HIINA TEHNOLOOGIA LEVIKU UUS TASE

Hiina tehnoloogiast lähtuvad ohud liiguvad lidar-süsteemiga magamistuppa ja garaaži.

Hiina ülemaailmne AI valitsemise initsiatiiv on järjekordne näide Lääne-vastase Hiina ökosüsteemi ülesehitamisest.

Hiina tehnoloogia levik kriitilisse taristusse ehk energiavõrkudesse ohustab Eesti julgeolekut.

Hiina ehitab üles oma standarditel põhinevat ja erinevate tehnoloogiaettevõtete lahendusi kombineerivat integreeritud poliitilist ja tehnoloogilist ökosüsteemi. Kuigi Hiina standardite „eksportimisest" ja seeläbi teadlikult sõltuvuse tekitamisest räägiti juba kümme aastat tagasi ning akadeemilised üleskutsed mõttekodade publikatsioonide kujul täitsid Hiina suurimate raamatupoodide riiuleid, on Hiina tehnoloogiline ökosüsteem jäänud keskmisele Lääne inimesele abstraktseks, kaugeks ja ohuspektrist välja. Hiina on aga viimased kümme aastat süstemaatiliselt ja selge eesmärgiga tegutsedes mõjutanud rahvusvahelistes standardikomisjonides standardeid Hiina tehnoloogiale soodsas suunas.

Hiina tehnoloogia esiletõus ja levik üle maailma on riigi suunatud strateegia, et kasvatada oma poliitilist mõjuvõimu.

Hiina tehnoloogia esiletõus ja levik üle maailma ei ole tingitud ainult Hiina talentide usinusest ja ettevõtlikkusest, vaid tegemist on väga selgelt Hiina riigi suunatud strateegiaga, et koos Hiina standardite eksportimisega ühtlasi kasvatada riigi poliitilist mõjuvõimu. Hiina eesmärk on jõuda punkti, kus tehnoloogia integreeritud lahendusi ei ole võimalik Lääne tehnoloogiaga asendada, nii ühildamatuse kui ka läbipõimumise tõttu.

Hiina Kommunistliku Partei (HKP) teadlik suund õõnestada Lääne mõjuvõimu ja liikuda „demokraatliku" ehk autoritaarsete riigikordade põhimõtete ja huvidega arvestava multipolaarse maailmakorra suunas ainult süvendab HKP veendumust ja tahet luua Läänest sõltumatu ökosüsteem. Selle kõige selgem kujustus on „Vööndi ja tee" initsiatiiv koos digitaalse Siiditeega. Samasse mustrisse paigutub ülemaailmne AI valitsemise initsiatiiv, mida Xi Jinping esitles oktoobris „Vööndi ja tee" tippkohtumisel ja mis on järjekordne näide Lääne-vastase Hiina ökosüsteemi ülesehitamisest.

Hiina riigiettevõtete puhul tuleb arvestada väga tõenäolist võimalust, et nende juurdepääs kapitalile võib olla palju soodsam kui n-ö Hiina tavaettevõtetel.

Nii avalik kui ka erasektor peaksid ettenägelikult ennetama Hiina tehnoloogia liigset levikut, sest on väga suur tõenäosus, et pigem varem kui hiljem tuleb geopoliitiliste arengute ja julgeolekuküsimuste tõttu teha valulik otsus Hiina tehnoloogiast loobuda. Valulik on see otsus muuhulgas seetõttu, et sõltuvuse tekitamiseks pakuvad just Hiina ettevõtted tooteid ja teenuseid soodsama hinnaga, mis mõistagi tundub efektiivne nii eraettevõtetele kui ka avalikule sektorile, kus sageli lähtutakse riigihangetes põhimõttest „soodsaim võidab".

Viimase aasta jooksul on selgelt näha olnud, kuidas Hiina tehnoloogia vallutab Eestis täiesti uut valdkonda – elektrivõrke. Balti regioonis tegutsev Huawei on pärast 5G-võrkudest väljajäämist võtnud sihikule pilveteenused ning päikese- ja tuulepargid. Nii Huawei kui juba ka teised Hiina ettevõtted soovivad Eesti elektrivõrke varustada päikese- ja tuuleparke elektrivõrkudega ühendavate inverterite ja energiasalvestussüsteemidega.

