Spitzer Jenő

A francia kibervédelmi és kiberbiztonsági rendszer egyes stratégiai aspektusai

Military and Intelligence CyberSecurity Research Paper
2021/3.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Franciaország a kontinentális Nyugat-Európa egyik legaktívabb külpolitikáját folytató szereplője, történelmi és gazdasági okokból is számos – gyakran komplikált biztonsági helyzetű – régióban érintett, és határain belül is a fenyegetések teljes spektrumára kell megoldásokat találnia. Természetes tehát, hogy a kibervédelem terén is aktív, mind stratégiai-policy szinten, mint államszervezési, szervezetalakítási szinten. A 2008-as Fehér Könyvet, mint alapdokumentumot nemzeti és katonai stratégiák kiadása követte. Szervezeteket tekintve a „hagyományos" nemzetbiztonsági szolgálatok, mint kulcsszereplők mellé pedig megjelentek a speciális összkormányzati kibervédelmi szervezetek és a katonai magasabb szintű kibervédelmi parancsnokság is. A tanulmány ezt a fejlődési ívet és a legfontosabb tartalmi és elhatárolási pontokat foglalja össze.

Kulcsszavak: kibertér, kibervédelem, hírszerzés, szabályozás, együttműködés

France is one the most active player in continental Western Europe in foreign politics, it has interests based on historic and economic reasons in many regions – often with complicated security circumstances – and has to find solutions for the the whole spectrum of threats on domestic soil as well. Certainly it is active in cyber defence on strategic-policy level and governmental organisation also. The White Book of 2008 as a groundbreaking document was followed by national and military strategies. In regard of organisations new actors emerged: agencies with whole-of-goverment approach and a high level military command, beside the „traditional" national security agencies as key actors. The following study sums this evolution up with the most important subjects and distinctions.

Keywords: cyberspace, cyber defense, intelligence, regulation, cooperation

BEVEZETÉS

Az internet robbanásszerű elterjedése és fejlődése új kihívások elé állította az államokat mind a fejlődési irányok, mind a biztonsági kérdések szempontjából. E kihívások mind technológiai, mind pedig társadalomtudományi – és ennek részeként jogtudományi – értelemben elemzések tárgyát képezik a külföldi[1] és hazai diskurzusban is[2]. Az ezeknek való

[1] Lásd: DODGE, Martin – KITCHIN, Rob: Mapping Cyberspace, London-New York, Routledge, 2001; SCHMITT, Michael N.: Tallinn Manual on International Law applicable to cyber warfare, Cambridge, Cambridge University Press, 2013; ZIOLKOWSKI, Katharina (szerk.): Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy, Tallinn, NATO CCD COE Publication, 2013.; SCHMITT, Michael N. (szerk.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cyber Defence Center of Excellence, Cambridge, Cambridge University Press, 2017.; CLEMENTE, Dave.: Cyber Security and Global Interdependence: What Is Critical?, London: The RoyalInstitute of International Affairs. 2013.; CLARK, Richard; KNAKE, Robert.: Cyber War: the next threat to national security and what to do about.New York: HarperCollins Publishers Inc. 2010.

[2] Ennek kapcsán lásd: KELEMEN Roland, SIMON László: A kibertérben megjelenő fenyegetések és

megfelelés érdekében az államok, így Franciaország is, adekvát védelmi és biztonsági stratégiákat fogadtak el, történelmüktől, működési módjuktól, valamint az információs és kommunikációs rendszerek összekapcsolásának módjától függően.[3]

A francia kibervédelmi stratégiát számos doktrinális és szervezeti sajátosság jellemzi. Bár az elmúlt évek nem várt módon tették próbára a rendszereinek már kimunkált kereteit[4], annak célja változatlanul az, hogy Franciaország számára biztosítsa azokat az eszközöket, amelyek állampolgárai kiberbiztonságának garantálásán túlmutatóan lehetővé teszik, hogy mint nemzetközi hatalmi aktor (az ENSZ Biztonsági Tanácsának állandó tagja, valamint nukleáris hatalom), a kibertérben képes legyen az érdekei védelmére és érvényesítésére is.

