Az Európai Unió
Tanácsa

Brüsszel, 2017. június 7.
(OR. en)

9916/17

CYBER 91
RELEX 482
POLMIL 58
CFSP/PESC 476

FELJEGYZÉS AZ „I/A” NAPIRENDI PONTHOZ

Küldi:	a Tanács Főtitkársága
Címzett:	az Állandó Képviselők Bizottsága/a Tanács
Előző dok. sz.:	7923/2/17 REV 2
Tárgy:	Tervezet – A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („kiberdiplomáciai eszköztár”) – A következtetések elfogadása

1. A PBB 2017. március 14-i ülésén az EKSZ/a Bizottság szolgálatai bemutatták a kiberműveletekkel szembeni közös uniós diplomáciai intézkedésekről („kiberdiplomáciai eszköztár”) szóló közös vitaanyagot[1]. A delegációk üdvözölték a vitaanyagot és azt a javaslatot is, hogy a kezdeményezéssel a kiberkérdésekkel foglalkozó horizontális munkacsoport (HWPCI) keretében foglalkozzanak tovább. Ennek nyomán a PBB felkérte a HWPCI-t, hogy – adott esetben a Tanács más előkészítő szerveivel is konzultálva – részletesen vizsgálja meg a dokumentumot, mielőtt a PBB június végén ezen vizsgálat eredményét figyelembe véve újra visszatér a kérdésre.

2. A közös vitaanyag a PBB-től kapott felkérésnek megfelelően bemutatásra és megvitatásra került a HWPCI 2017. március 22-i ülésén is. A delegációk üdvözölték a dokumentumot, és jelezték, hogy elegendő időre van szükségük annak részletes vizsgálatához. A következő lépések tekintetében sok delegáció érvelt amellett, hogy az eszköztár mellé tanácsi következtetéseket is kidolgozzanak.

[1] WK 2569/2017 INIT.

3. Az elnökség ezért elkészítette a 7923/17 dokumentumban foglalt tanácsi következtetéstervezetet, amelyet a HWPCI két egymást követő – 2017. április 19-i, illetve május 12-i – ülésén bemutattak és megvizsgáltak; ennek során a szöveget a tagállamok észrevételeinek megfelelően tovább egyszerűsítették és javították.

4. A tanácsi következtetések tervezetének végleges szövegét a márciusi felkérésnek megfelelően 2017. június 6-án benyújtották a PBB-nek, és arról a Tanács általi elfogadása céljából, több kiegészítéssel[2], megállapodás született.

5. Ennek alapján felkérjük a COREPER-t, hogy kérje fel a Tanácsot, hogy hagyja jóvá a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („kiberdiplomáciai eszköztár”) szóló tanácsi következtetéseknek a mellékletben foglalt tervezetét.

---

[2] WK 6162/2017 REV 1.

MELLÉKLET

TERVEZET – A TANÁCS KÖVETKEZTETÉSEI A ROSSZ SZÁNDÉKÚ KIBERTEVÉKENYSÉGEKKEL SZEMBENI KÖZÖS UNIÓS DIPLOMÁCIAI INTÉZKEDÉSEK KERETÉRŐL („KIBERDIPLOMÁCIAI ESZKÖZTÁR”)

Az Európai Unió Tanácsa elfogadta az alábbi következtetéseket:

1. Az EU tudatában van annak, hogy a kibertér jelentős lehetőségeket kínál, ugyanakkor folyamatosan változó kihívások elé is állítja az EU külső politikáit, beleértve a közös kül- és biztonságpolitikát is, és megállapítja, hogy egyre nagyobb szükség van arra, hogy megvédjük az EU, az uniós tagállamok és az uniós polgárok adatainak sértetlenségét és biztonságát a kiberveszélyekkel és a rossz szándékú kibertevékenységekkel szemben.

Az EU emlékeztet az Európai Unió kiberbiztonsági stratégiájáról szóló következtetésekre[3], különösen azon határozott szándékára, hogy megőrizze a kibertér nyitottságát, szabadságát, stabilitását és biztonságát, valamint hogy biztosítsa, hogy a kibertérben teljes körűen érvényesüljenek az alapvető jogok és a jogállamiság. Emlékeztet továbbá a kiberdiplomáciáról szóló következtetéseire[4], különösen arra, hogy a kiberdiplomácia közös és átfogó uniós megközelítése hozzájárulhat a konfliktusmegelőzéshez, a kiberbiztonságot fenyegető veszélyek mérsékléséhez, és a stabilitás növekedéséhez a nemzetközi kapcsolatok terén.

Az EU és tagállamai hangsúlyozzák, mennyire fontos az EU folyamatos szerepvállalása a kiberdiplomácia terén, valamint az, hogy biztosítva legyen a kibertámadásokkal szembeni ellenálló képesség hatékony erősítését szolgáló uniós kiberbiztonsági kezdeményezések koherenciája, és határozott szándékuk, hogy a hatékony szakpolitikai koordináció keretében fokozzák a kiberpárbeszédekre irányuló erőfeszítéseiket; emellett hangsúlyozzák a harmadik országokban való kiberkapacitás-építés fontosságát.

2. Az EU-t aggodalommal tölti el az állami és nem állami szereplők részéről mutatkozó, arra való fokozott képesség és hajlandóság, hogy céljaikat – különböző hatókörű, léptékű, időtartamú, intenzitású, összetettségű, kifinomultságú és hatású – rossz szándékú kibertevékenységek révén igyekezzenek elérni.

---

[3] 12109/13.
[4] 6122/15.

