Munk Sándor

A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései

DOI 10.17047/HADTUD.2018.28.1.113

A kibertér napjaink gyakran használt, népszerű kifejezése, azonban távol állunk az együttműködéshez szükséges mértékben egységes értelmezéstől. Jelen publikáció célja a kibertér fogalmához kapcsolódó, eltérő értelmezésekhez vezető fontosabb kérdések meghatározása, amely alapját képezheti az eltérő kibertér-értelmezések részletesebb tartalmi feltárásának, kapcsolatrendszerük feltérképezésének.

A kibertér napjainkban különböző alkalmazási területek, szakmai körök, sőt a mindennapi közbeszéd gyakran használt, népszerű kifejezése. A fejlett információtechnológia eredményeként kialakuló hálózatok egy olyan szolgáltatási, virtuális működési környezetté, sőt „életkörnyezetté" váltak, amelyek mindenki számára érzékelhető virtuális térként, világként megélhető környezetet alkotnak. Ebben a „térben" szereplők tevékenykednek, folyamatok zajlanak, események történnek, amelyek pozitív hatással, vagy negatív (káros, vagy akár pusztító erejű) következményekkel vannak a „hagyományos" világ szereplőinek életére, tevékenységére.

Mint minden fogalom, így a kibertér esetében is lehet öncélúan és elvontan – bár ekkor sem haszontalanul – terminológiai kérdéseket vizsgálni. Egy adott szakterület alapvető fogalmai esetében azonban (kivéve, ha a fogalmak meghatározása, tartalma viszonylag egyértelmű) az értelmezési kérdések vizsgálata kiemelt jelentőségű. Egy szakterület alapfogalmai és az azokat megnevező szakkifejezések, mint a szaknyelv alapvető összetevői, a szakterületi ismeretanyag cseréjének kulcsfontosságú feltételei.

Ha ugyanazon fogalom alatt különböző felek akár csak részben, de az alkalmazás szempontjából lényeges elemekben eltérő dolgot értenek, a fogalommal leírt dolog tulajdonságait eltérő módon látják, a fogalom körébe eltérő egyedi dolgokat sorolnak be, akkor a köztük lévő információcsere tartalmilag pontatlan lesz, és kapcsolódó megállapításaik is el fognak térni. Az alapfogalmak esetében az értelmezési kérdések vizsgálatának jelentőségét az is növeli, hogy ezekre további fogalmak épülnek, amelyek átörökítik az alapfogalom értelmezési eltéréseit (például a kibervédelem az a kibertérben végrehajtott védelem).

A kibertér és a hozzá kapcsolódó fogalmak esetében nem kérdéses, hogy – mint azt a következőkben részletesebben is bemutatom, elemzem – távol állunk az együttműködéshez szükséges mértékben egységes értelmezéstől. Ez részben a „kiber" jelzővel jellemezhető fogalmi rendszer viszonylagos újdonságából, részben az általa leírt dolgok, jelenségek, objektumok napjainkban is tapasztalható változásaiból következik.

Jelen publikáció célja a kibertér fogalmához kapcsolódó, eltérő értelmezésekhez vezető fontosabb kérdések meghatározása, amely alapját képezheti az eltérő kibertér-értelmezések részletesebb tartalmi feltárásának, kapcsolatrendszerük feltérképezésének. Ennek részeként meghatározza mindazon, eltérő értelmezésekhez vezető legfontosabb kérdéseket:

– amelyek a kibertér jellegéhez, legközelebbi fölérendelt nem-fogalmához kapcsolódnak;
– a kibertér összetevőire vonatkoznak;
– a kibertér szereplőire, és a kibertéri tevékenységekre, folyamatokra vonatkoznak.

A publikáció célja hangsúlyozottan kérdések meghatározása, nem pedig megválaszolása, ugyanis véleményem szerint a kérdésekre nincsenek „helyes", „jó" válaszok. A válaszokat tulajdonképpen jelentős részben az alkalmazási terület igényei, körülményei határozzák meg (vagyis nem válaszok, hanem nézőpontok), valamint a szakterület szakembereinek döntései határozzák meg (vagyis nem válaszok, hanem választások).

A cikk eredményei - reményeim szerint - kiinduló alapot biztosíthatnak ahhoz, hogy egyes alkalmazási, vagy szakterületek a kérdések megválaszolásával (ha eddig nem tették volna meg) maguk és mások számára is pontosabban meg tudják határozni kibertér értelmezésük részletes tartalmát, illetve hogy a különböző értelmezések összehasonlíthatóak, eltéréseik feltárhatóak, és ennek alapján a szakterületek együttműködésének lehetőségei – a kölcsönösen pontosabb megértésre alapozva – jobbak legyenek.

A kibertér jellege

Az első kérdéscsoport, amelyet a kibertér fogalmának értelmezéséhez fel kell tennünk, ahhoz kapcsolódik, hogy minek tekintjük a kiberteret, vagyis hogy egy arisztotelészi definíció esetében mi a legközelebbi fölérendelt nem-fogalom (genus proximum). A kibertér – mint szinte bármelyik más fogalom – szakirodalomban megtalálható definíciói természetesen nem mind felelnek meg a filozófia, a logika követelményeinek, azonban legtöbb esetben így is feltárható belőlük hogy a meghatározás megalkotói szerint a kibertér milyen magasabb szintű fogalom körébe tartozik. A legközelebbi nem-fogalom meghatározása segíti az értelmezést, de látnunk kell, hogy nem teszi egyértelművé, mivel általában a magasabb szintű fogalom értelmezése sem egyértelmű, sokszor köznapi értelmezések által befolyásolt.

A következőkben áttekintjük a kibertér legfontosabb definícióit, meghatározzuk, rendszerezzük, elemezzük a bennük szereplő, vagy kikövetkeztethető fölérendelt nem-fogalmakat. Majd erre építve meghatározzuk azokat a legfontosabbnak

tartott kérdéseket, amelyek megválaszolását elengedhetetlennek tartjuk a kibertér tartalmának értelmezéséhez, és amelyek alapján különböző értelmezések megkülönböztethetőek.

A kibertér katonai és más definíciói, értelmezései

A kibertér katonai, és más definíciói hosszú listát képeznek, amelyekben a kibertér különböző magasabb szintű fogalmak körébe van besorolva. A következőkben a fogalom megjelenésének, szélesebb körű alkalmazásának időrendjében bemutatjuk, rendszerezzük az Egyesült Államok haderejében, a NATO-ban, illetve a Magyar Honvédségben használatos meghatározásokat.

Az Egyesült Államok haderejének értelmezése szerint a kibertér az információs környezet (information environment) részét képező globális tartomány (domain), ahol az információs környezet az információt gyűjtő, feldolgozó, terjesztő, és felhasználó személyek, szervezetek, és rendszerek összessége, a tartomány kifejezés pedig hadviselési tartományt (warfighting domain) jelöl. A hadviselési tartományok (ti. a szárazföldi, a légi, a tengerészeti, az űr, és az információs[1]) az Összhaderőnemi Jövőkép 2020 (Joint Vision 2020) dokumentumban jelentek meg 2000-ben, mint amelyekben a katonai erőknek képeseknek kell lenniük tevékenykedni, műveleteket végrehajtani.

A NATO értelmezése[2] szerint a kibertér egy komplex dinamikus környezet, a működési környezet (operating environment) egyik összetevője.[3] A doktrínális dokumentumokban a kibertér formális definíciója nem szerepel. A NATO Kibervédelmi Kiválósági Központ (NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE) szakemberei által kidolgozott Tallinni Jegyzőkönyv szójegyzékében a kibertér, mint környezet szerepel.[4]

A kiberbiztonság Magyar Honvédségen belüli értelmezése formális definíció formájában eddig csak a Kibervédelmi Szakmai Koncepcióban jelent meg. Eszerint a kibertér egy dinamikusan változó tartomány, azonban a dokumentum a tartomány fogalmát nem értelmezi. A törzsszövegben a kibertérre vonatkozóan szerepel a „virtuális tér" jellemzés. A fogalmak listájában a kibertér mellett megjelenik a kiberkörnyezet is, azonban a kifejezés a törzsszövegben már nem található. A dokumentum hivatkozik az információbiztonsági törvényben szereplő globális és nemzeti kibertér fogalmakra, amelyeket a törvény elektronikus információs rendszerek, adatok/információk formájában megjelenő társadalmi és gazdasági folyamatok együtteseként definiál.

