



RIIGI INFOSÜSTEEMI AMET



RKK
ICDS

RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Droonide küberturvalisuse analüüs

*Viimastel aastatel üha populaarsemaks muutunud droonid on olemuselt
lendavad IT-süsteemid. Raport käsitleb nii droonide tavapäraseid
IT-küberriske kui ka neile lisanduvaid droonispetsiifilisi ohte ning
annab praktilisi näpunäiteid nende turvaliseks kasutamiseks.*

Juuli 2026

Sisukord

Lühikokkuvõte	3
Sissejuhatus	4
1. Droonide küberturvalisuse riskid	5
1.1. Õhusõiduk	5
1.2. Side- ja juhtimissüsteem	8
1.3. Maapealne osa	10
2. Soovitused ja järelused	14
Lühendid ja mõisted	16
Allikad	19

Lühikokkuvõte

1. Droonid on sisuliselt lendavad arvutid. Neil esinevad kõik tavapärased IT-süsteemide küber-riskid: **kommunikatsiooniriskid** (raadioside segamine ja võltsimine (*jamming* ja *spoofing*)), **andmeriskid** (andmeleke, krüpteerimata andmeside) ja **tarkvara haavatavused**.
2. Mitmed droonide kasutamisega kaasnevad küberohud **ei erine olemuselt teiste võrku ühendatud seadmete ohtudest**. Seetõttu on riske võimalik vähemalt osaliselt maandada, järgides **küberhügieeni**.
3. Küberohtudele lisanduvad **droonispetsiifilised riskid**. Droonid kui lendavad objektid sõltuvad sideühendusest ja sageli ka satelliitnavigatsioonist, mida on võimalik **ründajal häirida või tõkestada**.
4. Tavakasutaja jaoks pole kõige olulisem erinevate tehniliste kaitsemeetmete lisamine, vaid juba algusest peale turvaliste omadustega drooni ostmine, küberhügieeni järgimine ning küberteadlik käitumine.

Sissejuhatus

Euroopa Komisjoni hinnangul on droonidest ehk mehitamata õhusõidukidest (MÕS) saanud majanduse ja ühiskonna lahutamatu osa. Kasvanud on nii droonide kasutusvõimalused, kasutajate arv, kättesaadavus kui ka võimekus. Droonid ei ole enam pelgalt kaameratega mänguasjad, **vaid olulisi teenuseid pakkuvad lendavad IT-süsteemid**, mille riistvara, püsi- ja tarkvara, side, sensorid ja juhtimine moodustavad ühtse terviku. Sestap on **droonide küberturvalisus kriitilise tähtsusega**: ründajal on võimalik ära kasutada tarkvara turvanõrkusi, et manipuleerida lennuteekonda või katkestada ühendusi, koguda andmeid või võtta isegi droon üle ilma, et sellele füüsiliselt ligi pääseks.

Raport koosneb kahest osast. Esimeses osas kaardistatakse droonidega **seotud küberohte tavakasutaja vaatenurgast** ning aruande teises osas anname **praktilisi soovitusi nende riskide maandamiseks**. Juhised on piisavalt üldised, et aidata tavakasutajal droone turvalisemalt kasutada, kuid piisavalt põhjalikud, et kaardistada droonidega seotud küberohte Eesti keele ruumis.

Spetsiifilisemalt vastatakse raportis järgmistele küsimustele:

1. Millised on droonide kasutamisega seotud peamised küberturvalisuse riskid?

2. Kuidas on tavakasutajatel võimalik iseseisvalt riske maandada?

Kuivõrd eri droonitüüpe on mitmeid, keskendume analüüsis eelkõige tsiviilvaldkonnas kasutatavatele multirootoritega õhudroonidele (mehitamata õhusõidukitele, mis liiguvad enam kui kahe rootori (mootori) jõul), kui ei ole mainitud teisiti. Sellest hoolimata on analüüsi võimalik suures osas üldistada ka teiste droonitüüpidele.

Uuring tugineb kvalitatiivsele meetodile, kombineerides dokumendianalüüsi ja poolstruktureeritud intervjuusid Eesti avaliku ja erasektori ekspertidega. Analüüs ei avalda tundlikku informatsiooni ning ekspertide sõnavõttud on anonüümsed. Analüüs valmis Riigi Infosüsteemi Ameti (RIA) Küberturvalisuse Keskuse ja Rahvusvahelise Kaitseuuringute Keskuse (RKK) ekspertide koostöös.

1. Droonide küberturvalisuse riskid

Droon lendab reaalajas inimjuhtimisega või autonoomselt eelmääratud loogika alusel, ilma et pardal oleks piloot. Tänapäeval on enim levinud ja universaalseim droonitüüp **multirootoritega** droon, mis tõuseb õhku mitme rootori pöörlemisega tekitatud tõstejõu abil ning võib hõljuda ühe koha peal¹. Lisaks on üha sagedasem tehisintellekti kasutamine² drooni erinevates funktsioonides, näiteks navigeerimise ja objektituvastuse toetamiseks. Enamik droone tugineb positsioneerimisel GNSS-süsteemidele ning osa süsteeme kasutab andmesideks ka internetipõhiseid teenuseid.

Droon koosneb üldistatult kolmest kesksest osast, mis omakorda sisaldavad erinevaid komponente:

ÕHUSÕIDUK ISE

Näiteks kere või raam, rootorid, aku, lennujuhtimis-süsteem, navigatsiooni-süsteemid (GNSS), *payload* (kaamera, gimbal ehk stabi-lisaator, LiDAR jms).

SIDE- JA JUHTIMIS-SÜSTEEMID

Näiteks C2 (andmeside-ühendus) ning andmeside (telemeetria, video-edastus)

MAAPEALNE OSA

Näiteks pult, tahvelarvuti, telefon, rakendused.

Droonide kasutamise riskid on seotud peamiselt füüsilise turvalisuse, andmete turvalisuse ja privaatsusega³. Droonide küberohte tuleks käsitleda kolmel tasandil:

1 riistvara

2 püsi- ja tarkvara

3 side- ja andmekihid

Järgnevalt esitame droonidega seotud küberturvalisuse riske, kombineerides omavahel drooni erinevaid komponente ning kolme eelmainitud tasandit.

1.1. Õhusõiduk

Õhusõiduki enda puhul võib jagada küberriskid kolme gruppi: püsi- ja tarkvara kuritarvitamine, sensorite ja navigatsiooni manipuleerimine ning drooni füüsiline ja tarneahela manipuleerimine.

Püsi- ja tarkvara peamine risk on nende süsteemides olevate turvanõrkuste ärakasutamine. Nagu igas tarkvaras, on droonides nii teadaolevaid kui ka tundmatuid (nn nullpäeva) turvanõrkusi.

