Cser Orsolya

Biztonságunk egyik záloga a hatékony civil-katonai együttműködés

A biztonság az egyik legalapvetőbb emberi szükséglet, amely sohasem önmagában, hanem mindig a veszélyhelyzetre történő reagálásként jelenik meg. Egy állam belső biztonsága a politikai, társadalmi és a gazdasági rend megóvását, a veszélyek elhárítását jelenti. Kérdéskörébe tartozik a gazdasági terrorizmus egyik eszköze, a kibertámadás is. Ez utóbbi veszélyhelyzet fontos kérdés a cikk lényegét tekintve, mivel annak célja a pénzügyi válságok kezelése, az ezzel kapcsolatos banki feladatok, valamint a NATO 2012. évi válságkezelési gyakorlata (CMX 12).

A pénzügyi válságok [1] témakörének és azok kezelésének szorosan kapcsolódó területe a pénzintézeteknél történő értékmegőrzés.

A védelem- és hadigazdaságtan fogalmi rendszere, a szemlélet módja alkalmazható egy látszólag távoli területen, mint a bankszféra, amely értékeink védelmében tevékenykedik.

A gazdasági és a katonai hatalom, valamint növekedés egymással szorosan összefüggő fogalmak, e két terület segíti, előrébb viszi, illetve rossz esetben hátráltatja egymást.

A külső biztonság a nemzetközi rendszer tagjai közötti államközi és egyéb kapcsolatok összességét jelenti, vagyis a szövetségi politika, a katonai szövetségek és a nemzetközi szervezetek működésének garanciáját, melyek tekintetében elengedhetetlen, hogy a különböző országok, térségek egységes, korábban egyeztetett gazdaságpolitikát folytassanak.

Egy nemzet biztonságának alapvető feltételei

A biztonság [2] alapfeltétele a gazdaság zavartalan működése és a fejlődés feltételeinek biztosítottsága, melynek gazdasági szempontjai:

- a gazdasági stabilitás biztosítottsága (hatékony gazdasági szerkezet, biztonságos külgazdasági kapcsolatok, szabad verseny);
- a stabil pénzügyi feltételek megteremtése (mérsékelt infláció, rendezhető adósság és hitelállomány, ösztönző kamatrendszer).

A gazdasági háborúk – melyek felfoghatóak a gazdasági szankciók sorozataként is – kisebb-nagyobb mértékben végigkísérték a történelmet. Olyan konfliktusos viszonyok

voltak országok vagy azok csoportjai között, melyben a szemben álló fél ellen elsősorban (politikai célok elérése érdekében) tudatos és célirányos kár, gazdasági veszteség okozására irányultak.

A történelemben előforduló példák alapján egyértelművé vált a biztonság komplex jellege, globalitása. A biztonság szorosan összefügg a veszély, a kihívás vagy a fenyegetés fogalmával. A Hadtudományi Lexikon megfogalmazása szerint biztonság *„…az egyéneknek, csoportoknak, országoknak, régióknak (szövetségi rendszereknek) a maguk reális képességein, és más hatalmak, nemzetközi szervezetek hatékony garanciáin nyugvó olyan állapota, helyzete (és annak tudati tükröződése), amelyben kizárható vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak az ellene való eredményes védekezés feltételei*".[1] Ezek alapján a biztonság összetett fogalom és állapot, amelynek tartalma valamilyen formában érinti a társadalom valamennyi tagjának az életét. Az egyén és a társadalom biztonsága egymástól szétválaszthatatlan, szorosan összefüggnek.

A biztonságpolitika új, komplex meghatározása szerint a biztonság elemei a következők:

– a környezeti (ökológiai);
– a társadalmi (jogi, szociális);
– a politikai (diplomáciai);
– a gazdasági;
– az informatikai;
– a katonai.

A gazdasági biztonság [3] nagyon szoros kölcsönhatásban áll az államok szűkebb és tágabb környezetével. Azon okból, mivel létük érdekeit közvetlenül érintik, a gazdasági jellegű kihívások a társadalmak létét alapjaiban befolyásolják.

A legalapvetőbb igény az, hogy a társadalmat alkotó egyén emberi élethez méltó életkörülményei megteremtődjenek.

Az 1990-es években térségünk országai drámai gyorsasággal voltak kénytelenek átalakítani gazdasági-külgazdasági kapcsolataikat és hozzá kellett fogni a működő piacgazdaság kiépítéshez.

A gazdasági biztonságot fenyegető válság folyamatának időperiódusai:

– Múlt: kiindulópontok, tevékenységek, reflexek.
– Jelen:
  = belső hatás: a határidő és az események összetorlódása;
  = külső hatás: intézményi és közvéleményi reagálások.
– Jövő: új elvárások, folyamatok és magatartások "normális üzletmenet" új szabályokhoz és reagálásokhoz igazodva.

A válságok és kezelésük jellemzői

A válság [4] koncentrálja az események hatását, felerősíti az országban élő emberek, vagy egy nemzet tagjainak reagálását. A figyelem a válságba került szervezetre

1 Hadtudományi lexikon A–L. (Szabó József főszerk.) Budapest, 1995. Magyar Hadtudományi Társaság. 144. o.

koncentrálódik, amelynek változása elkerülhetetlen. Jelen esetben egy ország lakosságának többségét érintheti a cikkben szimulált nemzeti (országos) válság, ha terrorizmus által tervezett események megvalósulnak.

