

NEMZETBIZTONSÁGI SZEMLE

MMXIII.

I. ÉVFOLYAM I. SZÁM

KÜLÖNLENYOMAT



NEMZETI KÖZSZOLGÁLATI EGYETEM
NEMZETBIZTONSÁGI INTÉZET
BUDAPEST

Megosztani a megoszthatatlant – avagy megmaradni, épnek maradni a titok szolgálatában

Oláh László – Gyórfy Ágnes

Absztrakt

A speciális beosztás során szerzett élmények nagyon gyakran kívül esnek a mindennapok tapasztalatain. Ugyanakkor a személyiségbe történő feldolgozásuk és beintegrálásuk elengedhetetlen, hiszen a hivatásos szolgálat és az ilyen jellegű feladatok ellátása egész embert kíván. Ennek a munkának az elősegítése pszichológusi feladat, a folyamat minden egyes szakaszában. Ezt a munkát nehezíti az a beállítódás az állomány részéről, ami az élmények elfojtása, háttérbe szorítása és/vagy hasítása irányában hat. Ezeket az élményeket, érzéseket az állomány tagjaival való találkozás helyétől és helyzetétől függetlenül a pszichológus szakembernek egyaránt tartalmaznia kell. Ez a fajta tartalmazás egy speciális beállítódást igényel, mely egyben egy speciális megterhelést is jelent. A speciális beosztásban végzett-, valamint pszichológiai munka során fennáll a traumatizáció lehetősége is.

Az alábbiakban közölt cikkben rövid összefoglalása történik a fegyveres testületekben speciális beosztásokban szolgálók speciális megterhelésének hatásairól. A hatások az alapszemélyiségen keresztül értelmezhetők. A helyzet komplex, már a kiképzéstől kell tudatosítani, majd a megszerzett élményeket átdolgozni a személyiség szintjén. Átdolgozás nélkül tartós változások állhatnak be, amelyek az egyéni hatékonyságot csökkentik.

Kulcsszavak: műveleti pszichológia – élményfeldolgozás – mentálhigiénés támogatás – pályaszocializáció – pszichológiai felkészítés

Abstract

In this article our aim is to concise the effects of psychological burden on the armed forces members serving in special positions. These effects could be interpreted through the personality of the members. Being a member in of an organization like this forms a very complex situation that should be made conscious right from the first day of their entrance training. The experiences that gained here should be processed on the level of personality because without doing this changes can occur that could be irreversible and can have negative influence on effectiveness.

Megosztani a megoszthatatlant – avagy megmaradni, épek maradni a titok
szolgálatában

Keywords: *operational psychology – psychological proceeding of experiences – supporting mental health – profession socialization – psychological preparation*

Megosztani a megoszthatatlant – avagy megmaradni, épnek maradni a titok szolgálatában

A speciális beosztásban végzett szaktevékenység során szerzett élmények nagyon gyakran kívül esnek a mindennapok tapasztalatain. Ugyanakkor a személyiségbe történő feldolgozásuk és integrálásuk elengedhetetlen, hiszen az ilyen jellegű feladatok ellátása „egész embert kíván”: bármilyen technológia segíti is munkájukat, alapvető munkaeszközük a személyiségük. A feldolgozás és integráció feladatának az elősegítése pszichológusi feladat, a folyamat minden egyes szakaszában. Ezt a munkát nehezíti az állomány részéről az a – szakmai szerep részeként is megjelenő – beállítódás, ami pszichikus szinten az élmények elfojtása, háttérbe szorítása és/vagy hasítása irányában hat.

A pszichológus szaktevékenysége folyamán rendelkeznie kell a megértésen, a diszkréció képességén túl az ún.: „konténer funkcióval” is. A speciális beosztásban dolgozók – a bizalmi viszony kialakítását követően – a testi, gondolati élményeket, érzéseket esetenként töredékes formában megosztják a pszichológus szakemberrel, az állomány tagjaival való találkozás helyétől és helyzetétől függetlenül. Ezeket az élményeket és érzéseket a pszichológus szakembernek is egyaránt tartalmaznia kell, ezzel tehermentesítve – átmeneti jelleggel – a másik felet. Ez a fajta tartalmazás, egy speciális beállítódást igényel, mely egyben egy speciális megterhelést is jelent.

A titok

A titok fogalmát az értelmező kéziszótár így határozza meg: más (-ok) elől elhallgatott, elleplezett tény, dolog (Pusztai, 2003). Már ebből a definícióból is következik, hogy a titok, meg nem osztható és egyfajta falat képez, elszigetel a környezettől, az abba be nem avatottaktól. Az elhallgatás, elleplezés aktív pszichikus folyamatok eredményeként megjelenő viselkedést enged feltételezni, amelynek során a személy (-ek), csoportok nagyfokú pszichikus energiát fektetnek be a kontrollfunkciók fenntartása és hatékony működése érdekében függetlenül attól, hogy belső érzelmi – indulati életük mennyire telített, vagy a külvilágukban zajló események mennyire terhelők (Noelle-Neumann, 1984)

A titok jogi értelemben olyan ismeret, adat, információ, amely egy adott időpontban vagy időszakban csak korlátozott körben ismert (MÜK, 1999). Minden titok a nyilvánosságra hozatallal szűnik meg, azaz azáltal, hogy a korláto-

zott körön kívül is megismerhetővé válik. Tehát ez a korlátozás időben és/vagy térben, tartalomban, személyben egyaránt megvalósulhat.

„A titok véd, elfed és elszigetel. Titok az, amit az egyén, vagy a csoport el akar takarni. Ezzel szemben a tabu egy olyan tiltás, amelynek eredetét, okát sokszor homály fedí. Az egyén, a közösség védelmére szolgál, magától értetődő, meg nem kérdőjelezhető.” A szó eredeti jelentése: kimondhatatlan (Ribáry, 2011). A titok fogalma kapcsán fontos, hogy megemlítsük a hasonló jelentésű, részben átfedést mutató fogalmakat, ilyen az előbb említett tabu, a tiltás, illetve a nem tudás. Minden szervezet, illetve csoport, közösség esetében vannak tabuk, melyek kimondva – kimondatlan szabályozzák a közösség és az egyén életét és gondolkodását. A tabu esetében mintha a közösség minden tagja akár említés nélkül is tökéletesen tisztában lenne vele, hogy nem kimondható, nem tehető, nem közölhető, szinte formális szabályrendszer, tiltás sem szükséges hozzá. A belsővé vált fékező rendszer hatékony működése segít megelőzni pl.: a dekonspirációt, amelynek elkerülése alapvető feladatként jelentkezik a mindennapokban a feladatvégrehajtás során. A titok esetében a tiltás olyan szabályozó eszköz, mely kijelöli, mit lehet tenni és mit nem. Ebben az esetben viszont felmerül, hogy a generalizáció - mint mentális folyamat révén - sok olyan más viselkedés, gondolat is tiltás alá kerül, ami önmagában nem tilos, de kapcsolatban áll más, tiltott dologgal, aktivitással, így annak attribútumai mintegy átörökítődnek. A mindennapi élet szintjén is megfigyelhető, ha valamit el akarunk titkolni, már arról sem szívesen beszélünk, ami emlékeztet bennünket a titokra, hiszen az máris közelebb visz bennünket annak megosztásához.

A „nem tudás” is kapcsolható ezekhez az alapfogalmakhoz. Egyrészt a titok és tabu sérthető a nem tudás révén, amikor is a titok birtokosa eltérő norma-, és értékrendszerben találva magát nincs felkészítve pl., hogy a tudása átadhatóságának meddig terjednek a határai. Másrészt a titok birtokosa – birtokosai, „létrehozói” szabályozhatják a titok útját, kiadását, megőrizhetőségét azáltal, hogy kit, milyen mértékben, milyen időtartamban avat be vagy vonnak be a titok „bűvkörébe”. Sajátos módon jeleníti meg mindezt a „Mandzsúriai jelölt” című film, ahol azáltal kerül védelem alá a tervezett beavatkozás, hogy maga a résztvevő sem tud a szándékáról a cselekmény kivitelezését megelőzően, illetve annak végrehajtása során. Az információ az egyén tudattalanjában van kódolva: ezen információk normál tudati működésmódban nem integráns részei a személyiségnek, un. disszociált tudati tartalmakról van szó.