Az EU megerősíti, hogy a rossz szándékú kibertevékenységek kimeríthetik a nemzetközi jogot sértő cselekmény fogalmát, és hangsúlyozza, hogy nem helyénvaló, hogy államok nemzetközi jogban foglalt kötelezettségeiket sértő ikt-tevékenységeket folytassanak vagy tudatosan ilyeneket támogassanak, és nem szabadna tudatosan megengedniük azt, hogy területükön információs és kommunikációs technológiák felhasználásával nemzetközi jogot sértő cselekményeket kövessenek el, ahogy azt az ENSZ kormányzati szakértői csoportjának 2015. évi jelentése megfogalmazza.

3. Az EU emlékeztet a kibertámadásokkal szembeni ellenálló képességnek – különösen a kiberbiztonsági irányelv végrehajtása és az abban foglalt operatív együttműködési mechanizmusok révén történő – javítását szolgáló uniós és tagállami erőfeszítésekre, és arra, hogy az információs rendszerek ellen irányuló rossz szándékú kibertevékenységek az uniós jog meghatározása szerint bűncselekménynek minősülnek, és hogy az ilyen bűncselekmények eredményes nyomozása és büntető eljárás alá vonása továbbra is a tagállamok közös törekvését képezi.

Az EU és tagállamai nyugtázzák azt a folyamatban lévő munkát, amelyet az ENSZ-nek a nemzetközi biztonság összefüggésében az információs és távközlési technológiák területén tapasztalható fejleményekkel foglalkozó kormányzati szakértői csoportja végez a 2010., 2013. és 2015. évi jelentésekre[5] építve, és eltökélt szándékuk annak a konszenzusnak a határozott érvényesítése, hogy a meglévő nemzetközi jog alkalmazandó a kibertérre is. Az EU és tagállamai szilárdan elkötelezettek amellett, hogy aktívan támogassák a kibertérben tanúsított felelősségteljes állami magatartás önkéntes, nem kötelező erejű normáinak kidolgozását, valamint az EBESZ által hozott azon regionális bizalomépítő intézkedéseket, melyek célja az információs és kommunikációs technológiák használatából eredő konfliktusok kockázatának csökkentése[6].

Az EU újólag megerősíti, hogy elkötelezett a kibertérben folyó nemzetközi viták békés úton történő rendezése mellett, továbbá hogy az EU minden diplomáciai erőfeszítésének kiemelt célként arra kell irányulnia, hogy megerősített nemzetközi együttműködésen keresztül hozzájáruljon a kibertér biztonságához és stabilitásához, valamint hogy csökkentse az esetlegesen az ikt használatából eredő félreértések, konfliktusterjedés és konfliktusok kockázatát. E tekintetben az EU emlékeztet az ENSZ Közgyűlésének az ENSZ tagállamaihoz intézett azon felhívására, hogy az ikt használatában kövessék az ENSZ kormányzati szakértői csoportjának jelentéseiben foglalt ajánlásokat.

---

5 A/68/98 és A/70/174.

6 PC.DEC/1106 (2013. december 3.) és PC.DEC/1202 (2016. március 10.).

4. Az EU nyomatékosítja, hogy a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések várható következményeinek egyértelmű jelzése hatással van a kibertámadások potenciális elkövetőire, és ezáltal erősíti az EU-nak és tagállamainak biztonságát. Az EU emlékeztet arra, hogy továbbra is – minden hírszerzési forrás figyelembevételével meghozandó – szuverén politikai döntés marad annak megítélése, hogy az elkövetést állami vagy nem állami szereplőnek tulajdonítják-e, és ezt az állami felelősségre vonatkozó nemzetközi joggal összhangban kell meghatározni. E tekintetben az EU hangsúlyozza, hogy a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések nem mindegyikéhez szükséges az állami vagy nem állami szereplőnek való tulajdonítás.

5. Az EU megerősíti, hogy a közös kül- és biztonságpolitika területéhez tartozó intézkedések, beleértve szükség esetén a Szerződések vonatkozó előírásai alapján elfogadott korlátozó intézkedéseket is, alkalmas eszközök lehetnek a rossz szándékú kibertevékenységekkel szembeni közös uniós fellépésre és ösztönözhetik az együttműködést, előmozdíthatják az azonnali és a hosszú távú veszélyek csökkentését, valamint hosszú távon hatással lehetnek a potenciális támadók magatartására. Az EU az alábbi elvek alapján fogja folytatni a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretének kidolgozását:

- védeni kell az EU, az uniós tagállamok és az uniós polgárok sértetlenségét és biztonságát,
- figyelembe kell venni az érintett állammal fennálló uniós külkapcsolatok tágabb összefüggéseit,
- biztosítani kell a KKBP-célkitűzések elérését, az Európai Unióról szóló szerződésben foglaltakkal és az e célkitűzések elérése érdekébenmeghatározott megfelelő eljárásokkal összhangban,
- az intézkedéseknek a tagállamok által közösen kialakított helyzetismereten kell alapulniuk és meg kell felelniük az adott helyzet támasztotta igényeknek,
- az intézkedéseknek arányosnak kell lenniük a kibertevékenység hatókörével, léptékével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásaival,
- tiszteletben kell tartani az alkalmazandó nemzetközi jogot és nem szabad alapvető jogokat és szabadságokat sérteni.

6. Az EU felszólítja a tagállamokat, az Európai Külügyi Szolgálatot (EKSZ) és a Bizottságot, hogy teljes mértékben dolgozzák ki a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretét, és e tekintetben megerősíti az iránti elkötelezettségét, hogy a Bizottság, az EKSZ és más releváns felek közreműködésével folytassa a keretre vonatkozó munkát, különösen – többek között az előkészítő és kommunikációs eljárásokra is kiterjedő – végrehajtási iránymutatások kidolgozásával, valamint az eljárások megfelelő gyakorlatok keretében való tesztelésével.