A FRANCIA KIBERVÉDELEM STRATÉGIÁJÁNAK GLOBÁLIS IRÁNYAI

„Egy olyan időszakban, amikor az informatikai támadások bármelyik pillanatban súlyosan veszélyeztethetik a nemzet érdekeit, hazánknak a digitális szuverenitás hatékonyabb érvényesítése érdekében át kell alakítania a kibervédelemmel kapcsolatos álláspontját.”[5]. A 2018. február 12-én kiadott *Kibervédelmi Stratégia* ezzel a megközelítéssel azonosította az információs térben jelentkező veszélyeket és az azokkal szembeni fellépési képesség jelentőségét, továbbá jelentős szemléletváltozást tükröz az ország 2018-ban kiadott, Digitális Biztonságról Szóló Nemzeti Stratégiájával szemben. Ez azt jelenti, hogy eddig az időpontig Franciaország a kiberbiztonság technikai-katonai megközelítését tartotta megfelelőnek, azaz kizárólag az információs és kommunikációs rendszereik védelmén és

kihívások kezelésének egyes nemzetközi jogi problémái In: FARKAS Ádám, VÉGH, Károly (szerk.) Új típusú hadviselés a 21. század második évtizedében és azon túl– intézményi és jogi kihívások Budapest, Magyarország : Zrínyi Kiadó, 2020. 150-170.o.; KELEMEN Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése Honvédségi Szemle: A Magyar Honvédség központi folyóirata, 2020/4, 65-81. o.; FARKAS Ádám: A kortárs technológia-fejlődés és innováció viszonya honvédelmi szabályozással. MTA Law Working Papers 4: 4, 2021. 1-15. o.; KELEMEN Roland, FARKAS Ádám: To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare In: SZABÓ Marcel, GYENEY Laura, LÁNCOS Petra Lea (szerk.) Hungarian Yearbook of International law and European Law (2019) Den Haag, Hollandia : Eleven International Publishing (2020) pp. 203-226. o.; FARKAS Ádám: Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye? Gondolatok az angol National Cyber Force kapcsán. Military and Intelligence CyberSecurity Research Paper 2021/1.; VIKMAN László: A német kiberbiztonsági szisztéma áttekintése. Military and Intelligence CyberSecurity Research Paper 2021/2.

[3] DOUZET, Frédérick: Cyberespace : enjeux géopolitiques, Hérodote, n°152-153, 1er-2ème trimestre 2014, 313 o.

[4] Ennek kapcsán lásd: VERGARAM Ingrid: Face à la multiplication des attaques, la France accélère sa stratégie de cybersécurité. Le Figaro, 2021. február 17. https://www.lefigaro.fr/secteur/high-tech/face-a-la-multiplication-des-attaques-la-france-accelere-sa-strategie-de-cybersecurite-20210217 (Elérés dátuma: 2021. április 18.)

[5] *«A l'heure où les attaques informatiques sont susceptibles de porter à tout moment gravement atteinte aux intérêts de la Nation, notre pays doit adapter sa posture de cyberdéfense avec l'ambition de mieux faire respecter sa souveraineté numérique »* Franciaország 2018. február 12-én elfogadott Kibervédelmi Stratégiája 7. o.

ellenálló képességén alapuló, nagyobbrészt defenzív elgondolásra helyezkedtek. Ezt váltotta fel egy globális dimenzió, a digitális biztonság olyan megközelítését alkalmazva, amely minden gazdasági és társadalmi területet áthat és számításba vesz, és amelyben elhatárolódnak egymástól a defenzív és az offenzív feladatok. [6]

A katonai kibertevékenység előrelépése 2019. január 18-ra tehető, ekkor adták ki a Katonai Kiberstratégiát, amely az első olyan kifejezetten a kibervédelemre összpontosító katonai stratégiai dokumentum, amelynek bizonyos részeit nyilvánosságra hozták. Ezek ***„A katonai támadó kiberdoktrína nyilvános elemei”, valamint „A védelmi miniszter defenzív kiberpolitikájának nyilvános elemei”.***[7] Habár a nyilvánosságra hozott részdokumentumok figyelemre méltóak az offenzív kibertevékenységre tekintettel, tartalmuk nem szakít sem a Kibervédelmi Stratégiával, sem a Nemzeti Védelmi és Biztonsági Stratégiával, továbbá a már 2008-ban kiadott Fehér Könyv a nemzeti védelemről és biztonságról (a továbbiakban: Fehér Könyv) [8]. is elismeri az ilyen jellegű képességek szükségességét.[9] A két katonai kiberstratégiai dokumentum mindazonáltal fontos lépést jelent a francia kibervédelem katonai oldalán, nemcsak azáltal, hogy megszervezik és keretek közé helyezik az offenzív tevékenységet, hanem azáltal is, hogy az ország globális kiberhatalmi tényezőként való megjelenését is megerősíteni szándékozzák.