A fentebb leírt definíciók tartalmazzák a titok funkcióit: véd, elfed és elszigetel. Ez funkció kétélű fegyver az egyén szempontjából, de a közösségből is.

A funkció középpontjában a titok áll, s nem annak őrzői, birtokosai. Törvény-szerűen nemcsak a titkot, hanem annak őrzőit is elfedi, elszigeteli, mind érzelmileg, mind személyében. A titok elszigetel, lehetetlenné teszi az érzelmi megosztást, kitérülkötést, mindazt, ami minden barátság, minden valamirevaló érzelmi kapcsolat alapja: egyszóval lelki magányra kárhoztat (Fisher, 2005). A történelemben számos példa látható erre, amikor fontos információk, titkok akár generációkat, egész korszakokat túlélnek, illetve sokak fantáziáját megmozgatja a titkos társaságok léte.

A titokban mindig van valami izgalmas, vele együtt megjelenik a beavatás és a beavatottság vágya. Ezt egyéni szinten természetesen befolyásolja a titokhoz való személyes viszony, a családi alapszocializációs minták. Kinek-kinek a családjában hogyan kezelték a titkot, mi számított titoknak, tabunak, mit engedtek, mit tiltottak, hogyan lehetett egy-egy titok birtokába jutni, valamint ezek mellett mennyire volt jelen a család életében az intimitás, vagy az elszigetelődés, amelyek alapvető befolyással voltak az egyén pszichikus érése során. Ez a személyes viszony, illetve annak teljes érzelmi vonulata aktivizálódni fog a titkosszolgálathoz történő jelentkezéssel és a titkosszolgálatok világába történő szocializáció folyamatában.

Mivel a korlátozás az ilyen jellegű szervezetekhez bekerülőket esetében valamilyen mértékben a mindennapi élet minden területét érinteni fogja, így szép lassan a személyiség egésze megérintődik, a titok köré szerveződve átalakul, annak pszichodinamikai működési elveit követve. A beavatás során az egyén egyfajta átmeneten megy keresztül, aminek eredményeképpen élete korábbi szakaszából átvezetődik az újba, s szemlélete, életmódja visszavonhatatlanul megváltozik, átalakul. Eliade részletesen vizsgálja a beavatási rítusokat (Eliade, 2006), melyek különböző funkciójuk ellenére mind úgynevezett átmeneti rítusok. Ez az átmenetiség a korábbi események, történések felfüggesztését jelenti, jellemző rá az elkülönítés, a kiszakítás, a próbatételek sora, melynek révén a beavatandó meghal valami számára, életében véglegesen véget ér valami, hogy valami új számára születhessen meg: „az ember megsemmisíti a múltat, véget vet a létezésnek – amely elromlott –, hogy újrakezdjen egy másikat, egy megújítottat. A beavatási halál soha nem vég, hanem újrakezdés. [...] a másféle létmódba való átlépés alapfeltétele, elengedhetetlen próbatétel a megújodáshoz, vagyis az új élet megkezdéséhez.” (Eliade 2006, 331.). Akárcsak a mesék és a filmek hőseinél, akiknek történeteik szintén valamilyen alapvető emberi élethelyzet lélektani aspektusát képezik le.

A teher felvétele és a letehetetlen súlyok vitele az életúton és a pálya során

A címben foglaltak a titkosszolgálatok esetében felveti azt a speciális kérdéskört, hogy a titokhoz való viszony, vagyis a „titokbirtokosi lét” elnyeréséhez milyen próbatételeknek kell megfelelni a kiképzés és továbbképzés rendszerében? Mikor kezdődjön, milyen mértékben és hogyan történjen a leendő és a már meglévő állomány felkészítése, továbbképzése.

Az állományba kerüléskor (felvételes, felszerelő, stb.), illetve a szolgálati évek során a képzés egy újabb állomására érkezésekor az alábbi tematikus szempontok lehetnek fontosak:

- az egyén életútjának vizsgálata, amelynek során képet kaphatunk annak a személyiségfejlődés, illetve változás szempontjából koherens ívére;
- a normálistól eltérő pszichológiai állapotok feltérképezésére, amelyek – bár értelmezhető a külvilág hatására adott válaszként – fontos indikátorai az alkalmazhatóságnak, a reagálóképességnek és a képezhetőségnek. Nagyon fontos megfigyelnünk ezen állapotok képességrendszerre és a külvilág kölcsönhatásaira gyakorolt szerepét, hiszen – a teljesség igénye nélkül – ezek befolyással bírhatnak mind az egyéni hatékonyság, mind a normaszegések pszichikai okaira is;
- a képességek, készségek, attitűdök egységes rendszerének vizsgálata, amelyek a feladathoz való viszonyt aktuálisan, hosszú és rövidtávon meghatározzák.

Az állományba kerüléssel a következő alapvető pszichológiai az egyént és közvetlen szociális környezetét egyaránt érintő problémakörök vetődnek föl:

- az intimitás megőrzése – a titok védelme: ez a két folyamat törvényszerűen egymás ellen hat a családon, baráti társaságon belül, hiszen az intimitásnak elengedhetetlen feltétele a másik közelengedése. Gondoljunk bele, hogy egy olyan egyszerű kérdésre sem adható nyílt egyenes és részletekbe menő válasz, hogy: „milyen napod volt ma?”. Ebből az egyszerű interakcióból is keletkezhet konfliktus. Ennek megjelenése és erőssége az egyéni és családi dinamikától függ, és a szervezet és a kiképzés részéről is fontos, mikor és milyen módon szembesítjük – és készítjük fel – az egyént;

- az alapszocializáció egyénenként eltérő mivolta: elengedhetetlen a személyiség, és az egyéni alapszocializáció vizsgálata (Váriné, 1976), majd az erre épülő kiképzés és a feladatkeretbe történő beillesztés. Már a bekerüléskor vizsgálni kell, mi az alap, amire építhetünk a kiképzés során, ki-ki mit tesz hozzá a kiképzési csoport működéséhez. Fontos tisztázni, hogy a kiképző milyen jellegű mentorálást tud biztosítani az egységes alapok elérése érdekében. Az eltérő alapszocializáció alapján mindenkinek más lesz az a metódus, ami célravezető, amivel a leghatékonyabb kiképzés elérhető. Kérdésként merül föl, hogy mennyire lehetséges ezt figyelembe venni a kiképzés, felkészítés során;
- nyomomonkövetés – szűrővizsgálatok szükségessége: a jó kiképzés és felkészítés a pálya teljes spektrumában és időtartamában képzelhető csak el hatékonyan. A személyes sajátosságokra, alapszemélyiségre a pályán eltöltött idő és terhelés eltérő mértékben és jelleggel lesz hatással. A titok és annak megőrzése – szolgálata hosszú távon elkerülhetetlenül rombolja az egyén belső védekező mechanizmusait és borítja lelki egyensúlyát. A borulás iránya és mikéntje pedig mindig az alapszemélyiségből értelmezhető. Kiemelt szereppel bírnak tehát a szűrővizsgálatok, a preventív jellegű képzések és a személyes utánkövetés.

Az ember, aki túl sokat tudott...- néhány szó a kiképzésről

A kiképzés során tehát a következő pszichológiai jelenségre célszerű kiemelt figyelmet fordítanunk:

A belső egyéni normarendszer ütközése a testületi igényekkel: a kiképzés feladata az új identitás és normarendszer kialakítása, ami a feladatvégrehajtáshoz stabil alapot képezhet. Ez az új normarendszer esetenként rendkívül nehezen egyeztethető össze az egyén korábbi, személyiségéből és alapszocializációjából eredő normákkal – normarendszerrel, ami intrapszichés konfliktust szül (Csepe, 1986).

Ez az intrapszichés konfliktus részben annak révén csökkenthető, ha a kiképzés során a meglévő karakter és képesség rendszerre alapozva történik meg a jártasságok és készségek kialakítása, a szakszervezők megfelelő alkalmazásától a fedőszerep kialakításáig.

