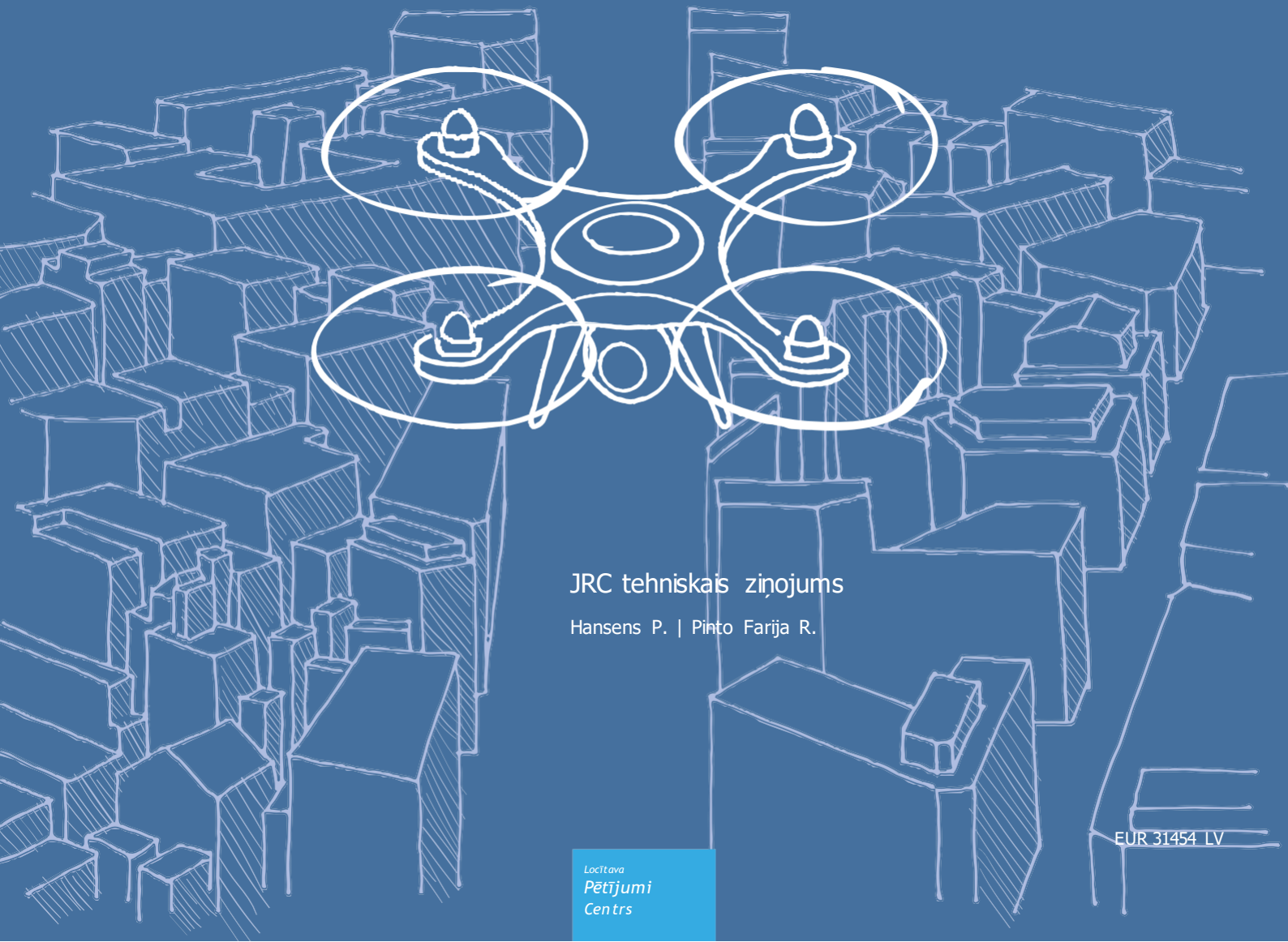
ISSN 1831-9424

European Commission

Aizsardzība pret bezpilota gaisa kuģu sistēmām

Rokasgrāmata par kritiskās infrastruktūras un publiskās telpas aizsardzību no UAS: piecu fāžu pieeja C-UAS ieinteresētajām pusēm



JRC tehniskais ziņojums

Hansens P. | Pinto Farija R.

EUR 31454 LV

Lokālā Pētījumi Centrs

Kontaktinformācija

Vārds: HANSEN Paul (JRC-GEEL)
Adrese: Eiropas Komisijas Kopīgais
pētniecības centrs
Retieseweg 111
2440 Geel
BEĻĢIJA/BELĢIJA

Tālr.: +32 (0)14 571 485 E-pasts: JRC-DRONE@ec.europa.eu

ES zinātnes centrs

https://joint-research-centre.ec.europa.eu

JRC132714
EUR 31454 LV

Drukāt	ISBN 978-92-68-06614-0	ISSN 1018-5593	doi: 10.2760/747997	KJ-NA-31-454-LV-C
PDF	ISBN 978-92-68-01253-6	ISSN 1831-9424	doi: 10.2760/18569	KJ-NA-31-454-LV-N

Luksemburga: Eiropas Savienības Publikāciju birojs, 2023 © Eiropas Savienība, 2023

Kā citēt šo ziņojumu: Hansen, P., Pinto Faria, R., Handbook on UAS protection of Critical Infrastructure and Public Space: A Five Phase approach for C-UAS stakeholders, Joint Research Centre, Publications Office of the European Union, Luksemburga, 2023, doi:10.2760/18132971, JRC13697.

Aizsardzība pret bezpilota gaisa kuģu sistēmām

Rokasgrāmata par kritiskās infrastruktūras un publiskās telpas aizsardzību no UAS: piecu fāžu pieeja C-UAS ieinteresētajām pusēm

JRC tehniskais ziņojums

Hansens P. | Pinto Farija R.

Saturs

Abstrakts

Efektīvam bezpilota gaisa kuģu sistēmu (C-UAS) risinājumam ir jāsadarbojas ar daudzām ieinteresētajām personām, lai vienotos par procesiem un procedūrām. Šo rokasgrāmatu izstrādāja Eiropas Komisijas Kopīgais pētniecības centrs (JRC), un tās pamatā ir DRONE projektā gūtā pieredze[1]. Ieteikumi izstrādāti sadarbības projekta ietvaros. Šajā rokasgrāmatā sniegtos ieteikumus atbalsta mērķtiecīgas konsultācijas un semināri ar galvenajām ieinteresētajām personām, piemēram, tiesībaizsardzības aģentūrām (LEA), iestādēm, regulatoriem un tehnoloģiju uzņēmumiem.

Rokasgrāmatā sniegti padomi, kā aizsargāties pret ļaunprātīgu UAS, un sniegtas vadlīnijas, atsauces, pieejas un apsvērumi. Tas aptver noteikšanu, izsekošanu, identifikāciju un neitralizāciju, izmantojot riska analīzes procesus, risinājuma izstrādi, ieviešanu un risinājuma darbību. Tas izskaidro, cik svarīgi ir apvienot sistēmas un procesus ar ieinteresēto pušu iesaistīšanu, lai radītu pilnīgu risinājumu.

