelektronikai zavarás esetén az ellenség célja a rádióelektronikai eszközeink működésének megnehezítése, hatékonyságuk lényeges csökkentése. Ebben az esetben lehet, hogy az információink védendő tulajdonságai nem szenvednek csorbát, viszont a továbbításuk ideje megnőhet, ami károsan befolyásolhatja a parancsnok döntési képességeit. A rádióelektronikai lefogás esetében az ellenség megakadályozza, hogy az információtovábbító eszközeinket használjuk, így az információk **rendelkezésre állása** megszűnik. Az ellenség a minél nagyobb hatás elérése érdekében különböző fegyverekkel el is pusztíthatja a végberendezéseket, az átviteli utat biztosító kábeleket, az adatokat tároló, feldolgozó vezetési pontokat. Az első esetben megszűnik az adatok **rendelkezésre állása,** a második esetben maguk az adatok is elpusztulnak.

[4] A védendő információ megjelenési formáiról lásd a titokvédelmi törvényt

Saját magunk

Az átviteli út során az információink biztonságára saját magunk vagyunk a legnagyobb ráhatással. Az átviteli utak tervezésekor véges erőforrásokat használunk fel, ezek például a frekvencia, és a vezetékek hossza (nyomvonala) is. A sugárzó eszközök alkalmazásakor tovább bonyolítják a helyzetet a különféle elektromos, elektronikus eszközeink alkalmazásai is. Még a funkcióinak megfelelően működő rádióelektronikai eszközök vevőberendezéseiben – az egymásra való hatás következtében – is nem szándékos zavarok keletkezhetnek. Ez a hatás teljesen azonos az ellenség szándékos zavarásával.

A vezetékes eszközök tekintetében is hasonló a helyzet. Saját tapasztalataim alapján elmondhatom, hogy a gyakorlatok vezetékes híradásának legnagyobb ellenfelei saját lánctalpas technikai eszközeink voltak, amelyek az ETNV kábelek szakadásainak a 90%-ért voltak felelősek.[5]

Mit tehetünk?

Mi az, amit tehetünk annak érdekében, hogy az információink az átviteli úton is biztonságban legyenek?

A lehetőségeink nagyon sokfélék lehetnek, az aktív cselekvéseinktől (melyek magukba foglalhatják az átviteli utakat felderítő, zavaró, pusztító erők fizikai megsemmisítését) a passzív szervezési intézkedések, technikai megvalósítások és rendszabályok bevezetéséig. A továbbiakban most csak a passzív lehetőségeinkkel kívánok foglalkozni.

Lehetőségeinket a veszélyeztető tényezőknek megfelelően három kategóriába lehet sorolni, így

- az ellenség tevékenységének hatását minimalizáló rendszabályok;
- szervezési intézkedések a saját zavarok kizárására;
- az összeköttetések tervezésekor a technikai és természeti jelenségek maximális figyelembe vétele.

Bár elméletben a fenti lehetőségek jól elhatárolhatók egymástól, gyakorlatban azonban ezeket komplex módon kell figyelembe venni a tervezéskor.

Szervezési, tervezési feladatok

Az átviteli utak kialakításakor, a bármiféle felderítésnek, zavarásnak legjobban ellenálló híradás szervezési forma a vezetékes vonalak alkalmazása. A vezetékek közül is – a mai technológiai fejlettségünk szintjén- az üvegszálas kábelek felelnek meg legjobban a követelményeknek.[6]

Azonban könnyen belátható, hogy ez nem mindig lehetséges, például nincs elég időnk arra, hogy kábeles összeköttetést építsünk ki, vagy pedig a kábeles összeköttetést nem tudjuk megvalósítani, mert mozgó eszközökkel kell kapcsolatot létesítenünk. Tehát a feladatunk, hogy amíg csapataink tevékenysége megköveteli a mobil vezetési rendszert, a vezeték nélküli eszközöket alkalmazunk, és amint a lehetőségünk van rá, ezeket az összekötetéseket le kell cserélnünk kábeles, lehetőleg optikai kábeles összeköttetésekre. Azonban a vezetékes átviteli utakat is védeni kell, a nyomvonalak kivitelezésekor kerülni kell a nagy forgalmú utakat. Ahol mód és lehetőség, illetve idő van álcázni kell ezeket, az utak keresztezésekor magas, vagy mély építést kell alkalmazni.