Szintén fontos szempont, hogy az egyént, a szakembert ezt követően se hagyjuk magára. A pályakép integráns részének kell lenni az egyéni és csoportos képzések és továbbképzések rendszerének. A képzések rendszere összekapcsolódik a mentálhigiénés szűrővizsgálat rendszerével, hiszen annak eredményei felhasználásával a képzés és az egyéni fejlődés és pályáiv hatékonyabbá, illetve sikeresebbé válhat, mind a szervezet, mind az egyén személyes szintjén. Nem elhanyagolható szempont az egyéni egészségfejlesztés sem, aminek segítségével a már kialakított képességek, készségek fenntarthatóvá és megőrizhetővé válnak, illetve csökkenthető a „burn out” veszélye is.

Kiemelt jelentőséggel bír, s egyben következik a már leírtak alapján, hogy az erős és speciális terhelés a továbbképzési helyzetben, egyéni és csoportszinten, nem megfelelően átgondolva akár árthat is. Különösen igaz mindez a szituáció alapú és/vagy extrém stressz helyzetekre történő felkészítésekre, ezért különös hangsúlyt kell fektetni az azt követő élményfeldolgozásra mind egyéni, mind csoportos szinteken. Sok esetben az ilyen gyakorlatoknál elsőként azok élményszerű jellege vagy korábbi tapasztalatokra való emlékeztető mivolta kerül előtérbe, mindkét esetben a bevonódás és a feladatvégrehajtás nem megfelelő minőségét eredményezheti. Az első esetben a bevonódás nem megfelelő mértékű, a második esetben pedig az élmény maga a korábbi helyzetre adott reakciókat idézi föl.

A kiképzés folyamatában emellett az ilyen jellegű gyakorlatok megtervezése és megfelelő időszakban történő beiktatása azért nagyon fontos, mert ha túl korán történik meg, akkor a pályától inkább elriaszthat, illetve irracionális szorongásokat építhet be, vagy azok élményszerúsége révén minden más kiképzési elem hatása elmaradhat az elvárttól. A nem megfelelően előkészített vagy túl korán alkalmazott gyakorlat során az egyén még nem rendelkezik a megfelelő szakmai tapasztalatokkal, illetve a nehezített helyzet megfelelő kezeléséhez szükséges pszichés védekező mechanizmusokkal, így mind a szakmai, mind az énkép súlyosan károsodhat. Semmilyen körülmények között nem lehet a kiképzés célja a kiképzendő állomány reagálóképességének csökkentése. Fontos megemlítenünk, hogy a gyakorlat minden esetben modellezni szándékszik a valódi szituációt, így abból akár pro akár kontra az egyén vagy csoport viselkedésére valós helyzetben vagy hosszútávú szakmai beválás, pályafutás tekintetében következtetések levonása csupán kevés eséllyel lehet helytálló.

Minden esetben figyelmet kell fordítani arra, hogy az élményfeldolgozás a modellhelyzetet, a gyakorlatot követően is megfelelően megtörténjen, mind egyéni, mind csoportszinten, akár egy valódi szakmai szituáció esetében, mert

ahogyan már korábban is említésre került, a titok elszigetel. Nem megosztható az élmény, a kiképzési helyzetről sem, így a család, barátok, ismerősök számára a helyzet feszültsége, érzelmi töltete érkezik meg, annak tartalma, háttere továbbra is a titok részét képezi. A kiképzés során ezért arra is tekintettel kell lennünk, hogy az egyén pályaszocializációja a titok kezelésére, birtoklására is kiterjedjen, illetve a szakmai közösségnek és kiképzésnek egyfajta érzelmi biztonságot is adjon, ami révén a szeparáció – izoláció feszültsége feloldódhat, így hosszútávon az énkép és a pályaidentitás nem vagy minél kevésbé károsodik. A hatékony kiképzési folyamat tehát elképzelhetetlen pszichológiai megalapozottság és érzékenység, valamint pedagógiai strukturáltság és felépítettség nélkül, a szakemberek team-munkája révén.

„Ugye, köztünk marad?!” – a pszichológus speciális terhelése

Ebben a közegben, az ilyen feladatokat ellátó állománnyal való munka során a pszichológus terhelése is rendkívül speciális. Ez a specifikáció már ott elkezdődik, hogy a fegyveres testület működési rendszere nehezen összeegyeztethető a pszichológusi alapbeállítódással, ami az empátia, elfogadás és diszkréció biztosítását involválja. Egy erősen hierarchikus rendszerben, ahol a szakember elkötelezettsége kettős: egyrészt a szervezet, másrészt az egyén felé valószínűleg, csak részben őrizhető meg a független szakértői, szakemberi szerep. Az empátia – objektivitás – diszkréció tengelye mentén a pszichológusnak egyszerre kell együttéreznie az egyénnel, segíteni őt, ugyanakkor egyaránt tekintettel lennie annak szakmai teljesítőképességére is, mikor veszélyezteteti esetleg állapota a feladatok végrehajtását, illetve mikor lehet / szükséges az állapot esetleges további jelzése a szervezet felé, a részleges diszkréció megőrzésével.

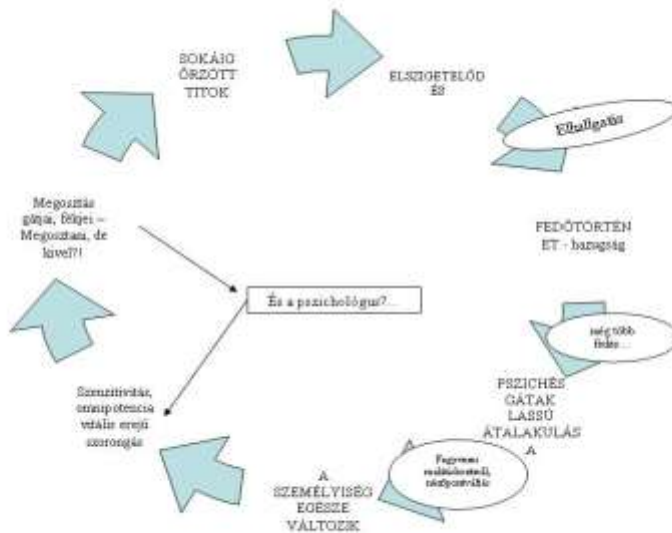
A pszichológusi szerepben egy másik dimenziót – tengelyt is elkülöníthetünk: a pszichológus – egyén – szervezet dinamikus egyensúlyát jelző tengelyt. Ez a tengely az előző jelenség egy más aspektusból történő bemutatását teszi lehetővé: míg az első az érzelmek kezelésére, e második az elköteleződés, illetve egyén és közösség kapcsolatára, esetenként dichotómiájára helyezi a hangsúlyt. A pszichológus szakember egy mindennaposnak mondható szűrő- vagy alkalmasság vizsgálat során egyrésztől figyelembe veszi, hogy az adott feladatra milyen személyiségű, beállítódású, készségű, képességű egyén szükséges, ugyanakkor látnia kell annak emberi oldalát is, ha most nincs is a feladatra megfelelő állapotban, segítséggel újra olyan állapotban lehet-e. Hol van tehát

az a határ, ahol az egyén és/vagy a szervezet károsodik a benntartással vagy a kikerülése?

Végül, de nem utolsó sorban ezekre a helyzetekre épül rá a titok légköre, ami a szakembert és benne az embert is egyaránt megéri. A pszichológusé tehát a titkok titka, s ez a teher nehezen megosztható, szakmai közösségbe sem vihető tovább annak teljességében. Egy szupervíziós szakmai közegben már maga a fegyveres testületben végzett munka is nehezen érthető, hiszen a benne való pszichológusi működés sok esetben ellentmond a szakma szabályainak. A magánéletbe, személyes szociális térbe bevihetetlen.