A válságot megelőző időszakot az előjelek stádiumának is lehet nevezni, amikor a figyelmeztető jelek megsokasodnak. Gyakran meg lehet határozni azt a fordulópontot, amely után a válság már elkerülhetetlen.

A válságkezelés alapvető területei a következők:

– a preventív (előrejelzés és kikerülő elhárítás, megelőzés);
– az aktív (az észrevehető jelek szerint biztosan bekövetkező válságok növekedésének és terjedésének megakadályozása, visszaszorítása);
– a reaktív (a kialakult válságot megszüntető stratégia és intézkedések, azaz válságkezelő politika).

A problémakezelés részekre osztható fel, melyek a következők:

– a diagnózis (kudarc- és sikertényezők felismerése);
– a helyzetértékelés;
– a terápia (operatív intézkedések a problematikus eltérés megszüntetésére).

Amennyiben az ellenlépések nem hatékonyak, a krónikus stádium következik, ahol a válság tovább szélesedik, súlyos veszteségek következnek be, és a megoldásra kevés esély van.

A NATO CMX-gyakorlatainak jelentősége

A válságok szélesedésének megelőzésére tervezik és hajtják végre a NATO CMX gyakorlatait minden évben, amikor szimulációval előidéznek valósnak tűnő helyzeteket, melyek válsághelyzeteket okozhatnak.

Fontos szempont a banki biztonság, melyet adott esetben kibertámadás érhet, ezért szükségszerű, hogy a bankok tekintetében a megfelelően biztonságos környezet biztosítva legyen. [5] Ennek érdekében a biztonságot be kell építeni, növelni szükséges az információs rendszerekben.

A rendkívüli események bekövetkezésének okai lehetnek szándékos vagy óvatlan magatartás (belső), illetve váratlan események összessége (külső), mint például egy természeti csapás. [6] Az adott magatartás, esemény következtében az élet és vagyonbiztonság súlyos veszélybe kerül, amely akadályozza, vagy megbénítja a bank normális működését. [7] A rendkívüli események megelőzése, megakadályozása, a keletkezett hátrány mértékének csökkentése érdekében a helyi katonai és rendőri szervekkel szoros együttműködést kell kialakítani.

Összességében a bankbiztonsági tevékenység tehát mindazon tervezési, szervezési, irányítási, végrehajtási és ellenőrzési feltételekről való intézményes gondolkodás, amely a pénzintézet saját tulajdonú tárgyainak, értékeinek, valamint az alkalmazottak és az ügyfelek biztonságának védelmét szolgálja.

Az új Nemzeti Biztonsági Stratégia [8]

2013. február 8-án a Kormány elfogadta Magyarország új Nemzeti Biztonsági Stratégiáját (NBS), melyben a nemzeti érdekek, a hazánk által is deklarált alapvető

demokratikus értékek, valamint a biztonsági környezet elemzése alapján meghatározza azokat a célokat, feladatokat és eszközöket, amelyekkel az EU- és NATO-tag Magyarország a 21. század elejének nemzetközi politikai, biztonsági rendszerében érvényesíteni tudja érdekeit. Ebben szerepelnek azon biztonsági elemek is, melyek egy pénzügyi krízis esetében (például kibertámadás az ország bankrendszere ellen) fontos szempontok annak érdekében, hogy a veszélyhelyzetet megszűntessék.

Az új NBS kidolgozását és elfogadását időszerűvé tette az, hogy a legutóbbi, 2004-es hasonló dokumentum elfogadása óta jelentős változások történtek globális téren és hazánk közvetlen biztonsági környezetében, valamint az euro-atlanti integrációs szervezetekben is: életbe lépett az Európai Unió Lisszaboni Szerződése (2009), a NATO pedig új Stratégiai Koncepciót fogadott el (2010). Mindez időszerűvé tette a magyar dokumentum felülvizsgálatát, követve az EU- és NATO-tagállamok gyakorlatát is.

Az új NBS ezért számos tekintetben folyamatosságot hordoz az előző, 2004-es stratégiával összehasonlítva, de ugyanakkor épít a releváns nemzetközi szervezetek, valamint a hazánkhoz hasonló méretű és adottságú szövetséges országok hasonló dokumentumaira is.

Az NBS célja, hogy iránymutatást nyújtson a kormányzati szektor számára biztonságpolitikai – azon belül pénzügyi – kérdésekben. Filozófiájában ezért átfogó és összkormányzati megközelítést követ. Az ország biztonsága azonban mindenekelőtt közügy, ezért a stratégia egyik feladata, hogy a szakmai körökön túl a mindennapi életben is hasznosítható támpontot nyújtson a hazai biztonságpolitikai gondolkodásban.

A Nemzeti Biztonsági Stratégiában megfogalmazódnak mindazon tényezők, melyek a pénzügyi biztonságot meghatározzák az egyes nemzetállamok gazdaságának működése tekintetében:

– pénzellátás – bankválság esetén a készpénzellátás korlátozása;
– azonnali betét kivétel pánik (ld. Postabank-botrány, 1997. február);
– pénzügyi tartalék – a krízishelyzetek esetére;
– pénzügyi moratórium – pénzintézetekből történő pénzkivétel korlátozása.