1 A kibertér befogadása mellett az utóbbi időben felmerült az elektromágneses spektrum, illetve az emberi „tartomány" hadviselési tartományként kezelésének ötlete, javaslata is.

2 AJP 3.2(A). Allied Joint Operations for Land Operations. NATO Standardization Office, 2016 március

3 A működési környezet összetevői a szárazföldi, tengeri, légi, űr-, és információs környezethez, ez utóbbin belül a kibertérhez kapcsolódó fizikai és nem fizikai területek és tényezők [Vö. AJP 01(E), Allied Joint Doctrine. NATO Standardization Office, 2017 február.], máshol ezek mellett megjelenik az elektromágneses környezet is. [Vö. AJP 3(B), Allied Joint Doctrine for the Conduct of Operations. – NATO Standardization Office, 2011 március]

4 Tallinn Manual on the International Law Applicable to Cyber Warfare (Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence). Cambridge University Press, 2013.

Ebből következően a szakmai koncepció és a törvény értelmezései nincsenek egymással összhangban.

A kibertér fogalmával, értelmezésével a hadtudományi kutatók közül elsősorban Haig Zsolt és Kovács László foglalkoztak. Értelmezésük szerint *„A harctéren a különböző hálózatba kapcsolt elektronikai rendszerek az információs színtérnek azt a részét használják, amelyben a különféle elektronikus információs folyamatok (elektronikai úton végrehajtott adatszerzés, adatfeldolgozás, kommunikáció, stb.) realizálódnak, illetve az elektronikai rendszerek elleni tevékenység és a védelem megvalósul. Az információs színtér e tartományát gyakran cybertérnek is nevezzük."* (Haig Zsolt – Kovács László 2008, 61–69.)

A NATO Kibervédelmi Kiválósági Központ kifejezés-jegyzéke több mint 40 kibertér definíciót tartalmaz. Mintegy negyedükben a magasabb szintű fogalom valamilyen környezet, másik negyedükben pedig tartomány. Ezek mellett néhány esetben találkozhatunk tér (space), illetve hálózat besorolással, illetve az elektronikus világ, összetett jelenség, eszközök és eljárások együttese, elektronikus médium, tevékenységi terület leírásokkal.

Összességében tehát megállapítható, hogy a meghatározások túlnyomó többségében:

– a kibertér egy sajátos (képzeletbeli, virtuális) környezet;
– a kibertér egy tartomány;
– a kibertér egy hálózat.

A fentiek közül a következőkben a kibertér, mint hálózat megközelítéssel – bár sok helyen találkozhatunk vele – részletesebben nem foglalkozunk, mert azt a fogalom leegyszerűsített, a katonai, védelmi alkalmazás szempontjából kevésbé használható értelmezésének tartjuk.

Kibertér, kiberkörnyezet, kibertartomány

A kibertér, a kiberkörnyezet, és a kibertartomány fogalmak általános összetevői közül az első kettő viszonylag egyértelműen értelmezett tartalommal bír. A *tér* (space) a dolgok és események viszonylagos helyének, irányának leírását biztosító viszonyítási rendszer. Ebben az értelemben a dolgok, események nem a tér részei, hanem a térben léteznek, történnek meg. A *környezet* (environment) általános értelemben minden (dolgok, körülmények, hatások), ami egy adott dolgon kívül van, de arra hatást gyakorol, létezését, működését befolyásolja. Ebben az értelemben egy adott dolog nem része a környezetének.

A *tartomány* (domain) kifejezéshez mind az angol, mind a magyar nyelvben több eltérő tartalmú értelmezés kapcsolódik, amelyek közül témánk szempontjából elsősorban a „valamilyen szempontból körülhatárolt (rész)terület" értelmezés használható. A katonai alkalmazásban a *domain* kifejezés a *műveleti tartomány* (domain of operation, domain of warfare, operational domain) értelmezésben fordul elő, amely az információs műveleti tartománynak (information domain) a négy „hagyományos", fizikai műveleti tartomány (szárazföldi, légi, tengeri, és űr) melletti megjelenésekor került be a szakmai dokumentumokba.

A tartomány és a környezet kifejezések sok esetben egymást váltva, néha szinonimaként szerepelnek. Az Egyesült Államok haderejében a tartomány kifejezés a

gyakoribb, a NATO dokumentumokban pedig ugyanannak a megjelölésére a környezet.[5] A kibertér meghatározásaiban szereplő tartomány tehát egy sajátos működési (műveleti, hadviselési) terület, amelyre sajátos körülmények jellemzőek, amelyben sajátos események, jelenségek történnek, sajátos képességekkel rendelkező erők működnek és sajátos tevékenységek folynak. Kiemelendő, hogy a katonai alkalmazásban a hagyományos műveleti tartományok egymással kölcsönös kapcsolatban álló, de egymástól elhatárolt területek.

A hivatalos katonai dokumentumokban elvi különbségtételt a kibertér, kibertartomány (cyber domain), és kiberkörnyezet (cyber environment) fogalmak tartalma között nem találunk. Az egyes megállapításokban a kibertér helyett a tartalom megzavarása nélkül szerepelhetne a kibertartomány, vagy a kiberkörnyezet kifejezés is (amely jobban is illeszkedne a megállapításban szereplő társ-fogalmakhoz, például a hagyományos műveleti területeket jelölő kifejezésekhez).

A kibertér jellegéhez kapcsolódó értelmezési kérdések

A kibertér értelmezési kérdései közül a következőkben néggyel foglalkozunk: ezek a virtuális jelleghez; ennek részeként a más tartományokkal fennálló kapcsolatokhoz; a globális, vagy alany-orientált jelleghez; és ehhez kapcsolódóan a tartomány-környezet különbségtételhez kapcsolódnak.

Az első kérdés az, hogy a kibertér tisztán virtuális, vagy vegyes jellegű (vagyis vannak fizikailag létező összetevői).[6] A kiberteret több definíció képzelt (notional), vagy virtuális környezetként határozza meg, mások viszont egyértelműen fizikai és nem-fizikai összetevőkből álló dologként írják le. Több meghatározás ennek hangsúlyozása nélkül összetevői közé sorol informatikai rendszereket, hálózatokat, eszközöket, illetve a kiberteret három rétegre [fizikai hálózati, logikai hálózati, kiber személyiség (cyber-persona)[7] rétegekre] tagolja.[8]

A következő kérdés az, hogy a kibertér milyen kapcsolatban áll a többi tartománnyal, elkülönül-e azoktól, vagy vannak velük átfedései. A kérdés a hagyományos fizikai tartományok (szárazföldi, tengeri, légi, űrbeli) esetében is felvetődik, és bár a válasz első ránézésre az, hogy ezek egymástól elkülönülnek, elhatárolhatóak, a meghatározások a szárazföldi és a tengeri tartományok esetében ennek részben

---

5 It [the operational environment] encompasses physical areas of the air, land, maritime, and space domains; the information environment (which includes cyberspace); the EMS; and other factors. (Vö. JP 3-0, Joint Operations. US Joint Chiefs of Staff, 2017 január, IV-1. o.) It [the battlespace] includes the land, maritime, air and space environments; the enemy and friendly forces present therein; facilities; terrestrial and space weather; health hazards; terrain; the electromagnetic spectrum; and the information environment in the joint operations area and other areas of interest. [Vö. AAP-6 NATO Glossary of Terms and Definitions (English and French). NATO Standardization Office, 2015. 2-B-3. o.]

6 Létezhet olyan értelmezés is, és vannak ehhez közelálló meghatározások is, amely szerint a kibertér tisztán fizikai jellegű.

7 A kibertérben információszerzésre, vagy mások befolyásolására használt, a szereplő valós identitását, vagy hovatartozását elrejtő személyazonosság. (Vö. Terms & Definitions of Interest for DoD Counterintelligence Professionals. Office of Counterintelligence, Defense CI & HUMINT Center, Defense Intelligence Agency, 2011 május.)

8 JP 3-12(R), Cyberspace Operations. US Joint Chiefs of Staff, 2013 február

ellentmondanak, az elkülönülés a határokon nem egyértelmű.[9] Amennyiben a kibertér vegyes jellegű, fizikailag létező összetevői egy időben részei a kibertérnek és egy fizikai tartománynak.