Šī rokasgrāmata ir Komisijas C-UAS paketes galvenā sastāvdaļa, par ko tika paziņots par pamatpasākumu saskaņā ar Komisijas paziņojumu "Dronu stratēģija 2.0 gudrai un ilgtspējīgai bezpilota gaisa kuģu ekosistēmai Eiropā"[2]. Šī pakete ietver īpašu C-UAS paziņojumu, kurā izklāstītas galvenās idejas ES nākotnes politikai par to, kā novērst iespējamos UAS radītos draudus.

Cenšoties sniegt pastāvīgu praktisku atbalstu ES dalībvalstīm un ieinteresētajām personām, JRC ir sagatavojis divas rokasgrāmatas; pirmā ir šī piecu fāzu pieeja C-UAS risinājuma izstrādei, savukārt otrajā ir ietverta virkne ieteikumu, lai novērtētu riskus, kas izriet no UAS ļaunprātīgas izmantošanas, kā arī ieteikumi par nemilitāro infrastruktūru fizisku aizsardzību pret šādiem draudiem.

1 ES zinātnes centrs, https://joint-research-centre.ec.europa.eu/scientific-activities-z/dronescounter-drones-and-autonomous-systems_en.

2 Komisijas paziņojums – Bezpilota lidaparātu stratēģija 2.0 viedai un ilgtspējīgai bezpilota gaisa kuģu ekosistēmai Eiropā, COM(2022) 652 galīgā redakcija, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0652 .

Ievads

Eiropā un pārējā pasaulē UAS (ko parasti dēvē par droniem) izmantošana pieaug. Kopējie pakalpojumi [3] attiecībā uz UAS ir definēti, lai palielinātu izmantošanu tādās nozarēs kā lauksaimniecība, transports, apsekošana un uzraudzība, skatīt 1. attēlu. ES drošības sistēma bezpilota gaisa kuģu ekspluatācijai un tehnisko prasību noteikšanai saskaņo Eiropas UAS tirgu, un tai vajadzētu palielināt ar UAS saistītos lietojumus, izstrādi un pakalpojumus.

Lai gan UAS var piedāvāt vērtīgas iespējas komerciāliem lietojumiem, pastāv arī ļaunprātīgas izmantošanas iespēja. UAS var izmantot privātuma noteikumu pārkāpšanai, spiegošanai, izmantojot kameru tehnoloģijas, telekomunikāciju signālu nolasīšanai, un kopā ar bioloģiskiem vai ķīmiskiem aģentiem, sprāgstvielām vai citiem ieročiem tie var kaitēt personām, traucēt pakalpojumu sniegšanai un sabojāt infrastruktūru.

Lai gan lielākā daļa UAS, kas izmantotas prettiesiski , iespējams, ietilpst neapzināta (neuzmanīga vai neapdomīga) kategorijā, nevajadzētu izslēgt, ka noziedznieki un teroristi varētu arvien biežāk ļaunprātīgi izmantot UAS, lai mērķētu uz publiskām telpām, personām un kritisko infrastruktūru (KI). Šī tendence jau ir novērota visā pasaulē, kur UAS tika izmantotas teroristu uzbrukumos. The *modi operandi* (*darbības veids)* un UAS incidentu mērķi ir tik dažādi, ka pretpasākumos jāiekļauj gan aktīvi, gan pasīvi elementi.

Lai gan ES noteikumi ir padarījuši UAS drošāku un vienlaikus apgrūtinājuši dažu veidu UAS ļaunprātīgu izmantošanu, straujais inovāciju temps un viegla piekļuve UAS nozīmē, ka incidentu skaits, visticamāk, palielināsies vēl vairāk. Pieaugot šo incidentu biežumam un ietekmei [4], nepieciešamība veikt preventīvus pretpasākumus un sagatavotība ir īpaši svarīga KI īpašniekiem un publisko telpu pārvaldītājiem .

Tirgū ir pieejami daudzi UAS un komponenti, kurus var modificēt konkrētam ļaunprātīgam mērķim. Tādēļ ir nepieciešami pretpasākumi, lai kontrolētu prettiesisku UAS izmantošanu vai ļaunprātīgu izmantošanu.

3 https://www.sesarju.eu/U-space.

4 https://transport.ec.europa.eu/system/files/2022-11/SWD_2022_366_drone_strategy_2.0.pdf

Šīs rokasgrāmatas darbības joma un mērķis

Šis ir pirmais izdevums dokumentam, ko var uzskatīt par dzīvu dokumentu, kas aptver strauji mainīgu jomu. Komisija cieši sekos līdzi attiecīgajiem regulējuma, procedūru un tehnoloģiju jauninājumiem un turpmākajos gados vajadzības gadījumā atjauninās rokasgrāmatu.

1. attēls: Kritiskās infrastruktūras veidu atlase, par ko šajā rokasgrāmatā sniegti ieteikumi

Šajā rokasgrāmatā nav ietverts plašs pārskats par pieejamajām C-UAS metodēm un tehnoloģijām. Tā vietā tā sniedz metodoloģiju un padomus, lai novērtētu C-UAS risinājuma vajadzības un to, kā to izstrādāt un ieviest. Tajā sniegti norādījumi, kā noteikt piemērotāko risinājumu, un piedāvāta pieeja šāda risinājuma ieviešanai un darbībai.

Lai gan starp risinājumiem ir daudz līdzību, ir arī skaidrs, ka "sudraba lodes" C-UAS risinājums nepastāv un, iespējams, neviens risinājums nebūs identisks. Ieteikumi ir pietiekami vispārīgi, lai veidotu stabilu pamatu turpmāku risinājumu izstrādei, kas pašlaik nepastāv.

Darba sākšanas, projektēšanas un uzstādīšanas fāzes tika pārbaudītas un pārbaudītas projektā kā daļa no JRC DRONE projekta koncepcijas pierādījuma, kas ietver dzīvu laboratoriju JRC Geel vietnē. Ieteikumi par uzstādīšanas un ekspluatācijas fāzēm ir balstīti uz vienotiem projekta un risinājuma ieviešanas principiem. Rokasgrāmatas ieteikumi ir C-UAS dzīvās laboratorijas pamats, kas būs atvērta ieinteresētajām personām, lai noteiktu regulējuma vajadzības, organizētu procesus un procedūras un optimizētu C-UAS risinājumus.

