EURÓPA ENERGIABIZTONSÁGA

EUROPEAN ENERGY SECURITY

SÓLYOM LEVENTE[1]

ABSZTRAKT

Az energiabiztonság megteremtése és fenntarthatósága egész Európának közös érdeke. Ennek geopolitikai, gazdasági és környezetvédelmi okai nyilvánvalóak. Az energiabiztonság „hármas" elve. A megújuló energiák alkalmazása garantálja-e az energiaellátás biztonságát? Az EU jelenlegi energiaszükségletének 53%-át importálja, évente 400 milliárd euróért. A kritikus energetikai infrastruktúrák és megújuló energiák kiberbiztonsága. Stratégiai perspektívák.

Kulcsszavak: energiabiztonság, energiapolitika, fosszilis üzemanyag, megújuló energia

ABSTRACT

Creating and maintaining the energy security is a common European interest. The geopolitical, economic and environmental reasons are obvious. The 'triple' principle of energy security. Does the use of renewable energies guarantee the security of energy supply? The EU imports 53% of its current energy needs for 400 billion euros annually. The cybersecurity of critical energy infrastructures and renewable energies. Strategic Perspectives.

Keywords: energy security, energy policy, fossil fuels, renewable energy

BEVEZETÉS

Nyugodt lélekkel kijelenthetjük, hogy az energiabiztonság a mai gazdaság és politika egyik legfontosabb témája. Az energia folyamatosan növekvő szerepe vitathatatlan modern életünkben. Magas életszínvonalunk sok energiát igényel, jóval többet, mint az elmúlt évszá-

[1] office@solyom.at | ORCID: 0000-0002-3489-3391 | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

zadokban és eközben gazdasági teljesítményünk zálogává is vált. Manapság magától értetődik, hogy az energia egyszerűen a rendelkezésünkre áll, és úgy gondoljuk, a készlet végtelen, közben energiaigényünk folyamatosan fog növekedni, mivel a növekvő gazdaság és az életszínvonal igényünk ezt megköveteli. Egyes vélemények szerint viszont az energia nemcsak a gazdasági növekedés alapja, hanem képes a szegénység csökkentésére, a társadalmi juttatások növelésére és bizonyos politikai függetlenség biztosítására is. Az energiaszakértők szerint a fosszilis tüzelőanyagok továbbra is dominánsak maradnak a globális energiafelhasználásban a következő 20 évben. Az ásványolaj és származékai, - melyek a legszélesebb körben használt üzemanyagok - valamint a földgáz iránti kereslet is növekszik a közeljövőben, ami az üzemanyag-kereskedelem világméretű bővülését eredményezi, különösen a cseppfolyósított földgáz (*liquefied natural gas **LNG***) területén. Mindez a tengeri tranzit- országok stratégiai jelentőségének növekedésével fog járni. Az érintett kormányok új kihívásokkal szembesülnek energiapolitikájuk során. Nem szabad elfelejteni azonban, hogy már átéltünk egy energetikai válságot, fájdalmas következményekkel. Ebből legalább egy dolgot megtanultunk: nem lehetünk biztosak abban, hogy az egyes országok és régiók mai nemzeti energiapolitikája továbbra is biztonságos utat jelent az energiaforrásokhoz, és megvéd minket az esetleges energiahiánytól, vagy időszakos kiesestől. Ezért kénytelenek vagyunk komolyan beszélni az energiabiztonságról és alternatívákat kell kidolgoznunk. Ennek érdekében el kell mélyíteni az energiaügyi párbeszédet, meg kell erősíteni az intézményközi együttműködést, és közös fellépésű, többoldalú energiapolitikát kell szorgalmaznia a régió országainak. Mindezen törekvések leg szakavatottabb koordinátora az Európai Biztonsági és Együttműködési Szervezet (a továbbiakban **EBESZ**), mint regionális biztonsági szervezet. Fő feladata a biztonság alábbi három dimenzióját megismertetnie a résztvevő államokkal és központosított irányítással összehangolni ezek tevékenységet:

- politikai-katonai dimenzió,
- gazdasági és környezeti dimenzió,
- emberi dimenzió.

MI AZ ENERGIABIZTONSÁG? A „HÁRMAS" ELV

Az energiabiztonság pontos meghatározása előtt, három fogalommal kapcsolatban kell néhány kérdést feltennünk, melyek nevezetesen a következőek: a termék, a gyártó és az ár.