A szakmai szerepre való felkészítés és abban való fejlődés, megőrzés elősegítése pszichológusi feladat, a folyamat minden egyes szakaszában. Ezt a munkát nehezíti az a beállítódás az állomány részéről, ami az élmények elfojtása, háttérbe szorítása és/vagy hasítása irányában hat. Hiszen egyfajta elsődleges énvédő mechanizmusként az egyén megpróbálja háttérbe szorítani, tudatáról leválasztani a nyomasztó, meg- nem-osztható élményeket, amik a titok részét képezik. Ezeket az élményeket, érzéseket az állomány tagjaival való találkozás helyétől és helyzetétől függetlenül a pszichológus szakembernek egyaránt tartalmaznia kell. Hiszen, ha ott a lehetőség, hogy mindaz megosztható, de nem kerül, továbbadásra, megkönnyebbülést jelent, a megosztás felszabadító jelleggel bír. Pszichológusként ezért a leghatékonyabb, ha azt a folyamatot segítjük elő egyén és közösség esetében, hogy a személyes érzelmeket osszák meg, a konkrét tartalom nélkül, az arról való leválasztással, aminek hatására az érzelmi feszültség feldolgozhatóvá, megoszthatóvá válik, de a titok nem sérül.

A titok jelensége és a titok légkörében végzett speciális feladatok tehát az egyént a következő folyamaton viszi végig, ami egyben tartalmazza a lelki egyensúly részleges vagy teljes, időleges vagy végleges kibillenésének lehetőségét is. A folyamatról gyakorlati tapasztalatok alapján alkotott koncepciót az 1. számú ábra tartalmazza.



1. ábra: Tánc a kardélen – a lelki egyensúly kibillenései
A „titok spirálja” koncepciója (Gyórfy)

A titok birtoklásának tehát ára van, ami a személyiség egészét áthatja, egyben véglegesen és visszavonhatatlanul megváltoztatja a világról, emberekről alkotott képet. Beépül az elhallgatás, ami lassan fedőtörténétté vagy élethuzugsággá válhat, hiszen olyan mindennapos kérdésekre sem lehet teljes tartalommal válaszolni, mint a hogy telt a napod, vagy mivel foglalkozol. Különös helyzetet jelent ebből a szempontból a külszolgalat, ahol a kapcsolattartás szinte a másik fél, családtag meghallgatására, illetve a saját személyes biztonság tudására korlátozódik. A titok elszigetelő jellege itt méginkább érvényesül. A feladatvégrehajtás idegen környezetben zajlik, ami szinte törvényszerűen felerősíti a fokozott szenzitivitást és a saját felelősségérzet megnövekedését. Ráadásul ezek az élmények, tapasztalatok csak a saját, fegyveres testületen belül értelmezhetőek azon kívül csak azok indulati töltése és az információ hiányban a civil szociális közeg értetlensége marad. A visszailleszkedés folyamatának elősegítése és nyomonkövetése elengedhetetlen. Nehéz visszatérni, visszatálatni a civil közegbe, akár részlegesen egy-egy feladatot követően, akár véglegesen kilépve a szervezetből, esetenként még egy-egy beszélgetési téma is nehezen felvethetővé válik. Ebben a szenzitív, beszűkült állapotban, a lelki

egyensúly kibillenésének irányát, mértékét és mélységét az alapszemélyiség fogja meghatározni, ezért a szűrővizsgálatok, visszaillesztés, élményfeldolgozás során erre mindig oda kell figyelnie a pszichológus szakembernek.

Ami mindent felülír – A pályaidentitás ára...

A fent leírtak alapján elszigetelődés alakul ki a pálya vitele során a civil társadalomtól, ami mintegy dichotóm állapotot képez az egyén életében, ahol a „dolgos hétköznapok” esetenként akár teljesen külön világot jelenthetnek a civil mindennapoktól. Joggal merülhet föl a kérdés, hogy a kiválás, nyugdíj esetén hogyan áll helyre újra az egyensúly, illetve milyen új egyensúlyi helyzet jöhet létre az egyén életében. Hogyan oldódhat föl a testületi tag magánya?

A gondolkodás megváltozásával az egyén és a társadalom viszonya megváltozik. Másként néz környezetére, esetleg más információkkal bír arról, annak működéséről, illetve az is más szemmel néz rá, hiszen az információ egyrésztől hatalom, ami akár szentitív paranoid gondolkodást, viselkedést is kiválthat, másrésztől a hatalom képviselője lesz, aki kíváncsiságot vagy ellenérzéseket ébreszt. Mindezt csak fokozhatja egy-egy elejtett mondat és a megfelelő időben történő hallgatás. Az egyénben végbemenő változásokat annak tágabb és szűkebb környezete egyaránt érzékeli, sok esetben előbb, mint az egyén észlelné vagy elfogadná.

Kiemelt jelentőséggel bír, hogy az egyéni fejlődés, személyes identitás ívében teljesül-e az egyéni cél, amiért értelmet nyer az áldozat, lemondás. Kap-e az egyén külső visszaigazolást is arra, hogy megérte, volt értelme az áldozatnak, a lemondásnak az intimitásról vagy marad az örök és megtörhetetlen izoláció?

A pszichológus feladatai, az átkeretezés jelentősége

A pszichológus feladatai tehát a következő kiemelt jelenségek mentén történnek a szervezeten belül:

1. *A segítségnyújtás biztosítása a szervezeten belül: a segítő beszélgetéstől, krízisintervención és a tanácsadáson át, a mély pszichoterápiáig, ahogyan a helyzet, a szervezet és az egyén állapota megkívánja.*
2. *A fegyveres és a civil realitás ismerete, egyensúlyának megtartása: az egyén pszichés egyensúlya megőrzésének elősegítése, az egyensúly kialakítása és megőrzésének támogatása a civil és a fegyveres testületi realitás között. Ennek hiányában, illetve hangsúlyeltolódása esetén a*

- lelki egyensúly könnyebben borulhat, illetve a mérleg két oldala közül valamelyik károsodhat: a feladatellátás vagy a magánélet.
3. *Személyes szintű fejlődési ív megtalálása, támogatása:* a lelki egyensúly egyik alapköve, ami mind a boldogságnak, mind a túlélésnek fontos eleme, a személyes cél megtalálása, mind kisebb, mind nagyobb célok tekintetében, a mindennapokban, a pályán és az élet egészében. Ennek áttekintése, összegzése, elősegítése annak összerendező és motiváló jellegéből adódóan fontos pszichológusi feladat.
 4. *Megfelelő szakmai felkészültségű pszichológus szakemberek és szupervízió biztosítása:* a pszichológus szakemberek részéről is kiemelt jelentőségű, hogy megfelelő felkészültséggel rendelkezzenek a feladathoz, ugyanakkor saját lelki egészségüket is megőrizték. Ehhez a szervezeten belül biztosított szupervízió és pszichológiai szakmai továbbképzések segítséget nyújthatnak.
 5. *A titok terhének levétele elbocsájtás, nyugdíj esetén...:* nem elhanyagolható feladat a szervezetbe történő integráció és a pályáiv támogatása mellett a rekonverziós folyamat és a civil szociális közegbe, realitásba való visszailleszkedés elősegítése sem. A szervezet sok elvárása, speciális terhelése révén változásokat idéz elő az egyénben, amit fontos, hogy amennyire lehetséges a kiváláskor tehermentesítsen, hiszen a megfelelő zárás a pályáiv és a hivatáshoz való viszony egészét meghatározza.

Összegezve, az egyén életében a titok világába történő belépéssel megváltozik az összes lényeges elem, hiszen a referenciakerete megváltozik. Az életének korábbi tapasztalatai egyrészt alapul szolgálnak későbbi működéséhez, másrészt ehhez tér vissza az extrém körülmények okozta kihívások átélése során.

A szervezetbe történő belépéssel, az ezt követő beavatással, vagyis a kiképzés végrehajtása során megkezdődik a személyiség átalakulása. Az átalakulást követően az érték és normarendszer jelentős változáson megy át, eltávolodva a „civil valóságtól”. A változás értelmezési kerete és célja egyértelmű: speciális szakmai szabályok alkalmazása révén megfelelni a szervezeti céloknak, és egyén szinten megfelelő eszközrendszerrel rendelkezni a személyes integritás megőrzése érdekében a hatékonyság és a reagálóképesség megléte céljából.