Piecu fāzu pieeja uz C-UAS risinājumu

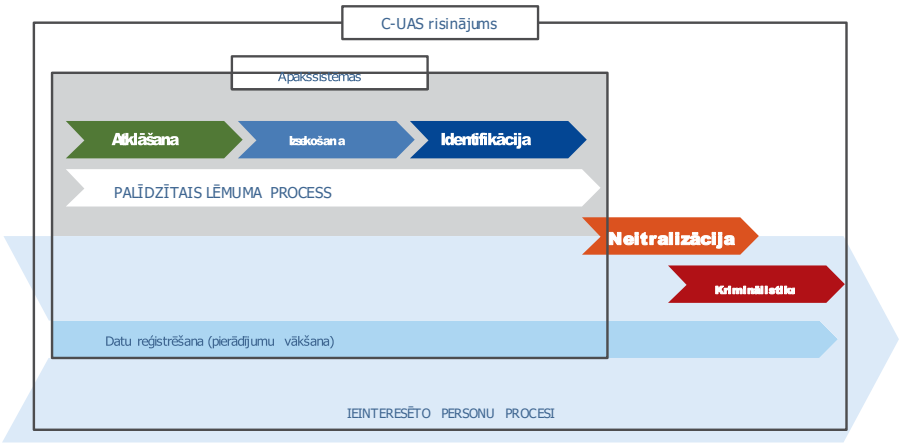
Ir skaidrs, ka C-UAS ir sarežģīts uzdevums un ka nav pieejama neviena "sudraba lodes" ieviešana, kas nozīmē, ka, visticamāk, nebūs standarta ieviešanas vai identisku risinājumu. Katrs risinājums būs jāpielāgo konkrētas vietas un tās vides vajadzībām. Tomēr ir elementi, kas ir kopīgi, un šajā dokumentā aprakstītie ieteikumi gūs labumu visām ieviešanām.

Ja parasti C-UAS aptver noteikšanu, izsekošanu, identifikāciju un zināmu neitralizāciju, šeit aprakstītā metodoloģija iesaka iekļaut arī notikumu reģistrēšanu un, kas ir ļoti svarīgi, visos līmeņos iesaistīt procesus, kas to saista ar ieinteresētajām personām. Notikumu reģistrēšana bieži tiek ignorēta, taču tā ir būtiska kriminālistikai un notikuma analīzei.

Pilnīgam risinājumam jāaptver visa C-UAS vērtību ķēde, skatīt 2. attēlu. Daudzām ieviešanām ir nepieciešama sistēma vai sistēmas, kas jāapvieno ar iesaistīto pušu procesiem un procedūrām. Šī rokasgrāmata palīdz lasītājiem izprast katru aspektu un virza viņus cauri piecām fāzēm, lai panāktu risinājumu. Katrā fāzē ir ieteikumi un elementi, kas jāveic pirms fāzes, fāzes laikā un pēc tās.

Šajā sadaļā ir aprakstīta atšķirība starp C-UAS risinājumu un C-UAS sistēmu un kāpēc ir jāievieš risinājums. 2. attēlā parādīta visa šajā rokasgrāmatā izmantotā vērtību ķēde.

2. attēls: C-UAS risinājumu vērtību ķēde



Nākamajā sadaļā ir aprakstītas ieteicamās risinājuma ieviešanas fāzes. Katra no fāzēm sākas ar to elementu sarakstu, kas ir nepieciešami, lai pabeigtu konkrētās fāzes ieteikumus. Tie ir jāpapildina ar informāciju par vietni. Katras sadaļas beigās ir kopsavilkums par to, kas tika risināts un kas ir nepieciešams, lai pārietu uz nākamo posmu. Šīs fāzes ieteicams veikt secīgā secībā. Ieteicamais process risinājuma iegūšanai ir parādīts 3. attēlā.

3. attēls: Piecas fāzes ess

Lasītājs redzēs, kādi elementi ir jāpabeidz un kura ieinteresētā puse būtu jāiesaista, lai šīs darbības pabeigtu. Šīs darbības būs nepieciešamas vēlāk procesos vai posmos.

Skaidrs, ka nevienu risinājumu nevar uzskatīt par statisku, un tam ir jāattīstās, mainoties vajadzībām, vietnēm, draudiem un ieinteresētajām personām. Tā kā izmaiņas var būt īslaicīgas vai pastāvīgas un notikt jebkurā laikā, risinājumi ir rūpīgi jāuzrauga un katra darbība jāatkārto, kad nepieciešams. Šīs metodoloģijas ievērošana padarīs izmaiņas strukturētākas.

Tālāk ir sniegts piecu posmu pārskats.

1. Sāciet ar C-UAS fāzi. Šajā fāzē ir aprakstītas pirmās ieteicamās darbības, izmeklējot vajadzību pēc C-UAS risinājuma, un tiek noteikti principi, mērķi un prasības pārējai projekta daļai. Daudzos gadījumos iekšējās kompetences ir jāpapildina ar konsultācijām.

   - Uzņēmējdarbības gadījums un nepieciešamība sākt darbu.
   - Mandāts, kas jāievēro.
   - Kur, kas un pret ko aizsargāties.
   - Identificējiet ieinteresētās puses un definējiet lomas un pienākumus.
   - Identificēt juridisko pamatu, lai sāktu īstenošanu.
   - Vietnei specifiskas informācijas vākšana. Nosakiet, kādas pilnvaras ir jāizpilda, kas ir gaisa telpas pārvaldītāji, kartes, plāni, apdrošināšana utt.
   - Budžeta ietvara piešķiršana procesa uzsākšanai.

2. Riska un draudu analīzes fāzē tiek pētīti, analizēti un dokumentēti vietnes UAS riski un draudi, lai izveidotu draudu reaģēšanas plānu. Šis plāns kalpo kā galvenais ieguldījums pretpasākumu atlases procesā.

- Identificējot, pret ko aizsargāties.
- Izpratne par riskiem un izpētīt, kā tos var integrēt pašreizējos riska plānos.
- UAS riska definēšana scenārijos.
- Vietnes kritisko līdzekļu identificēšana, kas ir neaizsargāti pret UAS.
- Vietnes apsekojums.
- Reģionālie faktori. Vai teritorijā notiek aktivitātes KI tuvumā, tuvu robežām, UAS pakalpojumu attīstība?
- No kādiem makro riskiem KI cenšas aizsargāties?
- Riskam un risinājuma mērķim atbilstoša mazināšanas līmeņa izvēle.
- Vietnes apdraudējuma-reaģēšanas plāna izveide.

3. Risinājuma izstrādes fāze saskaņo draudu un reaģēšanas plānu ar tehnoloģiju un ieinteresēto pušu procesu izmantošanu, lai efektīvi novērstu UAS risku. Vietnei specifiskā informācija un vajadzības tiks iekļautas dizainā. Dizains tiks saskaņots ar pārbaudes un verifikācijas procesiem. Tas ietvers risinājumu un tehnoloģiju pārbaudes plānus.

- Apvienojiet vietnes specifiku ar vajadzībām, risku un draudiem.
- Skaidri definējiet visu ieinteresēto pušu lomas un pienākumus.
- Definējiet, kā pārbaudīt risinājumu un apmācīt ieinteresētās personas.
- Pamatpakalpojumu minimuma ieviešana.
- Tehnoloģiju komponentu atlase, kas ļaus veikt nepieciešamos mazināšanas pasākumus.
- Detalizējiet dizainu arhitektūrā.

4. Risinājuma ieviešanas fāze sniedz norādījumus par to, kā ieviešamais risinājums izskatīs dažādus apsvērumus ieviešanas laikā.
Šajā posmā ir aprakstīts, kā izmantot dizainu, un sniegti norādījumi par to, kas palīdzēs ieviest risinājumu sadarbībā ar ieinteresētajām personām.