Näiteks droonide autopiloodi püsi-vara on tihti madalama võimekusega ning ei pruugi vastata kõrgetele turvalisuse standarditele. Riskide vähendamiseks soovitame püsivara regulaarselt uuendada, kasutada ainult krüptograafiliselt allkirjastatud uuendusi ning drooni puldina

Riskide vähendamiseks soovitame püsivara regulaarselt uuendada, kasutada ainult krüptograafiliselt allkirjastatud uuendusi ning drooni puldina eraldi seadet, mida ei kasutata muudeks toiminguteks.

eraldi seadet, mida ei kasutata muudeks toiminguteks. Eraldi seadme kasutamine vähendab riski, et juba eelnevalt kompromiteeritud seadme kaudu saab ligi droonis asuvale püsi- või tarkvarale.

Riski kujutab ka **pahatahtliku koodi käivitamine** drooni tarkvaras, mis põhineb tihti Linuxil. Kuna tarkvara kasutatakse näiteks automaatseks navigeerimiseks või kasuliku lasti (*payload*) töötlemiseks, võib turvanõrkuste ärakasutamisel saada ligi andmetele või muuta droonide lennutrajektoori. Riskide vähendamiseks tuleb rakendada küberturvalisuse baaspõhimõtteid – kasutada ainult ametlikku, krüptograafiliselt allkirjastatud tarkvara, hoida see uuendatuna ja vältida mitteametlikke tarkvaralaiendusi.

Tihti rakendavad tootjad droonidele tarkvara kaudu **erinevaid lennupiiranguid** – asukohapõhist tehnoloogiat, maksimaalkiirust ja -kõrgust ning keelualasid. **Juurligipääsu saavutamisel** on võimalik need piirangud eemaldada, võimaldades droonil lennata näiteks lennujaamade lähedusse, piirialadele või muudesse keelualadesse. See muudab turvanõrkused otseseks lennuohutuse riskiks ja riskiks, et droon ei vasta enam kehtivatele õigusaktidele. Kuna kasutaja ei saa lennupiiranguid riistvara tasemel rakendada, siis soovitame valida ainult tuntud tootjate droone, millel on lennupiirangud tehaseseadetes. Droonikasutaja peaks regulaarselt uuendama geo-andmeid ning vältima mitteametlikku püsivara, mis eemaldab piiranguid.

Juurligipääsu omandamisel on potentsiaalselt võimalik **muuta drooni seerianumbrit ja muid tunnuskoodi**, mida kasutatakse drooni tuvastamiseks õhuruumi haldussüsteemides ja kaugidentifitseerimise protokollides. Sellisel viisil muudetud droon võib esineda teise seadmena, mistõttu on drooni keerulisem tuvastada ning sellele vastutust omistada. See on eriti oluline õiguskaitse ja intsidentide uurimise kontekstis. Soovitame kasutada droone, millel on tootjapoolne lukustatud identifikaator (Remote ID ehk kaugtunnus).

Püsivara versiooni alandamine

(*firmware downgrade*) on rünnak, mille käigus asendatakse drooni uuendatud ja paigatud püsivara vanema versiooniga. Need sisaldavad sageli juba avalikult teadaolevaid haava-

tavusi ning seetõttu muutub droon haavatavaks (ründajal ei pea olema teadmisi nn nullpäeva nõrkustest). Rünnak võib toimuda nii füüsilise ligipääsu kui ka kompromiteeritud uuenduskanali kaudu. Soovitame rakendada krüptograafiliselt allkirjastatud püsivara versioonipoliitikat, mis lubab uuendamist vaid püsivara uusimale versioonile ning tõkestab vanema versiooni sunnitud paigaldamist. Tarkvara peaks uuendama ainult ametlikust allikast ning vältima vanemaid või mitteametlikke versioone. Lisaks soovitame hoida logi kõigist püsivara uuenduskatsetest.

Samuti on riskiks **peidetud tagauksed**, mille puhul pahavara jääb drooni külge isegi pärast taaskäivitusi ja uuendusi. Soovitame hankida droone ainult usaldusväärselt tootjalt ning paigaldada ainult ametlikku püsivara.

Samuti on riskiks **peidetud tagauksed**, mille puhul pahavara jääb drooni külge isegi pärast taaskäivitusi ja uuendusi. Tavakasutajal on raske taolist pahavara iseseisvalt tuvastada. Soovitame hankida droone ainult usaldusväärselt tootjalt ning paigaldada ainult ametlikku püsivara ning jälgida, et drooni käitumises ei ilmneks mingeid kõrvalekaldeid tavapärasest käitumisest (ootamatu andmeside, ebatavaliselt kiire aku tühjenemine jne).

Droonide sensorid ja kasulik last (kaamerad, kõrgusmõõtlad, termokaamerad, LiDARid jne) on eraldiseisvad alamsüsteemid iseseisva tarkvara ja liidestega. Kompromiteeritud sensor ei pruugi mitte ainult andmeid lekitada, vaid ka jagada **lennukontrollerile valeandmeid**. See mõjutab omakorda otseselt lennu ohutust: manipuleeritud kõrgusmõõtlja võib põhjustada kokkupõrke maa või muu objektiga. Sensorite kompromiteerimine võib mõjutada ka GNSS-i navigatsiooni.

Sensorite andmevooge ei saa tavakasutaja mõjutada, seega on mõistlik valida usaldusväärne droonitootja.

Riistvara osas on kõrgendatud riskiks sensorite, lennukontrolleri, puldi jms **füüsiline manipulatsioon tarneahela käigus**. Droonikomponendid, nagu näiteks lennukontroller või GPS moodul, on tihti tarnitud keeruka tarneahela kaudu, mille osas on keeruline teostada põhjalikku järelevalvet või kontrolli. Pahatahtliku tegevuse kaudu on võimalik tootmisprotsessis muuta tarkvara või paigaldada tagauksi. Seda riski on tavakasutajal sisuliselt võimatu kontrollida ning siinkohal peaks tuginema erinevatele riiklikele regulatiivsetele nõuetele.

Füüsiline ligipääs droonile või juhtimisseadmele on eraldiseisev risk, mis erineb tarneahelariiskist. Ründaja, kes saab drooni hetkeks enda valdusesse (nt maandumise, hoolduse või järelevalveta ladustamise ajal), võib salvestatud andmeid kiiresti kopeerida või paigaldada pahavara. Sellist rünnakut on hiljem väga raske tuvastada. Soovitame kasutada füüsilisi plommimis- ja võltsimistuvastuse meetmeid ning logida kõik juurdepääsusündmused droonile ja juhtimisseadmetele.