Az egyén életútjában a kiképzésnek kiemelt jelentősége van: át kell emelni az embert a civil világból a titok világába oly módon, hogy a személyiség szintjén jelentősnek nevezhető beavatkozással megőrizve a személy egyediségét,

ugyanakkor a személy önmaga határait meghaladva – a szakma szabályainak megfelelően – a reagálóképessége optimumát érje el. A kiképzés időben stabil, szakmailag megalapozott tudásrendszerének átadása lehetőséget teremt a hosszabb távú alkalmazkodáshoz és alkalmazáshoz.

A pszichológia tudományának eszközszerrendszere segít az átalakulás folyamatában az egyén önazonosságának fenntartásában és élmény szintű integrációjának megőrzésében, továbbá az életút folyamán az egyéni egyensúly fenntartásában, a szükséges korrekciók végrehajtásában. Összességében úgy végigkísérni az életútjukon a titok világában tevékenykedőket, hogy önmaguk egyszerre részesei, másrészt külső megfigyelői a folyamatoknak.

Irodalomjegyzék

- CSEPELI Gy., Bevezetés a szociálpszichológiába, Budapest, Tankönyvkiadó, 1986. ISBN 963-3898-14-5
- ELIADE, M., Mítoszok, álmok és misztériumok, Budapest, Cartophilus, 2006. ISBN 963-7448-14-4
- FISCHER, E., Modern mostohák, Saxum, Budapest, 2005. ISBN 978-9637-168376
- Magyar Ügyvédi Kamara 8/1999. (III.22.) MÜK Szabályzata az ügyvédi hivatás etikai szabályairól és elvárásairól
- NOELLE-NEUMANN, E., The spiral of silence: Public opinion- our social skin, Chicago: The University of Chicago Press, 1984. ISBN 978-0226-58-9367
- PUSZTAI F., (főszerk.), Gerstner, K., et al. (szerk.); Magyar értelmező kéziszótár, Budapest, Akadémiai kiadó, 2003. ISBN 963-0578-74-3
- RIBÁRY M., Családi titkok,
<http://www.prherald.hu/2011/09/csaladi-titkok/> letöltve: 2013. 02. 16.
- VÁRINÉ SZILÁGYI I., A szocializáció In: Szociálpszichológiai kutatások Magyarországon, Budapest, Akadémiai Kiadó, 1976. ISBN 963-05-0855-9

The authors point of view to the main threat to international security is the use of information and communication technologies are next: as an information weapon in the military-political purposes contrary to international law, to carry out hostile acts and acts of aggression aimed at discrediting the sovereignty, violation of territorial integrity of states and pose a threat to international peace, security and strategic stability; the purposes of terrorism, including for the provision of a destructive impact on the elements of critical information infrastructure, and to promote terrorism and bringing new supporters of terrorist activities; to intervene in the internal affairs of sovereign states, violation of public order, incitement of ethnic, racial and religious hatred, propaganda of racist and xenophobic ideas or theories that give rise to hatred and discrimination, incitement to violence; and to commit crimes, including those related to unauthorized access to computer information, with the creation, use and dissemination of harmful computer programs.

Настоящие Основы предназначены:

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года

Настоящие Основы предназначены:

- а) для продвижения на международной арене российских инициатив в области формирования системы международной информационной безопасности, включая совершенствование правового, организационного и иных видов ее обеспечения;*
- б) для формирования межгосударственных целевых программ в области международной информационной безопасности, в осуществлении которых участвует Российская Федерация, а также государственных и федеральных целевых программ в данной области;*
- в) для организации межведомственного взаимодействия при реализации государственной политики Российской Федерации в области международной информационной безопасности;*
- г) для достижения и поддержания технологического паритета с ведущими мировыми державами за счет более широкого использования информационных и коммуникационных технологий в реальном секторе экономики.¹⁹⁶*

¹⁹⁶ НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИИ (Информационная безопасность)
<http://www.scrf.gov.ru/documents/6/114.html> (letöltve: 2013. 10. 02.)

Oroszország állami politikájának alapjai a nemzetközi információs biztonság terén a 2020-ig terjedő időszakra

Napjainkban, a fegyveres küzdelem területén eljutottunk a kiberhadviselés korszakába, amikor már egyes országok kormányai kezdik átvenni a kiberbűnözők által kifejlesztett technológiákat és eszközöket. Megfigyelhető emellett a kiberterrorizmus és a kritikus infrastrukturális létesítmények elleni támadások számának a növekedése. Továbbá, a „piacon” egyedi igények szerint kialakított kémprogramokat is lehet már kapni. Olyan kiberhadviselési „fegyverekre” sikerült rábukkanni a szakembereknek az elmúlt években, mint a Stuxnet, a Duqu, a Flame vagy a Gauss, legutóbb pedig a Red October.

Az Egyesült Államok mind elméletben, mind gyakorlatban harcot folytat a terrorizmus, a cyberterrorizmus ellen. Az elmélet dokumentumai néhány év óta közismertek a közvélemény, a szakemberek és az egyetem hallgatói előtt.¹⁹⁷ Ezért csupán néhány véleményt ismertetünk, amelyek a dokumentumok megjelenése előtt hangzottak el, nagyon röviden.

Howard Schmidt, az Obama kormány korábbi kiberbiztonsági koordinátora arról beszélt a Kaspersky Kiberbiztonsági Csúcsértekezleten, hogy az áramellátó, pénzügyi szolgáltató, távközlési ágazatok válhatnak támadás célpontjává, és mivel ezek kölcsönös függőségben vannak egymással, bármelyik ágazatot éri a támadás, az egész rendszert megbéníthatja. A szakember nem tartja kizártnak a fegyveres erők számítógépes rendszerei elleni támadásokat sem.¹⁹⁸ James A. Lewis, aki a Center for Strategic and International Studies (CSIS - Stratégiai és

¹⁹⁷ Department of Defense Strategy for Operating in Cyberspace.
<http://www.defense.gov/news/d20110714cyber.pdf> (letöltve: 2013. 10. 09.)

The Comprehensive National Cybersecurity Initiative.

<http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>,
(letöltve: 2013 10. 09.)

Executive Order – Improving Critical Infrastructure Cybersecurity

[http://www.whitehouse.gov/the-press-office/2013/02/12/2013. 10. 09.](http://www.whitehouse.gov/the-press-office/2013/02/12/2013-10-09)

¹⁹⁸ Új veszélyek leselkednek a kibertérben. Kaspersky Kiberbiztonsági Csúcsértekezlet 2013. New York. (MTI – 2013. január 31.)

http://www.ma.hu/itmania.hu/160033/Uj_veszelyek_leselkednek_a_kiberterben (letöltve: 2013. 10. 10.)

Nemzetközi Tanulmányok Központja) munkatársaként a kiberbiztonság kérdéseivel foglalkozik, úgy látta, hogy a Plan X nyilvános bejelentése egyfajta fordulóponthoz jelent a kiberhadviselés titkosságáról folyó vitában. (Plan X: a kiberhadviselés megértetésére, tervezésére és irányítására szolgáló forradalmi technológia. A projekt felelőse a DARPA Defense Advanced Research Projects Agency – Fejlett Védelmi Kutatási Projektek Ügynöksége).

A szakember szerint mindez időszerű volt, tekintettel arra, hogy nyilvános dokumentumok alapján a világ 15 legnagyobb hadserege közül legalább 12 foglalkozik kiberhadviselési program (koncepció, doktrína) kidolgozásával és végrehajtó szervezetek létrehozásával.

„Számomra a Plan X a kiber támadási képességek hadműveleti célúvá alakítását és rutinszerűvé formálását jelenti – fogalmazott Lewis a The New York Timesnek nyilatkozva. – Ha pedig nyíltan lehet beszélni támadási célú nukleáris kapacitásokról és minden másról, miért ne lehetne a kiber hadviselésről?”