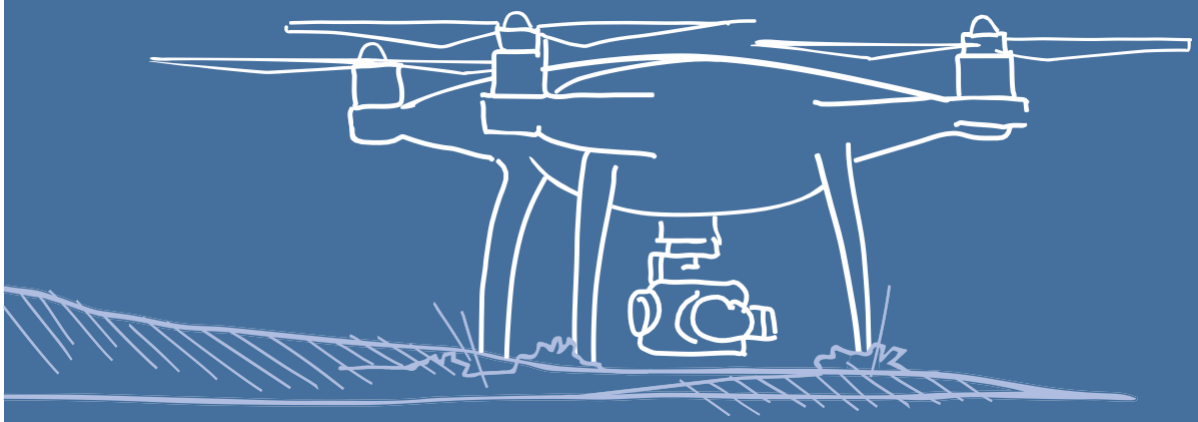
- Risinājuma uzstādīšana.
- Iespiešanās testi.
- Iekārtu kalibrēšana un testēšana.
- Pēc ieviešanas darbības plānu un risinājumu pieņemšanas kritēriju izveide.
- Risinājuma pieņemšanas kritēriji un testēšana.
- Ekspluatācijas rokasgrāmatas un pāreja uz servisa režīmu.

5. Darbības fāze attiecas uz to, kā risinājums tiek uzturēts darboties spējīgs, un tas ilgtermiņā ir saskaņots ar vietnes apdraudējumiem. Risinājumam ir nepieciešama apkope un atjauninājumi tā kalpošanas laikā, un tas var attīstīties atkarībā no izmaiņām, piemēram, jauniem riskiem, vietnes izmaiņām vai īpašiem notikumiem (piemēram, ļoti svarīgas personas (VIP) apmeklējums). Šīs fāzes detaļas ir atkarīgas no risinājuma pretpasākumu konfigurācijas.

- Risinājuma darbība.
- Saziņa un ieinteresēto personu informēšana.
- Risinājuma atjaunināšana.

1

Pirmā fāze / Darba sākšana ar C-UAS



"Darba sākšanas" fāze ir pirmais solis, kas tiek sperts, lai nodrošinātu vietasaizsardzību pret UAS, kas nesadarbojas. Tas ietver C-UAS risinājuma nepieciešamības izpēti un nosaka vietnes principus, mērķus un pirmās prasības C-UAS draudu un risku analīzei, risinājuma izvēles procesam un tā ieviešanai. Pirms C-UAS projekta uzsākšanas ir svarīgi saprast, ka informētība, reglamentējošās jomas un procedūras var palielināt un atbalstīt pasīvos pretpasākumus (atturēšanu) bez lieliem iepriekšējiem ieguldījumiem no pašas vietas.

Nolūks aizsargāt pret UAS ir pats pirmais C-UAS risinājuma izstrādes posms, un tas kalpo par C-UAS iespēju turpmāku izpēti. Šis nolūks var rasties no jebkura avota, piemēram, no konstatēta UAS trafika palielināšanās ap vietu, dalībvalsts izlūkdienestu padoms, jaunu riska objektu uzstādīšana objektā vai normatīvā regulējuma izmaiņas. Šis nolūks ietilpst plašākā organizatoriskā kontekstā, un to ietekmē politiski, ekonomiski, sociāli, tehnoloģiski, vides vai juridiski faktori. Skaidra uzņēmējdarbības izraisītāja identificēšana ir būtiska, lai pamatotu visas ar C-UAS saistītas iniciatīvas. Ierosinātāju piemēri varētu būt incidents ar bezpilota lidaparātu (UAS) citā objektā vai jauni tiesību akti, kas nosaka nepieciešamību pēc C-UAS risinājuma.

1. PIRMĀ FĀZE — SĀKŠANA

Šajā posmā nepieciešamā informācija:

- izpratne par draudiem (augsts līmenis);
- likumdošanas izpratne;
- augsta līmeņa prasības;
- informācija par vietni un vidi.

Šīs fāzes beigās jums ir jābūt šādai informācijai:

- Projekts un skaidri mandātu apraksti.
- Izpratne par to, kas pret ko un kur ir jāaizsargā.
- Tehnoloģiju izmantošanas ierobežojumi skaitītāja risinājumā.
- Noskaidrotas vajadzības pēc C-UAS risinājuma ar noteiktām biznesa vajadzībām un projekta pārvaldību. Tam jāietver skaidra darbības joma, mērķi un rezultāti.
- Vietas informācija un vides informācija, kas varētu ietekmēt C-UAS risinājumu.
- Ieinteresēto pušu analīze (augsts līmenis).
- Izpratne par pamata pakalpojumu minimumu, kas ļauj sagatavot ieviešanu.

Šajā pirmajā fāzē ir ieteicams apkopot augsta līmeņa C-UAS prasības turpmākai pilnveidošanai visā projekta laikā. Šīs prasības ietver:

- vietai specifiskas vajadzības un ierobežojumi, kas jāņem vērā projektā un risinājumā;
- informācija par vidi;
- tehnoloģiju izmantošana (piemēram, atļauja izmantot radaru tehnoloģiju, IKT sistēmas un datus, lai paliktu uz vietas specializētos serveros);
- izlūkdati (piemēram, iestāžu informēšana C-UAS incidenta gadījumā);
- juridiskās un regulējošās robežas;
- jebkuras citas jomas, kas attiecas uz C-UAS risinājumu.

Šajā fāzē ir svarīgi arī uzsākt augsta līmeņa ieinteresēto pušu apzināšanu un uzsākt sarunas ar tām.

DEFINĪCIJA

Pretdarbība pret UAS ir likumīgi un droši atklāt, izsekot, identificēt un mazināt bezpilota gaisa kuģu sistēmu riskus.

C-UAS sistēma ir risinājuma sastāvdaļa, kas paredzēta C-UAS veikšanai.

C-UAS risinājums ir C-UAS sistēmu, ieinteresēto pušu un to darbībā iesaistīto procesu kolekcija.

1.1 PROJEKTS UN SKAIDRS MANDĀTS

Lai projekts būtu veiksmīgs, ir svarīgi, lai būtu skaidra definīcija un pilnvaras sākt C-UAS risinājuma ieviešanu. Ir ļoti ieteicams dokumentēt šo nolūku aizsargāt vietuvai infrastruktūru, un tas atvieglos lēmumu pieņēmēju un ieinteresēto personu dalību.