Fontos kiemelni, hogy a Kibervédelmi Stratégia pillérei között az elrettentés, a védekezés, a megelőzés és a fellépés mellett a megismerés és az előrejelzés pillérei is szerepelnek, amelyek alapvetően határozzák meg a kibervédelem szervezeti és funkcionális kereteit. A fellépés, megismerés és előrejelzés hármasa egyúttal megerősíti és megkerülhetetlenné teszi a titkosszolgálati szerepkört a hatékony kibervédelemben.

A francia kibervédelmi modell a következő szereplőkre épül:

- az Információs Rendszerek Biztonságáért Felelős Nemzeti Ügynökség (ANSSI[10]), amely az állam kibervédelméért és a defenzív kibertevékenység legfelső szintű koordinációjáért és technikai felügyeletéért – a miniszterelnök felügyelete alá utalva – felelős;
- a védelmi miniszter irányítása alá tartozó Kibervédelmi Parancsnokság (COMCYBER[11]), mint operatív elem;
- a védelmi miniszter irányítása alá tartozó nemzetbiztonsági szolgálatok (DGSE[12], DRSD[13], DRM[14]) és

[6] A francia kiberstratégia fejlődésével összefüggésben lásd: DESFORGES, Alix: Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l’exemple de la France. Thèse, Université Paris, 2018.

[7] On relèvera ici encore le choix de séparer distinctement les missions offensives des missions défensives même si, comme l’affirme les Éléments publics, la lutte informatique offensive peut être mise au service de la lutte informatique défensive.

[8] Livre blanc de la défense et de la sécurité nationale.

[9] Fehér Könyv 53. o.

[10] Agence nationale de la sécurité des systèmes d'information.)

[11] Commandement de la cyberdéfense

[12] Direction générale de la sécurité extérieure (Külső Biztonsági Főigazgatóság)

[13] Direction du renseignement et de la sécurité de la défense (Katonai Hírszerzési és Védelembiztonsági Igazgatóság)

[14] Direction du renseignement militaire (Katonai Felderítő Igazgatóság)

– a belügyminiszter szakosított nemzetbiztonsági szolgálata (DGSI[15]).[16]

A DEFENZÍV ÉS AZ OFFENZÍV TEVÉKENYSÉGEK ELHATÁROLÁSA, AZ INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁÉRT FELELŐS NEMZETI ÜGYNÖKSÉG ÁLTAL IRÁNYÍTOTT SZERVEZETI MODELL

A digitális szuverenitás biztosítása érdekében *Franciaország a 2008-ban kiadott, a védelemről és a nemzetbiztonságról szóló Fehér Könyv óta folyamatosan erősíti szervezeti, kapacitásbeli, humán és jogi eszközeit a kibervédelem biztosítása körében.* A Fehér Könyv a kibertér tekintetében kiemelt jellemzőként azonosította annak stratégiai jelentőségét, ami a francia stratégiai dokumentumok körében is komoly újításként hatott és ezzel – más államok törekvéseihez hasonlóan – majd tíz évvel előre vetítette azt az irányváltást, ami a NATO szintjén is végbe ment a walesi[17] és a varsói[18] csúcstalálkozókkal.

A Fehér Könyv által képviselt szemléletváltással összefüggésben az egyik legjelentősebb lépésként 2009-ben létrehozták az Információs Rendszerek Biztonságáért Felelős Nemzeti Ügynökséget (Agence nationale de la sécurité des systèmes d'information, a továbbiakban: ANSSI), az Információs Rendszerek Biztonságáért Felelős Központi Igazgatóság utódjaként[19], 2013 óta pedig az információs rendszerek biztonságáért felelős, általános hatáskörű nemzeti hatóságként látja el feladatát. [20] A miniszterelnök által rendeletben létrehozott, a védelmi és biztonsági főtitkárságnak, mint miniszterelnöki szervezeti egységnek az irányítása alá tartozó, főigazgató által vezetett *ANSSI általános feladatköre a védelmi és biztonsági főtitkár támogatása az információs rendszerek biztonsága terén fennálló hatásköreinek gyakorlásában.*[21] . Több szakterületet lát el technikai segítséggel, úgy mint