A termék:

- A legfontosabb energiaforrások mindig és mindenki számára elérhetők-e?
- A termelő tudja-e ezeket folyamatosan biztosítani?
- Megbízható-e az erőforrás-tartalékok nyilvános becslése?
- Az illető ország kormányzásában meghatározó elv-e az átláthatóság?
- Mennyibe kerül a nyersanyagok kitermelése vagy előállítása?
- A termelő országok gazdaságilag megengedhetik-e maguknak az ehhez szükséges beruházásokat?
- A külföldi vállalkozók részvételét szívesen látják-e a termelő országokban?

A gyártó:

- Hol található földrajzilag az energiaforrás?
- A termelési/lelő hely könnyen megközelíthető-e?

- Szükséges-e az export vagy az import lebonyolításához harmadik országot tranzitálni?
- Vannak-e alternatív szállítási útvonalak?
- Hogyan és kik szervezik a szállítást?
- Milyen kockázatot jelent a szállítás megszakítása?
- Megkerülhető-e bizonyos beruházások révén a tranzitálási szakasz?
- A fogyasztó országok megengedhetnek-e maguknak ilyen befektetéseket?
- Kinek a tulajdonában van a szállítási hálózatot?

Az ár:

- Mennyibe kerül a beszerezhető energia?
- Ki határozza meg az árat, különösen a földgáz és az olaj esetében?
- Van-e garancia a hosszú távú szállítási szerződésekre?
- Mennyire átláthatóak ezek a szerződések?
- Milyen szerepet töltenek be a kormányzati ügynökségek?
- A termelő országok hajlandóak-e / képesek-e befektetni a szállításba?

Ezen előzetes kérdések alapján megállapítható, hogy egy országnak vagy régiónak mekkora az energiabiztonsága. Ha mindhárom pont kérdéseire pozitív a válasz, akkor nagy valószínűséggel biztosítva van, ha ezek közülük egy vagy több nem teljesül, vagy kérdéses, az energiaellátás nem biztosított (OSCE Yearbook, 2018).

Egy másik tény, hogy a globális éghajlat gyorsabban változik, mint valaha, és az európai emberek egyre jobban tájékozottak e veszélyről. A tudást, felismerést pedig cselekedeteknek kell követnie. Az embereknek, a kormányoknak és a vállalkozóknak el kell ismerniük, hogy a környezetbarát energiaformákra való áttérés se nem drága se nem fájdalmas feladat. Éppen ellenkezőleg, előnyökkel jár, úgy mint: költségcsökkentés, új iparágak megjelenése, új munkahelyek teremtése és egyben az életszínvonal emelkedése.

A 2015. évi párizsi éghajlati megállapodás megmutatta, hogy a világ csak akkor képes korlátozni az éghajlatváltozást, ha lemond a fosszilis üzemanyagokról. A CO_2-kockázat egy sajátos gond. Az éghajlati megállapodás felhívta a figyelmet a megújuló energia alkalmazásának lehetőségeire és az energiahatékonyság előnyeire. Az elmúlt száz évben az országok geopolitikai ereje az energiaforrásaiktól függött. A jövőben fontos lesz a legjobb környezetvédelmi technológiák versenyképes bevezetése.

Azok az országok, amelyek elősegítik a napenergia és a szélenergia, az intelligens hálózatok és az energia-tárolás széleskörű implementálását, egy lépéssel a többiek előtt fognak járni.

Az európai gazdaság azonban továbbra is nagymértékben fog függeni a fosszilis üzemanyagoktól, különösen a fűtés és szállítás területén.

Az EU-ban a járművek több mint 90% -a fosszilis üzemanyagot használ. Ha csökkenne az autók száma a városokban, azonnal több hely maradna a gyalogosok, a kerékpárosok, és a tömegközlekedés számára. A belvárosok szennyezettségi szintje jó irányban változna, tisztább lenne a levegő és tüneményesen javulna a közegészség. A dízelgáz-kibocsátás káros hatásának ismerete valószínűleg növelné az elektromos járművek nép-szerűségét is.

Valójában a fő gond a lakosság energiahordozók iránti szemléletében rejlik mivel túl hosszú ideig voltak kitéve az földgáz és a kőolaj kitermelés geopolitikai érdekeinek.