Projekta plānskalpos kā ceļvedis projekta vadītājam, kā arī ieinteresētajām personām, un tajā būs C-UAS mērķa, darbības jomas, paredzamā laika grafika un budžeta apraksts, lomas un pienākumi, kā arī pieeja ieinteresēto personu komunikācijai.

Projekta plānam ir jāietver:

- Skaidrs mandāts un pamatojums aizsardzības projekta uzsākšanai. Tam vajadzētu nākt no augstākās iespējamās hierarhijas un varas līmeņa.
- C-UAS risinājuma mērķi, apjomu un rezultātu.
- Vietai nepieciešamo seku mazināšanas līmeni (piemēram, vai mērķis ir uzraudzīt, veikt vieglu iejaukšanos vai stingru iejaukšanos).
- Risinājuma atbilstība vietas drošības vajadzībām.
- Stratēģiskie īstermiņa un ilgtermiņa mērķi.
- Ieguldījumu pamatojumu un budžeta ietvaru.
- C-UAS risinājuma juridiskais pamats.
- Pirmās ieinteresētās puses, kuras jāiesaista, un definētas lomas un pienākumi.

Šāds projekta plānsvar būt saskaņots ar pašas vietasprojektu vadības metodoloģiju.

1.2 RISINĀJUMS SISTĒMAS VIETĀ

Ir svarīgi, lai procesa sākumā būtu skaidrs priekšstats par to, kas ir nepieciešams, lai mazinātu visus identificētos riskus. Izšķiroša nozīme ir izpratnei par atšķirību starp C-UAS sistēmu un risinājumu. C-UAS sistēmas lielākoties sastāv no vairākiem tehnoloģiju komponentiem, kas ir apvienoti un saistīti. Parasti tie ietver noteikšanas, izsekošanas un identifikācijas komponentus, noteikta veida operatoru, kas palīdz kategorizēt UAS un draudus, dažus sistēmas reģistrēšanu un dažos gadījumos neitralizāciju, skatiet 2. attēlu.

Lai gan daudzos gadījumos tas var palīdzēt mazināt risku, ieteicams izmantot C-UAS kā pilnīgu risinājumu. Risinājums var ietvert vairākas sistēmas un papildu pakalpojumus un procesus. Lai gan tas sarežģīs ieviešanu, tas noteikti veicinās labāku aizsardzību. Labi ieviests risinājums arī atvieglos attīstību līdztekus izmaiņām (īslaicīgām vai fiksētām) apdraudējuma ainavā.

Papildus C-UAS sistēmas elementiem C-UAS risinājums, skatīt 2. attēlu, ņem vērā arī projekta un ieinteresēto pušu procesus, organizāciju un ārējos faktorus, piemēram, reģionālos noteikumus. Risinājums varētu ietvert arī tādas informācijas neitralizāciju un reģistrēšanu, kas nepieciešama notikumu kriminālistikas analīzei un turpmākiem uzlabojumiem.

Risinājums ir jāintegrē pašreizējos ieinteresēto personu procesos un jāspēj apmainīties ar informāciju starp ieinteresētajām personām.

2. attēlā parādīta C-UAS risinājuma vērtību ķēde, un zemāk esošajā sarakstā ir aprakstīti daži svarīgi elementi, kas ir iekļauti visos risinājumos.

- Atklāšanas tehnoloģijas, izsekošanas un identifikācijas sistēmas. Tie varētu būt no dažādiem piegādātājiem un apvienot izvadi, izmantojot sensoru saplūšanu.
- Atbalstītie lēmumu pieņemšanas procesi un automatizēti procesi ar savstarpēji saistītām sistēmām. Tas palīdzēs operatoriem optimāli izmantot risinājumu.
- Datu reģistrēšana, kas ietver gan notikumus no sistēmām, gan no ieinteresēto pušu procesiem. Visi notikumi ir jāapvieno un jāiekļauj novērojumi, notikumi, par kuriem ziņots citos veidos (tālrunī vai manuāli), U-Space [5] un bezpilota gaisa kuģu sistēmu satiksmes vadības (UTM) notikumi, citas ģeogrāfiskās zonas un kaimiņi, sabiedriskie dienesti, tiesībaizsardzības aģentūras (LEA) utt.
- Ir jāiekļauj daudzi ieinteresēto pušu procesi, un risinājuma daļai jābūt pastāvīgai novērtēšanai.

  Procesos jāiekļauj sekojošais:
  - » Paziņojums iestādēm incidenta gadījumā.
  - » Mijiedarbība un līgumi ar LEA. Tas ietvers to, ko un kam negadījuma gadījumā sazināties, kas ko dara un kad.
  - » Līgumi ar gaisa telpas pakalpojumu sniedzējiem (UTM, U-Space).
  - » Mijiedarbība ar varas iestādēm un kaimiņiem.
  - » Datorizēta nosūtīšana.
  - » Neitralizācijas atļaujas pieprasījums ieinteresētajai personai, kurai ir pilnvaras to izlemt.
  - » Kriminālistikas datu apmaiņa.
  - » Saziņa ar ieinteresētajām personām, kuras ietekmē vai ietekmē risinājums.

5 https://www.sesarju.eu/U-space.

1.3 SAVIETOJAMĪBAS UN KONSTRUKCIJAS PRINCIPI

Jebkurš C-UAS risinājums ir sadarbspējas vingrinājums juridiskā, organizatoriskā, semantiskā un tehniskā līmenī. Ieinteresētajām personām ieteicams izmantot šajā sadaļā aprakstītos projektēšanas principus un katru rokasgrāmatas posmu pārbaudīt, lai tie atbilstu Eiropas sadarbspējas sistēmai [6], skatiet 4. attēlu.

4. attēls: Eiropas sadarbspējas sistēma

Avots: Eiropas sadarbspējas sistēma (pielāgota).

- Juridiskā sadarbspēja ļauj organizācijām, kas darbojas saskaņā ar dažādiem valsts tiesiskajiem regulējumiem, politikām un stratēģijām, sadarboties. Valstu tiesību akti un politika varētu bloķēt sadarbību, tāpēc ir jāpanāk skaidras vienošanās par to, kā risināt dažādu ieinteresēto personu grupu tiesību aktu atšķirības.
- Organizatoriskā savietojamība attiecas uz veidu, kādā valsts pārvaldes iestādes (t.i. valdības aģentūras un organizācijas) saskaņo savus Projektus, pienākumus un cerības, lai sasniegtu kopīgi saskaņotus mērķus. Praksē organizatoriskā sadarbspēja nozīmē projekta un attiecīgās informācijas dokumentēšanu un integrēšanu vai saskaņošanu.
- Semantiskā savietojamība nodrošina, ka tiek saglabāts un saprasts precīzs apmainīto datu un informācijas formāts un nozīme: "nosūtītais ir saprotams". Tas ietver sintaktiskos aspektus, piemēram, terminoloģiju, ko izmanto, lai aprakstītu jēdzienus un aprakstot precīzu informācijas formātu.
- Tehniskā savietojamība attiecas uz lietojumprogrammu un infrastruktūru sistēmu un pakalpojumu saistīšanu. Aspekti ietver saskarnes un pakalpojumu specifikācijas, kā arī datu un metadatu standartus un formātus.