[15] Direction générale de la sécurité intérieure (Belbiztonsági Főigazgatóság)
[16] A külföldi nemzetbiztonsági szolgálatokról lásd: BÉRES János (szerk.): Külföldi nemzetbiztonsági szolgálatok. Budapest, Zrínyi Kiadó, 2018, 103-107. o.
[17] Ennek kapcsán lásd az Észak-atlanti Tanács ülésén résztvevő NATO-tagállamok állam- és kormányfőinek közös nyilatkozatát, amelynek 72-73. pontjai kitérnek a kibertérben rejlő fenyegetések súlyára, továbbá a szervezet kiberképességeinek fejlesztési objektíváira. A nyilatkozat a NATO kollektív védelmi tevékenységének kategóriájába emelte a kibertérből érkező fenyegetéseket.
Online: https://www.nato.int/cps/en/natohq/official_texts_112964.htm (Elérés dátuma: 2021. augusztus 14.)
[18] A varsói kommüniké 70-71. pontjaiban megerősítette a walesi deklarációt, egyúttal a kiberteret műveleti területként értelmezi.
Online: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (Elérés dátuma: 2021. augusztus 14.)
[19] Décret n°2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».
[20] Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, article 21.
[21] Décret n°2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ». art. 3.

- a digitális technológiáért és az állami információs és kommunikációs rendszerért felelős tárcaközi igazgatóság,
- az elektronikus hírközlésért felelős miniszter nyílt elektronikus hírközlő hálózatai, és
- a létfontosságú infrastruktúra információs elemei.[22]

A hatóság a francia kibervédelem szervezési sarokkövének is tekinthető, a francia kibervédelmi stratégia koordinálásáért felelős szervezet, amelynek feladatait a 2013-as[23] és 2018-as[24] katonai tervezési törvények fokozatosan terjesztették ki. Feladatainak bővülése és a 2015-ös digitális biztonságról szóló nemzeti stratégia, majd a 2018-as kibervédelmi stratégia által elfogadott megközelítés további szereplőkkel, például a belügyi, az igazságügyi és a külügyi tárcával szembeni pozícióját is megszilárdította és *egy erős, az ANSSI által vezetett és koordinált ágazatközi mechanizmust hozott létre.*[25]

Mint az információs rendszerek biztonságáért felelős nemzeti hatóság, javaslatot tesz a miniszterelnöknek a hatóságok és a létfontosságú szereplők információs rendszereinek biztonságát érintő vagy fenyegető válsághelyzetek reagálására irányuló intézkedésekre, és a miniszterelnök által meghatározott iránymutatások keretében koordinálja a kormányzati fellépést. E tevékenységi körben elvégzi az állami szervek, állami és magánszolgáltatók információs rendszereinek az ellenőrzését is. Ehhez tartozóan olyan mechanizmusokat is bevezethet, amelyek képesek egyrészt az érintett információs rendszereket fenyegető veszélyek előrejelzésére, másrészt a válaszlépések koordinálásának kiszolgálására.[26] Az ANSSI által koordinált tárcaközi szisztémát egy *olyan szervezési és irányítási modell határozza meg, amelynek alapvetése az offenzív (hírszerzési és műveleti) és a defenzív (elhárító és hálózatvédelmi) kapacitások elhatárolása.* Az elhatárolás egyúttal lehetőséget teremt az ANSSI számára a katonai kibervédelemmel való koordinatív együttműködésre, valamint a vállalati szereplőkkel történő hatékony kapcsolatteremtésre.[27] A modell alapján az ANSSI nem rendelkezik offenzív műveletek végrehajtásához szükséges képességgel, ugyanakkor az elhatárolás ellentmondást hordoz magában, mivel a nemzetbiztonságot veszélyeztető kibertámadások azonosítása és semlegesítése érdekében jogosult olyan lépéseket tenni, amelyek során hozzáférést kísérel meg vagy alakít ki a támadást indító informatikai rendszerekhez, ez pedig bizonyos fokú támadó kibertevékenységet szükségszerűen maga után von[28].