Drooni kloonimine on keerukas mitmeastmeline rünnak, kus ründaja saab esmalt droonile füüsiliselt ligipääsu, taasloob pöördprojekteerimise (*reverse engineering*) teel selle tarkvara, krüptograafilised võtmed ja identifikaatorid ning loob samaviisiliselt käituvat kloonitud drooni. Kloonitud droon võib seejärel käituda volitatud seadmena, pääseda ligi droonihaldussüsteemidele ning avastamata tegutseda. Soovitame kasutada usaldusväärseid droonitootjaid ning kontrollida oma kontrol registreeritud seadmete nimekirja.

Nakatunud droon ei ole ainult passiivne andmelekk allikas. Ründaja võib kasutada drooni **luurevahendina**, suunates selle tundlike asukohtade kohale ning kogudes salaja video-, audio- või muid sensorandmeid. Oht on eriti akuutne tööstus-, kaitse- ja julgeolekuvaldkonnas, kus droonid lendavad piiratud juurdepääsuga aladel. Soovitame rakendada drooni asukohapõhise tehnoloogia piiranguid ning logida kõik kasuliku lasti käivitamised.

Nakatunud droon ei ole ainult passiivne andmelekk allikas. Ründaja võib kasutada drooni **luurevahendina**.

Kõigi rünnakute (sh andmeside võltsimise (*spoofing*), segamise (*jamming*), C2 lingi kompromiteerimise ja tarkvara ärakasutamise) lõppeesmärgiks võib olla **drooni täielik füüsiline ülevõtmine**. Ründaja, kes suunab drooni enda valitud asukohta, saab nii drooni kui ka selle kasuliku lasti, kaasa arvatud salvestatud andmed, kaamera ja muud seadmed, füüsiliselt kätte. See tähendab, et küberoht võib muutuda füüsiliseks ohuks ning häirida näiteks lennuliiklust. Soovitame defineerida selged asukohapõhise tehnoloogia piirid ning häiremehhanismid trajektoori kõrvalekallete tuvastamiseks.

Viimase riskina toome esile **ebaturvaliselt säilitatud andmed**, mis võivad sisaldada tundlikku informatsiooni. Soovitame krüpteerida lennulogisid võtmega, mis ei asetse droonis endas, ning rakendada pärast andmete üleslaadimist automaatset logikustutamist.

Tavakasutaja jaoks ei ole õhusõidukiohud võrdselt tõenäolised. Kõige olulisemad on need, mis ei eelda ründajalt eriressursse ega füüsilist ligipääsu ning mis võivad puudutada kõiki kasutajaid ehk eelkõige püsi- ja tarkvaraga seotud riskid ning ebatuurvaliselt salvestatud andmed. Seevastu drooni kloonimine ja tarneahela riistvara manipuleerimine eeldavad märkimisväärsed ressursse ning sihtmärkideks on pigem tundlikumat infot omavad isikud ja asutused.

1.2. Side- ja juhtimissüsteem

Side- ja juhtimissüsteemi küberriskid võib jagada kolme peamisesse kategooriasse: juhtimis-seadmete ja maapealse juhtimissüsteemi turvanõrkused, sidekanali kättesaadavuse ründed ning sidekanali autentsuse ja konfidentsiaalsuse ründed.

Side- ja juhtimissüsteemide riistvara peamine risk on võltsitud või pahatahtlikult muudetud puldid ja juhtimisseadmed, mis võivad sisaldada **eelinstalleeritud pahavara või tagauksi**. Soovitame hankida juhtimisseadmeid ainult usaldusväärsetelt tarnijatelt ning kontrollida nende tarkvara terviklikkust enne kasutuselevõttu.

Püsi- ja tarkvara osas on side- ja juhtimissüsteemide puhul riskiks **maapealse juhtimisjaama (GCS) tarkvara turvanõrkused**. GCS tarkvara töötleb sisendeid erinevatest allikatest – droonilt, missioonifailidest ja kolmandate osapoolte rakendustest – ning turvanõrkuste ärakasutamise-ga on võimalik saada ligipääs lennuandmetele või anda droonile pahatahtlikke käske. Samuti on riskiks nõrk või puuduv tuvastamine maapealse juhtimisjaama ja drooni vahel, mille korral võib ründaja luua ühenduse drooniga ilma operaatori teadmata. Soovitame hoida maapealse juhtimisjaama tarkvara regulaarselt uuendatuna, kasutada selle jaoks eraldiseisvat seadet ning rakendada vastastikust autentimist maapealse juhtimisjaama ja drooni vahel.

Sageli alahinnatud riskiks on **nõrk või vale konfigureerimine** – vaikumisi paroolid, liiga laiad ka-sutajaõigused, avatud võrgupordid ja puudulikud tulemüürid. Tegu ei ole tarkvara, vaid inimlike vigadega seadistamisel, mistõttu jäävad need tihti tähelepanuta. Ründaja, kes leiab droonisüs-teemi, mis kasutab vaikumisi paroole või millel on avatud haldusliides, ei vaja keerukaid meeto-deid ligipääsu saamiseks. Soovitame järjepidevalt seadistused üle vaadata ning kasutada turva-lise konfiguratsiooni kontrollnimekirju.

Krüptograafiliste võtmete ja autentimisandmete lekkimine on eraldiseisev risk, mis võib tekkida mitmel viisil – võtmed on kõvakodeeritud tarkvarasse, salvestatud droonile endale, või lekivad andmepüügi kaudu. Kui ründaja saab kätte autentimisandmed, muutuvad kõik muud turvameet-med sisutühjaks, sest ta pääseb süsteemi legitiimse kasutajana. Soovitame kasutada riistvaralisi turvamoduleid võtmete hoid-miseks, vältida võtmete salves-tamist droonidele endile ning rakendada võtmete regulaarset uuendamist.

Külghkanali rünnakute läbiviimine eeldab märkimis-väärset tehnilist pädevust ja füüsilist ligipääsu siht-märgile. Seetõttu on külghkanali ründed eriti riskantsed kõrge väärtusega droonisüsteemidele.

Külghkanali ründed (*side-channel attacks*) ei ründa tarkvara ega protokolle otseselt, vaid kasuta-vad krüptograafiliste võtmete taasloomiseks riistvara füüsikalisi omadusi (elektrivoolu tarbimist, elektromagnetkiirgust või ajastust). Drooni juhtimisseadmed ja pardaarvutid teostavad krüpto-graafilisi operatsioone, mille käigus tekkivaid füüsikalisi signaale on võimalik spetsiaalse mõõt-misseadmega kätte saada. Külghkanali rünnakute läbiviimine eeldab märkimisväärset tehnilist pädevust ja füüsilist ligipääsu sihtmärgile. Seetõttu on külghkanali ründed eriti riskantsed kõrge väärtusega droonisüsteemidele. Tavakasutaja ei saa seda riski maandada.

