MMXIII. I. ÉVFOLYAM I. SZÁM

NEMZETBIZTONSÁGI SZEMLE

KÜLÖNLENYOMAT

NEMZETI KÖZSZOLGÁLATI EGYETEM
NEMZETBIZTONSÁGI INTÉZET
BUDAPEST

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

Koós Gábor – Szternák György

Absztrakt

A dokumentumban az Oroszországi Föderáció szempontjából négy fő kiberveszélyt emelnek ki a szakemberek.
- Az első: az információs és kommunikációs technológiák, eszközök alkalmazása információs fegyverként katonai és politikai célok elérése érdekében.
- A második: az említett technológiák, eszközök alkalmazása a terrorizmus céljai megvalósítására.
- A harmadik: a kiberbűnözés. Egyebek között a törvénytelen hozzájutás a számítógépes információhoz, kártékony programok kidolgozása és terjesztése.
- A negyedik: veszélyként emelték ki az internetes technológiák, eszközök alkalmazását az állam belügyeibe való beavatkozáshoz, a közrend megzavarásához, az erőszakra felhívó eszmék terjesztéséhez.
Az Oroszországi Föderáció szövetségeseivel karöltve – elsősorban a Sanghaji Együttműködési Szervezet, a Független Államok Közössége és a BRICS[195] államok tagjaival együtt – száll szembe ezekkel a kihívásokkal.

Kulcsszavak: *kiberveszélyek és válságok; információs és kommunikációs technológiák; kiberterrorizmus; jogi szabályozás lehetősége; az együttműködés lehetőségei.*

Abstract

Principles of State Policy of the Russian Federation in the field of international information security in 2020
Russian Policy on Cyber Defense the authors provide review Principles of State Policy of the Russian Federation in the field of international information security in 2020. The security environment of the twenty-first century has changed remarkably. The Russian Federation and other modern societies and economies are wired together by networks, cables and the IP addresses of our computers.
The authors analyzed General Provisions; the purpose and objectives of the state policy of the Russian Federation; The main directions of the state policy and Mechanisms for the implementation of the state policy of the Russian Federation.

[195] *Brazília, Oroszországi Föderáció, India, Kínai Népköztársaság, Dél-Afrika*

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.

[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 fordulópontot 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://ujszo.com/online/kulfold/2012/10/17/eloterbe-kerulhet-a-kiberhadviseles (letöltve: 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 hackerek 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, „e*gy 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 meg[201] – 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 kérdéskörről 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.

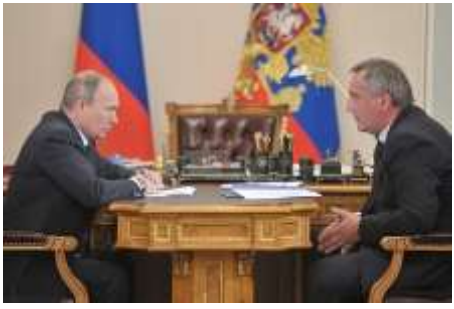
Dmitrij Rogozin következetes volt, mert egy évvel a lisszaboni tanácsülés után már miniszterelnök-helyettesként Moszkvában megbeszéléseket kezdeményezett az orosz kibernetikai parancsnokság létrehozásának érdekében. Kitartott amellett, hogy sürgősen létre kell hozni az állami infrastruktúra és a

[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 Oroszorszag megszabja a kiberbiztonsagi jatekszabalyokat (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 kibercsapatok létszá-mának 900 főről 4900 főre való emelését. Ez az információ lökést adott az orosz fejlsztéseknek, és magasabb sebességű üzemmódra kapcsolva hozzáláttak a munkának. Ezt erősítette fel nagymértékben a E. Snowden által nyilvánosságra hozott információ halmaz, és a körülötte kialakult „tűrhetetlen állapot" is, amely rávilágított arra hogy az Egyesült Államok „különleges szolgálatai" 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 régebbről 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 rádioelektronikára, és nemzeti elektronikai gyártástechnológiára különben az információs hálózatunk kívülről támadható kiberfegyverré válhat.



2. ábra: Elnöki megbeszélés / Az Orosz föderáció és az orosz hadiipari komlpexum elnökének megbeszélése[203]

A másik fontos lépés a saját szoftver, azaz felhsználói 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-tanusítványt megszerezte. Oroszországban jelenleg ez az egyetlen operációs program és mind a három – az Oroszországi Föderáció Biztonsági Szolgálata, Védelmi Minisztérium és a Technikai Export Ellenőrzési

[203] *http://en.ria.ru/ (letöltve: 2013.10.10.)*

Föderációs Szolgálat– információvédelmi tanusító renszerében 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-kozmikus hadműveletek elrendelésének pillanatában a saját műholdak info-kommunikációs rendszere kinek a részére továbbítja az adatokat. Ezeknek a problémáknak a megoldásáról jelenleg semmi sem hallaható 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-kozmikus 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] – fogalmaznak 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 jövendő 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 ellentevékenységet biztosító információs és kommunikációs technológiák felhasználása jogi hátteréről. 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 hoznák létre az orosz struktúrát/szervezetet.

Előzetesen a kibernetikai parancsnokság az Oroszországi Föderáció Védelmi Minisztériuma főcsoportfőnökség szinten szerveződne, de feladatait a Légikozmikus 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 válaszcsapások 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://hacktivity.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.)