[22] Décret n°2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ». art. 5.
[23] Ibid., articles 21 et 22
[24] Loi n°2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, article 34.
[25] Revue stratégique de cyberdéfense, 52-55. o.
[26] Décret n°2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ». 2-4. cikk
[27] DANILO, D'Elia, La cybersécurité des opérateurs d'importance vitale: analyse géopolitique des enjeux et des rivalités de la coopération pulbic-privé, Thèse, Université Paris 8, 2017, 116-117. o.
[28] Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à

Az ANSSI-ről összességében elmondható, hogy a miniszterelnök közvetlen alárendeltségébe tartozó védelmi és biztonsági titkárság irányításával olyan ágazatok feletti, koordinációt biztosító szerv, amely a digitalizáció sokrétűsége és a digitális tér mára már végtelen kiterjedtsége okán technikai, műszaki és tudományos platformot biztosít, megalapozva a kibervédelem érdemi képességeit. Kiemelendő ugyanakkor az is, hogy mindez a rendvédelmi, a katonai és méginkább a nemzetbiztonsági szolgálatok hírszerző és elhárító képességeinek bedolgozása nélkül izolált és kihasználatlan eszközként állna rendelkezésre.

A HADERŐ HELYE A FRANCIA KIBERVÉDELEM RENDSZERÉBEN

A francia kibervédelmi tevékenység fentiekben kifejtett elhatárolási alapjából magától értetődően következik a haderő megkérdőjelezhetetlen és kiemelt szerepe, ami a védelmi miniszter feladat- és hatáskörében nyugszik. 2008-ban a védelemről és a nemzetbiztonságról szóló Fehér Könyvben a kibertér egy olyan újfajta cselekvési területként került meghatározásra, amelyben már katonai műveletek zajlanak.[29] A kibertérnek, mint a fegyveres összecsapások terepének ez a bemutatása az, ami a védelmi miniszter különleges helyét biztosítja.[30]. A fegyveres erők vezérkarának műveleti főnökhelyettese mellé *2011-ben nevezték ki a – védelmi miniszternek közvetlenül tanácsot adó – kibervédelmi parancsnokot*[31] amely jól jelzi a fegyveres erők hosszútávú és szervezett berendezkedését a kibervédelem és a kiberhadviselés területén.[32]

A 2013-as katonai tervezési törvény érdemi léptékváltást jelentett, amiben sor került a kibervédelem valódi operatív láncolatának megszervezére. *A fejlődés 2017-ben a Kibervédelmi Parancsnokság (Le Commandement de la Cyberdéfense, a továbbiakban: COMCYBER) létrehozásával folytatódott, amely közvetlenül a fegyveres erők vezérkari főnöke alá van rendelve.* A COMCYBER a fegyveres erők valamennyi kibervédelmi erőiből álló operatív parancsnokság, amely a védelmi ágazaton belül közel 3400 katona felett gyakorol irányítási jogkört. A 2014-2019-es katonai tervezési törvény időszaka alatt a kiberhadsereg létszáma a korábbiakhoz képest megduplázódott (elérve a 3200 főt), a 2019-2025-ös időszakra pedig pedig további 1000 fős létszámnövekedést határoz meg a tervezési törvény.

A 2017 májusában rendelettel létrehozott COMCYBER feladatai a következők:

– a vezérkari főnöknek, mint az információs rendszerek biztonságáért felelős minősített hatóságnak a felelősségi körébe tartozó információs rendszerek védelme;

2019 et portant diverses dispositions concernant la défense et la sécurité nationale, 21. cikk.

[29] Livre Blanc de la défense et de la sécurité nationale, 2008, 53. o.

[30] DESFORGES, Alix, Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France, 120-156. o. MÁSODIK ELŐFORDULÁS!

[31] A beosztást 2019 szeptembere óta Didier Tisseyre vezérőrnagy látja el, elődei Arnaud Coustillière ellentengernagy (2011-2017) és Olivier Bonnet de Pailleret vezérőrnagy (2017-2019) voltak.

[32] Code de Défense, D. 3121-24-2. cikk

- a Védelmi Minisztérium információs rendszereinek védelme, kivéve két nemzetbiztonsági szolgálat, a Külső Biztonsági Főigazgatóság (DGSE) és a Katonai Hírszerzési és Védelembiztonsági Igazgatóság (DRSD) rendszereit;
- a katonai kibervédelmi műveletek tervezése, szervezése és végrehajtása a vezérkari főnök műveleti helyettesének felügyelete mellett;
- hozzájárulás a kibervédelmi humánerőforrás-politika kidolgozásához;
- a fegyveres erők és az állami szervek nemzeti és nemzetközi kibervédelmi politikához való hozzájárulásának koordinálása, különösen az együttműködési tervek kidolgozása és végrehajtása tekintetében
- a kibervédelemre vonatkozó konkrét műszaki követelmények meghatározásának összehangolása;
- a Védelmi Minisztérium kibervédelmi modelljének koherenciája és általános koordinációja;
- a kibervédelmi tartalék fejlesztése és kezelése.