Side- ja andmekihi tasandil kujutab endast küberohtu **raadioside segamine (jamming)**. Rünnaku

järel võib katkeda side drooni ja maapealse kontrolleri vahel ning droon jätkab lendu eelprogrammeeritud marsruuti või käsku täites (nt kojulend või maandumine). Soovitame kasutada droone, millel on FHSS sagedusega raadiovõimekus, mida on keerulisem segada, ning vajadusel ka alternatiivseid sidekanaleid droonidega (näiteks LTE). Lisaks tasuks mõelda, milline eelprogrammeeritud käsk anda droonile, kui side katkeb, et droonil oleks võimalik ohutult maanduda.

Ühenduse katkestamise (*de-authentication*) rünnak erineb segamisest selle poolest, et ründaja ei häiri raadiosidet, vaid saadab võltsitud protokollikäsu, mis katkestab drooni ühenduse maapealse juhtimissüsteemiga. Droon tõlgendab seda volitatud käsuna ning lülitub tõrkekindlasse (*failsafe*) režiimi, mis olenevalt eelprogrammeeritud käsust võib tähendada kontrollimata maandumist või kojulendu. Rünnak tugineb protokollile endale ning seetõttu on seda võrreldes tavalise segamisega raskem tuvastada. Soovitame kasutada autenditud sideprotokolle, kus lahutuskäsklused on krüptograafiliselt allkirjastatud.

Side- ja juhtimissüsteemide puhul tuleb pöörata tähelepanu **vahendajarünnetele**. Rünnakus positsioneerib kurjategija end maapealse juhtimissüsteemi ja drooni vahele, mis võimaldab tal kuulata pealt käske või neid muuta.

Soovitame kasutada vastastikust TLS-põhist (*Transport Layer Security*) autentimist kõigis maapealse juhtimissüsteemi sideühendustes ning kontrollida sertifikaatide kehivust iga ühenduse loomisel.

Külgkanali rünnakute läbiviimine eeldab märkimisväärt tehnilist pädevust ja füüsilist ligipääsu sihtmärgile. Seetõttu on külgkanali ründed eriti riskantsed kõrge väärtusega droonisüsteemidele.

GPS/GNSS-signaali võltsimise (*spoofing*) korral saadab ründaja pärisignaalist tugevama võltsignaali, mille tagajärjel arvab droon, et asub vales asukohas ning muudab seejärel enda liikumistrajektoori. Võltsimine on odav, kuid tehniliselt keerukam kui segamine. Soovitame kasutada mitmeid süsteeme (näiteks GPS ja Galileo), mis suudavad vajaduse korral võltsimist tuvastada.

Kordusrünnaku (*replay attack*) korral salvestab ründaja volitatud juhtimiskäsud ning esitab need hiljem uuesti. Droon tõlgendab neid seejärel päriskäskudena. Näiteks võib ründaja salvestada „maandu“ käsu ning aktiveerida selle kriitilisel hetkel, ilma et tal oleks ligipääs sidesüsteemile. Soovitame valida krüpteeritud sidemega droone (mitte avatud krüpteerimata Wifi/MAVLink) ning mitte nõrgendada vaikumise peale pandud turvaseadeid.

Tehisintellekti kasutavate droonisüsteemide puhul võib esile kerkida viiba manipuleerimise (*prompt injection*) rünnak, kus kurjategija sisestab tehisintellektile/mudelile/andmevoogudele pahatahtlikke käskke. Kuna drooni töö tugineb tehisintellektile, tundub droonile, et tegu on volitatud käskudega. Viiba manipuleerimise rünnaku riski saab maandada, kui kasutaja valideerib enne töötlemist kõiki tehisintellektisüsteemide sisendandmeid, piirab tehisintellekti mooduli õigusi kriitiliste lennukäskude andmisel ning auditeerib järjepidevalt mudeli otsuseid.

Telemeetria ja videopildi **krüpteerimata edastamine** võimaldab pealtkuulamist või segamist, millega võidakse paljastada tundlikke andmeid. Soovitame kasutada näiteks AES-256 krüpteeringut kogu telemeetria ja videovoo edastamisel ning keelata krüpteerimata sideprotokollide kasutamine seadistuste tasemel.

Enamik droone edastab kaugidentifitseerimise (Remote ID) nõude alusel avalikult oma identifikaatorit, asukohta ja sageli ka operaatori asukohta. Eelnevalt kirjeldatud seerianumbri võltsi-

mise asemel on siin risk vastupidine – see võib **paljastada operaatori asukoha**. Kuna signaal on mõeldud avalikult loetavaks, saab igaüks sobiva vastuvõtja abil tuvastada nii drooni kui ka piloodi asukoha. Risk süveneb, kui tootja kasutab krüpteerimata lahendusi. Kuna tegemist on seadusest tuleneva nõudega, ei saa seda riski täiesti elimineerida. Soovitame kasutada droone, mis järgivad standardset kaugidentifitseerimise lahendust, ning lennata positsioonidelt, mis ei paljasta tundlikke asukohti ega isikuid.

Side- ja juhtimissüsteemi rünnete puhul on tavakasutaja jaoks kõige olulisem sideturvalisus juba drooni ostuhetkel ja selle seadistamisel, sest ülejäänud kaitsemeetmed (näiteks autenditud protokollid, TLS jne) on tootja poolt seadistatud. Segamine ja GNSS-võltsimine on lihtsamad ründed, kuid vajavad teatud seadmeid ning füüsilist lähedust. Külgkanali ründed on pigem kõrge väärtusega isikute ja asutuste murekohaks.

1.3. Maapealne osa

Drooni maapealse osa puhul võib küberriskid jagada kolme kategooriasse: lõppseadme ja rakenduse kompromiteerimise, pilve- ja taustsüsteemide kompromiteerimise ning andmekaitse, privaatsuse ja logimisega seotud riskid.

Drooni maapealse osa peamine risk on **maapealsete süsteemide** (näiteks serverite, pilvekeskkondade või haldustarkvara) **kompromiteerimine**. Erinevalt droonist endast on maapealne süsteem tihti ühendatud laiemal võrguga, suurendades ründepinda. Kurjategija võib nõrkade paroolide, andmepüügi ja andmelekkede kaudu konto üle võtta. Sel viisil satuvad missiooniandmed, logid või kasutajainfo volitamata isiku kätte. Soovitame rakendada tugevat juurdepääsukontrolli (sh tugevaid paroole) ja mitmeastmelist autentimist ning krüpteerida pilves säilitatavad andmed. Lisaks tasuks arvestada drooni kompromiteerimise võimalust välismaale reisimise puhul, eriti riikides, kus julgeoleku- või luureasutustel on ulatuslikud volitused seadmetele ligipääsuks.

Soovitame rakendada tugevat juurdepääsukontrolli (sh tugevaid paroole) ja mitmeastmelist autentimist ning krüpteerida pilves säilitatavad andmed.