Mindezek fontosságát felismerve a NATO Miniszteri Irányelveknek (2012) megfelelően azon szakembereket, akiknek a válságkezelésre jó szaktudásuk és képességük van, együtt kell tartani, időnként gyakorlatoztatni, és ez alatt szimulációs döntéseket meghozatalára bíztatni őket. E célt szolgálják a Crisis Management Exercise (CMX) gyakorlatok, melyeket a Honvédelmi Minisztérium által vezetett szakember-gárdának évente el kell végeznie, év közben pedig az adott témakörben történő folyamatos felkészülés jegyében kell telnie a közös munkának.

Annak a tudásbázisnak, amely ezen tevékenységeken keresztül az évek során kialakul, adott válság vagy krízishelyzet esetében azonnal alkalmazhatónak kell lennie.

A NATO 2012. évi válságkezelési gyakorlata [9]

Az első CMX-gyakorlatot 1992-ben tartották meg, az idei a tizennyolcadik alkalom. A tervezésben és a végrehajtásban a tagállamok közül – Izland kivételével – mind a huszonhét tagország részt vesz, a NATO-partnerség keretében meghívást kapott Finnország és Svédország, továbbá a Nemzetközi Atomenergiai Ügynökség (IAEA), a

Nemzetközi Vöröskereszt (ICRC), illetve most először az Európai Külügyi Szolgálat (EEAS) képviselője. Magyarország a NATO-hoz történő csatlakozása, 1999 óta vesz részt a gyakorlaton.

A 2012. évi CMX-gyakorlat tárgya a NATO 2012. évi válságkezelési gyakorlatához (CMX 12), és egyben a Cyber Coalition 2012 (CC 2012) elnevezésű kibervédelmi gyakorlatához kapcsolódó nemzeti feladatok végrehajtása, melyhez a felhatalmazást a védelmi felkészítés egyes kérdéseiről szóló 1182/2012. (VI. 1.) Korm. határozat 1. számú melléklet 5. bekezdés a) pontja adja. A szövetségi szintű célkitűzések között a terrorizmus és proliferáció mellett megjelenő új kihívás, a kibertérből érkező támadások elleni kollektív fellépés gyakorlása volt, amely feladat a gyakorlaton is szerepelt.

A CMX 12 gyakorlaton a 27 tagország és a két partnerország képviseletében mintegy 2500 fő vett részt. A gyakorlat elképzelt földrajzi környezetben játszódott, annak menetét a közelmúltban bekövetkezett események és a reális kockázatok felmérése alapján tervezték meg.

A NATO szerepvállalásának elemei a következőkben összefoglalhatók:
- NATO-szerepvállalás területen kívüli konfliktusok kezelésében.
- Hagyományos és új típusú szerepvállalás.
- Új típusú biztonsági kihívások (együttes) megjelenése.
- A terrorizmus és proliferáció elleni fellépés, valamint a kiberbiztonság, mint napjaink kiemelt biztonsági feladatai.
- Együttműködés más nem nemzetközi szervezetekkel.
- Partnerországok bevonása a művelet tervezésébe és végrehajtásába.

Magyarország érdekeltségei a szimulációban kijelölt sziget és ország vonatkozásában:
- Diplomáciai viszony, de számottevő kapcsolatok nélkül.
- Egyik országnak sincs diplomáciai képviselete Magyarországon.
- Vitatott területeken érdekeltségek, és az ebből fakadó konfliktusok.
- Tevékenység: 50 fő magyar szakértő, olaj- és gáz-feltárások és -kitermelés helyi munkásokkal.
- 15 fős magyar rendőri kontingens.
- Szélsőséges csoportok magyarországi jelenléte (térségbeni menekültekkel érkeztek).
- Csoportok támogatottsága a szigetről érkezett hallgatók körében.
- Potenciális támadások kritikus infrastruktúrák ellen Magyarországnak a szigettel kapcsolatos politikája megváltoztatása érdekében.

A CMX 12 gyakorlat céljai, tevékenységi körei

A gyakorlat célja a szövetség válságkezelési eljárásainak gyakorlása stratégiai politikai szinten, amelyben a tagországok, a NATO-parancsnokság, a stratégiai parancsnokságok civil és katonai szakemberei vesznek részt. Ezáltal a válságkezelés hazai szakértői és döntéshozói részt vesznek a NATO konzultációs és döntéshozatali folyamatában, továbbá gyakorolják Magyarország polgári és katonai válságkezelési eljárásait.