A COMCYBER szervezetrendszerét főbb elemekként a következő szervezetek jelentik:

- Az Információs Rendszerek Biztonságának Ellenőrzési Központja (Le Centre d'audits de la sécurité des systèmes d'information, CASSI) az a nemzeti központ, amelynek ellenőrzési feladata két területre terjed ki: az információs rendszerek biztonságára és a féregtámadásokra.
- Az Informatikai Védelmi Elemző Központ (Le Centre d'analyse de lutte informatique défensive, CALID) az informatikai védelem operatív szakértői központja. A nap 24 órájában irányítja a kibertámadások észlelését, feldolgozását és az azokra való reagálást.
- A Kibervédelmi Tartalékos és Műveleti Készenléti Központ (Le Centre de la réserve et de la préparation opérationnelle de cyberdéfense, CRPOC) feladata elsődlegesen a toborzás, továbbá a nemzeti és nemzetközi kibervédelmi gyakorlatok szervezése révén a személyi állomány képzése és operatív felkészítése.

A NEMZETBIZTONSÁGI SZOLGÁLATOK HELYE SZEREPE A FRANCIA KIBERVÉDELMI ÉS – BIZTONSÁGI RENDSZERBEN

Ahogyan az a fentiekből több ponton is kiolvasható, az ANSSI és a COMCYBER mellett a nemzetbiztonsági szolgálatok önálló szereplői a kibervédelelmnek. Ebben a szerepkörben

- ellátják az ágazati információs rendszerek védelmét,
- hírszerző-felderítő kompetenciájuk által, előrejelzésekkel, sebezhetőségi kockázatelemzéssel erősítik meg a védelmi képességeket, támogatják a műveleti tevékenységet,

– részt vesznek a kibertérből érkező támadásokkal szembeni katonai fellépésben.

Fontos azonban kiemelni, hogy *a nemzetbiztonsági szolgálatok a „hagyományos" feladatrendszerük és a kibertérben végzett tevékenységük, illetve ezek kombinálódása miatt sem kerülhetők meg sem az ANSSI sem pedig a COMCYBER hatékony működése tekintetében.*

A védelmi miniszter alárendeltségében lévő nemzetbiztonsági szolgálatok kibertevékenysége egymástól jól elhatárolható feladatkörökre bomlik:

– a Katonai Hírszerzési és Védelembiztonsági Igazgatóság (la direction du renseignement et de la sécurité de la défense, *DRSD) a defenzív kibertevékenységekhez járul hozzá a működési területén és a védelmi iparban folytatott elhárítói feladatokkal*;
– a Katonai Felderítő Igazgatóság (la direction du renseignement militaire, *DRM) a katonai érdekű, kibertérből származó információk gyűjtését végzi*;
– a Külső Biztonsági Főigazgatóság (la direction générale de la sécurité extérieure, *DGSE) pedig offenzív kiberműveleteket hajthat végre.*

A Katonai Hírszerzési és Védelembiztonsági Igazgatóság a védelmi kódex D. 3126-6. cikke értelmében a feladatkörében tudhatja a kibervédelem több aspektusát is, elhárító tevékenysége kiterjed a terrorizmus, a kémkedés, a felforgató tevékenységek, szabotázsok és a szervezett bűnözés területeire, az azokban rejlő fenyegetésekre. Mindezt kiegészíti egy 2013 október 22-i védelmi miniszteri rendelet, amely a DRSD szervezeti és működési szabályzata.[33] A szabályzó kitér a szervezeti egységek, mint aligazgatóságok és központok tevékenységeire, ezek közül kiemelendő a Nemzeti Szakértői Központok Aligazgatósága, amely magáért az ágazati kibervédelemért felel, egész pontosan a feladata a védelmi minisztérium és a védelmi ipar létesítményeinek és információinak biztonságához hozzájáruló vizsgálati, auditálási és ellenőrzési feladatok folyamatos elvégzése. A szisztémában a kiberbiztonsági részleget egy tanácsadási, megelőzési és ellenőrzési központ jelenti, amelyet technikai oldalról egy információs és kommunikációs rendszerek központja is támogat. Ez utóbbiban többek között egy információvédelmi iroda működik.[34]