[5] A 80-as évek vége 90-s évek eleje. Az ETNV kábelek akkor még korszerűnek számítottak. A 90 % becsült adat.

[6] Az üvegszálás technológiával, annak előnyeivel, megvalósításával is sok egyéb irodalom foglakozik ezért itt ezekre nem térek ki.

A vezeték nélküli rendszerek tervezésekor a legfontosabb feladat a frekvencia management (menedzsment), melynek során figyelembe kel venni az évszaknak, napszaknak, az állomások egymástól való távolságának megfelelő frekvencia kiválasztást oly módon, hogy a különböző állomások egymás munkáját, összeköttetését ne zavarják. Technikai lehetőségünk figyelembevételével törekednünk kell a kevésbé felderíthető, szórt spektrumú és hopping rádiók alkalmazására. Nem szabad elfelejteni ellenben, hogy ez a technológiai is felderíthető. Szintén a felderíthetőség csökkentése érdekében irányított antennák alkalmazása célszerű.

A vezeték nélküli eszközök, különösen a rövidhullámú és ultrarövid-hullámú eszközök esetében, pontos felderítési információk birtoklása során lehetősége van az ellenségnek a rádióforgalmi rendszerekbe való belépésre, valamely ellenállomás megszemélyesítésére, és ez által megtévesztő információk közlésére. Ennek veszélyeire már a tervezés szakaszában gondolni kell. Az ellenállomások hitelesítésére - és ez által az információk hitelesítésére- alapvetően kétfajta lehetőség biztosított: az aszimmetrikus és a szimmetrikus megoldási lehetőség. Az aszimmetrikus megoldás a digitális aláírásra alapul, amelynek kialakítása még nem valósult meg a Magyar Honvédségben. A szimmetrikus technika egyik lehetősége az ismertető jel kérés-adás, illetőleg a forgalmi adatok gyakori váltása, amely megnehezíti, esetleg lehetetlenné teszi a rendszer időben történő felderítését.

Rendszabályok

A rendszabályok bevezetésével csökkenthetjük a saját zavarás létrejöttét, az ellenséges felderítés hatásosságát és ezzel az ellenséges zavarás lehetőségét.

A rendszabályok a különböző átvitelt biztosító berendezéseink üzemeltetésére vonatkozó megkötések lehetnek. Ilyen megkötések lehetnek a rádiótilalom, a kisugárzó eszközök forgalmának minimalizálása, irányított antennák használata, csak az összeköttetés fenntartásához szükséges adó teljesítmény használata, mely rendszabályokkal az ellenséges rádióelektronikai felderítést nehezíthetjük meg.

De ugyan ilyen rendszabály lehet a hálózat forgalmának folyamatosan azonos szinten tartása, amivel viszont a hálózat analízist nehezítjük meg.

Befejezés

A cikkemben rámutattam, arra hogy az információk, adatok védelme az átviteli út folyamán nem egyszerű feladat. Minden egyes átviteli út tervezésekor, üzemeltetésekor elemezni kell a konkrét helyzetet, az alakulat feladatát, a technikai megvalósítás lehetőségeit, az adott terület földrajzi adottságait, az időjárás körülményeit, az ellenség technikai lehetőségeit.

Felhasznált irodalom:

1. 179/2003. (XI. 5.) Kormányrendelet a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól
2. Bokor-Tolnai-Tamási-Varga Rádióelektronikai harc, Zrínyi katonai kiadó, Budapest, 1982 ISBN 963 326 112 0
3. Informatikai Tárcaközi Bizottság 8. ajánlás Internet letöltés: http://www.itb.hu/ajanlasok/a8/html/a8_m4_4-8.htm 2007. november 2.
4. 1995. évi LXV. Törvény az államtitokról és a szolgálati titokról
5. Dr. Haig Zsolt mk. alezredes, egyetemi docens: Az információbiztonság komplex értelmezése Internet letöltés: http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles6/haig_rw6.pdf