Magyarország számára ez kiváló alkalom a hazai válságkezelési rendszer poli tikai, katonai döntés-előkészítő és döntéshozatali folyamatainak, valamint a NATO-

központtal és a tagországokkal való együttműködés gyakorlására. A főbb nemzeti célkitűzések az alábbiakban fogalmazhatóak meg:

- Részvétel a Szövetség tagállamai közötti konzultációs és kollektív döntéshozatali folyamatban, valamint a Szövetség válaszlépéseinek kidolgozásában.
- A hazai válságkezelési rendszer döntés-előkészítő-, és döntéshozatali folyamatainak, a válságkezelési rendszabályok vételének és feldolgozásának gyakoroltatása.
- Átfogó megközelítés keretében a polgári, rendvédelmi és katonai szervek együttműködésének gyakoroltatása.
- A nemzeti álláspontok kialakítására irányuló döntés-előkészítési tevékenységek és a vonatkozó döntések meghozatalának gyakoroltatása.
- A válságreagálási rendszabályok bevezetésének előkészítésekor és annak végrehajtása időszakában a minisztériumok és a védelmi igazgatás területi szervei együttes válságkezelő tevékenységének a gyakoroltatása.
- A kibervédelemben érintett hazai és NATO szervekkel való szoros együttműködés gyakorlása.

A CMX 12 gyakorlati célja mind a NATO, mind hazánk tekintetében kettős értelemben vizsgálható. A NATO célok a következők:

- A Szövetség tagállamai közötti konzultációs és kollektív döntéshozatali eljárások gyakoroltatása kis intenzitású válságkezelés során. Az új NATO Stratégiai Koncepció, a válságkezelési eljárások tesztelése globális kiber-, terror- és ABV-fenyegetettség helyzetében.
- A kollektív védelmi képesség demonstrálása a nem hagyományos biztonsági kihívások ellen.

Hazánk céljai:

- Részvétel a NATO konzultációs és döntéshozatali folyamataiban, továbbá Magyarország polgári, és katonai válságkezelési mechanizmusainak gyakoroltatása a konfliktushoz kapcsolódó, a hazánkat közvetlenül érintő fenyegetések elhárításán keresztül.
- A politikai, katonai döntés-előkészítő-, és döntéshozatali folyamatok, a válságkezelési rendszabályok vételének és feldolgozásának, valamint a polgári és katonai szervek együttműködésének gyakoroltatása.
- NATO-információk feldolgozása, a nemzeti álláspontok kialakítása és megküldése.
- A Magyarországot közvetlenül érintő fenyegetettségek felszámolásának gyakoroltatása.
- A NATO-szervek és a nemzetbiztonsági szolgálatok közötti együttműködés gyakoroltatása.
- A NATO Válságreagáló Kézikönyvben és a Nemzeti Intézkedések Gyűjteményében foglaltak együttes használatának gyakorlása.
- A NATO-médiaesemények feldolgozása, tájékoztatók kiadása.
- Kibervédelmi együttműködés gyakoroltatása a hazai és a NATO szervek között.

A CMX 12 egy olyan belső vezetési gyakorlat, amely a tervezésre és a döntéshozatalra összpontosít. Célja, hogy a résztvevők stratégiai politikai szinten a szövetség válságkezelési eljárásait gyakorolják. Ezen a tagországok, a NATO-parancsnokság, a stratégiai parancsnokságok civil és katonai szakemberei vesznek részt. Ellentétben egy „élő gyakorlattal", itt nem történik katonai erők „mozgása". Magyarországon a gyakorlat vezetősége, a végrehajtó és biztosító állomány vesz részt, összesen százhúsz fővel.

A gyakorlat forgatókönyve teljes mértékben kitalált eseményeken alapul, elképzelt földrajzi környezetben játszódik (válsághelyzetben fokozódó vegyi, biológiai, nukleáris fenyegetés, a tömegpusztító fegyverek elterjedése, a NATO stratégiai intézményei ellen végrehajtott nagyfokú kibertámadás történik). A munkacsoportok feladata, hogy előkészítsék a kormány döntését arra vonatkozóan, milyen jellegű szakmai és döntéshozói tevékenységre van szükség – a rendelkezésre álló feltételeket, eszközöket figyelembe véve – az elképzelt válsághelyzet leküzdésére. A szerzett tapasztalatok hatékonyabbá, gyorsabbá teszik a stratégiai döntések meghozatalát, ami egy válsághelyzet kezelése és felszámolása során kulcsfontosságú szereppel bír.

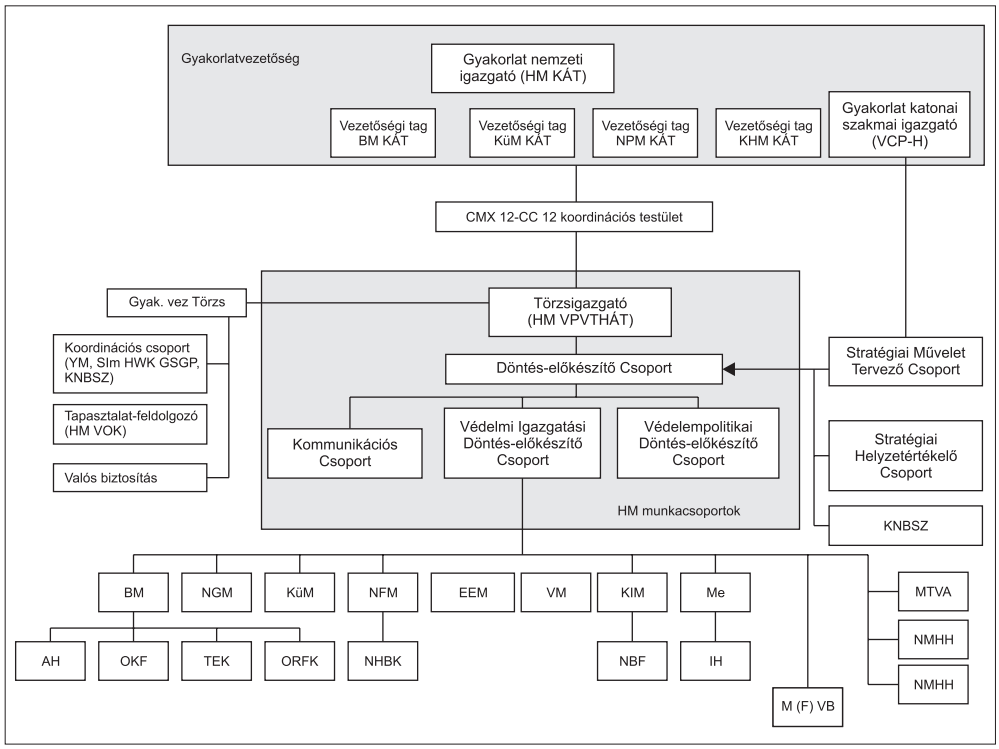
Hazánk aktív szerepet vállalt a gyakorlat tervezésében és megvalósításában. A feladatok végrehajtása, a döntéshozatali folyamatok modellezése a kormányzat aktív bevonásával történt.