Az energiahordozók terén bekövetkezhető paradigmaváltás aktív szereplőkké tehetné az egyént, mint a társadalom legkisebb sejtjét, a magáncégeket és a helyi önkormányzatokat, a megújuló energiaforrásokból történő villanyáram termelésben. Saját maguk villamos

energiát tudnának előállítani, és intelligens vezérlők segítségével használhatnák fogyasztásuk optimalizálására.
Az EU politikája több mint 20 évvel ezelőtt kezdte el az átmenetet az energiahordozók terén Európában. Így a mai politikai döntések, a következő évtizedek fejlődéséhez fogják megteremteni a szükséges keretet. Helyes döntésekkel, az EU megmentheti a Földet egy végzetes éghajlati változástól, és Európát a zöld technológiák éllovasává teheti (Heinrich Böll Stiftung).

TOVÁBBRA IS NYITOTT KÉRDES MARAD, HOGY A MEGUJULÓ ENERGIÁK (ME) ALKALMAZÁSA GRANTÁLJA-E AZ ENERGIAELLÁTÁS BIZTONSÁGÁT?

Napjaink átfogó, energiabiztonságról szóló viták fő témája, az **ME** jövőjéről fog szólni, a fosszilis korszak szén-dioxid-mentes átmenetelének szemszögéből nézve. A világ energiafelhasználói összetételének szén-dioxid-mentesítése sokszínű politikai dimenzióit fog létrehozni – például az olaj- és gáztermelő országok új stratégiai érdekvilágát – de sajnos ezt a nagyszereplők részben, gyakran teljes mértékben figyelmen kívül fogják hagyni, vagy mellőzik. Ez vonatkozik számos új technológia bevezetésére, a digitalizálás biztonsági vonzatára, valamint az állami, kereskedelmi és magán energia-infrastruktúrák fokozódó összekapcsolódására. Az **ME** és az egyéb „zöld-technológiák" egyre növekvő függőségének kérdése az úgynevezett kritikus alap és ásványi anyagoktól (például az akkumulátorok és az elektromobilitás) egymástól elszigetelten kerülnek vita tárgyává, és nagy ívben elkerülik a közvélemény figyelmét, de még a nagypolitika napirendjére sem kerülnek. Már egyértelművé vált, hogy a nemzetközi energiapolitika és biztonság **ME**-alapú korszaka nem a geopolitika, az új kockázati kihívások, sebezhetőségek és biztonsági tényezők végmegoldását jelenti. Ugyanakkor az ellátásbiztonság hagyományos geopolitikai kockázatai semmiképpen sem tűnnek el – legalábbis egy hosszabb, nem fosszilis korszakra való átmeneti időszakában. A tengeri biztonsági dimenziók és az új hatalmi-politikai rivalizációk (USA-Kína, Kína-India, Kína-Japán, USA-Oroszország stb.) szintén növekedhetnek.

A KRITIKUS ENERGETIKAI INFRASTRUKTÚRÁK ÉS MEGÚJULÓ ENERGIÁK KIBERBIZTONSÁGA

2017 tavaszán a „WannaCry" kibervírus (Wikipédia szócikk) több mint 200.000 számítógépet, titkosított adatokat tartalmazó a merevlemezt fertőzött meg világszerte, mintegy 150 országban. A hackerek 300 euró fizetséget kértek Bitcoinban az áldozatoktól, hogy a dekódoláshoz szükséges kódot megkapják. A „WannaCry" az Egyesült Királyságban, a Nemzeti Egészségügyi Szolgálatára (NHS) mért csapása során, ahol az informatikai hálózat egyharmadát lebénította, felfedte potenciális pusztító hatását a kritikus infrastruktúrákra, jelen esetben a kórházakra. A vírus a világ legnagyobb vállalatait is megfertőzte, és ismételten hangoztatták a hackerek,
az előkövetkezendőkben kormányok, vállalatok és a kritikus infrastruktúrák, számítógépes támadásokkal szembesülhetnek.
A biztonsági szakértők körében a „kritikus infrastruktúrákat" különösen veszélyeztetettnek tekintik, mivel ezek létfontosságúak az állam és állami funkciók fenntartásához, úgymint