Eraldi riskina tuleb välja tuua **mobiilirakenduse kompromiteerimine**. Droonide juhtimisrakendused töötavad tihti isiklikel nutiseadmetel, mida kasutatakse paralleelselt muude igapäevaste toimingutega. See suurendab ründepinda oluliselt, sest nutiseadme uuendamata operatsioonisüsteem, pahatahtliku rakenduse allalaadimine või andmepüük võivad anda ründajale ligipääsu juhtimisrakendusele ning selle kaudu droonile. Lisaks võib kompromiteeritud uuenduskanal kaasa tuua pahavara ka maapealsesse tarkvarasse. Soovitame kasutada droonijuhtimiseks eraldi seadet ning hoida mobiilirakendus ja operatsioonisüsteem alati uuendatuna.

Teenustõkestusrünne (DoS/DDoS) maapealse infrastruktuuri vastu ei kompromiteeri süsteemi otseselt, kuid võib raskendada droonihaldust või muuta selle võimatuks. Ründaja võib üle koormata maapealse juhtimissüsteemi, pilvehaldusplatvormi või sidevõrgu, mille tagajärjel kaotavad operaatorid droonidega ühenduse ja need lülituvad etteplaneeritud autopiloodile või tõrkekindlale režiimile. Taolise rünnaku allikaid on mitmeid ning sestap on selle tõkestamine keerukam. Soovitame kasutada liikluse piiramist (*rate limiting*) ja kõrvalekallete tuvastamist enne, kui need

jõuavad maapealse serverini, eraldada kriitilised haldusliidestused avalikust võrgust ning kavadada eelnevalt käitumisreeglid juhaks, kui maapealne ühendus katkeb.

Droonihaldussüsteemid suhtlevad üha enam pilveteenuste ja kolmandate osapooltega **rakendusliideste (API)** kaudu. Nõrgalt kaitstud API (nt puuduva autentimise, liiga laia ligipääsuga võtmete või valideerimata sisendite korral) võib anda ründajale ligipääsu missiooniandmetele, logidele, kasutajakontodele või isegi droonijuhtimise funktsioonidele, ilma et oleks vaja maapealse juhtimissüsteemi tarkvarasse sisse murda. See oht on eriti suur, kui maapealne juhtimissüsteem on ühendatud kolmandate osapoolte platvormidega, nt kaarditeenuste, logistikasüsteemide või lennuinfo teenustega. Soovitame läbi mõelda, kas on vaja siduda droone kolmandate teenustega.

Droonide haldussüsteemide turvanõrkuste ärakasutamisega on võimalik mõjutada korraga mitut drooni ning pääseda ligi salvestatud missiooniandmetele, logidele ja kasutajakontodele. Soovitame rakendada tugevat juurdepääsukontrolli, mitmeastmelist autentimist ning krüpteerida kõik pilvekeskkonnas säilitatavad andmed.

Droonid koguvad oma töö käigus suures koguses (**isiku**)andmeid (nt GPS-trajektoore, videomaterjali ja sensorandmeid), mille kaudu võib olla võimalik tuvastada isikuid või asukohti. Kompromiteeritud droon võib ründajale edastada reaalsajas asukoha- ja videoandmeid. Sel viisil saab kurjategija kasutada drooni jälgimisvahendina. Lisaks kaasnevad andmelekkega õiguslikud riskid isikuandmete kaitse üldmääruse (GDPR) alusel. Soovitame taas kord rakendada vähimate õiguste põhimõtet, krüpteerida kõik kogutavad andmed ning määratleda selged andmete säilitamise ja kustutamise reeglid.

Kompromiteeritud droon võib ründajale edastada reaalsajas asukoha- ja videoandmeid. Sel viisil saab kurjategija kasutada drooni jälgimisvahendina.

Puudulik logimine ja (turva)seire ei ole otsenerünnak, kuid lihtsustab järgnevaid rünnakuid, sest ründaja võib avastamatategutseda süsteemispikka aega. Soovitame tugineda keskele logimisele kõigi droonisüsteemide komponentide puhul, määratleda automaatsed häiremehhanismid kahtlaste sündmuste tuvastamiseks ning tagada logide terviklikkus kirjutuskaitstud salvestuse abil. Vaid sel viisil on võimalik ebatavalist andmeedastust, käske ja ebaõnnestunud autentimiskatseid tuvastada.

Puudulike/ebapiisavate logide kõrval on eraldiseisvaks ohuks olemasolevate **logide aktiivne manipuleerimine**. Ründaja, kes on saavutanud ligipääsu drooni või maapealsele süsteemile, võib kustutada või muuta lennulogisid, et varjata rünnaku jälgi ja takistada hilisemat analüüsi. See erineb oluliselt puudulikust logimisest, kuna ründaja tegutseb teadlikult tõendite hävitamiseks. Soovitame logid kohe salvestada eraldi, võrguvälisesse kohta, kuhu droon ise hiljem ligi ei pääse ega saa neid muuta.

Droonide maapealse osa juures on tavakasutaja jaoks kõige olulisem tema seadme ja konto turvalisus. Nendega seotud riske saab ta mõjutada palju suuremal määral kui pilveteenuste, API ja teenustökestusega seotud ohte.

Kombineerides omavahel drooni erinevad osad ja küberohtude kolme tasandit saame järgneva kokkuvõtliku droonide küberohtude tabeli:

	Riistvara	Püsi- ja tarkvara	Side- ja andmekihid	Küberohud
Õhusõiduk	Kere/raam, mootorid, akud, lennujuhtimis-süsteem, navigatsioonimoodul, sensorid, <i>payload</i>	Autopiloodi tarkvara, sensorite tarkvara, navigatsiooni- ja stabiliseerimistarkvara, <i>payloadi</i> juhtimistarkvara, pardasüsteemide uuendamistarkvara	Sensorite sisend-andmed, GNSS-signaalid, <i>payloadi</i> andmevood, krüpteerimata logid ja salvestatud andmed	Kompromiteeritud tarneahel, tagauksed, sensorite ja kasuliku lasti ning süsteemide andmete manipuleerimine ja ära kasutamine, <i>spoofing</i> , pardasüsteemi haavatavused, füüsiline kaaperdamine kübervahendite abil, luureandmete kogumine <i>payloadi</i> kaudu, füüsiline ligipääs, drooni kloonimine ja pöördprojekteerimine, identiteedi võltsimine, tarkvaraversiooni vanandamine
Side- ja juhtimis-süsteem	Raadiosidemoodulid, antennid, videoedastusmoodulid, telemetriamoodulid, mobiilside- või satelliitmoodulid	Sideprotokollid, krüptograafilised lahendused, telemetria tarkvara, videoedastustarkvara	Juhtimiskäsud, telemetria, videoedastus, <i>payloadi</i> andmeside, võrguühendused, autentimis- ja võtmehetuseandmed, Remote ID/Drone ID asukoha paljastamine	Häirimine, võltsimine, pealtkuulamine, vahendusründed, nõrga krüpteeringu ära kasutamine, viibasüst, nõrk konfigureerimine, võtmete lekkimine, ühenduse katkestamise ründed, kordusründed, külkanali ründed
Maapealne osa	Pult, tahvelarvuti, telefon, serverid, tugiinfrastruktuur	Maapealne tarkvara, mobiilirakendus, konto- ja kasutajahaldus, pilveteenused	Kasutajakonto andmed, logid, pilvesünkroniseerimine, tarkvara allalaadimine, API-liidesed	Pahavara juhtseadmes, konto ülevõtmine, mobiilirakenduse turvanõrkused, pilveskeskkonnas kompromiteerimine, andmeleke, tarkvarauuendusega tekkivad riskid, nõrk konfigureerimine, kasutaja privaatsuse rikkumine, asukoha jälgimine, füüsiline ligipääs, puudulikud logid ja monitooring, logide manipuleerimine, DoS/DDoS-rünnakud, nõrgalt kaitstud API-d