Inverter on seade, mis muudab päikesepaneelis toodetud elektri kliendile tarbitavaks. Päikesejaama haldamiseks ja selle seisu jälgimiseks on inverterid ühendatud internetti ehk nende abil on võimalik kaugelt mõjutada päikesejaamade tööd, näiteks muuta tööparameetreid ja võimsust. Nagu teistegi elektrooniliste seadmete puhul on ka inverterite puhul tarvis teha tarkvarauuendusi ja järgida tootja soovitusi. Kriitilisi funktsioone täitvate toodete pakkujaid peab aga saama usaldada, et nad ei hakka tootega ja seega kriitilise teenusega mistahes viisil manipuleerima. Mida rohkem Eesti elektrist toodavad päikesepargid, seda suurem mõju oleks sellisel manipulatsioonil riigi elektritootmisvõimsusele. Niisiis tuleb vältida olukorda, kus keegi kolmas osapool võib hakata riigi elektrivarustust ära kasutama luureinfo kogumiseks või majandusliku ja poliitilise surve avaldamiseks.

Hiina inverterite ja energiasalvestussüsteemide kasutuselevõtt Eesti elektrivõrkudes aga tähendab varem või hiljem 5G stsenaariumi kordumist ehk ettevõtted ja riik peavad endale siin väga selgelt aru andma, kuhupoole Hiina tehnoloogiat Eesti elektrivõrkudesse ehk kriitilisse taristusse sisse tuues liigutakse. Huawei töö Eesti suunal on väga järjekindel, põhjalik, süstemaatiline ja Shenzheni peakorteriga kokku lepitud.

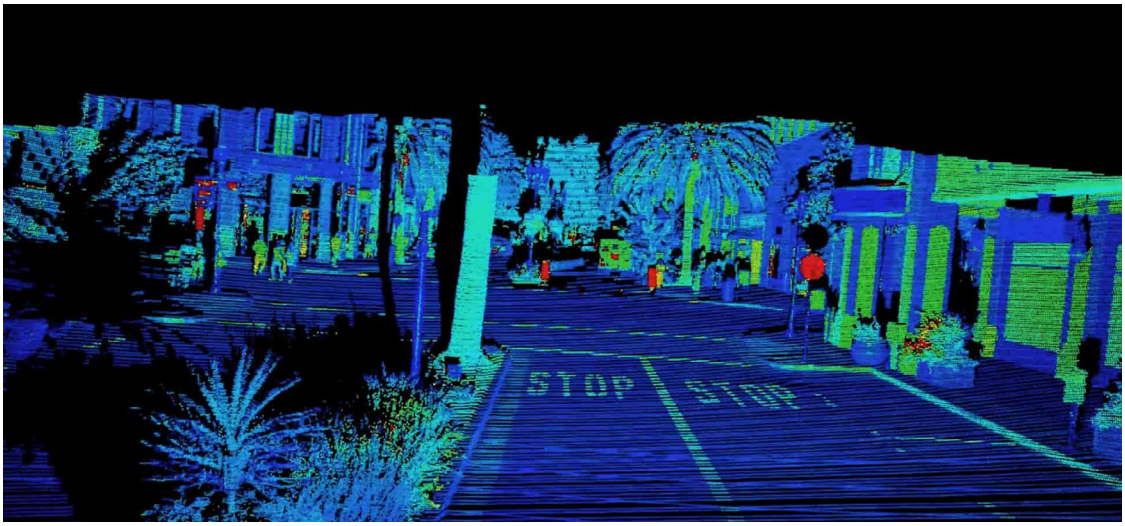
Suur väljakutse Hiina tehnoloogiaettevõtete puhul on nende võimalik riiklik seotus.

Hiina varjab üha kiivamalt ettevõtete taustainfot, varjudes andmete julgeoleku kontseptsiooni taha, mille kohaselt teatud andmed ei tohi liikuda Hiina piiridest välja. See puudutab ka Hiina ettevõtete taustainfot, millele juurdepääsu takistamiseks on Hiina riiklikud asutused kehtestanud paari viimase aasta jooksul ridamisi piiranguid.