Telekommunikációs rendszerek, logisztikai rendszerek, energiaellátás, egészségügyi ellátás, pénzügyi és egyéb érzékeny szolgáltatások, melyek magas belső bonyolultságúak és a nagyfokú kölcsönhatásuknak köszönhetők könnyen sebezhetőség.
A 2001. szeptember 11-i terrorista támadások óta a kritikus infrastruktúrák egyre inkább a számítógépes támadások célpontjává váltak, különösen az energiaágazatban. (Például a ***Stuxnet***, egy számítógépes féreg, amelyet 2010 júniusában fedeztek fel és először ***RootkitTmphider*** néven vált ismertté) (Wikipédia szócikk).
Az USA villamosenergia-hálózatában, 2009-ben, vírusokat észleltek, melyek valószínű-leg Kínából és Oroszországból kerültek a rendszerbe és az Egyesült Államokat, egy kényes külpolitikai vitában zsarolhatóvá tette. Egy újabb, de sokkal összetettebb, bonyolultabb kibertámadások sorozata 2014-ben érte az Egyesült Államokat. Az érzékeny műveleti és kommunikációs folyamatok/hálózatok károsítása vagy zavarása a „kritikus infrastruktúrák" területén, messzemenő politikai, társadalmi és gazdasági következményekkel járhat, amely más (szomszédos) államra is kihatással lehet.
A modern iparosodott társadalmakban az összes kritikus infrastruktúrát, egyre növekvő integrált hálózatépítés jellemzi, amelyben két elem kapcsolódik szorosan egymáshoz: az elektromosság és a világméretű internet.
Ha az elektromos áramot - a modern iparosodott államok és társadalmak „ütőerét" - vagy az internetet sikerül hosszú távra megszakítani, akkor az életfontosságú állami szolgáltatások működése, például az energia- és vízellátás, és sok más kritikus infrastruktúra, már nem garantálható. Az iparosodott társadalomban, minél inkább hálózatba vannak kötve a kritikus infrastruktúrák, az interneten keresztül, annál nagyobb a sebezhetőség kockázata.
Az európai energiaellátás és a kritikus energetikai infrastruktúrák elleni számítógépes támadások, valószínűleg a legnagyobb veszélyt jelentik számunkra. A kritikus energia-infrastruktúrák magukban foglalják a létesítményeket és energiatermelő hálózatokat, az olaj- és gázkitermelő egységeket, a tárolókat és finomítókat, az LNG-terminálokat, valamint a szállítási és elosztó rendszereket. Különösen sebezhetőek és érzékenyek a ***SCADA*** rendszerű (Wikipédia szócikk) energiaszabályozó központok.
Az EU 28 tagállama, 2005 óta felismerte a kritikus infrastruktúrákkal szembeni kiberbántalmazások lehetséges veszélyeit, és éppen ezért dolgozták ki a megfelelő nemzeti és többoldalú ellenstratégiákat a kritikus infrastruktúrák megerősítése és megszilárdítása érdekében, de még mindig hiányzik a teljes kivitelezés úgy állami, mind uniós szinten. A nemzetbiztonsági elgondolások itt sem elegendőek, mivel az ilyen számító-gépes támadások példátlan kifinomultságot értek el, és a digitális rendszerek, hálózatok sebezhetősége az utóbbi években exponenciálisan növekedett.
Manapság ezek a regionális villamosenergia-hálózatok az egyes tagországokra is kiterjedtek és liberalizáltan kapcsolódnak egymáshoz, az EU-27 közös energiapiac keretén belül. (korábban UCTE, ma ENTSO-E). Ez a, tagállamok energiabiztonságának erősítése érdekében kifejlesztett kapcsolat, egyre nagyobb mértékben függ a partnerek villamosenergia-hálózatainak stabilitásától.