Tabel 1. Droonide peamised küberohud. Autorite koostatud eri allikate põhjal ^{4,5,6,7,8,9,10,11,12,13,14}.

Lisaks eelkirjeldatud tehnilistele ohtudele tuleb arvestada mõne laiema küberohuga, mida ei ole otstarbekas siduda ühe konkreetse drooni komponendiga. Organisatsioonisisene oht (*insider threat*) on olukord, kus pahatahtlik või hooletu operaator, tehnik või tarnija võib tahtmatult või tahtlikult kahju tekitada. Ohtu on keeruline tuvastada, sest siseringil on volitatud ligipääs süsteemile juba olemas. **Sotsiaalne manipuleerimine** (*phishing*, *vishing*) on sageli esmane rünnakuvektor, mis eelneb tehnilistele rünnakutele, ning on kaetud osaliselt konto ülevõtmise kirjelduses. **Tehisintellektimudelite mürgitamine** on kujunenud ohuks droonisüsteemides, kus kasutatakse masinõpet objektituvastuseks või navigatsiooniks ning kus manipuleeritud treeningandmed võivad muuta mudeli käitumist ettearvamatul viisil. Neid ohte ei ole tabelisse lisatud, kuna need ei

seostu üheselt konkreetse riistvara- või tarkvarakomponendiga, vaid hõlmavad droonisüsteemi kui tervikut.

Globaalselt kõige levinumad on Hiina firma DJI droonid. Hinnanguliselt omavad nad 70–90% tsiviildroonide turust ning nende seadmed on odavamad, paremad ning hea tarkvaraökosüsteemiga. Reaalseid samaväärseid alternatiive sisuliselt pole, eriti tavakasutaja hinnaklassis. Küberturvalisuse mõttes ei ole DJI droonid ohtlikumad teistest droonidest, kuigi osa uuringuid on tuvas-
tanud mõned aastad tagasi olulisi küberturvalisuse riske, eriti seoses andmete liikumisega Hiina.

Lisaks tehnilistele aspektidele tuleks arvestada Hiina päritolu toodete puhul ka ühe laiema riskiga, mis on seotud Hiina seadusandlusega. Välisluureamet kirjutas oma aastaraamatus¹⁴, et Hiina 2017. aasta rahvusliku luureseaduse kohaselt peavad kõik Hiina ettevõtted tegema riigi luureasutustega koostööd, sealhulgas vajadusel ka andmeid jagama ja seda ka juhul, kui andmeid hoitakse Euroopas. See on pigem õiguslik ja poliitiline risk ning ükski audit ei saa seda ümber lükata. Oluline on rõhutada, et see ei tähenda, et DJI droone tuleks vältida, küll aga soovitame mõelda Local Data Mode'i (LDMi) kasutamisele, mis tuntavalt vähendab seda riski.

2. Soovitused ja järeldused

Droonide tavakasutajatel on väga keeruline ennast kaitsta keerukate küberrünnete vastu. Enamik tehnilisi kaitsemeetmeid on tootja või regulaatori, mitte kasutaja otsustada.

Kõige mõistlikum on osta võimalikult turvaliste omadustega droon ning jälgida küberhügieeni põhimõtteid ja käituda küberteadlikult.

Oluline on mõista, et droon on küberturvalisuse vaatest oma olemuselt sarnane teiste internetiga ühendatud seadmetega ning seda tuleks ka samaväärselt kohelda. Lisaks tuleks enne drooni ostu juba tutvuda vastava seadusandlusega.

Soovitame olla teadlik droonikasutaja ja enda ning teiste turvalisuse huvides pidada silmas järgnevaid aspekte. **Drooni ostes** eelista juba ostuhetkel turvaliste omadustega drooni. Nendeks on krüpteeritud side, mitme satelliidisüsteemi tugi (näiteks GPS + Galileo), krüptograafiliselt allkirjastatud uuendused, sagedushüppega (FHSS) raadio ja võimalusel riistvara tasemel identiteedikaitse.

OLULISED KÜBERHÜGIEENI PÕHIMÕTTED

- 1. Kasuta tugevaid ja unikaalseid paroole.**
Ära kasuta sama parooli mitmes kohas, muuda kohe ära vaikimisi paroolid.
Võimalusel lülita sisse mitmeastmeline autentimine (MFA).
- 2. Uuenda regulaarselt drooni püsi- ja tarkvara.**
Samuti uuenda juhtimisseadme tarkvara ning laadi alla tarkvara ainult ametlikust rakendusepoest või tootja lehelt.
- 3. Kasuta droonijuhtimiseks eraldi seadet,** mida sa ei kasuta igapäevatoiminguteks, ja võimalusel ka eraldi võrku.
- 4. Krüpteeri lennulogid ja tundlikud salvestused.**
Kaal andmete kustutamist, kui neid enam vaja pole.
- 5. Ära jäta drooni ega juhtimisseadet järelevalveta.**
Hetkeline füüsiline ligipääs on omaette risk.

Vaata lisaks küberhügieeni kohta www.itvaatlik.ee

Lisaks on oluline meeles pidada, et droonide lennutamise puhul kehtivad erinevad reeglid, olenevalt drooni eripäradest.