6 https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail.

Ieviešot risinājumu, ieteicams ievērot šos principus visos posmos.

Papildus sadarbspējai visiem risinājumiem jābūt:

- atbilstošs -risinājumam ir jāatbilst KI vai publiskās telpas vajadzībām, kurā tas tiek īstenots, un tam būtu jāmazina identificētais risks;
- efektīvs -tādējādi risinājums mazinās riskus un incidentus, kad tie notiks;
- efektīva -efektīvi mazināt riskus un incidentus (šim nolūkam risinājumam ir jābūt labi ieviestam un pareizi jādarbojas);
- saskaņots -saskaņoti risinājumi ir saskaņoti ar pasākumiem, kas veikti līdzīgās KI vai publiskajās telpās, un ieviešanu apkārtnē;
- ietekmīgs -risinājumu ietekme būtu jāmēra, pamatojoties uz to, kā tie mazina vai samazina incidentu sekas;
- ilgtspējīgs -ilgtspējīgi risinājumi attīstīsies līdz ar vides izmaiņām, draudiem un KI.

Projektu vadības metodoloģijas izmantošana [7] ļaus projektu vadītājiem sniegt risinājumus un priekšrocības savām organizācijām, efektīvi pārvaldot visu savu projektu dzīves ciklu. Tas atvieglos vajadzību standartizāciju, strukturēšanu un organizēšanu un risinājuma ieviešanu.

Izstrādājot risinājumu, ļoti ieteicams izmantot atvērtos sakaru standartus un protokolus. Piegādātājam var būt patentēts protokols, kas tiek izmantots un darbojas labi, taču, pieslēdzoties citām sistēmām un integrējot sistēmu lielākā risinājumā, tas bieži vien kļūst apgrūtinoši un sarežģīti, jo nepieciešami papildu resursi un laiks.

1.4 KO AIZSARGĀT PRET KURU UN KUR?

Būtisks solis risinājuma definēšanas procesa sākumā ir definēt un aprakstīt pirmās C-UAS risinājuma augstā līmeņa vajadzības. Šajā posmā, iespējams, nav skaidras izpratnes, definīcijas vai apraksta, no kā aizsargāties. Būtiski, ka pirms risinājuma projektēšanas un tehnoloģiju sistēmu izvēles šīs definīcijas ir aprakstītas. Daudzos gadījumos var būt ļoti grūti iegūt skaidru atbildi, un, lai precizētu pieeju, ir nepieciešami riska novērtējumi. Uzsākot UAS aizsardzības izpēti, ir svarīgi jau zināt, ko aizsargāt, juridisko izklāstu, KI biznesa vajadzības, integrācijas līmeni ar gaisa telpas pārvaldību, valsts un reģionālās robežas, kas ko drīkst darīt un apsvērumus par integrāciju ar ieinteresētajām pusēm.

Jo labāk ir izstrādāts apraksts, jo vieglāk būs izdarīt izvēli vēlākā procesā. Visi parametri ir cieši saistīti, un tie ir jāreģistrē, kā rezultātā tiek izveidots augsta līmeņa apraksts, kas nepieciešams nākamajām riska novērtējuma un risinājuma izstrādes fāzēm.

7 Skatīt PM² projektu vadības metodoloģiju.

No kā aizsargāties?

Efektīvi pretpasākumi ir atkarīgi no mērķa veida (piemēram, cilvēki, VIP personas, dati, infrastruktūra), tā ievainojamības un vainīgā nolūka. Šajā fāzē ir ļoti svarīgi arī dokumentēt UAS veidu, ko varētu izmantot uzbrukumā.

Iespējamās draudu kategorijas, kas pēdējos gados ir identificētas civilajā kontekstā, ir šādas.

- **Bīstamo kravu pārvietošana**. UAS kravnesība pēdējos gados ir palielinājusies, pateicoties efektīvākiem dzinējiem un akumulatoriem, kas nozīmē, ka tos var izmantot improvizētu sprāgstvielu, granātu vai ķīmisku, bioloģisku, radioloģisku un kodolvielu pārvietošanai nodrošinātā perimetrā. Mūsdienu UAS spēj pārvadāt ievērojamas kravas lielos attālumos, ar lielāku precizitāti, izmantojot kameras un ierīces. Kravu var novietot interesējošā vietā, piemēram, uz ēkas jumta, to var atbrīvot ar speciāli izstrādātu mehānismu vai iedarbināt, atrodoties gaisā, vai pat apzināti vadīt pret atklātu objektu kamikadzes uzbrukumā. Potenciālie mērķi ietver konkrētas personas, KI, publiskās telpas un informācijas tehnoloģiju sistēmas un pakalpojumus (piemēram, enerģijas ražotne, finanšu institūcija, valsts pārvalde, aizsardzības infrastruktūra).

- **Kontrabanda / piegāde.** UAS izmantošana aprīkojuma piegādei noteiktās vietās jau ir novērota vairākos gadījumos visā Eiropā, jo tās var viegli apiet tradicionālos kontroles punktus un drošās zonas. Piegādāto aprīkojumu (piem., šaujamieroci) var izmantot agresors, kurš jau ir iekļuvis drošā zonā, izmantojot parasto kontroles procedūru. Piemēram, dažādas kravas (piemēram, mobilie tālruņi, narkotikas, nelegālas preces, ieroči) jau ir piegādātas cietumos vai kontrabandas ceļā pāri starptautiskajām robežām.

- **Propaganda.** UAS var izmantot arī protestētāji un teroristu grupas, lai fiksētu savas darbības, izplatītu skrejlapas vai citus materiālus publiskās vietās, lai pastiprinātu propagandas centienus. Filmētos materiālus var pārraidīt tiešsaistē, lai piesaistītu līdzjūtējus un mudinātu vervēt jaunus teroristus vai protestētājus, jo tas rada priekšstatu par veiksmīgu organizāciju ar apņēmīgiem dalībniekiem.

- **Traucējumi un iejaukšanās.** Pat UAS klātbūtne var būt pietiekama, lai traucētu aktīva normālai darbībai drošības problēmu dēļ, kas rodas no šādas darbības (piemēram, iejaukšanās civilajā aviācijā, lidojums virs auditorijas mūzikas priekšnesuma laikā). Var tikt traucēti arī dažāda veida masu pasākumi pilsētu teritorijās, izraisot apmeklētāju panikas reakcijas, kas var izraisīt ievainojumus/ upurus vai radīt labvēlīgus apstākļus sekundāram uzbrukumam (piemēram, novirzīt cilvēkus noteiktās vietās).