Tehát a közös európai energia- és elosztórendszer csak annyira erős, mint ennek leggyengébb láncszeme

A Német Szövetségi Technológiai Felmérési Hivatal (TAB) által 2011-ben elvégzett kockázatelemzés arra a következtetésre jutott, hogy a több napig tartó nemzeti áramkimaradás,

kevesebb, mint egy héten belül az állam és a közrend teljes összeomlásához vezethet. Így, a közös és integrált európai energiapolitika és a transznacionális villamosenergia-hálózatok megteremtés egyrészt erősítik az energiabiztonságot, különösen egy válság idején, másrészt számos új, unión belüli, láncreakciószerű sérülékenységhez vezetnek.
Az új technológiák, például az intelligens hálózat ***Smart Grid*** (Wikipédia szócikk) és az intelligens mérés ***Smart Metering*** (Gabler Wirtschaftslexikon) bevezetése, valamint az ezzel járó villamosenergia-ágazat jövőbeli digitalizálása, elkerülhetetlenül növelni fogja a hackerek támadásfelületét. Emiatt új biztonsági intézkedések, standardok bevezetésére lesz elkerülhetetlenül szükség, de a belátható jövőben sem lesz szavatolható a teljes védelem, akármilyen mélyreható stratégiai lépéseket is tesznek.
2015. december 23-án, a történelemben meg soha nem látott cyber-támadás érte Ukrajnát. Első alkalommal hajtottak végre sikeresen számítógépes támadás az energiaágazat ellen, teljes áramszünetet okozván Ukrajna három nyugati tartományában. MIntegy 225.000 ember maradt 6 órán át áram nélkül, összességében 27 villamosenergia-elosztó létesítmény állt le, 103 várost teljesen és 186 várost részben zártak ki az energiaellátásból (Wikipédia szócikk). Az aggodalmat, nem utolsó sorban, az tetézte, hogy az Egyesült Államokban és az EU-ban az energiaellátás szinte teljes mértékben automatizált és hálózatba kötött. Valójában Ukrajna ehhez képest előnyös helyzetben volt, mivel manuálisan állíthatta vissza az energiaellátást, az elavult megszakítók és vezérlőpultok által. Utólag az amerikai és az európai villamosenergia-szakértők megállapították, hogy az Egyesült Államok és az EU-államok elvileg jobban fel vannak készülve egy ilyen kibertámadás megakadályozására, de a fejlett automatizálás, digitalizálás és hálózatépítés miatt, az energiaellátás viszonylag gyors helyreállíthatósága sokkal nagyobb gondokba ütközött volna.
Az Egyesült Államokban 2011 novemberében az illinoisi Springfieldben található Curran-Gardner vízművet orosz hackertámadás érte (Sucker, 2011). A támadás maga, a SCADA rendszerek távvezérelt karbantartási funkciójára irányult, amellyel a vezérlőrendszereket manipulálták. A vízszivattyú újra és újra be- és kikapcsolt, amíg a túlterhelés miatt végül kiégtek, anélkül, hogy a vízműveknek valamilyen nemű beavatkozási lehetősége lett volna.
2014-ben, Németországban, egy acélipari vállalat ellen történt támadás, minek következtében az ellenőrző és megfigyelő rendszer teljesen lebénult, és ennek eredményeként a kohó már nem tudott szabályozottan leállni, és az egész rendszer súlyos károsodást szenvedett (Scherschel, 2014). Az incidens után, 2014 májusában készített tanulmány szerint, a németországi nagyipari berendezések százainak és még a számítóközpontoknak sincs megfelelő védettsége.
2012 decemberében az ***50 Hertz*** nevű német villamosenergia-társaság beismerte, hogy egy súlyos, öt napos kieséssel járó, számítógépes támadás célpontja volt, amiről beszámoltak a szövetségi kormánynak (Fuest, 2012).
2016 áprilisában az ***RWE,*** mint a Grundremmingen atomerőmű üzemeltetője, bejelentette, hogy rosszindulatú programokat talált a feltöltő gép rendszerében, amelyet nyilvánvalóan internetkapcsolat létrehozására szántak (Zeit Online). Szerencsére a külső kapcsolat nem jöhetett létre, mivel a vezérlő rendszert (***SCADA***), valamint a feltöltő gépet, korábban lekapcsolták az internetről.
Az Egyesült Államok szakértői, 2009-ben, még idejében figyelmeztették az energiahálózatot működtető szerveket egy esetleges cyber-támadásról, amely 700 milliárd dollár kárt okozott volna a gazdaságnak, és hatásában felért volna 40-50 hurrikán egyidejű pusztításával.