Matthew Waxman, a Columbia Egyetem jogászprofesszora, korábbi védelmi minisztériumi tisztségviselő szerint azért fontos nyíltan beszélni a kiberhadviselési politikáról, mert az Egyesült Államok számára így válik lehetővé, hogy egyértelművé tegye szándékait a konfliktus új és gyorsan fejlődő formájának a kezelésében. Waxman úgy véli, hogy most, amikor az Egyesült Államok előkelő helyen áll a támadó jellegű kiberképességeket tekintve, meg kell ragadnia a lehetőséget arra, hogy megalkossa a saját maga és mások számára a kötelező érvényű szabályokat.

1. ábra: Az US Kibernetikai parancsnoksága címere



„Ez egy derék célkitűzés – húzta alá Daryl G. Kimball, a Fegyverzetellenőrzési Szövetség ügyvivő igazgatója –, de egyben veszélyt is rejt magában: minél több szó esik ugyanis az Egyesült Államok kiber-hadviselési képességeiről, annál inkább érezhetik úgy más országok is, hogy fokozniuk kell saját programjaik fejlesztési tempóját, aminek hatására a világ aztán egyszer

csak eléri a kiber-fegyverkezési verseny csúcspontját.”¹⁹⁹

¹⁹⁹ Előtérbe kerülhet a kiber hadviselés

<http://ujsozso.com/online/kulfold/2012/10/17/eloterbe-kerulhet-a-kiberhadviseles> (le-töltve: 2013. 10. 08.)

Az Egyesült Államokban, a Pentagonon belül nemrég kiberparancsnokság alakult, és a tervek szerint a számítógépes hálózatok elleni hadviselésre, a saját rendszer védelmére szánt összegek abban az esetben is nőni fognak, ha a katonai költségvetés összességében csökken. Ez a döntés azt igazolja, hogy az Egyesült Államok komolyan számol a jövőben, a számítógépes rendszerei elleni támadásokkal más országok részéről.

Az amerikai elgondolások szerint a kiberhadviselésre ugyanaz a munkamegosztás lesz jellemző, mint a terrorizmus elleni harcra. A fegyveres erő katonai műveleteket folytat le a hadviselés szabályai szerint a felderített ellenséggel (terroristákkal) szemben. A hírszerző szervek adatai alapján, pedig különleges műveletei akciókat hajtanak végre, a kiberparancsnokság vezetésével, olyan területeken – a pilóta nélküli eszközök felhasználásával –, amelyeket hivatalosan nem minősítettek háborús övezetnek.

A tanulmány további részében vizsgáljuk meg – a címben jelzett dokumentum elemzése alapján –, hogyan gondolkodnak minderről az Oroszországi Föderáció szakemberei.

„A kiberbiztonság kérdéseit általában a hardverek versenyeként értelmezik, amelynek keretében az egyik fél támad, a másik meg védekezik. A gonosz hackerok pedig figyelik ezt. A valóságban nemzeti szinten a kiberbiztonságnak műszaki és ideológiai aspektusa van. Az Egyesült Államok nagyon jól felfogta a világhálóra gyakorolt hatás elvi fontosságát. Az Egyesült Államok a közelmúltban megalakította a „digitális külkapcsolatok csapatát”, amelynek tagjai a társalgási hálózatokban az amerikai álláspontot védik” – hangsúlyozta Jevgenyij Poliscsuk professzor.²⁰⁰

Oleg Demidov politológus véleménye szerint: *„évről évre nő az infrastruktúra számítógépes technológiáktól való függése az iparilag fejlett országokban: digitális rendszerekre való áttérés a vízenergiában, az atomenergiában, a közúti, légi- és a vasúti közlekedésben. Ahol számítógép van, ott a veszély is nagy, hogy feltörik annak rendszerét, amely technológiai katasztrófához vezet.”* A modern világban a legveszélyesebb fegyver, egy profi hacker kezében lévő számítógép. A kiberbiztonság biztosítására egyes országok azt javasolják, hogy használjuk a már meglévő nemzetközi jogi normákat. Más szóval, *„egy nemzetközi rendszer kiépítéséről van szó, amely biztosítja az információs világ technológiáinak biztonságát. Ezzel a problémával a NATO tallinni kiberbiztonságért*

²⁰⁰ *Russia steps up fight against cyberterrorism, 2011. 01. 30.*

<http://en.rian.ru/russia/20101012/160922978.html> (letöltve: 2013. 10. 08.)

felelős központja foglalkozik. A konfliktusos helyzeteket a már meglévő nemzetközi jogi szabályozások alapján oldhatják meg²⁰¹ – állítja Oleg Demidov.

Az Inforus cég elnöke, Andrej Maszalovics véleménye szerint: „jelenleg a kiberfegyver oly hatalmas erő, hogy egész régió energetikai rendszerét, vasúti és légiközlekedési struktúra elemeit is üzemképtelenné teheti. Ez már nem elméleti dolog, hanem reális veszély. Véleményem szerint, ki kell dolgozni külön nemzetközi egyezményeket, amelyek szabályoznák a kibertechnológia használatát az országok számára. Ezt a lehetőséget támogatja Oroszország. Ennek a módszernek megvannak az előnyei és a hátrányai is. Az előnye, hogy a kiberfegyverek kidolgozásának és használatának teljes betiltását kell elérni. A hátránya – emberek milliárdjainak van hozzáférése a kibertechnológiákhoz. A dzsint kiengedtük a palackból és visszazárni oda – ez igen nehéz feladat.”²⁰²

Dmitrij Rogozin még az Oroszországi Föderáció NATO nagyköveteként 2011-ben nemegyszer a nyilvánosság előtt kifejtette, hogy az orosz diplomácia minden erőfeszítése ellenére sem sikerült ezzel kapcsolatos témakör napirendre tűzése/vétele a lisszaboni Oroszország-NATO csúcstalálkozón. Partnereinkről, e tényeket megelőzően tudni lehetett, hogy erről a kérdéskörrel nem akarnak megbeszéléseket folytatni. Erről először és később többször is nyilatkozott a jelenlegi orosz katonai-ipari komplexum elnöke. A nyilatkozat rövid tartalmát ismertetjük

Emlékeztetett arra is, hogy 2009-ben Strasbourgban és Keelben a NATO terminológia kiberbiztonságot a kibervédelemre cserélte. A volt NATO nagykövet szerint „a natosok előszeretettel használják a védelem fogalmat/szót, amikor támadásról beszélnek.” Megemlíti Dmitrij Rogozin, hogy 2009-ben a NATO egy év alatt a kiberprogramokra a korábbi költségvetési fejezetét 40-szeresére növelte, és hogy kire is gondoltak egy kibertámadás objektumaként, nem nehéz kitalálni.

Dmitrij Rogozin következetes volt, mert egy évvel a lisszaboni tanácsülés után már miniszterelnök-helyettesként Moszkvában megbeszéléseket kezdeményezett az orosz kibernetikai parancsnokság létrehozásának érdekében. Kitartott amellett, hogy sürgősen létre kell hozni az állami infrastruktúra és a

²⁰¹ *A kibertámadások korszaka: az erős államok gyengesége.*

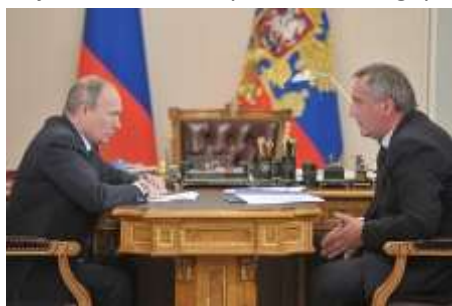
http://hungarian.ruvr.ru/2013_09_06/A-kibertamadasok-korszaka-az-eros-allamok-gyengesege/ (letöltve: 2013. 10. 10.)

²⁰² [http://hungarian.ruvr.ru/20130723/Oroszország megszabja a kiberbiztonsági játékszabályokat](http://hungarian.ruvr.ru/20130723/Oroszország%20megszabja%20a%20kiberbiztonsagi%20jatekszabalyokat) (letöltve: 2013.10.10.)

fegyveres erők információs biztonságát. Az amerikai DAPRA mintájára javaslatot tettek a Perspektivikus Kutatások Alapjának/Fond létrehozására.