Nem egyértelmű a kibertér elhatárolása az elektromágneses tartománytól, vagy környezettől sem. A két tartomány szoros kapcsolata nehezen kérdőjelezhető meg, a kibertér hálózatainak összeköttetései között a vezetékes vonalak mellett jelentős szerepet játszanak az elektromágneses spektrumot használó vezetéknélküli összeköttetések is. Az Egyesült Államok szárazföldi haderejének szabályzata például a két tartományt, és az ezekben végzett műveleteket összehangolt egészként tárgyalja.[10] A két tartomány viszonyára vonatkozóan a szakirodalomban részletes elemzést nem találtam.

Végül világosan meghatározandó a kibertér viszonya a napjainkban kissé háttérbe szoruló információs tartománnyal, környezettel is. A legtöbb katonai meghatározás szerint a kibertér az információs környezet része, de ez nem minden meghatározásban szerepel. Ennek részeként tisztázni kell a kibertér kapcsolatát az információs környezet fizikai, logikai, illetve kognitív dimenzióival is. Ezek közül az utóbbi, mint már utaltunk rá, a szakmai körökben újabb műveleti tartományként is felmerült.

A harmadik kérdés úgy fogalmazható meg, hogy a kibertér globális jellegű, vagy egy adott szereplő szempontjából értelmezett, körülhatárolt. A legtöbb meghatározásban nincs utalás a szereplő-orientált megközelítésre, így ezek – bár nem zárják ki a másik változatot – a globális jelleget sugallják. Több esetben találkozhatunk azonban a szereplő-orientált megközelítéssel is, amelyek nemzeti kibertérről beszélnek.[11] A két megközelítés nem zárja ki egymást, ugyanis egy szereplő-orientált kibertér nyilvánvalóan a globális kibertér valamely szempontok alapján körülhatárolt része, azonban egy meghatározásból – ha nem tartalmaz jelzős megkülönböztetést – egyértelműen ki kell tűnnie, hogy melyik megközelítésre épül.

Végül a negyedik kérdés lényege, hogy a kibertér egy tartomány (amelynek a szereplő is része), vagy egy környezet (amelynek az adott szereplő nem része). Ez a két megközelítés sem áll szemben egymással, mivel a tartomány egy szereplő kibertérbeli környezetének, illetve a szereplő, erőforrásai, és tevékenységei kibertérbeli megjelenésének együttese. A környezet-alapú értelmezés jól illeszkedik a védelmi, katonai alkalmazás gyakorlatába, ahol a saját erők, illetve a műveleti környezet különböző összetevői [köztük a kiber(téri) környezet] önállóan kerülnek elemzésre, értékelésre, a helyzetismeret azonban már egy tartomány valamennyi információját (saját erők, szembenálló erők, semleges erők helyzete, szándéka, tevékenysége, illetve további események, jelenségek) tartalmazza.

---

9 A tengeri tartományhoz tartoznak az óceánok, tengerek, öblök, torkolatok, szigetek, part menti területek és az ezek fölötti légtér, beleértve a tengerpartokat is. (Vö. JP 3-32, Command and Control of Joint Maritime Operations. US Joint Chiefs of Staff, 2013 augusztus)

10 FM 3-38, Cyber Electromagnetic Activities. Headquarters Department of the Army (US), 2014 február

11 Magyarország kibertere / magyar kibertér (Vö. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.), Amerika kibertere (Vö. The National Strategy to Secure Cyberspace. The White House, Washington, 2003 február)

A kibertér összetevői

A kibertér összetevőire vonatkozó értelmezési kérdések arra irányulnak (és a kibertér eltérő értelmezései eszerint különböztethetőek meg), hogy mely objektumokat tartunk a kibertér összetevőinek, és melyeket nem. A kibertér összetevőinek körére vonatkozó kérdések első csoportja szorosan kapcsolódik a kibertér jellegére vonatkozó értelmezési kérdéshez. Más összetevők tartoznak ugyanis egy virtuális, és mások egy vegyes (virtuális és valós) jellegű kibertérhez. Az összetevőkre vonatkozó második kérdéscsoport a kibertér és más tartományok átfedéseire, az egy időben több tartományhoz is tartozó objektumokra vonatkozó értelmezésbeli különbségekhez kapcsolódik. A védelmi, katonai alkalmazásban az összetevők köre egyben a kibertérre vonatkozó helyzetismeret tartalmát, a helyzet elemeinek körét is meghatározza. A következőkben először a kibertér virtuális, majd az esetleges fizikailag létező összetevőit, végül az ezekre vonatkozó értelmezési kérdéseket vesszük sorra.

A kibertér virtuális összetevői

A kibertér lényegét – akár tisztán virtuális, akár vegyes (virtuális és valós) jellegűnek tekintjük – a virtuális *része*, egy *elképzelt világ* képezi, amelybe egy ember beleképzelheti magát, amelyben információkat szerezhet, cserélhet, nyújthat, kommunikálhat másokkal, tevékenységeket hajthat végre, és akár „mozoghat" is.

Az emberek kizárólag végberendezések segítségével „léphetnek be" a kibertér virtuális világába; cserélhetnek információt, működhetnek együtt a kibertérbe „belépett" más szereplőkkel; észlelhetik a kibertérben létező dolgokat, és eseményeket; illetve vehetik igénybe a kibertérben elérhető szolgáltatásokat. A végberendezések ma még elsősorban „hagyományos" informatikai eszközök, de közel a világ, amelyben ezek közé már széles körben informatikai implantátumok, ember-gép interfészek is tartoznak.

A kibertér világa a létező hagyományos világunktól eltérően nem egy folytonos, két- vagy háromdimenziós tér, hanem – az alapját képező hálózathoz igazodóan – egymással összekapcsolt csomópontokból álló, diszkrét jellegű tér.[12] A kibertér helymeghatározásai csomópontokat, és azokon belüli helyeket jelölnek meg.

A kibertér egy nézőpontból *az összekapcsolódó informatikai rendszerek, eszközök, hálózatok által nyújtott képességek, szolgáltatások együttesének egy újszerű tálalása, metaforája*, amelyet a világméretű, szinte egyedüliként rendelkezésre álló hálózat (az Internet), és annak egyre bővülő felhasználása tett lehetővé, sőt szükségessé. A térként történő kezelés előzményei a mindennapi szóhasználatban már korábban is megjelentek: „belépek" a hálózatba, a rendszerbe, „felmegyek" a webre, „kalandozok" a weben, „meglátogatok" egy webhelyet és így tovább.

Az információkhoz történő hozzáférést, az információcserét, valamint más információs funkciókat (ezek között kiemelten a technikai eszközök vezérlését)

12 A matematika eszköztára véges halmazok esetében is biztosít lehetőséget topológia leírására, távolságok (metrikák) bevezetésére és használatára.

biztosító informatikai szolgáltatásoknak egy virtuális világ segítségével történő megjelenítése az igénybevétel kényelmességét, hatékonyságát szolgálja azzal, hogy ezeket a funkciókat a valós világban végrehajtott tevékenységekhez hasonlóvá teszi. Minden művelet, ami a kibertérben „végrehajtható", megvalósítható „hagyományos" informatikai formában is, de a legtöbb esetben kevésbé kényelmesen, hatékonyan.

A *kibertér virtuális összetevői* fizikailag nem létező dolgok, amelyek egyik része a valós világ bizonyos dolgainak helyettesítője, reprezentációja, másik része mögött létező valós dolog nem áll. Bármely létező dologgal[13] kialakítható az azt leíró adatok formájában létező reprezentációja, amely informatikai eszközökkel kezelhető, és amelynek segítségével a dolog a kibertér virtuális világában megjeleníthető, érzékelhetővé, kezelhetővé tehető. Ugyanilyen leíró adatokkal létrehozhatóak a valóságban nem létező dolgok is. Hogy a kibertérben milyen dolgokat azonosítunk, mit tekintünk összetevőnek, emberi döntés, értelmezés, felhasználói igény függvénye, ami nincs máshogy a valós világban sem.[14]

A kibertér virtuális összetevőinek köre tehát *értelmezés kérdése, alkalmazási területfüggő*, amely két szinten is alakítható. A kibertér virtuális részének hátterét megteremtő infrastruktúra fejlesztői egyes adatcsoportokat már eleve önálló összetevőként jeleníthetnek meg, tesznek elérhetővé, kezelhetővé. Ezen felül a kibertér „használói" a kibertér bizonyos elemeinek együttesét önálló egységet alkotó összetevőként azonosíthatnak, azonban ezek megjelenítése, kezelése a kibertér „beépített" összetevőihez képest kevésbé kényelmes, hatékony. Mivel a kibertér informatikai eszközök által „létrehozott" környezet, az informatika eszköztára lehetőséget biztosíthat a kibertér új összetevő típusokkal, és ezek kezelésének lehetőségével történő kibővítésére, de összetevő típusok megjelenítésének, kezelésének módosítására, vagy akár eltávolításukra is.