Uut etappi Hiina tehnoloogiast lähtuvates ohtudes tähistab lidar-süsteemi üha laiem kasutuselevõtt alates koduelektroonikast kuni isesõitvate autodeni. Lidar-süsteem skaneerib seadme iseseisvaks toimimiseks kogu selle ümbruskonda. Lisaks seadme ümbruses olevatele pindadele valgustatakse läbi objektid, et näha nende taga asuvaid potentsiaalseid ohte. Näiteks isesõitval autol on vaja hinnata, kas tee ääres seisva auto taga võib sõidutee suunas veereda pall või liikuda laps, ning selleks on vaja auto läbi valgustada.

Välisluureametil on väga kindlalt teada üks Hiina isesõitvatele autodele lidar-süsteemi arendav ettevõte, kelle sõnul on lidar-süsteemi eesmärk skaneerida kogu isesõitva auto

ümbruskond ning saata need andmed Hiinas asuvasse andmekeskusesse. Printsiibis peaks iseseisvaks toimimiseks andmeid koguv seade kõik seadme toimimiseks mittevajaliku ära kustutama, kuid selle Hiina ettevõtte eesmärk on skaneerida kogu keskkond ning saata kõik andmed Hiinas asuvasse andmebaasi. See tähendab, et Hiina tehnoloogiaga isesõitvaid autosid on võimalik luure eesmärgil ära kasutada.



Illustratsioon. Lidar-tehnoloogiaga skaneeritud ümbruskond.

Allikas: seyond.com

Täpselt samasugune kogu ümbruskonna skaneerimise oht kaasneb ka tavalise koduelektroonika, näiteks robottolmuimejatega. Lisaks on oht, et Hiina tehnoloogiaettevõtete isikustatud teenused koos kontodega mobiilirakendustes koguvad infot tarbija kohta.

Siit edasi tuleb pöörata tähelepanu Hiina videorakendusele TikTok ja selle omanikule ByteDance'ile. TikTok on klassikaline näide segasest taustast ja andmete kogumisest mõne uue võimekuse väljaarendamiseks. Nimelt on TikToki emafirma ByteDance registreeritud Kaimanisaartel. ByteDance'i tegelik peakontor asub aga Pekingis, kus ByteDance on registreerinud firma nimega Douyin Co., Ltd. Sellel on aga 0 töötajat ehk tegemist on Kaimanisaartele registreeritud ettevõtte Hiinas asuva formaalse kehandiga.

Douyin Co., Ltd. omab firmat nimega Beijing Douyin Information Service Co., Ltd., millel on 1947 töötajat ning mis on ByteDance'i tegelik peakorter, asukohaga Pekingis Haidiani linnaosas AVIC Plaza nimelises hoones. Mitmete alluvusahelate vahendusel on selles ettevõttes aga 1%-line osalus Hiina riiklikul küberkontrollikeskusel National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC). CNCERT/CC kuulub Hiina Küberruumi Keskkomisjoni (Central Cyberspace Affairs Commission) alla, mis omakorda kuulub Hiina Kommunistliku Partei Keskkomitee alla. Küberruumi Keskkomisjon töötab välja ja viib ellu Hiina küberruumi puudutavat poliitikat ja otsuseid. Tekib küsimus, miks seda 1%-list osalust vaja on.