A gyakorlat résztvevői

A gyakorlat résztvevői a tagországok mellett a szövetség politikai és katonai döntéshozó és döntés-előkészítő, irányító szervezetei: az Észak-atlanti Tanács, a NATO bizottságok és a stratégiai parancsnokságok. A végrehajtás során a résztvevők a NATO válságkezelési eljárásait gyakorolják, amelynek fő célja a jelen kor kihívásai elleni egységes fellépéshez szükséges döntések konszenzus útján történő meghozatala.

A CMX 12 olyan kormányzati szintű törzsvezetési gyakorlat, melyen részt vesznek az érintett minisztériumok (HM, BM, KIM, NGM, EMMI, NFM, VM) képviselői, illetve meghatározott, kijelölt intézményei. A gyakorlatot a HM Védelmi Hivatala vezeti. A gyakorlatban résztvevő további szervek:

– Magyarország Állandó NATO Képviselete.
– Katonai Nemzetbiztonsági Szolgálat.
– Információs Hivatal.
– Alkotmányvédelmi Hivatal.
– A megyei és a fővárosi védelmi bizottságok csoportjai.
– BM Országos Katasztrófavédelmi Főigazgatóság.
– Terrorelhárítási Központ.
– Országos Rendőr-főkapitányság.
– Nemzeti Biztonsági Felügyelet.
– Médiaszolgálatatás-támogató és Vagyonkezelő Alap.
– Nemzeti Média és Hírközlési Hatóság.
– PTA Nemzeti Hálózatbiztonsági Központ.
– HungaroControl Zrt.



Az ábrán látható hármas tagozódási szint a tevékenység jellegét is megkülönbözteti:

- Legfelsőbb szint (Gyakorlatvezetőség) – kormányzati döntéshozatal.
- Középső szint – központi döntés előkészítés, koordináció, végrehajtás.
- Legalsóbb szint-területi működtetés.

A hazánkban végrehajtott gyakorlat végrehajtói a következőkben felsorolt csoportokat jelentik:

- A gyakorlatvezetőség feladata a CMX 12 gyakorlat végrehajtása során a nemzeti döntések meghozatala, a gyakorlat levezetésének irányítása.
- A koordinációs testület csoportjának tagjai a gyakorlat végrehajtásakor folyamatosan kapcsolatban állnak egymással és szükség szerint személyesen egyeztetnek. A stratégiai fontosságú döntések meghozatalának támogatása érdekében a csoport tagjai minden esetben jelen vannak a CMX-gyakorlat vezetőségi ülésein, szükség szerint segítik a gyakorlatvezetőséget a stratégia szintű döntések meghozatalában.
- A központi döntés-előkészítő csoport feladata a gyakorlatvezetőség által meghozandó döntések előkészítése, döntési változatok kidolgozása, nemzeti álláspont előkészítése. A vezető NATO-szervek által hozott döntések elemzése, a nemzeti intézkedések jóváhagyásra történő előkészítése.
- A gyakorlattervezők folyamatosan figyelemmel kísérik a gyakorlat lefolyását a meghatározott célkitűzések megvalósulása érdekében.
- A végrehajtó csoportok a felkészülési időszakban kiadott anyagokban a kialakult politikai-katonai helyzet tanulmányozzák, elemezik és értékelik. A napi események figyelembevételével javaslatokat dolgoznak ki a lehetséges nemzeti álláspontokra vonatkozóan, majd azokat döntésre előterjesztik a gyakorlatvezetőség részére.

A CMX 12 gyakorlat következtései [10]

A NATO 2012. évi válságkezelési gyakorlatán (CMX 12) a résztvevő civil és katonai szakemberek bebizonyították: Magyarország felkészült arra, hogy gyorsan, hatékonyan kezelje és hárítsa el a válsághelyzeteket a NATO szövetségi kötelékében, melyet az alábbiakban szakembereink is megerősítenek. Idén először tartották közösen a CMX 12-t a CC 12 elnevezésű kibervédelmi gyakorlattal. A gyakorlat előkészítésében Magyarország is részt vett; a szimuláció szerint az országban támadás érte a bankrendszert és a légi irányítást, amelyek emiatt összeomlanak. Mindehhez mintaként a 2007-es, Észtország elleni kibertámadást vették alapul.