Hamarosan, az elhangzott kezdeményezések hatására az Oroszországi Föderáció Fegyveres Erő Vezérkara bekapcsolódott a kiberparancsnokság létrehozásába, és ekkor érkezett egy közlemény az Egyesült Államokból, miszerint a Pentagon követeli a 2013 évi költségvetésben a kiber csapatok létszámának 900 főről 4900 főre való emelését. Ez az információ lökést adott az orosz fejlesztéseknek, és magasabb sebességű üzemmódra kapcsolva hozzáálltak a munkának. Ezt erősítette fel nagymértékben a E. Snowden által nyilvánosságra hozott információ halmaz, és a körülötte kialakult „túrhetetlen állapot” is, amely rávilágított arra hogy az Egyesült Államok „különleges szolgálatait” a világ bármely országának számítógépes- és más kommunikációs hálózatát ellenőrzi/felügyeli. *„Ebben semmi meglepő nem volt a szakembereink számára, de ez most a puszta valóság, ami felszínre került, mivel más forrásokból erről már régebről értesültünk. Ez a tény ami aktív tevékenységre ösztönöz. A kibernetikai parancsnokság létrehozásában nem kételkedünk, a megvalósulás folyamatát felgyorsítottuk.”*

Van két fontos dolog, ami ezt a folyamatot akadályozhatja. Az egyik ha a fejlesztéseket import számítógép technológiák felhasználásával végezzük,



ebből következik, hogy szükség van saját fejlesztésű radioelektronikára, és nemzeti elektronikai gyártástechnológiára különben az információs hálózatunk kívülről támadható kiberfegyverré válhat.

2. ábra: Elnöki megbeszélés / Az Orosz föderáció és az orosz hadiipari komplexum

elnökének megbeszélése²⁰³

A másik fontos lépés a saját szoftver, azaz felhasználói programbiztosítás kell a erőszak-szervezetek részére, ezen a területen az utóbbi időszakban már eredményeket értünk el. Így a hírekből tudhatjuk, hogy az Astra Linux Special Edition program a Minőség-tanúsítványt megszerezte. Oroszországban jelenleg ez az egyetlen operációs program és mind a három – az Oroszországi Föderáció Biztonsági Szolgálat, Védelmi Minisztérium és a Technikai Export Ellenőrzési

²⁰³ <http://en.ria.ru/> (letöltve: 2013.10.10.)

Föderációs Szolgálat– információvédelmi tanusító rendszerében sikeres volt. Ez a rendszer biztosítja a korlátozott felhasználást, ellenőrzi, korlátozza felhasználói jogokat és biztosítja a titkos ügyvitelben a „Szigorúan Titkos” államtitkok titokgazdáinak műveleteit, tevékenységét. Az Oroszországi Föderáció Fegyveres Erőinél a programot rendszeresítették. Ugyanakkor, a védelmi iparban dolgozó fejlesztőmérnökök elmondhatják, hogy alapjában import számítógép elembázissal dolgoznak. A mikroáramkörök külfölről történő beszerzése miatt lehetetlenség megjósolni, hogy a légi-kozmosz hadműveletek elrendelésének pillanatában a saját műholdak infokommunikációs rendszere kinek a részére továbbítja az adatokat. Ezeknek a problémáknak a megoldásáról jelenleg semmi sem hallható és tudható.²⁰⁴ A tanulmánynak ebben a részében ismertetjük a dokumentum legfontosabb megállapításait, valamint a nemzetközi információs biztonság orosz értelmezését, a jogi szabályozás, a nemzetközi együttműködés lehetőségét, a megvalósítás orosz javaslatait.²⁰⁵

Alapvetések

A jelenlegi meghatározások az Oroszországi Föderáció stratégiai tervezésének részét képezik. Az alapvetések a nemzetközi információs biztonság területén megjelenő főbb veszélyeket fogalmazzák meg. Ezek meghatározzák az Oroszországi Föderáció nemzetközi információs biztonságának célját, feladatait, irányait, a működtetés mechanizmusát és megvalósítását.

A jogi háttér az alapvetések megfogalmazásához az Oroszországi Föderáció Alkotmánya, az aláírt nemzetközi szerződések, a korábban elfogadott, és a témához kapcsolódó törvények, valamint az Egyesült Nemzetek Szervezetének Alapokmánya. A dokumentumban foglalt alapvetések megerősítik az Oroszországi Föderáció Nemzeti Biztonsági Stratégiájában megjelenő tételeket a 2020-ig terjedő időszakra. A dokumentum az Oroszországi Föderáció információ

²⁰⁴ *Кибервойска готовят к боям. Но они могут оказаться неподконтрольны российскому командованию*

http://nvo.ng.ru/realty/2013-10-11/2_red.html (letöltve: 2013. 10. 18.)

²⁰⁵ *A szerzők az orosz nyelvű dokumentum legfontosabb megállapításait (tartalmi kivonatát) ismertetik magyar nyelven azzal a szándékkal, hogy a témával bővebben foglalkozó kutatók a dokumentumot megismerhessék. Ezzel a tanulmánnyal kívánjuk alátámasztani a hadtudományi kutatások egyik fontos eredményét, miszerint a jövő katonai műveletei a légi-kozmosz térben és a kibertérben fognak elkezdődni.*

biztonságának doktrínáját, a külpolitikai koncepciókat és más, stratégiai tervezési célkitűzéseket tartalmazza.

A dokumentum rendeltetése

- a) A dokumentumban megfogalmazott orosz javaslatok nemzetközi fórum elé terjesztése, az információbiztonság nemzetközi rendszerré történő kialakításához. Beleértve a jogalkotás, a szervezési és más formák kifejlesztését.
- b) Nemzetközi célprogramok kialakítása a nemzetközi információs biztonság területén, amelyekben az Oroszországi Föderáció részt vesz, az állami és föderációs célprogramok kidolgozásával.
- c) Az Oroszországi Föderáció állami politikájának realizációja a nemzetközi intézményközi együttműködésben, a nemzetközi információs biztonság területén.
- d) A technológiai szintű egyensúly elérése és fenntartása a világ vezető hatalmaival az információs és kommunikációs technológiák széles körű alkalmazásával, valós gazdasági szektorban.

A nemzetközi információs biztonság orosz értelmezése

„A nemzetközi információs biztonság alatt a globális információs tér olyan állapotát értjük, ahol kizárt az emberi jogok, a társadalom, az információs területek megsértése az állam törvényeivel, romboló és ellentétes ráhatás a kritikus nemzeti infrastruktúra elemeire”²⁰⁶ – fogalmazznak orosz szakértők.

Az Oroszországi Föderáció a nemzetközi információs biztonság értelmezése (orosz fogalma) közreadásával kívánja a két- és többoldalú tárgyalások hatékonyságát elősegíteni. Más szóval, világossá tette, hogy a jövődő tárgyalásokon az orosz szakértők hogyan értelmezik az információs biztonság és a nemzetközi információ biztonság elméleti, gyakorlati, technikai és technológiai tartalmát, kérdéseit.

²⁰⁶ *Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. 1. oldal.*
<http://www.scrf.gov.ru/documents/6/114.html> (letöltve: 2013. 10. 08.)

Az Oroszországi Föderáció állami politikájának céljai és feladatai

A dokumentumnak ebben a részében megfogalmazásra került a nemzetközi jogi környezet kialakításában való részvétel igénye. Továbbá, hogy az Oroszországi Föderáció részt kíván venni a többoldalú, a regionális és a világméretű rendszerek kialakításában.

Szükségesnek tartják olyan feltételek megteremtését, amelyek korlátozzák az információs és kommunikációs eszközök szabad kereskedelmét ellenséges tevékenységek és agresszív cselekmények esetén. Különösen azokban az esetekben, amikor az állami szuverenitás megsértése, a területi egység megbontása, a nemzetközi biztonsági helyzet fenyegetése a célpont.

Az Oroszországi Föderáció részt kíván venni az ellentevékenységek feltételei megteremtésében, az információs és kommunikációs technológia használatának területén, nemzetközi szinten is. Ezzel együtt az Oroszországi Föderáció szükségesnek tartja az államok technológiai szuverenitását, továbbá az egyenlőtlenségek megszüntetését a fejlett és fejletlen országok között a nemzetközi együttműködés hatékonysága érdekében.