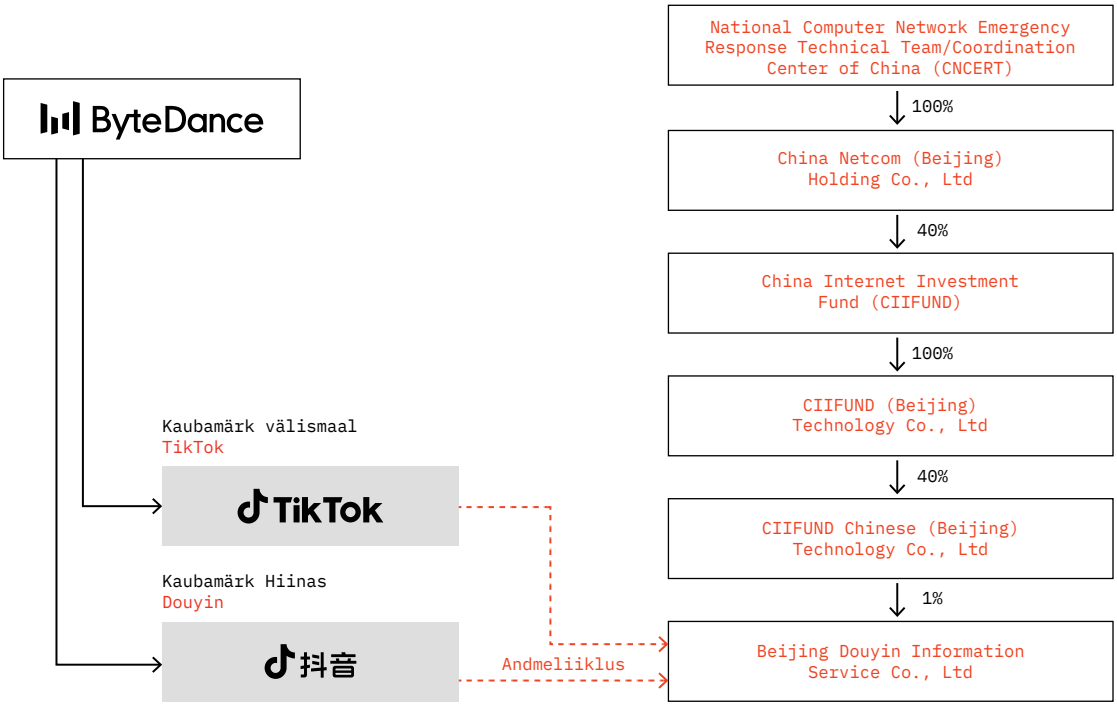
Möödunud aasta 23. märtsil USA Kongressi ees toimunud TikToki arupärimisel ütles TikToki tegevjuht Shou Zi Chew otse, et hetkel liiguvad TikToki videorakenduse abil üle maailma kokku kogutud andmed otse Pekingisse Beijing Douyin Information Service'i omandusse. Sama firma omandusse tuleb ka Hiinast Douyini-nimelise videorakenduse kaudu kogutud info. See tähendab, et CNCERT/CC-l on juurdepääs nii Hiina riigi sees Douyini kaudu kui ka välismaalt TikToki videorakenduste abil kogutud andmetele.

Andmete massiline kogumine annab ByteDance'ile võimaluse arendada tehisintellekti.

Hiinal on vaja juurdepääsu erineva päritoluga inimeste visuaalsetele ja käitumuslikele andmetele, et seeläbi arendada globaalse võimekusega täiuslikku tehisintellekti. Hiinast kogutud andmed sellist võimalust ei pakuks, sest inimeste väljanägemine ning kultuurilisest taustast tingitud käitumismuster erinevad suurest osast muust maailmast oluliselt.

Lisaks tehisintellekti arendamisele võivad kasulikud olla ka muud rakenduse kogutud andmed. TikTok kogub ulatuslikult infot seadme ja selle kasutaja kohta, näiteks telefonis olevate kontaktide, kalendri, teiste rakenduste, WiFi ühenduste ja asukoha kohta. Selline teave võib olla kasulik luureinfo kogumisel, väljapressimiseks, samuti ka küberrünnete jaoks, sest selle põhjal saab teha just selle inimese jaoks disainitud veenva õngitsuskirja, et saada ulatuslikum ligipääs tema ja/või tema tööandja võrgule, eriti kui kasutaja tööandja on asutus või ettevõte, mis Hiinale strateegiliselt huvi võiks pakkuda.

Lisaks TikTokile kuulub Douyin Co., Ltd-le ka ettevõte ja kaubamärk nimega Toutiao. Nii Toutiao kui ka Beijing Douyin Information Service'i juriidiline esindaja on üks ja sama isik. See tähendab, et TikTok ja Toutiao on omavahel tihedalt seotud. Toutiao eripära Hiina turul seisneb selles, et ta pakub teenusena kasutaja käitumismustri põhjal tehisintellekti väljaarendatud personaalseid uudisvoogusid. Sisuliselt tähendab TikToki kasutamine, et aidatakse Lääne julgeolekuarhitektuuri ümber kujundada sooviva autoritaarse riigi osalusega ettevõttel tehisintellekti välja arendada.



TikToki omanduse skeem