A kibertér virtuális összetevői nevesítve a definíciók túlnyomó többségében nem szerepelnek. A NATO Kibervédelmi Kiválósági Központ szójegyzékében található meghatározások közül csak kettőben találkozhatunk általános utalással.[15] A virtuális összetevőkre vonatkozó információk általában csak fogalmakhoz kapcsolódó értelmezésekben, leírásokban fordulnak elő. Az USA hadereje *Kibertéri műveletek* doktrínájában például szerepel a kibertér három rétege: a fizikai hálózati, a logikai hálózati, és a kiber személyiségi rétegek, amelyek közül a két utóbbi virtuális összetevőket tartalmaz.[16]

A továbbiakban a kibertér virtuális összetevői körét két alkalmazási terület, *a kiberbiztonság,* és a *kiberműveletek* szempontjából vizsgáljuk. Ezen alkalmazási területek közös nézőpontja, hogy a kibertérben olyan tevékenységeket lehet végrehajtani,

13 Élőlények (emberek, stb.), élettelen dolgok (természeti objektumok, tárgyak, eszközök, stb.), állapotváltozások (események, jelenségek, folyamatok, stb.).

14 Emberi értelmezés kérdése például a hegy, a növény, vagy a technikai eszköz fogalma, és hogy mit tekintünk egy adott hegynek, egy adott növénynek, egy rendszernek.

15 Tallinn Manual: nem-fizikai összetevők, belga forrás: tartalmaz fizikai és virtuális dolgokat. [Vö. Haig Zsolt – Kovács László: Fenyegetések a cybertérből. Nemzet és Biztonság, 2008 (I.)/5. 61–69. o.]

16 JP 3-12(R), Cyberspace Operations. US Joint Chiefs of Staff, 2013 február

amelyek révén hozzá lehet férni a valós világ más szereplői által használt informatikai, és ezeken keresztül más rendszerekhez, infrastruktúrákhoz, befolyásolni (megakadályozni, nehezíteni, módosítani) lehet működésüket, szolgáltatásaikat, és ezzel hatást lehet gyakorolni az érintett szereplők állapotára, képességeire, tevékenységére. A kiberbiztonság célja az ilyen káros tevékenységek észlelése, megakadályozása, következményeik csökkentése, és felszámolása, a kiberműveleteké pedig az ilyen tevékenységek végrehajtása.

A kibertér virtuális összetevőinek legfontosabb típusát (csoportját) a magát a kibertér virtuális infrastruktúra elemei, a teret alkotó hálózati csomópontok (köztük hálózati kapcsolóelemek) és hálózati összeköttetések reprezentációi, logikai szintű leírásai alkotják. Ezen összetevők, mint erőforrások, legfontosabb tulajdonságai közé azonosítójuk (azonosítóik), alapvető jellemzőik (képességeik), más erőforrásokkal fennálló kapcsolataik, valamint a szolgáltatások nyújtását, illetve fogadását, és a kezelésüket biztosító elérési pontjaik, illetve a kezelési/szolgáltatási felületek (interfészek) leírása tartozik. A kibertér virtuális erőforrás-összetevői, a valós világhoz hasonlóan egységes egészként azonosított összetettebb erőforrásokba, rendszerekbe, hálózatokba csoportosíthatóak, vagyis vannak (lehetnek) elemi és összetett kibertéri erőforrások.

A virtuális erőforrás-objektumok mögött állhatnak valós informatikai eszközök és összeköttetések, de ez nem feltétlenül van így. Napjainkban a virtualizációs technikák már régóta biztosítják fizikailag nem létező eszközök, összeköttetések „létrehozását", és rendelkezésre bocsátását. A gazdaságossági szempontok miatt, a felhő alapú technológia lehetőségeire is építve folyamatosan bővül a virtuális számítógépek, tárolók, összeköttetések mennyisége.

A kibertér virtuális összetevőinek második típusába a kibertérben elérhető információ reprezentációk tartoznak. Az információk[17] a kibertérben adatok formájában jelennek meg, áramlanak, érhetőek el. Az adatok által hordozott információk vonatkozhatnak a valós világ dolgaira, de leírhatnak a valóságban nem létező dolgokat is. Az információ-reprezentációk a kibertér csomópontjaiban hozhatóak létre, kerülnek tárolásra, férhetőek hozzá, illetve az összeköttetéseken keresztül továbbíthatóak, áramlanak.

A harmadik csoportba a kibertér virtuális szereplői, aktív összetevői (személyek, szervezetek, csoportok) sorolhatóak. A szereplők a kibertérben azonosítók, „fiókok", profilok, legmagasabb szinten virtuális személyiségek formájában jelennek meg. Ezek jelentős része mögött a valós világ őket létrehozó és általuk képviselt szereplői állnak, amelyekkel elvileg, de nem mindig, és nem könnyen, összekapcsolhatóak.[18] A kibertér szereplői között lehetnek automatizált módon működő, de valós szereplők által irányított, vagy akár autonóm módon működő szintetikus szereplők is.

17 Jelen publikációban információ alatt az emberi tudatban létező, az adatoknak, környezeti hatásoknak tulajdonított jelentést értjük, amely az emberi tudaton kívül különböző formákban jelenhet meg.

18 Az összekapcsolhatóság, a felhasználói viselkedéselemzés (profilozás) jogi problémáiról lásd például. Kiss Attila és Krasznay Csaba publikációját [Vö. Kiss Attila – Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. Információs Társadalom, 2017 (XVII.)/1. 55–71. o.]

És végül a kibertér lényeges összetevőit képezik a kibertérben folytatott tevékenységek, bekövetkező események, megvalósuló folyamatok. A kibertér eseményei, tevékenységei elemi szinten a kibertér összetevőinek állapotában, tulajdonságaiban bekövetkező változások, vagy változás sorozatok. A tevékenységeket a kibertér virtuális szereplői kezdeményezik, hajtják végre (információ reprezentációkat cserélnek más szereplőkkel, szolgáltatásokat vesznek igénybe kibertéri erőforrásoktól, sérülékenységeket használnak ki stb.). Az események a szereplők szándékaitól függetlenül következnek be.

Összegezve tehát a kibertér virtuális összetevői közé az információkat, szolgáltatásokat nyújtó virtuális erőforrások (infrastruktúra elemek); az információ reprezentációk; a szereplők; valamint a kibertérben zajló, érdeklődésre számot tartó események, tevékenységek (köztük támadások) tartoznak.

A kibertér fizikai összetevői

Amennyiben a kiberteret virtuális jellegűnek értelmezzük, akkor a kibertérnek nincsenek fizikai összetevői, csak azt megvalósító – a kibertéren kívüli – rendszerek, hálózatok, eszközök, infrastruktúrák. A kibertér-meghatározásokban azonban *számos fizikai összetevő* jelenik meg, ami a kibertér vegyes jellegű értelmezésére utal. Ezek az összetevők teljes egészében a számítástechnika, a távközléstechnika, az infokommunikációs technológia, illetve a tágabb értelemben vett információtechnológia (informatika[19]) körébe tartoznak.

A kibertér egységesen elfogadott értelmezések, és sok esetben a definíciókban konkrétan megfogalmazottak szerint is az elektronikus technológiákhoz kapcsolódik, nem képezik részét a hagyományos technikai eszközök, rendszerek. A kibertér fizikai rendszerei, eszközei információkat rögzítenek, tárolnak, továbbítanak, dolgoznak fel (alakítanak át, hoznak létre), és jelenítenek meg (bocsátanak rendelkezésre) oly módon, hogy az információkat elektronikus[20] adatok hordozzák, reprezentálják.