- **Izlūkošana, novērošana un izlūkošana.** UAS var izmantot arī informācijas vākšanai un darbību novērošanai, galvenokārt izmantojot kameras, tostarp kameras ar nakts redzamības vai siltuma sensoriem. Tas ļauj vainīgajiem no droša attāluma ievākt informāciju par potenciālā mērķa ievainojamību un izmantot tās uzbrukuma laikā vai pat sniegt reāllaika informāciju uzbrukuma laikā. Pēdējā laikā ir izstrādāti arī jaudīgi mikrofoni, kas ļauj noklausīties privātas/ konfidenciālas sarunas. Turklāt privātus attēlus, ko uzņēmusi UAS, kas pārkāpj personu privātumu, var izmantot noziedzīgiem nolūkiem, piemēram, krāpšanai vai šantāžai.

- **Iestrēgšana.** UAS, kas uzstādīts ar atbilstošu elektronisko aprīkojumu, var izmantot kā vietējo traucētāju, lai traucētu perimetra drošības sistēmas, GPS sistēmas vai mobilā tālruņa signālus. Šī taktika var radīt papildu ievainojamības, kuras var izmantot vainīgais vai pat būtiski ietekmēt aktīva (piemēram, lidostas) darbību.

- **Kiberuzbrukumi.** UAS var radīt kiberdrošības draudus, mērķējot uz vietējiem bezvadu tīkliem un pārtraucot sakarus, piegādājot ļaunprātīgu programmatūru, nolaupot un/ vai manipulējot ar sensitīviem datiem. To var izdarīt ar īpašu aprīkojumu, kas iegūst piekļuvi bezvadu sistēmai. Turklāt UAS var būt kiberuzbrukuma (t.i. UAS uzlaušanas) mērķis, jo vainīgie var iegūt kontroli un mainīt tā maršrutu, piekļūt tās datiem vai tos iznīcināt (piemēram, pakalpojuma atteikums).

Palielinoties UAS komerciālajai, profesionālajai un izklaidējošajai izmantošanai un tā kā daudzas ar UAS izmantošanu saistītās tehnoloģijas joprojām attīstās, draudu kategorijas, kas apkopotas 5. attēlā, noteikti attīstīsies nākotnē. Uzlaboti akumulatori un dzinēji nodrošinās ilgāku lidojuma laiku ar palielinātu kravnesību, savukārt ātrāki mobilie tīkli (5G) nodrošinās tālsatiksmes saziņu, un mākslīgā intelekta lietojumprogrammas var izmantot, lai uzlabotu sadarbību starp UAS, lai tie varētu veidot barus.

No kā aizsargāties?

Parasti incidentu dalībnieki tiek grupēti šādās kategorijās: saticīgi/uzmanīgi, bezjēdzīgi, neuzmanīgi un noziedznieki/teroristi. Negadījuma laikā var nebūt iespējams noteikt, kurš "C" tas ir, un klasifikācija, iespējams, būs iespējama tikai pēc incidenta analīzes laikā. Neatkarīgi no iemesla, ja UAS tiek atklāts vietā, kur tai nevajadzētu atrasties, tai ir attiecīgi jāvēršas. Pareizu klasifikāciju var izmantot, lai atjauninātu draudu attēlu turpmākiem atjauninājumiem un risinājuma attīstībai.

Lai klasificētu pilota nolūku vai motivāciju, draudu novērtējumā var izmantot atbilstošo, neapdomīgo, neuzmanīgo un noziedzīgo klasifikāciju, sk. 6. attēlu.

- **Atbilstošs/uzmanīgs** - pilots ievēro noteikumus un noteikumus, bet var ciest no tehniskiem vai ekspluatācijas apstākļiem, kuru dēļ bezpilota gaisa kuģis var iekļūt aizliegtajā zonā un kļūt par neatļautu bezpilota gaisa kuģi (piemēram, kontroles zaudēšanas, vēja vai tehniskas darbības traucējumu dēļ).

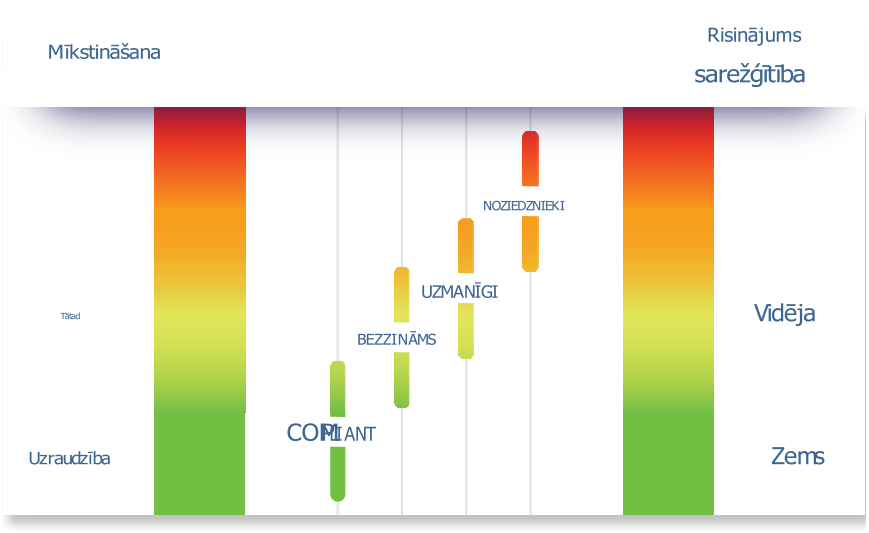
- **Bezjēdzīgs** - personas nezina vai nesaprot piemērojamos noteikumus un ierobežojumus. Rezultātā tie darbojas zonā, kas ir ierobežota. Parasti viņiem nav nodoma nodarīt ļaunumu.

- **Neuzmanīgs** - personas zina piemērojamos noteikumus un ierobežojumus, bet pārkāpj tos vainas vai nolaidības dēļ. Rezultātā viņi lido ar savi em bezpilota lidaparātiem aizliegtajās zonās.

- **Noziedznieks/terorists** - personas, kuras neatkarīgi no tā, vai zina piemērojamos noteikumus un ierobežojumus, aktīvi cenšas ļaunprātīgi izmantot UAS, lai traucētu drošību un drošību KI zonās vai publiskajās telpās.

Ir skaidrs, ka nepieciešamais risinājums ir pilnīgi atšķirīgs atkarībā no tā, pret ko un pret ko jūs aizsargājat. Var pieņemt, ka noziedznieki veiks izsmalcinātus un apzinātus uzbrukumus. Tie varētu izmantot modificētus UAS un, piemēram, modificētus UAS sakaru signālus, lai tie varētu izvairīties no atklāšanas, izsekošanas vai identifikācijas.

Aizsargājoties pret noziedzniekiem, risinājumam bieži būs nepieciešama "stingra" mazināšana, un tāpēc tie ir vissarežģītākie un izaicinošākie apdraudējumi, no kuriem aizsargāties, skatiet 7. attēlu.



Bieži vien ir jānošķir sadarbīgās un nesadarbīgās UAS.

- UAS pilots kurš sadarbojas ievēros likumdošanas prasības un viņam būs nepieciešamās atļaujas lidot gaisa telpā. Tas ir salīdzināms ar iepriekš minēto atbilstošo personu. Tomēr ārēju faktoru dēļ lidojums tomēr var pārvērsties par apdraudējumu, kas ir jāmazina.

