LIETUVOS RESPUBLIKOS SEIMO NARIAI

Gedimino pr. 53, LT-01109 Vilnius, Lietuva Tel.: (8~5) 239 6983 El. p.: laurynas.kasciunas@lrs.lt

Nacionaliniam saugumui užtikrinti svarbių objektų apsaugos koordinavimo komisijai

2019-01-28

DĖL KOMPANIJOS „HUAWEI“ TECHNOLOGIJŲ NAUDOJIMO NACIONALINIAM SAUGUMUI UŽTIKRINTI SVARBIAME ŪKIO SEKTORIUJE

Šiuo metu plėtojamos penktosios kartos mobiliojo ryšio, žinomo kaip 5G, technologijos leidžia pasiekti daug didesnę duomenų perdavimo spartą, užtikrinti aukščiausios kokybės ryšį ir sukuria naujos kartos skaitmeninių technologijų pagrindą. Pavyzdžiui, atsiranda galimybė sukurti vadinamąjį daiktų internetą (angl. – *Internet of Things*) – t. y. transporto priemonių, buitinės technikos ir pan. tinklą, leidžiantį reikiamą techninę ir programinę įrangą turintiems daiktams kontaktuoti, sąveikauti, keistis duomenimis, nuotoliniu būdu valdyti mechanizmus be jokio vėlinimo. Taigi, visa tai atvers naujų galimybių žmonėms ir verslui. Todėl nenuostabu, kad pasaulyje vyksta intensyvi konkurencija tarp verslo įmonių ir valstybių dėl lyderystės diegiant 5G ryšį.

2018 m. gruodžio mėn. telekomunikacijų bendrovė „Telia Lietuva“ pirmoji Lietuvoje įjungė naujos kartos 5G ryšį. Tuo pačiu metu bendrovė „Telia“ 5G ryšį paleido ir Estijoje, Suomijoje ir Švedijoje.

5G ryšio plėtra turės įtakos ir kibernetiniam bei nacionaliniam saugumui. Nors 5G ryšio duomenų apsauga yra patobulinta, tačiau būtent šioje srityje kyla nemažai iššūkių ir rizikų. Kalbant apie 5G ryšio plėtrą ir tam naudojamą įrangą, atkreiptinas dėmesys, kad šiuo metu rinkoje dominuoja keturi pagrindinių 5G ryšio technologijų gamintojai: Švedijos „Ericsson“, Suomijos „Nokia“ ir Kinijos „Huawei“ bei „ZTE“.

Jungtinių Amerikos Valstijų Strateginių ir tarptautinių studijų centro 2018 m. ataskaitoje teigiama, jog kompanijos „Huawei“ ir „ZTE“ buvo subsidijuojamos Kinijos vyriausybės tam, kad jos įgytų ne tik stiprias pozicijas rinkoje, bet ir žvalgybinį pranašumą. Tai leidžia joms savo produkciją pardavinėti už mažesnę kainą. Pavyzdžiui, „Huawei“ įranga kainuoja maždaug 20–30 proc. mažiau nei kitų konkurentų siūlomi technologiniai produktai, kompanija užsienio klientams

siūlo palankias išperkamosios nuomos sąlygas. Ataskaitoje taip pat pažymima, jog „Huawei“ vadovybė turi glaudžius ryšius su Kinijos žvalgybos tarnyba.[1]

Telekomunikacijų sektorius yra nacionaliniam saugumui užtikrinti svarbus ūkio sektorius, todėl dviejų kompanijų, susijusių su trečiosios šalies žvalgyba, veikla šiame sektoriuje pagrįstai kelia saugumo rizikas. Su šnipinėjimu ar ypatingos svarbos infrastruktūros objektų veiklos sutrikdymu susijusios rizikos galima išengti tik tuomet, jei visa ryšio technologijų tiekimo grandinė yra saugi. Tačiau plačiai žinoma Kinijos agresyvi kibernetinio šnipinėjimo kampanija iš tiesų kelia susirūpinimą, kad ši šalis gali pasinaudoti galimybėmis, kurias ji įgauna kaip pasaulinė 5G ryšio technologijų tiekėja.[2] Pavyzdžiui, daugybė telekomunikacijų įrangos yra sujungta su gamintoju, per kurį jam gali būti siunčiami pranešimai apie tos įrangos būklę ir, prireikus, gaunami programinės įrangos atnaujinimai bei klaidų pataisymai. Todėl net jei parduodama įranga yra visiškai saugi, vėliau gamintojas, siųsdamas programinės įrangos atnaujinimus, gali sukurti tam tikras saugumo spragas, kurios ilgainiui gali būti panaudotos šnipinėjimui ar sabotažui. Taigi, mažesnė įrangos kaina reiškia mažesnį saugumą. Tuo tarpu nors kitų, bet abejonių dėl patikimumo nekeliančių, gamintojų įranga nors ir yra brangesnė, tačiau tai gali būti suprantama kaip priemoka už saugumą. Klausimas, kiek šalių tai suvokia ir yra pasirengusios tą priemoką mokėti.