A kibertér informatikai eszköz összetevői esetében az adott funkcionalitást biztosító hardver és szoftver elemeket egységes fizikai egészként kell kezelnünk, mivel az egyes funkciók megvalósítása a külvilág számára láthatatlan és érdektelen módon lehet „huzalozott", szoftver-alapú, vagy vegyes.

A kibertér (vagy az azt megvalósító környezet) fizikai összetevői hagymahéjszerűen bővülő rétegekbe csoportosíthatóak. Az összetevők magját a kibertér első értelmezéséhez kapcsolódóan (amely szerint a kibertér az Internet általa teremtett új világ) az Internet fizikai összetevői, az összekapcsolódott hálózatok csomópontjai és ezek összeköttetései képezik. Mivel az Internet fogalmában is keveredik az IP-adatcserét biztosító rendszer, illetve az erre épülő szolgáltatásokat (levelezés, web stb.) is

19 Jelen publikációban informatikai eszköz alatt a szűkebb értelemben vett infokommunikációs rendszerek, eszközök mellett minden, alaprendeltetése szerint információs tevékenységet támogató technikai rendszert, eszközt értek.

20 Napjainkban az elektronikus jelző az eredeti értelmezésnél (elektronokhoz kapcsolódó; az elektromosan töltött részecskék mozgásával foglalkozó elektronika elveire, módszereire épülő) tágabb tartalmúvá vált, vonatkozik magnetikai, optikai (optoelektronikai) összetevőkre is.

magában foglaló rendszer, szűkebb értelemben ebbe a körbe csak az IP-hálózati - kapcsolóeszközök, a köztük lévő összeköttetések, esetleg még a tartománynév rendszer[21] eszközei tartoznak.

Az Internet összetevői önmagukban csak egy átviteli infrastruktúrát alkotnak, felhasználói szolgáltatásokat nem nyújtanak. Ezeket *az* Internetre csatlakozó számítógépek (számítógépes rendszerek, eszközök) biztosítják, amelyek közé általános célú (levelező, web, tárhely, stb.) és speciális tartalmú (banki, média, jogtár, stb.) szolgáltatásokat nyújtó kiszolgálók, valamint végberendezések tartoznak. A végberendezések azok az eszközök, amelyek segítségével „be lehet lépni" a kibertérbe, együtt lehet működni a kibertérbe „belépett" más szereplőkkel, érzékelni lehet a kibertérben létező dolgokat, és eseményeket, illetve igénybe lehet venni a kibertérben elérhető szolgáltatásokat.

A kibertér fizikai összetevőinek harmadik rétegét a tágabb értelemben vett informatikai rendszerek, eszközök alkotják. Napjainkban nincs egyetértés abban, hogy hol húzódnak a számítógép-fogalom határai, a közbeszéd - és gondolatban sokszor a szakemberek egy része is - számítógép alatt csak a hagyományos asztali számítógépeket, laptopokat, vagy kézi számítógépeket érti. Így ebbe a rétegbe tartoznak az Internetre kapcsolódó, alaprendeltetésük szerint információs tevékenységeket támogató, de az előző rétegbe nem sorolt további eszközök, valamint a nem információs alaprendeltetésű, de beágyazott számítástechnikai összetevőik segítségével, információs képességekkel rendelkező eszközök (amelyek köre, szerepe a Dolgok Internete formájában folyamatosan bővül).[22]

A kibertér meghatározásai nem adnak útmutatást arra, hogy a kibertér részét képezik-e az Internethez nem kapcsolódó, de azonos technológiára épülő hálózatok, rendszerek, eszközök.[23] A választás elméleti szempontból szabad: lehet egymásból el nem érhető, elszeparált részekből álló, de egységes (egyetlen) kiberteret értelmezni, de lehet ezeket a részeket önálló, esetleg eltérő sajátosságokkal is rendelkező kibertereknek tekinteni. Az elméleti megfontolás tehát többféle lehet, de a gyakorlatban a létesítmény elleni támadást mindenki kibertámadásnak (vagyis valamilyen szinten a kibertérhez kapcsolódó tevékenységnek) tekinti. Az Internet tehát – bár sok meghatározásban kiemelt szerepet játszik – nem feltétlenül képezi egyedüli alapját, összetevőjét a kibertérnek.

Végül a kibertér fizikai összetevői között felmerülnek, egyes definíciókban meg is jelennek a fizikai (elektronikus) adathordozók. Ezek segítségével a kibertérben adatok formájában rendelkezésre álló információk kinyerhetőek, vagy éppen a kibertérbe „betáplálhatóak", a kibertéren keresztül továbbíthatóak, eloszthatóak. Segítségükkel a kibertér módosítható, kibertéri tevékenységek kezdeményezhetőek, befolyásolhatóak (akadályozhatóak, meghamisíthatóak).

---

21 Domain Name System (DNS)

22 Okos telefonok, navigációs eszközök, médialejátszó eszközök, digitális fényképezőgépek, térfigyelő kamerák, érzékelő/mérésadatgyűjtő eszközök,

23 Gondoljunk például Irán natanzi nukleáris anyag dúsító létesítményének önálló hálózatára, eszközrendszerére.

Vegyes jellegű kibertér-értelmezés esetén a fentiekben bemutatott fizikai összetevők kettős jellegűek. Részét képezik a kibertérnek, de részét képezik a valós fizikai térnek, a megfelelő hagyományos (szárazföldi, tengeri, légi, vagy űrbeli) tartománynak is. Ennek két fontos következménye is van. Az első az, hogy rajtuk keresztül a kibertér és a valós fizikai tér *hely* fogalmai összekapcsolódnak, a kibertér helyeihez földrajzi helyek is tartoznak. A másik pedig az, hogy a kibertéri és a valós fizikai térbeli tevékenységek a másik térre (világra) is hatással vannak. Fizikai pusztítással kibertéri összetevők, és kibertéri tevékenységgel fizikai rendszerek, eszközök válhatnak működésképtelenné.

A kibertér összetevőihez kapcsolódó értelmezési kérdések

Annak megválaszolása, hogy milyen összetevőket tartunk a kibertér részének, elsősorban attól függ, hogy a kiberteret tisztán virtuális jellegűnek, vagy fizikai összetevőket is tartalmazónak tekintjük. Ennek is figyelembevételével a következőkben a virtuális összetevőkhöz kapcsolódóan három, a fizikai összetevőkhöz kapcsolódóan két kérdést emelek ki. Előzetesen még egyszer hangsúlyozni szeretném, hogy a kérdések megválaszolása értelmezés, alkalmazási területi nézőpont, és igényfüggő.

A kibertér virtuális összetevőihez kapcsolódó első és legfontosabb kérdés az, hogy melyek a kibertérnek az adott alkalmazási terület szempontjából jelentőséggel bíró virtuális összetevői. Ezek közé minden bizonnyal beletartoznak a kibertér infrastruktúra elemei, azonban a fentiekben bemutatott további összetevő típusokra ez már nem biztos, hogy igaz. Tehát a kérdés úgy is feltehető, hogy az adott alkalmazási terület szempontjából szükséges (figyelemmel kísérendő, felhasználható, befolyásolandó) összetevők-e a kibertérben elérhető információ reprezentációk, a kibertéri szereplők, illetve a kibertérben bekövetkező események, végrehajtott tevékenységek (illetve ha igen, akkor ezek mely altípusai).

A második kérdés az, hogy a kibertér infrastruktúra elemei, szereplői mind fizikailag létező dolgok helyettesítői, elérési lehetőségei, *vagy a kibertérben vannak a valóságban nem létező összetevők* (tisztán virtuális eszközök, szereplők) is. A válasz elvileg egyértelmű, mert mindenképpen lehetnek (sőt vannak) az utóbbi csoportba tartozó összetevők is. Emiatt a kérdés úgy is megfogalmazható, hogy az adott alkalmazási terület szempontjából van-e jelentősége tisztán virtuális kibertéri összetevők figyelembe vételének.

Végül az előző kérdéshez részben kapcsolódik az a kérdés, hogy az adott alkalmazási terület számára *a* kibertér virtuális összetevői, vagy a mögöttük álló valós dolgok szerepe elsődleges (esetleg összetevő típusonként eltérő módon). Egyes alkalmazási területek számára a virtuális összetevők mögött álló dolgok (például kiszolgáló eszközök) léte, jellemzői, földrajzi helye lehet teljesen lényegtelen, más alkalmazási területek esetében pedig a tevékenység céljai, tárgyai éppen a létező dolgok (például ellenségek, bűnözők, stb.), amelyekkel fizikai valójukban is szándékaik, feladataik vannak.