A Külső Biztonsági Főigazgatóság a védelmi kódex D. 3126-2. cikke szerint a kormánnyal és a kormányzati szervekkel, továbbá a kormánnyal összeköttetésben álló szervezetekkel együttműködésben látja el a feladatait, ami nem más, mint a nemzetbiztonsági érdekek mentén releváns hírszerzés, a felkutatott információk felhasználása, továbbá az országot az államterületen kívül fenyegető kémtevékenység felderítése, elhárítása. Szervezeti és működési szabályzatát szintén védelmi miniszteri rendelet határozza meg, megjelölve egy műszaki igazgatóságot, amelynek feladata a műszaki eredetű hírszerzési információk kutatása és felderítése, valamint a Külső Biztonsági

[33] Arrêté du 22 octobre 2013 portant organisation de la direction du renseignement et de la sécurité de la défense

[34] Arrêté du 22 octobre 2013 portant organisation de la direction du renseignement et de la sécurité de la défense 7.cikk.

Főigazgatóság műszaki területekre vonatkozó iránymutatásaira való javaslattétel.[35]

Az ország területén kívüli kibervédelemre és felderítésre a francia jogrendszer a 2015. november 30-i törvényben határozza meg a jogi kereteket, ennek tárgya a nemzetközi elektronikus hírközlés felügyelete is. Nyílt joganyag az offenzív tevékenységeket nem részletezi, de a DGSE feladat- és hatásköri spektrumából, továbbá a francia szakirodalomból ez a képesség a nemzetbiztonsági szolgálat kompetenciái közé sorolandó.[36]

Az, hogy mindez egyúttal az ANSSI-nek, mint legfelső koordinatív szervnek és és a COMCYBER-nek, mint tisztán katonai vezetési elemnek a nemzetbiztonsági szolgálatokra való támaszkodását jelenti, azzal is alátámasztható, hogy a kibertér műveleti területté változva képes osztani az államok közötti fegyveres tevékenységek jogi sorsát, ellenben a hírszerző és felderítő tevékenység a nemzetközi jog szabályanyagának „szürke zónájába" tartozik.

A nemzetbiztonsági szolgálatok a francia kibervédelmi és –biztonsági rendszerben sajátos és megkerülhetetlen komponensek, a katonai műveleti képességek támogatása, az információs rendszervédelem és a megelőzésben, előrejelzésben való közreműködés alapelemei hagyományos feladataik révén, illetve a kibertérben ellátott új feladatok és azok hagyományos feladatkörrel való kombinálódása miatt is. Nem szabad egyúttal megfeledkezni arról sem, hogy a digitalizáció a szolgálatok klasszikus feladatait is fokozottan érinti és áthatja, és ez a nemzetbiztonsági tevékenységek jellegéből adódóan folyamatos ellátást igényel, túlmutatva egy-egy válsághelyzeten vagy célzott műveleten, ami szintén erősíti azt a modellt, amelyben a katonai erő és az összkormányzati cselekvés is jelentősen támaszkodik a nemzetbiztonsági szolgálatokra.

ÖSSZEGZÉS

Az informatika és az internet térnyerése a kiberteret megkerülhetetlen közegként betonozta be, amely, mint egyfajta hézagokat kitöltő tényező kapcsolja össze a korábban egymással kontaktusban nem lévő elemeket. Emellett a kihívások teljességgel új körét gördítette az államok elé, amelyek saját szuverenitásuk, továbbá az állampolgárok élet- és vagyonbiztonsága érdekében vagy kényszerpályán mozogva, vagy tudatos stratégiával - elejét véve a kihívások konkrét fenyegetéssé alakulásának - léphetnek fel mindezekkel szemben.

Franciaország kibervédelmi keretei két szempontból is éles határvonalat húznak. A fentiekben említett ellentmondástól eltekintve az offenzív és a defenzív tevékenységek között definiált határ húzódik, továbbá a szervezeti felépítés az ágazatköziség jelentőségét is felismerve külön szereplőket hozott létre a polgári és a katonai oldalon, de önállóságot biztosított a nemzetbiztonsági szolgálatoknak azok szakfeladatainak sajátosságára és folyamatos ellátására figyelemmel.