A szakemberek felhívták a figyelmet, hogy az ilyen típusú támadásoknál elsősorban a megelőzésre kell törekedni, mivel a más szervezetek által előre tervezett és célzott támadásra szinte lehetetlen felkészülni.

Ez a mostani volt az első alkalom, amikor a gyakorlaton egy kibertámadásnál esély nyílt a NATO-szerződés 5. cikkelyének érvényesítésére, vagyis a tagállamok közösen léptek fel a támadás elhárításáért és a rendszerek helyreállításáért.[2] Ilyen a valóságban akkor fordulhat elő, ha például az alapinfrastruktúrát támadják meg informatikai eszközökkel.

A Honvédelmi Minisztérium véleménye szerint több szempontból is újdonságot hozott a NATO éves válságkezelési gyakorlata idén. Nemzetközi és hazai vonatkozásokban is számos újdonság jelezte: a CMX 12 immár az egyik legjobban előkészített, magyar részvételű nemzetközi honvédelmi gyakorlattá vált, amelyet közel egyévnyi előkészítés és több tervezői NATO-szintű és hazai tervezői konferencia után rendeztek meg. Sőt, helyesebb rögtön két gyakorlatról beszélni, hiszen a CMX 12-vel egy időben, azzal szoros együttműködésben zajlott a CC 12 gyakorlat is. A két eseményt közösen (és ebből kifolyólag költséghatékonyan) tervezték-szervezték meg. Itt illik kiemelni azt a magyar sikert, hogy a CC 12 gyakorlat hat szimulált eseménye közül kettőnek a magyar Nemzeti Biztonsági Felügyelet (NBF) szakemberei készítették el a forgatókönyvét. Mindezt úgy, hogy az NBF 2011-ben vett részt először ezen a gyakorlaton. A gyors siker így komoly elismerést jelent a hazai szakemberek számára.

A két gyakorlat összefonódását közvetlenül a valós élet indokolta. Mint ahogyan a napjainkban zajló gázai konfliktus is jelzi, ma már nincsen „valódi" háború kibertámadások nélkül. Egy honvédelmi gyakorlat esetén ma már mindenféleképpen kell számolni a kibereseményekkel is, így minden szempont indokolta, hogy a válságkezelési és a kibertámadási NATO-gyakorlaton a lehető legszorosabb együttműködés valósuljon meg. Ez olyannyira sikerült, hogy például amikor a CMX 12 forgatókönyve szerint informatikai támadás érte a honvédelmi gyakorlaton részt vevő tagállamokat, akkor ez a CC 12 gyakorlaton meg is történt és ott „le is játszották" az eseményt, s ennek hatásai már a CMX 12-ben is jelentkeztek.

A CMX 12 gyakorlaton alapvetően olyan események forgatókönyveit játszották végig, amelyek a valós világban is megtörténhetnek. Esetünkben egy, az Indiai-óceánon

2 A NATO-t alapító Washingtoni Szerződés 5. cikkelye kimondja: ha valamelyik európai vagy észak-amerikai szövetségest támadás éri, azt valamennyiük elleni támadásnak tekintik.

elhelyezkedő, mesterséges megosztással kialakult két ország közötti konfliktust modelleztek. Az egyik ország a NATO segítségére számíthatott, de a „rossz ország" is számos támogatót vonultatott fel mind a terrorszervezetek, mind a kiberhadviselés területén. A kialakult konfliktus során NATO-tagországokat ért terrortámadási kísérlet (Magyarországon a repülőgép-katasztrófa mellett egy HÉV-szerelvény ellen követtek el robbantásos merényletet), illetve kibertámadás. A következmények elhárításában és a kialakult helyzet kezelésében nemcsak a legmagasabb kormányszinten dolgoztak a szakemberek, hanem – idén először – a megyei védelmi bizottságok is fontos szerepet kaptak.

A Megyei Védelmi Bizottságok (MVB) a területi működtetésért felelősek a veszélyhelyzet beálltakor. Ezek azok a szervek, amelyeknek mindenről tudniuk kell, ami a megyét tekintve fontossággal bír, megyei érdekeltségű. A MVB elnökei kezében van a döntés, így minden információs és egyéb tevékenységbe be kell őket avatni. Ezen szervek:

– eljárnak a biztonságot érintő ügyekben;
– tájékoztatást nyújtanak a lakosság számára;
– rendészeti feladatokat látnak el (például a bankok előtti lázongásokkal szemben);
– megteremtik a pénzszállítás biztonsági feltételeit.

Végül a CMX-gyakorlatok szövetségi végrehajtásával kapcsolatban fontos megemlíteni, hogy a tervezés és végrehajtás során a NATO a saját eljárásainak tökéletesítése mellett – a valós válságreagálási műveletek során szerzett tapasztalatok alapján – igyekezett az együttműködők körét szélesíteni, a válságkezelés folyamatába új szervezeteket meghívni. Ennek szellemében lényeges előrelépésnek tekinthető, hogy a 2012. évi gyakorlat a NATO és az Európai Unió közötti szorosabb együttműködés jegyében zajlott, és a végrehajtásában a döntések előkészítésében első alkalommal működött közre az Európai Unió Külügyi Szolgálata (European External Affairs Service – EEAS).