A kibertér fizikai összetevőihez kapcsolódó legfontosabb kérdés (amennyiben valaki a kiberteret vegyes jellegűnek tekinti) megítélésem szerint az, hogy hol húzódik ezen összetevők körének határa, mely rendszerek, eszközök tartoznak a kibertér fizikai összetevői közé, és melyek nem.

– ide sorolandóak-e az Internetre csatlakozó, de nem hagyományos informatikai rendszerek, eszközök;
– ide sorolandóak-e az Internetre még közvetlenül sem csatlakozó, de azonos technológiára épülő autonóm informatikai rendszerek, eszközök;
– és ide sorolandóak-e (figyelembe veendőek-e) az elektronikus adathordozók.

Végül kérdésként fogalmazható meg, hogy milyen szempontok alapján sorolhatóak be a valós fizikai dolgok a kibertér összetevői, a hagyományos fizikai tér (terek) összetevői körébe, vagy mindkettőbe.

Szereplők, tevékenységek, folyamatok a kibertérben

A kibertér szereplőinek, tevékenységeinek, eseményeinek értelmezése szorosan kapcsolódik a kibertéri helyzetismerethez (cyber situational awareness), kiber helyzetképhez (cyber operational picture). A helyzetismeret általában a helyzetre vonatkozó adatok gyűjtésének, feldolgozásának és értékelésének eredménye, a kialakult helyzet mentális képe. Ez nem egyszerűen az összegyűjtött (megszerzett) és szintetizált információk összessége, hanem ezeknek meghatározott szempontoknak eleget tevő, célorientált értelmezés és következtetések segítségével kiegészített rendszere. A helyzetkép a helyzetismeret valamilyen, jellemzően vizuális formában történő megjelenítése.

A kibertér szereplőire, tevékenységeire, folyamataira vonatkozó értelmezési kérdések arra irányulnak (a kibertér eltérő értelmezései eszerint is megkülönböztethetőek), hogy kiket tekintünk a kibertér szereplőinek, illetve miket tekintünk kibertéri eseményeknek, tevékenységeknek. A kibertérben elméletileg aktív szereplők nélkül is következnek be események (változások), ezért a továbbiakban elsőként a kibertéri eseményekre vonatkozó értelmezési kérdéseket vizsgáljuk meg. Ezt követően számba vesszük a kibertér szereplőihez, végül a szereplők által végrehajtott tevékenységekhez kapcsolódó értelmezési kérdéseket.

A kibertér eseményei

A kibertér eseményei a kibertér összetevőinek állapotában, tulajdonságaiban bekövetkező változások. Ezek köre a kibertér összetevőinek köréhez hasonlóan értelmezés kérdése, alkalmazási terület függő. Különböző felek – ahogy eltérő összetevőket tekinthetnek a kibertér részének – ezen összetevőkhöz kapcsolódó eltérő eseményeket tekinthetnek kibertéri eseményeknek is. A felek értelmezése a kibertéri események köréről lehet bennfoglaló, átfedő, vagy elkülönülő is.

A témánkhoz szorosan kapcsolódó kiber-helyzetismeret, kiber-helyzetkép tartalma általában tágabb, mint kibertéri események köre, részét képezik, képezhetik a kibertér környezetében végbemenő események is. A kibertér környezete eseményeinek lehetséges köre a kibertér globális, vagy körülhatárolt értelmezésétől is függ. Globális értelmezés esetén a kibertéren kívül nincsenek kiber-összetevők, így a környezet esetében csak valós összetevőkhöz kapcsolódó események jöhetnek szóba. Lokális értelmezés esetében viszont a kibertéri eseményekkel megegyező típusú, a globális kibertér környezeti eseményei is lehetnek.

Jelentősebb értelmezési kérdés annak megválaszolása, hogy a kibertéri események biztonsági események-e. Mivel a kibertér fogalma, értelmezése a gyakorlatban szorosan kapcsolódik a kiberbiztonsághoz, kibervédelemhez, abban lényegében egyetértés van, hogy (bár értelmezésük nem egységes) a kiberbiztonsági események a kibertér kiemelt eseményei közé tartoznak. A kibertér eseményei közé sorolhatóak azonban nem biztonsági jellegű, de az adott alkalmazási terület számára érdeklődésre számot tartó, a kibertér, vagy környezetének összetevőihez kapcsolható események is. Ilyenek lehetnek például adott szolgáltatás igénylése, új felhasználó létrehozása, vagy meghatározott számú szolgáltatási igény kielégítése, felhasználó szám elérése.

A kibertéri biztonsági események értelmezése esetében tisztázandó, hogy ezek közé tartozik minden, a biztonság esetleges, elvileg lehetséges megsértését eredményező *esemény* (event), vagy ezek közül csak a működési folyamatokat, a biztonságot nagy valószínűséggel fenyegető *biztonsági események* (incident).[24] Elsőként ki kell hangsúlyoznunk, hogy a szakirodalomban eltérések vannak a (biztonsághoz) kapcsolódó] esemény és biztonsági esemény, valamint az információbiztonsági, elektronikus információ biztonsági, IT-biztonsági és kiberbiztonsági esemény fogalmak közti eltérések, kapcsolatok értelmezésében (ez utóbbiak részletes szakirodalmi hivatkozásaitól jelen publikációban eltekintünk).

A NATO Kibervédelmi Kiválósági Központ fogalomjegyzékében hivatkozott két meghatározás szerint a *kiberesemény* (cyber event) kiberbiztonsági változás, amely hatással lehet a szervezeti működésre (továbbá a küldetésre, képességekre, vagy jó hírnévre).[25] A *kiberbiztonsági esemény* (cyber incident) pedig számítógép-hálózatok felhasználásával végrehajtott tevékenység, amely tényleges vagy potenciális káros hatást gyakorol egy informatikai rendszerre és/vagy a benne található információkra.[26] Ez utóbbi dokumentum szerint a *biztonsághoz kapcsolódó esemény* (security-relevant event) olyan esemény (jelzés), amelynek potenciális biztonsági vonatkozásai lehetnek egy rendszerre, vagy környezetére, és amely további tevékenységeket (feljegyzést, kivizsgálást, reagálást) igényelhet.[27]

Végül értelmezési kérdés lehet az is, hogy a kibertéri események *elemi események*, vagy *összetett események* is. A kibertér esetében is, mint általában, elemi esemény alatt egy adott időpontban megfigyelt, érzékelt, mért, jelzett változást értünk. Az elemi eseményekből logikai műveletekkel összetett események definiálhatóak (például adott időtartam alatt legalább *n* meghibásodás bekövetkezése; adott időtartamon belül *n* különböző típusú fenyegetés bekövetkezése), amelyek megtörténtét már az elemi eseményeket érzékelő szereplő, rendszer határozza meg.

---

24 Analógiaként lásd az ISO 27000:2016 'information security event' és 'information security incident' fogalmait [ISO/IEC 27000:2016(E), Information technology – Security techniques – Information security management systems – Overview and vocabulary. Fourth Edition. International Organization for Standardization – International Electrotechnical Commission, Genf, 2016. 6. o.]

25 Framework for Improving Critical Infrastructure Cybersecurity. Draft Version 1.1National Institute of Standards and Technology, 2017 január, 112.

26 CNSSI 4009, Committee on National Security Systems (CNSS). Committee on National Security Systems, 2015 április, 40.

27 CNSSI 4009, Committee on National Security Systems (CNSS). Committee on National Security Systems, 2015 április, 112.

A kibertér szereplői

A kibertér szereplői aktív összetevők, amelyek kibertéri tevékenységeket valósítanak meg, változásokat, változás sorozatokat idéznek elő a kibertér összetevőinek állapotában. A szereplőkhöz kapcsolódó, típusaikra és jellemzőikre vonatkozó eltérő értelmezések a kibertéri eseményekhez hasonlóan alkalmazási terület függőek. Ezek közül két jellegzetes alkalmazási terület, megközelítés a kiberbiztonsági eseménykezelés, illetve a katonai – vagy speciális rendeltetésű – erők kiberműveletei. A következőkben először a kibertér szereplőinek köréhez, majd a szereplők jellemzőihez kapcsolódó értelmezési kérdéseket vesszük sorra.