1. Hoia end kursis droone puudutava seadusandluse ja lennupiirangutega Transpordiameti kodulehel. Eestis peab registreerima ennast drooni käitajaks, kui selle kaal on 250 grammi või rohkem või kui droonil on kaamera või muu andur, mis suudab koguda isikuandmeid.
2. Hangi droon ja juhtimisseade ainult usaldusväärsest ja ametlikust allikast ning väldi mitte-ametlikku tarkvara või püsivara, mis eemaldab piiranguid.
3. Enne lendu kontrolli õhuruumi piiranguid ametlikult droonikaardilt Estonian Drone Map, kus kuvatakse ka NOTAM-lennundusteateid. Välti rahvarohkeid kohti.
4. Tutvu oma drooniga, selle omadustega ning arvesta maastiku eripäradega – näiteks avamerel ulatub raadioside segamine tunduvalt kaugemale. Jälgi drooni ka lennu ajal, sh ajal, mil see on automaatrežiimil. Erinevate kõrvalekallete varajane tuvastamine on operaatori vastutus.
5. Idapiiri lähedal arvesta tugeva GPS-signaali häirimisega, mis võib põhjustada kontrolli kaotuse, drooni füüsilise hävimise või andmete kadumise. Soovitame lennutada droone piirist ohutus kauguses, st vähemalt viie kilomeetri kaugusel.
6. Eelprogrammeeri drooni tegevus side katkemise või kontrolli kaotuse puhul, et vähendada ohtu endale ja teistele.
7. Arvesta, et kui droon teeb otseülekannet sotsiaalmeediasse, salvestab andmeid ka platvormi server.
8. DJI droonide puhul kasuta võimalusel Local Data Mode'i.

Lühendid ja mõisted

AES-256 krüpteering (ingl. *Advanced Encryption Standard, 256 bits*) – laialdaselt kasutatav sümmeetrilise krüpteerimise algoritm, mis kaitseb andmeid 256-bitise võtmega, muutes need ilma õige võtmeta praktiliselt loetamatuks.

C2 (ingl. *Command and Control*) – andmesideühendus, mille kaudu juhitakse drooni lendu.

DJI Local Data Mode (lühendina LDM) – DJI droonide funktsioon, mis lülitab välja internetiühenduse ja takistab seadmel andmete edastamise tootja serverisse lennu ajal.

Droon – mehitamata õhusõiduk (MÕS), ka UAV (ingl. *Unmanned Aerial Vehicle*)

FHSS-raadio (ingl. *Frequency-Hopping Spread Spectrum*) – raadioside vorm, kus saatja ja vastuvõtja vahetavad edastavat sagedust kiiresti ja etteantud mustri järgi, mistõttu signaali on raskem segada või pealt kuulata.

Geotsoon – eelmääratletud geograafiline ala, millele on kehtestatud digitaalsed piirangud või reeglid, näiteks drooni lennukeeld või kõrguspiirang. Tavaliselt kehtestatakse GPS-põhise positsioneerimise alusel.

Gimbal – mehhaaniline stabiliseerimissüsteem, mille eesmärgiks on hoida kaamera või mõni muu sensor stabiilsena liikumise ajal.

GPS (ingl. *Global Positioning System*) – Ameerika Ühendriikide poolt arendatud ja hallatav satelliitnavigatsioonisüsteem, mis võimaldab määrata asukohta, kiirust ja aega, kasutades selleks satelliitidelt saadud signaalide triangulatsiooni. Droonide kontekstis on GPS kriitiline positsioneerimise ja autonoomse lennu jaoks, kuid selle signaali on võimalik häirida või eksitada, mis võib viia kontrolli kadumiseni drooni üle.

GNSS (ingl. *Global Navigation Satellite System*) – üldmõiste kõikide globaalsete satelliitnavigatsioonisüsteemide kohta, nagu GPS, Galileo (Euroopa Liit), GLONASS (Venemaa), BeiDou (Hiina).

GNSS-häirimine (ingl. *GNSS jamming*) – raadiosignaali tahtlik häirimine, mille eesmärgiks on blokeerida või segada GNSS-signaalide vastuvõttu, muutes seadme asukoha, kiiruse ja aja määramise ebatäpseks või võimatuks. Tegemist on aktiivse häiringuga, kus vastuvõtja ujutatakse üle tugeva mürahäirega.

GNSS-signaali võltsimine (ingl. *GNSS spoofing*) – raadiosignaali tahtlik võltsimine, mille eesmärgiks on eksitada vastuvõtjat, edastades sellele valesid satelliidisignaale ning mõjutades seeläbi seadme asukoha, kiiruse ja aja arvutust. Tegemist on aktiivse häiringuga, kus vastuvõtja petetakse usaldama vale signaali ehtsa GNSS-signaali asemel.

Häirimine (ingl. *jamming*) – laiem mõiste tahtlikule raadiosignaali häirimisele, mille eesmärgiks on halvata või nõrgestada drooni side- või navigatsioonikanaleid, muutes selle juhtimise, positsioneerimise või andmeedastuse ebatäpseks või võimatuks. Droonide puhul võib häirimine sihtida GNSS-i, C2-linki, videopilti või telemeetriat.

Juurpääs (ingl. *root access*) – kõrgemad juurdepääsuõigused operatsioonisüsteemis, mis võimaldavad kasutajal piiranguteta muuta süsteemi faile, seadistusi ja funktsioone.

Droonide puhul võimaldavad juurpääsuõigused muuta püsivara, paigaldada tarkvara või muuta süsteemi turvaseadeid.

Kasulik last (ingl. *payload*) – drooni põhifunktsionaalsusest eraldiseisev kasulik seade või süsteem, mida droon kannab konkreetse ülesande täitmiseks, näiteks kaamera, LiDAR või kõlar.

Kaugidentifitseerimine (ingl. *Remote ID*) – süsteem, mis võimaldab drooni ja selle tegevuse reaajas tuvastamist, edastades andmeid nagu identifikaator, asukoht, kõrgus ja kiirus, ning võimaldab drooni kaugelt jälgida ning seostada konkreetse lennuga.

Lennujuhtimissüsteem (ingl. *Flight Control System, FCS*) – drooni pardasüsteem, mis töötleb sensorandmeid ning juhib automaatselt mootoreid ja stabiilsust, et tagada kontrollitud ja stabiilne lend lähtuvalt piloodi või automaatika sisendist. Koosneb riistvarast, püsivarast ja algoritmidest.

LiDAR (ingl. *Light Detection and Ranging*) – sensor, mis saadab välja laserimpulsse ning mõõdab peegeldunud signaali tagasijõudmise aega, et arvutada objektide kaugust. Kasutatakse takistuse tuvastamiseks, kõrguse hindamiseks, keskkonna kaardistamiseks ja navigeerimise toetamiseks.

Liikluse piiramine (ingl. *rate limiting*) – meede, mis piirab, kui palju päringuid või andmeid saab teatud aja jooksul süsteemile saata, et vältida selle ülekoormamist. Droonide kontekstis aitab see kaitsta maapealset infrastruktuuri teenustõkestusrünnakute vastu.