Az Oroszországi Föderáció állami politikájának fő irányai

Az Oroszországi Föderáció állami politikájának fő irányait az információs és kommunikációs technológiai rendszerek kialakításában két- és többoldalú, regionális és világméretű szinteken jelölték meg, amelyek lényege a következő:

Az orosz kezdeményezések elfogadtatása, majd a kidolgozás feltételeinek megteremtése az ENSZ Biztonsági Tanácsában a nemzetközi információ biztonság területén. Közreműködés az ENSZ dokumentumok megszerkesztésében más tagállamok szakértői csoportjaival, elsősorban a nemzetközi információs és kommunikációs technológia alkalmazásának szabályai kialakításában, megszerkesztésében. Szükségesnek tartják a két- és többoldalú szakértői tanácskozások rendszeres megtartását az együttműködés, az együttes tevékenység sikere érdekében.

Az Oroszországi Föderáció a nemzetközi információ biztonsági rendszerek kialakítása során a Sanghaji Együttműködési Szervezet tagországaival, a Független Államok Közösségével és a BRICS országokkal kíván együttműködni. Ugyanakkor nem zárkózik el más országoktól és szervezetektől sem az együttműködés kérdésében. Az orosz kezdeményezések sikeres végrehajtása érdekében állami szinten szakértői csoportokat alakítanak ki, tudományos igényű kutatásokat folytatnak, felhasználva a hazai és nemzetközi tapasztalatokat is.

Az Oroszországi Föderáció állandó és a részt vevők számára nagyon hasznos párbeszédet kíván folytatni a nemzetközi információs biztonságot fenyegető kihívások és veszélyek kezelésének lehetőségéről, az ellentétekenységet biztosító információs és kommunikációs technológiák felhasználása jogi háttéréről. Hozzá kívánnak járulni mind elméletben, mind a gyakorlatban a regionális és globális rendszerek kiépítéséhez.

Az Oroszországi Föderáció a hazai információs és kommunikációs technológiák védelme érdekében a belső intézkedéseken túl, szükségesnek tartja az államok közötti biztonsági és jogi szabályok megalkotását, a szuverenitás megtartása mellett.

Az állami politikai megvalósításának folyamata

Az állami politika (a nemzetközi információs biztonság) megvalósítása érdekében a végrehajtó hatalom szerveinek tevékenységére van szükség, a föderális jogállam viszonyai között. Ebben a tevékenységben az Oroszországi Föderáció valamennyi állami szintű szervezete (Elnök, Parlament, Elnöki Adminisztráció stb.) részt fog venni.

Befejezésül, a dokumentumhoz kapcsolható legfrissebb információ:

Az Oroszországi Föderáció Védelmi Minisztériumából egyre gyakrabban elhangzó közlemény, hogy 2014-ben az Oroszországi Föderációban a Védelmi Minisztériumban megjelenik a Kibernetikai Parancsnokság. Más közlemények pedig arról szólnak, hogy egy új struktúra megjelenése várható, mint amit az Egyesült Államokban, Izraelben és a Kínában már rendszeresítettek. A rendeltetése az állam biztonsága és védelme a virtuális térben, mind béke mind háborús időszakban. Nem hivatalos források egyre többször említik meg, hogy a kibernetikai parancsnokság létrehozásával kapcsolatos programok előrehaladott állapotban folynak.

A katonák jelentős lépést tettek a virtuális világba 2007-ben, amikor is a Barksdale AFB légi bázison (Louisiana) – „ideiglenes jelleggel” – létrehozták az US AF alárendeltségében az első kibernetikai parancsnokságot. A kipróbált amerikai mintára analóg módon hozták létre az orosz struktúrát/szervezetet.

Előzetesen a kibernetikai parancsnokság az Oroszországi Föderáció Védelmi Minisztériuma főcsoportfőnökség szinten szerveződne, de feladatait a Légi-koszmikus Parancsnokság állományában hajtaná végre. Később, mint önálló

fegyvernem működne. Tehát eljött az ideje, hogy az Oroszországi Föderáció Fegyveres Ereje is belépjen a virtuális térben folyó küzdelembe.²⁰⁷

A 21. században az egyes országok számítógépes, információs és kommunikációs struktúrája rohamos fejlődésének szükséges velejárója, hogy az informatikailag fejlettebb országok egyre nagyobb veszélynek vannak kitéve, hiszen a számítástechnika és az Internet a világgazdaság civilszférájától, a katonai szervezeteken keresztül, egészen a kormányzatokig mára csaknem mindenhol jelen van. Célpontnak számíthatnak a bankok, a közlekedés, a pénzügyi rendszerek, a távközlés, a rendőrség, a katonai létesítmények, a haditechnikai eszközöket gyártó vállalatok, az energiaellátás, melyek esetleges támadása során az állami infrastruktúra is érzékenyen károsodhat, de célpont lehet akár az otthoni személyi számítógépünk is.

Az észak-írországi G8-találkozón az Egyesült Államok és Oroszország közös nyilatkozatban tájékoztatta a világ közvéleményét a kettejük közt létrejött kiberbiztonsági megállapodásról – írta a The Washington Post.

„Tudatában vagyunk annak, hogy a számítógépes technológiát érintő fenyegetések politikai-katonai és bűnügyi fenyegetéseket ugyanúgy tartogatnak, mint terrorista-jellegűeket, valamint annak, hogy ezek a legsúlyosabb helyi és nemzetközi méretű kihívások közé tartoznak, melyekkel a XXI. században kell szembesülnünk” – mondta Obama amerikai és Putyin orosz elnök a közös nyilatkozatban.²⁰⁸

Az idézett amerikai és orosz állásfoglalások, valamint a doktrína tartalma alapján különös gondot kell fordítani információs társadalmunk polgárainak az informatikai biztonság területén való megfelelő oktatására a hazai egyetemeken, hiszen nem csak az informatikai szakembereknek van szüksége ezekre az ismeretekre, hanem a laikus felhasználóknak is, közös informatikai biztonságunk megteremtése érdekében.

²⁰⁷ *Кибервойска готовят к боям. Но они могут оказаться неподконтрольны российскому командованию.*

http://nvo.ng.ru/realty/2013-10-11/2_red.html (letöltve: 2013. 10. 18.)

²⁰⁸ *U.S. and Russia sign pact to create communication link on cyber security (szerző:.....)*

http://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html (letöltve: 2013. 10. 10.)

Irodalomjegyzék

- Gyányi Sándor: Cyber-támadások elleni védekezés és a válaszcsepások lehetőségei
Hadmérnök III. évfolyam 2. szám 2008. június,
http://hadmernok.hu/archivum/2008/2/2008_2_gyanyi.pdf (letöltve: 2013. 10. 08.)
- Haig Zsolt – Kovács László: Fenyegetések a cybertérből
Nemzet és Biztonság 2008. május, 61-69. oldalak
- Kovács László: Az információs terrorizmus eszköztára
Hadmérnök Robothadviselés 6. Tudományos Szakmai Konferencia 2006. november 22.
http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html (letöltve: 2013. 10. 08.)
- Kovács László: Információs terrorizmus: cyber bűnözés és cyber terror
<https://hactivity.com/hu/letoltesek/archivum/15/>
- The Tallinn Manual
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Eston.
<http://www.ccdcoe.org/249.html> (letöltve: 2013. 10. 08.)
- Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials.
<http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html> (letöltve: 2013. 10. 08.)
- Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года.
<http://www.scrf.gov.ru/documents/6/114.html> (letöltve: 2013. 10. 08.)
- Политика РФ в обеспечении информационной безопасности.
<http://newsland.com/news/detail/id/1224250/> 2013. 10. 10.
<http://www.infosecurity.ru/> (letöltve: 2013. 10. 10.)
- Póserné Oláh Valéria: Számítógép-hálózati támadások.
Hadmérnök Robothadviselés 6. Tudományos Szakmai Konferencia 2006. november 22.
http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html (letöltve: 2013. 10. 08.)