Šiuo atveju atkreiptinas dėmesys, kad kai kurios užsienio valstybės uždraudė Kinijos informacinių ir ryšio technologijų kompanijoms „Huawei“ ir „ZTE“ dalyvauti plėtojant 5G ryšio technologijas šalyse. Pavyzdžiui, 2018 m. rugpjūčio mėn. Australija ir Naujoji Zelandija įvedė draudimą naudoti šalyje Kinijos bendrovių „Huawei“ ir ZTE įrangą 5G ryšio tinklo kūrimui, kilus įtarimams, kad šios kinų įmonės gali turėti ryšių su užsienio vyriausybėmis ir todėl gali kelti grėsmę saugumui. Kiek anksčiau, tų pačių metų gegužę, JAV Pentagonas uždraudė Kinijos bendrovių „Huawei“ ir ZTE išmaniųjų telefonų pardavimą karinėse Jungtinių Valstijų bazėse. Draudimas taip pat taikomas mobiliajam internetui skirtiems modemams ir kitai mobiliojo ryšio produkcijai. Be to, JAV prezidentas Donaldas Trumpas taip pat ragina sąjungininkus Europoje uždrausti „Huawei“ kompanijai prieigą prie mobiliųjų tinklų.[3]

Įvairios valstybės, įskaitant Jungtinę Karalystę, Vokietiją, Norvegiją, yra išreiškusios susirūpinimą dėl „Huawei“ technologijų naudojimo kuriant naujos kartos 5G ryšio tinklus.[4]

---

[1] James A. Lewis, „How 5G Will Shape Innovation and Security: A Primer“. *A Report of the CSIS Technology Policy Program.* Washington, DC: Center for Strategic and International Studies, December 2018, p. 2, 10, <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdf> [Žiūrėta 2019-01-28].

[2] Ten pat, p. 1–2.

[3] ELTA, „Australija uždraudė „Huawei“ plėtoti 5G ryšio tinklus”. LRT.lt, 2018 m. rugpjūčio 23 d., <https://www.lrt.lt/naujienos/mokslas-ir-it/1/224388/australija-uzdraude-huawei-pletoti-5g-rysio-tinklus> [Žiūrėta 2019-01-14].

[4] Gwladys Fouche, „Norway considering whether to exclude Huawei from building 5G network“. Euronews, 2019 m. sausio 9 d., <https://www.euronews.com/2019/01/09/norway-considering-whether-to-exclude-huawei-from-building-5g-network?fbclid=IwAR3Qzsaq5ONP3rvsKa09PIJ30sPX4UeHnibJFSpFRg45KLCq8H3fK14YExo> [Žiūrėta 2019-01-14].

Tokie atvejai kelia rimtų abejonių, kad „Huawei“ technologijos gali būti naudojamos Kinijos žvalgybos tikslams. Be to, 2017 m. Kinijoje įsigaliojo naujas nacionalinės žvalgybos įstatymas, pagal kurį netgi privačios šios šalis organizacijos ir privatūs asmenys turi įsitraukti į Kinijos žvalgybinį darbą. Kyla klausimas, ar Kinijos vyriausybė galėtų spausti kompaniją „Huawey“ technologinėje įrangoje palikti vadinamąsias „landas“ (angl. – *backdoors*), kurios ilgainiui gali būti panaudotos bandant prieiti prie informacijos, šnipinėjimo ar netgi sabotažo tikslams.

Pažymėtina, jog „Telia Lietuva“, plėtodama Lietuvoje 5G ryšį, naudoja būtent „Huawei“ technologinę įrangą. Telia Lietuva, AB yra trečios kategorijos nacionaliniam saugumui užtikrinti svarbi įmonė. Todėl, atsižvelgiant į visa tai, prašome įvertinti, ar „Huawei“ technologinių produktų naudojimas strategiškai svarbiame ūkio sektoriuje neprieštarauja nacionaliniam saugumui. Esame tikri, jog atsakingos institucijos turėtų įvertinti visas grėsmes ir rizikas bei pateikti strateginę reikšmę nacionaliniam saugumui užtikrinti svarbioms įmonėms išvadas ir/ar rekomendacijas dėl ryšio technologijų naudojimo, t. y. rekomenduojant ar įpareigojant naudoti tik Europos Sąjungos, Europos Ekonominės Erdvės ar NATO šalių technologinius produktus nacionaliniam saugumui užtikrinti svarbiuose ūkio sektoriuose.

Seimo nariai