Maapealne juhtimissüsteem (ingl. *Ground Control* või *Ground Control Station, GCS*) – maapealne süsteem, mille kaudu saab operaator drooni jälgida, seadistada ja juhtida, sealhulgas hallata lennuparameetreid ja telemeetriat ning anda operatiivseid käske.

Organisatsioonisisene oht (ingl. *insider threat*) – süsteemile volitatud ligipääsuga inimesest tulenev oht, näiteks töötaja, tehnik või tarnija, kes võib tahtlikult või hooletusest kahju tekitada.

Pöördprojekteerimine (ingl. *reverse engineering*) – protsess, mille käigus analüüsitakse valmis toodet (näiteks drooni tarkvara või riistvara), et mõista selle ülesehitust ja tööpõhimõtet.

Püsivara (ingl. *firmware*) – seadmesse sissehitatud tarkvara, mis juhib vahetult riistvara tööd ja põhifunktsioone. Näiteks drooni sees olev lennujuhtimissüsteem.

Riistvara (ingl. *hardware*) – arvuti või muu elektroonilise seadme füüsiliste komponentide kogum, mis moodustab süsteemi materiaalse osa ning millel töötab tarkvara ja püsivara, võimaldades seadme funktsioonide täitmist.

Reaajas kinemaatiline positsioneerimine (ingl. *real-time kinematic, RTK*) – täppispositsioneerimise meetod, kus kasutatakse vähemalt kahte GNSS-vastuvõtjat. Üks paikneb droonis ning teine on läheduses asuv staatiline baasjaam. Meetod parandab positsioneerimise täpsust, kuid eeldab stabiilset ja pidevat andmesidet drooni, maapealse juhtimissüsteemi ja baasjaama vahel.

Sensorid (ehk andurid) – seadmed, mis koguvad andmeid drooni enda oleku või ümbritseva keskkonna kohta ning muudavad need digitaalseks informatsiooniks, mida süsteem saab töödelda. Sensorid võivad mõõta asendit, kiirust, kaugust või visuaalset informatsiooni.

Side (ingl. *communication link*) – droonide ja teiste süsteemide vaheline andmevahetuskanal, mille kaudu liigub info, sealhulgas juhtimiskäsud ja andmed. See hõlmab endas nii juhtimissidet (C2) kui ka andmesidet, näiteks telemeetriat ja reaajas videovoogu.

Tarkvara (ingl. *software*) – programmide ja rakenduste kogum, mis töötab seadme riistvaral ning võimaldab seadme kasutajapoolset juhtimist, seadistamist ja andmete töötlemist. Näiteks drooni maapealne juhtimistarkvara.

Telemeetria (ehk kaugmõõtmine) – andmevoog, mille droon edastab maapealsele juhtimissüsteemile, et anda reaajas ülevaade drooni olekust ja tegevusest. See võib sisaldada näiteks kõrgust, asukohta, lennusuunda, kiirust ning sidekanalite kvaliteedi näitajaid.

TLS (ingl. *Transport Layer Security*) – krüptograafiline protokoll, mis tagab kahe osapoolse vahelise andmeside konfidentsiaalsuse, terviklikkuse ja autentsuse, krüpteerides edastatava info ja kontrollides suhtluspoolte identiteeti.

Vahendusrünne (ingl. *man-in-the-middle attack*, MITM) – küberrünne, kus ründaja asetub kahe osapoolse (näiteks drooni ja maapealse juhtimissüsteemi või drooni ja operaatori) vahelisse suhtlusesse ning saab jälgida või muuta nende vahel edastatavaid andmeid ilma osapoolte teadmata.

Viiba manipuleerimine (ingl. *prompt injection*) – generatiivse tehisintellekti rünnak, kus pahahtlik sisend manipuleerib drooni juhiseid või käitumist, et panna see eirama algseid piiranguid või täitma soovimatuid juhiseid. Droonide kontekstis on see oluline juhul, kui süsteemides kasutatakse suurte keelemudelite (LLM) põhiseid komponente näiteks juhtimise, analüüsi või otsuste toetamiseks.

Vähimate õiguste põhimõte (ingl. *principle of least privilege*) – turvapõhimõte, mille kohaselt antakse igale kasutajale, süsteemile või rakendusele ainult need õigused, mis on tema ülesande täitmiseks minimaalselt vajalikud.

Võltsimine (ingl. *spoofing*) – laiem mõiste raadiosignaali tahtliku petmise kohta, mille eesmärgiks on eksitada drooni navigatsiooni- või positsioneerimissüsteemi, edastades sellele valesid GNSS-signaale ning mõjutades seeläbi seadme asukoha, kiiruse ja aja arvutust. Tegemist on aktiivse ründega, kus vastuvõtja usub, et saab ehtsaid satelliidisignaale, kuigi tegelikult juhitakse teda valeandmetega.

Allikad

- 1 Tartu ülikool, [Droonid maateadustes: lisamaterjal](#).
- 2 Kheireddine Choutri et al. [Leveraging Large Language Models for Real-Time UAV Control](#). Innovations in NLP and Large Language Models: Shaping the Future of AI, 02.11.2025.
- 3 Eda Marchetti et al. [Cybersecurity Testing in Drones Domain: A Systematic Literature Review](#). Institute of Electrical and Electronics Engineers, 2024.
- 4 Kanada Küberturvalisuse keskus, [Cyber security considerations for drone use \(ITSAP.00.143\)](#), jaanuar 2026.
- 5 International Civil Aviation Organization, [Remotely Piloted Aircraft System \(RPAS\) Concept of Operations \(CONOPS\) for International IFR Operations](#), märts 2017.
- 6 PX4 Autopilot, [ESCs & Motors](#). Viimati loetud: 23.07.2026.
- 7 PX4 Autopilot, [PX4 System Architecture](#). Viimati loetud: 23.07.2026.
- 8 A Survey of Security Challenges and Solutions for UAS Traffic Management (UTM) and small Unmanned Aerial Systems (sUAS). [Arxiv.org](#). Viimati loetud: 6.08.2026
- 9 info.mitrengenuity.org, Open Generation Overview of Security of Uncrewed UAS, Jan 2023
- 10 Nico Schiller et al. [Drone Security and the Mysterious Case of DJI's DronelD](#). Ruhr University Bochum, 2023.
- 11 Eda Marchetti et al, Cybersecurity Testing... 2024.
- 12 Vikas Sihag et al, [Cyber4Drone: A Systematic Review of Cyber Security and Forensics in Next-Generation Drones](#), Drones 2023.
- 13 Robert Tollast, [Drones: Decoupling Supply Chains from China](#), The Royal United Services Institute for Defence and Security Studies, 2025.
- 14 Välisluureamet, Eesti rahvusvahelises julgeolekukeskkonnas, 2019.