Ha ez a támadás sikeres lett volna, egy beláthatatlan végű láncreakciót okozott volna a kontinensen.
Ehhez hasonló volt a 2006-os Emsland-i, emberi tévedés okozta műszaki hiba, melynek következtében 15 millió ember, 12 országot (beleértve Marokkót is) maradt villanyáram nélkül (Spiegel Online).
Mindezeket az eseteket a példa kedvéért említettem a teljesség messzemenő kiaknázása nélkül. Nap mind nap áll elő zavar a rendszerben, történnek balesetek, de egyre inkább foglalnak koronás helyet a kicsapongó időjárás okozta zavarok is. Ha nem is a fent említett méretűek, nagyon sok embernek tudnak alapvető gondot okozni, sokszor ember-életet követelve. Szélviharok, jégeső, áradások nemcsak az egyéni javakat, hanem a háztartási energiaellátást is pillanatok alatt károsítja, vagy teszi tönkre. Mivel ezek az idejárási jelenségek egyre nagyobb gyakorisággal jelentkeznek, komolyan el kell gondolkodni az egyének, a családi háztartások energiabiztonságáról és a kármegelőzésről. Erről ír Szűcs () *„Rendkívüli időjárási viszonyok közötti energiabiztonság megvalósításának lehetőségei családi ház esetében”* című tanulmányában.

ÖSSZEGZÉS ÉS STRATÉGIAI PERSPEKTÍVÁK

A 2030/2040-es időhorizontra tervezett paradigmaváltás, melyek végcélja a fosszilis alapú energiaforrások lecserélése megújuló energiaforrásokkal, az ***OPEC*** földgáz és kőolajtermelő országait kész tények elé állítja: új jellegű, intelligens befektetési, innovációs és oktatási politika révén, próbálják meg sikeresen diverzifikálni teljes gazdaságukat, a nyersolaj és földgáz kiviteléből származó óriási bevételi források révén, vagy pedig, elkerülhetetlenül szembesülni fognak belpolitikai, vagy akár regionális konfliktusokkal.
Közép és hosszútávon a szén-dioxid-mentesítési politika még nagyobb biztonsági kihívásokhoz vezet, a regionális és a globális stabilitás szempontjából, mivel sok olaj- és gáztermelő államnak nincs politikai akarata, gazdaságilag alternatív fejlesztési lehetősége a megvalósításra, és / vagy nincs elegendő pénzügyi forrása az ilyen finanszírozási stratégiákra.
Ugyanakkor be kell látni, hogy éppen új ***ME***-alapú energiakorban fognak, jellegzetes függőségi, kötődöttségi viszonyok kialakulni a kockázati rizikó és energiabiztonság kárára.
Ez különösen igaz a kiberbiztonságra, amelynek stratégiai jelentősége az energiabiztonság szempontjából legalább annyira nagy lesz, mint amit az olaj- és gázbiztonságra hagyományosan fordítanak. A kiber-támadások fenyegetését és hatékonyságát most a szárazföld, víz, légi és világűri harcvitel, új, ötödik frontjának tekintik. Példátlan kihívást jelentenek a nemzetközi közösség számára. Ezek a veszélyek egyre inkább megkérdőjelezik létjogosultságukban, a nemzeti és a kollektív biztonság, valamint a védelem és az elrettentés hagyományos módszereit és gondolatait. A számítógépes hadviselés új korszakát tehát már a történelmi technológiai ugrásokkal is el lehet érni.
Az internet és a stabil áramellátás kulcsfontosságú, de ugyanakkor a legnagyobb biztonsági veszély, láncreakció szerű hatás, az ellátás biztonságára, a nemzeti határokon túlmenően is.

HOGYAN TOVÁBB?

A közeljövőben számos energiaügyi határozatra lesz szükség, az elkövetkező évtizedek irányán elvei meghatározásához, és amennyiben jól koordinálják, hozzájárulnak az érintett országok gazdasági stabilitásához. Nincs olyan globális szervezet, amely az energiaügyekért felelős lenne, mivel az energia valódi társadalom-keresztmetszeti kérdéssé vált, és ezt, az egyes országok, szak-szervezetek konkrétan, saját szempontjuk szerint vizsgálják. Ezt a megítélést nem kétszeri munka elvégzésének kell tekinteni, hanem egy komplementáris tevékenységeknek.

Azt leszögezhetjük, hogy mindezek mellett az ***EBESZ*** alapvető megbízatása a biztonság. Amikor energiaügyi kérdésekkel foglalkozik, akkor biztonságpolitikai szempontból az ellátás biztonsága, a szállítás és a tranzit biztonsága, valamint az ellátási zavarok megelőzése a kitűzött cél.