A kibertér szereplőire vonatkozó első, alapvető kérdés, hogy egyáltalán vannak, vagy nincsenek szereplők. Az első megközelítés szerint a kibertér egy *üres* színtér, amelyben események történnek, de ezek esetleges kiváltói nem képezik vizsgálat tárgyát. A második megközelítés szerint vannak azonosított szereplők, ebben az esetben kérdés, hogy ezek csak passzív, vagy aktív szereplők is. Az előbbiek olyan szereplők, amelyek a kibertér infrastruktúra-elemeit, erőforrásait működtetik, vagy ezek szolgáltatásait veszik igénybe (üzemeltetők, felhasználók). Az utóbbiak pedig olyan szereplők, amelyek célja kibertéri erőforrások működésének, szolgáltatásainak megakadályozása, korlátozása, vagy a működési, szolgáltatási szintek megóvása, fenntartása.

A következő fontos kérdés, hogy a kibertér szereplői (amennyiben vannak) csak virtuális, vagy virtuális és valós szereplők. Ezek között elsődleges szerepet a kibertér *bennszülött*, virtuális szereplői játszanak, amelyeket a szakirodalom kiber, online, vagy digitális identitásnak (cyber, online, digital identity), vagy kiber személyiségnek (cyber persona)[28] nevez. Az identitás ebben az értelemben leegyszerűsítve valaki, vagy valami alapvető jellemzőinek, és tevékenységeinek összessége,[29] a személyiség pedig valaki identitásának önmaga által közreadott, vagy mások által érzékelt összetevőinek együttese.

A virtuális szereplők, identitások jelentős része valós szereplő, identitás megjelenési formája a kibertérben, de lehetnek autonóm módon működő, valós szereplők vagy programok által létrehozott virtuális szereplők (például robotok) is. A virtuális és a valós szereplők közötti kapcsolat nem mindig, vagy nem könnyen azonosítható. Ezen kívül egy valós szereplőhöz tartozhat több virtuális szereplő, és egy virtuális szereplőhöz tartozhat több valós szereplő.

Végül eltérés lehet abban, hogy a kibertér szereplői *csak elemi*, vagy *összetett* szereplők. Ez utóbbi két értelemben is lehetséges. Az első az, amikor az ugyanazon virtuális szereplőhöz tartozó több valós szereplőt (például szervezeti e-mail fiók) együtt csoportként, szervezetként is azonosítunk, figyelembe veszünk. A második pedig az,

---

28 A kiber személyiség a kibertérben használt identitás, amelyet egy szereplő – valós identitásától és hovatartozásától elválasztva – információszerzésre, vagy mások befolyásolására használ. (Vö. GL-50 o. Terms & Definitions of Interest for DoD Counterintelligence Professionals. Office of Counterintelligence, Defense CI & HUMINT Center, Defense Intelligence Agency, 2011 május. GL-50 o.)

29 Amelynek segítségével valaki, valami megkülönböztethető másoktól, önállóan azonosítható, elnevezhető.

amikor a különböző virtuális szereplőket a saját, vagy a mögöttük álló valós szereplők jellemzői, tevékenységei alapján együtt csoport szereplőként (például összehangoltan működő kiber támadó csoport) is kezelünk.

A kibertér szereplőinek jellemzői esetében mindenekelőtt az a kérdés, hogy *mi azonosítja* a virtuális szereplőket. A virtuális szereplők azonosítása a különböző alkalmazási területeken eltérő célokat szolgálhat. Ezek közé tartozhatnak például a következők:

– a virtuális szereplő kibertéri helyének azonosítása;
– a virtuális szereplő kibertéri tevékenységének megakadályozása, korlátozása;
– a virtuális szereplő eltávolítása a kibertérből, megszüntetése;
– a virtuális szereplő azonosítása együttműködési információcsere során;
– a virtuális szereplő mögött álló valós szereplő azonosítása.

A kibertér hálózati jellegéből, valamint a TCP/IP protokoll alkalmazásának hegemóniájából következően a kibertéri tevékenységeket végrehajtó szereplők legalacsonyabb szinten (hamis, vagy valós) IP-címhez, magasabb szinteken különböző azonosítókhoz (felhasználónév, e-mail cím, fiók, stb.) köthetőek.

További fontos értelmezési kérdés lehet a *kibertéri szereplők besorolása*, amely az előző kérdésekhez hasonlóan alkalmazási terület függő. Az eltérések azonban információcsere során nehezítik a közös érdeklődésre számot szereplők egymással összhangban álló besorolását. Besorolásokkal elsősorban a kiberbiztonsági területen, a fenyegetéseket szándékosan, vagy gondatlanul kiváltó szereplők (threat actor) esetében találkozhatunk. A gyakorlatban több ilyen besorolás, tipológia is létezik (például Marinos, Louis – Belmonte, Adrian – Rekleitis, Evangelos 2016), és ezek bemutatásával, elemzésével is foglalkoztak már kutatók. (Bruijne, Mark de – Eeten, Michel van – Gañán, Carlos Hernández – Pieters, Wolter 2017)

A kibertér tevékenységei

Tevékenység alatt általánosságban aktív szereplők által végrehajtott szándékos, tudatos, célirányos cselekvéseket értünk. Nincs ez másként a kibertéri tevékenységek esetében, amelyeket így a kibertér szereplői által végrehajtott szándékos, célirányos cselekedeteknek tekinthetünk. A kibertéri tevékenységek közvetve, vagy közvetlenül hatással vannak a kibertér összetevőire. A tevékenységeket végrehajtó szereplők, és ezzel maguk a tevékenységek célja a kibertér összetevőinek kívánt állapota, állapotváltozása. A kibertéri tevékenységek köre, típusai az ebben a pontban tárgyalt más összetevőkhöz hasonlóan erősen alkalmazási terület függő. A következőkben megfogalmazzuk a kibertéri tevékenységek létére, tartalmára, típusaira, illetve az összehangolt tevékenységrendszerekre vonatkozó értelmezési kérdéseket.

A kibertéri tevékenységekre vonatkozó legáltalánosabb értelmezési kérdés, hogy *folynak-e a kibertérben tevékenységek*, vagyis egyes kibertéri események, folyamatok hozzákapcsolásra kerülnek-e kibertéri szereplőkhöz. Ha a kibertérben nincsenek, vagy nem kerülnek azonosításra szereplők, nincsenek, nem lehetnek tevékenységek sem. Természetesen a kibertéri események, folyamatok mögött – azok okaiként, vagy megvalósítóiként – ekkor is állhatnak szereplők és tevékenységek, azonban ezek az adott alkalmazási terület érdeklődésére nem tartanak számot.

A következő kérdés, hogy a kibertéri tevékenységek csak *virtuálisak*, vagy lehetnek *valósak is*. A kérdés lényege abban áll, hogy kibertéri tevékenységnek tekintjük-e virtuális jellegű kibertér esetében a virtuális összetevők mögött álló, de annak részét nem képező, vegyes jellegű kibertér esetében pedig a kibertér részét képező fizikai dolgokra irányuló tevékenységeket (például kiszolgáló számítógépek fizikai támadását). Az nem kérdéses ugyanis, hogy a valós dolgokra irányuló tevékenységek hatást gyakorolnak az általuk megvalósított virtuális dolgokra is.

Jelentős kérdés a kibertéri tevékenységek és kibertéri események viszonyának értelmezése is. Ezek megkülönböztetése nem egyszerű, és nem is egységes, legtöbbször nem is kerül rá sor (például amikor egy informatikai rendszerben bekövetkező eseményt támadásnak nevezünk). Pedig egy szereplő által végrehajtott tevékenység és az annak eredményeként bekövetkező változások megkülönböztetése számos esetben fontos lehet. Egy korai, már kevéssé alkalmazott megközelítés (Howard, John D. – Longstaff, Thomas A. 1998) szerint például az esemény egy célponton (kibertéri összetevőn) végrehajtott művelet, amelyből rengeteg következik be. Az események egy része egy sebezhetőséggel, az ezt kihasználó eszközzel, és az esemény nem jogosulatlan eredményével együtt alkot támadást. Végül egy támadás a támadó szereplővel és célkitűzésével együtt válik biztonsági eseménnyé (incidenssé).