* * *

A Honvédelmi Minisztérium, valamint a Nemzetbiztonsági Felügyelet (NBF) szakembereinek véleménye szerint Magyarország kiválóan szerepelt a NATO éves válságkezelési gyakorlatán (CMX 12) és a Cyber Coalition 2012 elnevezésű kibervédelmi gyakorlaton. Hazánk nagyon jól vizsgázott a szimulációban; a hatóságok, szervezetek kiválóan együtt tudtak működni, viszont az informatikai rendszerek kapacitását növelni kell, és nagyobb figyelmet kell fordítani a rendszereket működtető emberekre. A további szükséges lépésekről a gyakorlat eredményeinek részletes értékelése után döntenek.

A bankrendszert érintő végkövetkeztetések és teendők [11]

A NATO 2012. évi CMX gyakorlatának egy, ámde nem elhanyagolható része volt az a kibertámadás, amely hazánk bankrendszerének megbénítását tűzte ki céljául, mivel országunk NATO tagországként részt vett a szimulált szigeten történő békefenntartási folyamatban, az afrikai terroristák elleni harcban. Ez a perifériás esemény csupán egy kicsiny részt jelentett a gyakorlatban a többi katonai esemény között.

A Nemzetgazdasági Minisztérium kizárólag a törvény- és egyéb jogszabályalkotás révén vesz rész ebben a feladatban.

A pénzügyi rendszer elleni támadást a Gyakorlat idején konkrétan nem szimulálták, hanem egy tényként vetődött fel annak előtte és végül a mindent lezáró Jelentés szintjén. Ebben a hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény alapján a következők állapították meg:

– A pénzügyi szolgáltatási tevékenység csak a működési kockázatok csökkentését szolgáló információs és ellenőrzési rendszer, valamint a rendkívüli helyzetek kezelésére vonatkozó terv megléte esetén kezdhető meg, illetve folytatható.
– A pénzügyi intézménynek ki kell alakítania a pénzügyi, kiegészítő pénzügyi szolgáltatási tevékenységének ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét és gondoskodnia kell az informatikai rendszer kockázatokkal arányos védelméről. A szabályozási rendszerben ki kell térni az információtechnológiával szemben támasztott követelményekre, a használatából adódó biztonsági kockázatok felmérésére és kezelésére a tervezés, a beszerzés, az üzemeltetés és az ellenőrzés területén.
– A biztonsági kockázatelemzés eredményének értékelése alapján, a biztonsági kockázattal arányos módon, gondoskodni kell legalább az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról, valamint olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, és alkalmas e naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, illetve lehetőséget nyújt a nem rendszeres események kezelésére.
– A pénzügyi intézménynek tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez meg kell valósítania a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket és rendelkeznie kell legalább a következőkkel:
  = A szolgáltatások ellátásához szükséges informatikai rendszerrel, valamint a szolgáltatások folytonosságát biztosító tartalékberendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb – a tevékenységek, illetve szolgáltatások folytonosságát biztosító – megoldásokkal.
  = Az informatikai rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és annak környezete) olyan biztonsági mentésekkel és mentési renddel (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend), amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik. Ezen mentéseket kockázati szempontból elkülönítetten és tűzbiztos módon kell tárolni, valamint gondoskodni kell a mentések forrásrendszerrel azonos szintű hozzáférés védelméről.
  = A szolgáltatásai folyamatosságát akadályozó rendkívüli események kezelésére szolgáló tervvel.

Végezetül a rendkívüli helyzetek kezelésének módjára az alábbiak fogalmazhatótak meg:

– A pénzintézetnek a mérete, az általa végzett pénzügyi, kiegészítő pénzügyi szolgáltatási tevékenysége jellege, nagyságrendje, összetettsége arányában megbízható irányítási rendszerrel kell rendelkeznie, és ennek keretén belül köteles a felmerülő kockázatok azonosítására, mérésére, kezelésére, nyomon követésére és jelentésére szolgáló hatékony eljárásokat alkalmazni.
– Az előbbiek mellett írásban rögzített eljárásrendekkel, szabályzatokkal kell rendelkeznie a működési kockázatok mérésére, kezelésére, valamint vészhelyzeti és üzletmenet-folytonossági tervvel a folyamatos működés fenntartása, továbbá a súlyos üzletviteli fennakadásokból következő esetleges veszteségek mérséklése érdekében.

Mindezen – egyebekben üzleti titkot képező – eljárások, szabályzatok, intézkedési tervek megfelelőségét a Pénzügyi Szervezetek Állami Felügyelete (PSZÁF) köteles ellenőrizni. Mivel a Nemzetgazdasági Minisztériumnak (NGM) mint szabályozói szervnek erre ténylegesen nincs, és nem is lehet rálátása, ezért ennek megfelelően megfontolandó az ügymenetbe a PSZÁF bevonása.