A francia kibervédelmi elgondolásokat erős szabályozottság

[35] Arrêté du 10 mars 2015 portant organisation de la Direction générale de la sécurité extérieure, 7.cikk

[36] ARPAGIAN, Nicolas, La cybersécurité, PUF « Que sais-je », Párizs, 2010, 106. o.

jellemzi, ami egyszerre jelenik meg a stratégiai elgondolás részletessége és a jogszabályi keretek tekintetében. A szabályozottság erősségét leginkább a koherencia biztosítja, amit a stratégia nagyban egészít ki, direktívaként szerepeltetve Franciaországnak a nemzetközi közösségben betöltött – sokszor kezdeményező, aktív – szerepének a kibertérben való fenntartását is.

FELHASZNÁLT FORRÁSOK

[1] ARPAGIAN, Nicolas, La cybersécurité, PUF « Que sais-je », Párizs, 2010, 106. o.

[2] BÉRES János (szerk.): Külföldi nemzetbiztonsági szolgálatok. Budapest, Zrínyi Kiadó, 2018, 103-107. o.

[3] CLARK, Richard; KNAKE, Robert.: Cyber War: the next threat to national security and what to do about.New York: HarperCollins Publishers Inc. 2010.

[4] CLEMENTE, Dave.: Cyber Security and Global Interdependence: What Is Critical?, London: The RoyalInstitute of International Affairs. 2013.

[5] DESFORGES, Alix: Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France. Thèse, Université Paris, 2018.

[6] DODGE, Martin – KITCHIN, Rob: Mapping Cyberspace, London-New York, Routledge, 2001;

[7] DOUZET, Frédérick: Cyberespace : enjeux géopolitiques, Hérodote, n°152-153, 1er-2ème trimestre 2014, 313 o.

[8] FARKAS Ádám: Kibertér művelet: hírszerző, rendészeti és katonai műveletek elegye? Gondolatok az angol National Cyber Force kapcsán. Military and Intelligence CyberSecurity Research Paper 2021/1.;

[9] FARKAS Ádám: A kortárs technológia-fejlődés és innováció viszonya honvédelmi szabályozással. MTA Law Working Papers 4 : 4, 2021. 1-15. o.;

[10] KELEMEN Roland, SIMON László: A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái In: FARKAS Ádám, VÉGH, Károly (szerk.) Új típusú hadviselés a 21. század második évtizedében és azon túl– intézményi és jogi kihívások Budapest, Magyarország : Zrínyi Kiadó, 2020. 150-170.o.;

[11] KELEMEN Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése Honvédségi Szemle: A Magyar Honvédség központi folyóirata, 2020/4, 65-81. o.;

[12] KELEMEN Roland, FARKAS Ádám: To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare In: SZABÓ Marcel, GYENEY Laura, LÁNCOS Petra Lea (szerk.) Hungarian Yearbook of International law and European Law (2019) Den Haag, Hollandia : Eleven International Publishing (2020) pp. 203-226. o.;

[13] SCHMITT, Michael N.: Tallinn Manual on International Law applicable to cyber warfare, Cambridge, Cambridge University Press, 2013;

[14] SCHMITT, Michael N. (szerk.): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cyber Defence Center of Excellence, Cambridge, Cambridge University Press, 2017.

[15] VERGARAM, Ingrid: Face à la multiplication des attaques, la France accélère sa stratégie de cybersécurité. Le Figaro, 2021. február 17. https://www.lefigaro.fr/secteur/high-tech/face-a-la-multiplication-des-attaques-la-france-accelere-sa-strategie-de-cybersecurite-20210217 (Elérés dátuma: 2021. április 18.)

[16] VIKMAN László: A német kiberbiztonsági szisztéma áttekintése. Military and Intelligence CyberSecurity Research Paper 2021/2.

[17] ZIOLKOWSKI, Katharina (szerk.): Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy, Tallinn, NATO CCD COE Publication, 2013.;

[18] Franciaország 2018. február 12-én elfogadott Kibervédelmi Stratégiája

[19] Livre blanc de la défense et de la sécurité nationale (Fehér Könyv a nemzeti védelemről és biztonságról)


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Military and Intelligence CyberSecurity Research Paper 2021/3.

Szerző(k) / Author(s):
Dr. Spitzer Jenő

Kézirat lezárásának ideje / Manuscript closing time:
2021.08.23.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD
Dr. Magyar Sándor PhD

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Prof. Dr. Resperger István PhD

Elérhetőségek /Contacts:
https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/researchpaper

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.