A kibertéri tevékenységekkel kapcsolatos értelmezési kérdés az is, hogy a kibertéri erőforrások működtetése, szolgáltatásaik igénybevétele, illetve működésük, szolgáltatásaik támadása és védelme közül mely tevékenységtípusok tartoznak ide. Az erre adott válasz jelentős mértékben eltér a kibertéri szolgáltatásokhoz, a kiberbiztonsághoz, illetve a kiberhadviseléshez kapcsolódó alkalmazási területek esetében. Ehhez kapcsolódik az a kérdés, hogy a kibertéri tevékenységek részletesebb besorolása milyen módon történik. Erre vonatkozóan a legtöbb, de nem egységes eredmény a kibertéri támadó tevékenységekhez, támadásokhoz kapcsolódik, amelyek részét képezik a kiberfenyegetések besorolási rendszereinek, taxonómiáinak (attack taxonomies, threat taxonomies).

Végül alkalmazási területeket megkülönböztető értelmezési kérdés, hogy a kibertéren egyedi tevékenységek, vagy összehangolt tevékenységrendszerek, műveletek kerülnek-e végrehajtásra. Ez utóbbi magasabb szintű, szélesebb körű, a kiberhadviselés igényeit kielégítő megközelítés, amely több összefüggés feltárására, szemléltetésére, illetve összetett műveletek megtervezésének támogatására alkalmas.

Összegzés

Jelen publikáció meghatározta, rendszerezte a kibertér fogalmához, valamint annak összetevőihez kapcsolódó, eltérő értelmezésekhez vezető, legfontosabbnak tartott kérdéseket. E kérdések meghatározásának célja az volt, hogy elősegítse az egyes alkalmazási területek kibertér értelmezései részletes tartalmának tisztázását, lehetővé tegye különböző értelmezések összehasonlíthatóságát, eltéréseik feltárását, mindezzel a köztük fennálló információcsere eredményességét, hatékonyságát.

Az értelmezési kérdések első nagy csoportját a kibertér jellegéhez kapcsolódó kérdések alkotják. Talán a legfontosabb kérdés, hogy a kibertér tisztán virtuális, vagy vegyes jellegű (vagyis vannak fizikailag létező összetevői is). Eltérő értelmezések

vannak azzal kapcsolatban, hogy a kibertér milyen kapcsolatban áll a hagyományos fizikai (szárazföldi, tengeri, légi, űrbeli), vagy az elektromágneses tartományokkal, elkülönül-e azoktól, vagy átfedi azokat. Végül álláspontot kell foglalni abban a kérdésben is, hogy a kibertér globális jellegű, vagy egy szereplőhöz kötődik, és korlátos.

A kibertér összetevőihez kapcsolódóan is számos értelmezési kérdés vethető fel. Elsőként, hogy mik tartoznak a kibertér virtuális összetevői közé: vannak-e a kibertérben szereplők, és zajlanak-e benne szándékos, célirányos tevékenységek. Az értelmezést világítja meg az a kérdés is, hogy az adott alkalmazási terület számára a kibertér virtuális összetevői, vagy a mögöttük álló valós dolgok szerepe elsődleges. Végül talán az egyik legfontosabb kérdés, hogy – közvetlenül, vagy közvetve – mely rendszerek, eszközök tartoznak a kibertér fizikai összetevői közé, és melyek nem (például a hálózatra csatlakozó nem hagyományos informatikai eszközök, a hálózatra nem csatlakozó, de azonos technológiára épülő autonóm eszközök).

A kibertér eseményeihez, szereplőihez és tevékenységeihez kapcsolódó értelmezési kérdéseire adott válaszok túlnyomó többsége alkalmazási terület függő megközelítést tükröz. Kérdés, hogy a kibertéri események csak biztonsági események-e, hogy ezek közé tartoznak-e a biztonság megsértésének elvi lehetőségét hordozó események (security event), vagy csak a biztonságot megsértő biztonsági események (security incident). Kérdés továbbá, hogy a kibertéren csak aktív (támadó, védő) szereplők tevékenykednek, vagy passzívak (szolgáltatók, alkalmazók) is. A kibertér jellegéhez igazodóan határozható meg, hogy a kibertéri szereplők csak virtuális, vagy valós szereplők is. Eltérő értelmezést takarhat a szereplők azonosításának módja, és a besorolásuk alapját képező osztályozási rendszer. A kibertéri tevékenységekhez kapcsolódóan kérdés, hogy körük mire terjed ki, és besorolásuk hogyan történik. Végül eltérő célt szolgál az elemi kibertéri tevékenységekre, illetve az összetett kibertéri műveletekre épülő megközelítés.

A publikáció végén még egyszer szükséges hangsúlyozni, hogy a megfogalmazott kérdésekre többféle, a különböző alkalmazási területek számára megfelelő válasz adható. A kérdések feltevésének célja az alkalmazási terület által használt értelmezés tartalmának egyértelműsítése, részletezése, más értelmezésekkel való összevethetőségének elősegítése. A kérdések végiggondolása és megválaszolása nélkül nem egyértelmű például, hogy egy adott alkalmazási terület mit tekint a kibertér részének és mit nem; hogyan értelmezi a virtuális és a valós összetevők szerepét; vagy kiket tekint a kibertér szereplőinek.

FELHASZNÁLT IRODALOM

Joint Vision 2020. US Joint Chiefs of Staff, 2000 május

AJP 3.2(A), Allied Joint Operations for Land Operations. NATO Standardization Office, 2016 március

Tallinn Manual on the International Law Applicable to Cyber Warfare (Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence). Cambridge University Press, 2013

60/2013 (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról

AJP 01(E), Allied Joint Doctrine. NATO Standardization Office, 2017 február

AJP 3(B), Allied Joint Doctrine for the Conduct of Operations. NATO Standardization Office, 2011 március

Haig Zsolt – Kovács László (2008): Fenyegetések a cybertérből. Nemzet és Biztonság, 2008/5. 61–69. o.

NATO Cooperative Cyber Defence Centre of Excellence: Cyber Definitions. https://ccdcoe.org/cyber-definitions.html (Letöltve: 2017. 07. 22.)

JP 3-0, Joint Operations. – US Joint Chiefs of Staff, 2017 január.

AAP-6 NATO Glossary of Terms and Definitions (English and French). NATO Standardization Office, 2015

JP 3-12(R), Cyberspace Operations. US Joint Chiefs of Staff, 2013 február

FM 3-38, Cyber Electromagnetic Activities. Headquarters Department of the Army (US), 2014 február

Terms & Definitions of Interest for DoD Counterintelligence Professionals. Office of Counterintelligence, Defense CI & HUMINT Center, Defense Intelligence Agency, 2011 május

JP 3-32, Command and Control of Joint Maritime Operations. US Joint Chiefs of Staff, 2013 augusztus

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

The National Strategy to Secure Cyberspace. The White House, Washington, 2003 február.

Kiss Attila – Krasznay Csaba (2017): A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. Információs Társadalom, 2017/1. 55–71. o.

ISO/IEC 27000:2016(E), Information technology – Security techniques – Information security management systems – Overview and vocabulary. Fourth Edition. International Organization for Standardization – International Electrotechnical Commission, Genf, 2016

Framework for Improving Critical Infrastructure Cybersecurity. Draft Version 1.1 National Institute of Standards and Technology, 2017 január.

CNSSI 4009, Committee on National Security Systems (CNSS). Committee on National Security Systems, 2015 április

ISO/IEC 24760-1:2011, Information Technology – Security Techniques – A framework for identity management. Part 1: Terminology. International Organization for Standardization – International Electrotechnical Commission, Genf, 2011

Marinos M., Louis - Belmonte, Adrian - Rekleitis, Evangelos (2016): ENISA Threat Landscape 2015. – European Union Agency for Network and Information Security, 2016 január

Bruijne, Mark de – Eeten, Michel van – Gañán, Carlos Hernández – Pieters, Wolter (2017): Towards a new cyber threat actor typology. A hybrid method for the NCSC cyber security assessment. Faculty of Technology, Policy and Management Delft University of Technology, Delft, 2017 július

Howard, John D. – Longstaff, Thomas A. (1998): A Common Language for Computer Security incidents. Sandia Report SAND98-8667. Sandia National Laboratories, 1998 október