A Magyar Nemzeti Bank (MNB) alapfeladata a fizetési és elszámolási rendszerek felvigyázása, e rendszerek biztonságos és hatékony működése, továbbá a pénzforgalom zavartalan lebonyolítása érdekében. Ennek okán fontos kikérni az MNB szakembereinek véleményét is az adott válsághelyzet gyakorlatával kapcsolatosan.

A 2012. július 14. napjától hatályos 2011. évi a Magyar Nemzeti Bankról szóló CCVIII. törvény alapján az MNB alapvető és egyéb feladatai ez érintett téma tekintetében az alábbiakban foglalható össze:

– Az MNB más felelős hatóságokkal együttműködve feltárja a pénzügyi közvetítőrendszer egészét fenyegető üzleti és gazdasági kockázatokat, elősegíti a rendszerszintű kockázatok kialakulásának megelőzését, valamint a már kialakult rendszerszintű kockázatok csökkentését vagy megszüntetését.
– Feltárja a pénzügyi közvetítőrendszer egészét fenyegető üzleti és gazdasági kockázatokat, elősegíti a rendszerszintű kockázatok kialakulásának megelőzését, valamint a már kialakult rendszerszintű kockázatok csökkentését vagy megszüntetését.
– Az MNB elnöke a rendszerszintű kockázatok felépülésének megakadályozása vagy a kockázatok csökkentése érdekében rendeletet adhat ki.
– Amennyiben olyan körülmény áll fenn, amely miatt a hitelintézet működése a pénzügyi rendszer stabilitását veszélyezteti, az MNB a hitelintézetnek rendkívüli hitelt nyújthat.
– Az MNB sürgős, rendkívüli, a pénzügyi rendszer egészének stabilitását és a pénzforgalom zavartalanságát veszélyeztető esetben hitelt nyújthat, amelynek lejárata legfeljebb három hónap lehet.

Mindezek alapján az MNB elnöke rendeletben szabályozza, hogy a rendszerkockázatok felépülésének megakadályozása vagy a kockázatok csökkentése érdekében szükséges intézkedéseket: a túlzott hitelkiáramlást megakadályozó előírásokat, a rendszerszintű likviditási kockázatok felépülését megakadályozó likviditási követelményeket,

felépítésének és működésének feltételeit, a rendszerszinten jelentős intézmények csődvalószínűségét csökkentő többletkövetelményeket.

* * *

Összességében tehát megállapítható, hogy az NGM csak a szabályozás elméleti oldaláról érintett, a gyakorlati tennivalók tekintetében a PSZÁF és az MNB, esetleg a Magyar Államkincstár (MÁK) bizonyul illetékes szervnek. Ennek érdekében a jövőre vonatkozóan mindenképp érdemes kidolgozni egy olyan gyakorlati szabályozást – a többféle területen használt legjobb gyakorlatok módszerével (Best Practise) –, amely által az állami szervek összehangoltan és azonnali reagálással képesek fellépni az őket ért támadások ellen. Ebben tehát kulcsfontosságú szereppel bír az NGM-en kívül a 3 állami, pénzügyi felügyeleti szervünk, úgymint a PSZÁF, az MNB és a MÁK. Minden pozitívan előremutató eredmény, megoldás eléréséhez z általuk közösen megfontolt és kimunkált tevékenységre van szükség a jövőben a bankokat fenyegető kibertámadások ellen.

FELHASZNÁLT IRODALOM

[1] Kolozsi Pál Péter: Monetáris politika, érdekcsoportok, pénzügyi válság. (ÁSZ Pénzügyi szemle 2013. május 7. http://www.penzugyiszemle.hu/vitaforum/monetaris-politika-erdekcsoportok-penzugyi-valsag letöltés ideje: 2013. május 20.)

[2] Inotai András: Válság után? (ÁSZ Pénzügyi Szemle 2011. http://www.asz.hu/penzugyi-szemle-cikkek/2011/valsag-utan/352-368-inotai.pdf letöltés ideje: 2013. május 9.)

[3] Dr. Hadnagy Imre: A biztonság korszerű értelmezése – avagy a biztonság ma már sokkal bizonytalanabb, mint korábban bármikor. (http://vedelem.hu letöltés 2013. május 9-én)

[4] Kiss Petra: A magyar stratégiai gondolkodás változása a nemzeti biztonsági stratégiák tükrében. (Hadtudomány 2012. 3–4. szám 68–79. oldal)

[5] Tomolya János – Padányi József: A Terrorizmus jelentette kihívások. (Hadtudomány 2012. 3–4. szám 34–67. oldal)

[6] Kovács László – Illés Zsolt: Cyberhadviselés. (Hadtudomány 2011. 1–2. szám 29–41.)

[7] Haig Zsolt: Az információs hadviselés kialakulása, katonai értelmezése. (Hadtudomány 2011. 1–2. szám 12–28.)

[8] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról

[9] CMX 12: 4 nap együttműködés. (http://honvedelem.hu letöltés 2013. május 11.)

[10] CMX 12: Tervezés és döntéshozatal. (http://honvedelem.hu letöltés 2013. május 11.)

[11] Cser Orsolya: Válságkezelés és banküzemi szabályozás 2004. (Corvinus Egyetem / Gazdálkodási Kar / Védelemgazdasági szak – egyetemi szakdolgozat)