Regionális szervezetként, az ***EBESZ*** helyszíni jelenléttel rendelkezik számos Eurázsia országban, ahol az energiaügyi kérdések különös jelentőséggel bírnak. Ez vonatkozik az energiatermelőkre és a tranzit országokra, valamint azokra az államokra, amelyek energiahelyzete bizonytalan. Politikai platformként az ***EBESZ*** előmozdíthatja az alternatív útvonalak kialakításáról folytatott vitát. Regionális szervezetként ösztönözheti a szorosabb együttműködés egyes formáit, mint például a már létező európai energiaközösség esetében. Válságkezelési megbízással rendelkező szervezetként az ***EBESZ*** hozzájárulhat az energiaügyi kérdéseket érintő regionális viták megoldásához. Amint azt a fentiekben hangsúlyoztam, az energiabiztonság nagyon összetett kérdés, amely jogi, geopolitikai, gazdasági és technikai szempontokat is magában foglal.

Összességében úgy gondolom, hogy egy ilyen érzékeny téma szoros nemzetközi együttműködést igényel.

FELHASZNÁLT IRODALOM

Auswirkungen einer Kartellbildung im Gassektor. https://kups.ub.uni-koeln.de/3332
http://www.forensic-investigations.de/Fi-Blog/Kritische-Infrastrukturen-gehackt-Einbruch-in-US-amerikanische-Wasser-Ver-und-Entsorgungswerke (letöltés ideje: 2019.08.02.)
https://de.wikipedia.org/wiki/Hackerangriff_auf_die_ukrainische_Stromversorgung_2015 (letöltés ideje: 2019.08.02.)
https://de.wikipedia.org/wiki/Intelligentes_Stromnetz (letöltés ideje: 2019.08.02.)
https://de.wikipedia.org/wiki/Stuxnet (letöltés ideje: 2019.08.02.)
https://de.wikipedia.org/wiki/WannaCry (letöltés ideje: 2019.08.02.)
https://wirtschaftslexikon.gabler.de/definition/smart-metering-53998 (letöltés ideje: 2019.08.02.)
https://www.boell.de/de/stiftung/wer-wir-sind (letöltés ideje: 2019.08.02.)
https://www.heise.de/security/meldung/BSI-Sicherheitsbericht-Erfolgreiche-Cyber-Attacke-auf-deutsches-Stahlwerk-2498990.html (letöltés ideje: 2019.08.02.)
https://www.spiegel.de/panorama/stromausfall-die-spur-fuehrt-nach-papenburg-a-446546.html (letöltés ideje: 2019.08.02.)

https://www.welt.de/wirtschaft/energie/article111369975/Russische-Hacker-attackieren-Stromnetzbetreiber.html (letöltés ideje: 2019.08.02.)
Krämer, Luis-Martín (2011): *Die Energiesicherheit Europas in Bezug auf Erdgas und die OSCE Yearbook 2018 Yearbook on the Organization for Security and Co-operation in Europe* (OSCE) Herausgegeben vom Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg / IFSH, 2019, 368 S., Gebunden, ISBN 978-3-8487-5691-9 (letöltés ideje: 2019.08.02.)
Pietsch, Christoph (2009): *Energiesicherheit. Europas Herausforderung im 21.* Jahrhundert. Seminararbeit. https://www.grin.com/document/143558 (letöltés ideje: 2019.07.20.)
Schröder, Hans-Henning – Tull, Denis M. (Hg.) (2008): Europäische Energiesicherheit 2020, Stiftung Wissenschaft und Politik, https://www.swp-berlin.org/publikation/europas-energiesicherheit-2020 (letöltés ideje: 2019.07.15.)
Supervisory Control and Data Acquisitions ttps://de.wikipedia.org/wiki/Supervisory_Control_and_Data_Acquisition (letöltés ideje: 2019.08.02.)
Szűcs, Endre (2010): *Rendkívüli időjárási viszonyok közötti energiabiztonság megvalósításának lehetőségei családi ház esetében* pp. 12-17. Paper: 8. In: Rácz, Pál (szerk.) IESB-2010, Budapest, Magyarország: Óbudai Egyetem