- UAS pilots, kas nesadarbojas aptver bezjēdzīgos, neuzmanīgos un noziedzniekus. Šis lietotājs lidos tur, kur viņam patīk, viņam var būt ļaunprātīgi nodomi vai tas var radīt draudus nejaušības vai nepareizas darbības dēļ.

Neatkarīgi no izmantotās kategorizācijas, protams, ir svarīgi atcerēties, ka īstā kategorija var nebūt zināma.

Kur aizsargāties?

Izlemjot, ko aizsargāt, ieteicams sadalīt vietnes elementus. Vai dažas daļas ir svarīgākas un tām nepieciešama lielāka aizsardzība? Kur atrodas visvairāk importētie elementi? Vai tie atrodas tālu vai tuvu vietas robežām vai robežām, kas varētu būt svarīgas? Vides faktori, piemēram, lauku vai pilsētu apkārtne, ir jādokumentē.

PADOMS

Ja bezpilota gaisa kuģis atrodas gaisa telpā, kur tam nevajadzētu atrasties, pārkāpjot noteikumus un noteikumus, tas var radīt risku, un tas būtu jāmazina ar pieņemtajiem pasākumiem.

1.5 IEINTERESĒTO PUŠU VADĪBA

C-UAS risinājuma ieviešanas procesa sākumposmā jāiesaista ieinteresētās personas. Kad vienošanās ar iekšējām projketa vienībām ir apstiprinātas un lēmums par risinājuma izstrādes uzsākšanu ir pieņemts, ir laiks paskatīties uz iekšējām un ārējām ieinteresētajām pusēm. Kā redzams 2. attēlā, ieinteresēto pušu iesaistīšanas process ir ļoti svarīgs un aptver visas sistēmas. Jebkurā projektu vadības metodoloģijā būs iekļauts kāds ieinteresēto pušu elements.
Ieinteresēto pušu identificēšana un analīze var būt laikietilpīga un visaptveroša. Tas regulāri jāpārskata, lai nodrošinātu, ka tas ir atjaunināts un pilnīgs. Sāciet ar zināmajām ieinteresētajām pusēm un balstieties uz tām.

Ieinteresēto pušu iesaistīšana C-UAS risinājuma izstrādē ir būtiska. Dažas no priekšrocībām ir šādas.

- Projekta panākumu nodrošināšana. Ieinteresētās puse var sniegt vērtīgu ieguldījumu visā projekta dzīves ciklā, sākot no sākotnējiem plānošanas posmiem līdz īstenošanai un novērtēšanai. Viņu iesaistīšanās nodrošina, ka projekts atbilst viņu cerībām, vajadzībām un mērķiem, kas palielina veiksmes iespējamību.

- Risku identificēšana. Ieinteresētās puses var identificēt iespējamos riskus, kas var ietekmēt projekta panākumus. Tas ļauj projektu vadītājiem mazināt vai izvairīties no šiem riskiem, pirms tie kļūst par būtiskām problēmām.

- Atbalsta gūšana. Iesaistot projektā ieinteresētās puses, jūs varat iegūt viņu atbalstu un dalību, kas var palīdzēt pārvarēt pretestību pārmaiņām vai jebkādus iespējamos šķēršļus, kas var rasties projekta laikā.
- Pārvaldot cerības. Ieinteresēto pušu iesaistīšana var palīdzēt pārvaldīt viņu cerības un novērst pārpratumus. Tas palīdz nodrošināt, ka ikvienam iesaistītajam ir skaidra izpratne par to, kas no viņiem tiek gaidīts un ko projekts vēlas sasniegt.
- Komunikācijas uzlabošana. Ieinteresēto pušu iesaistīšana palīdz izveidot skaidru saziņas līniju starp projektu vadītājiem, ieinteresētajām pusēm un komandas locekļiem. Tas veicina caurskatāmību, samazina konfliktus un ļauj labāk izprast projekta gaitu un rezultātus.

Iesaistīto ieinteresēto pušu dažādības dēļ ir ieteicams un svarīgi pirmo ieinteresēto pušu karti izveidot pēc iespējas agrāk.

Kartējumā vismaz jānorāda dalībnieki, kurus ietekmējis risinājums, un tie, kas ir iesaistīti risinājuma darbībā vai informācijas apmaiņā ar to. Sākumā šīs ārējās ieinteresētās puses var aprobežoties ar brīdinājuma zonu un UAS ģeogrāfiskās zonas perimetru.

Tā kā C-UAS risinājumi apkārtnē un apkārtnē būs nozīmīgs informācijas avots un, lai izvairītos no tehnoloģiju traucējumiem, būtu jāiekļauj arī ieinteresētās puses no tiem.

LEA (vietējās, reģionālās un federālās) ir svarīgas ieinteresētās puses notikumu uzraudzībā un neitralizēšanā. Pienākumi dažādiem LEA līmeņiem būs atšķirīgi, un ir svarīgi noteikt pienākumus.

Tālāk ir sniegts to prioritāro ieinteresēto pušu saraksts, ar kurām jāapspriežas jebkurā projektā:

- risinājuma galalietotāji;
- līdzīgas KI vietnes;
- iestādes un regulatori vietnei, kas jums jāaizsargā;
- iestādes, kurām ir riska un draudu novērtēšanas kompetence;
- risinājuma infrastruktūras un atrašanās vietas regulējošās institūcijas;
- aizsargājamās vietas apsaimniekošana;
- drošība un drošums;
- institūcijas, kas regulē aizsargājamo vietu;
- LEA (vietējā, reģionālā un federālā);
- risku mazināšanā iesaistītās institūcijas (kurām ir atļauja to darīt);
- izlūkošanas un drošības aģentūras;
- gaisa telpas pārvaldītāji un UTM/U-Space ieinteresētās personas ap aizsargājamo vietu;
- kaimiņi ap aizsargājamo objektu;
- regulējošās institūcijas, kas ļauj izmantot tehnoloģijas (piemēram, radiolokācijas frekvences un iespējama traucēšana);
- sistēmu integratori.

Protams, ieinteresētās puses atšķiras atkarībā no konkrētās īstenošanas. Daudzas ieinteresētās puses un dalībnieki ir saistīti ar izpratni par draudiem un atbilstošiem riskiem. Tāpēc laba ieinteresēto pušu pārvaldība ir svarīga visos risinājuma izstrādes un ieviešanas procesa posmos.

8. attēlā ir RASCI (atbildīgs, atbildīgs, atbalstošs, konsultēts, informēts) tabulas piemērs [8]ko varētu izmantot, lai kartētu ieinteresēto pušu iesaisti. Šāda tabula būtu jāpapildina ar īpašām ieinteresētajām pusēm, kas identificētas un saistītas ar aizsargājamo vietu. Fāze seko C-UAS projektēšanas procesa ceļvedim, kā parādīts 14. attēlā.

PADOMS

Ir jābūt skaidram, ka iesaistītās ieinteresētās pusess atšķiras atkarībā no risinājuma. Jo augstāka ir aizsardzība, jo sarežģītāka ir ieinteresēto pušu pārvaldība.

Projektēšanas fāzē tiks sīkāk izstrādāta ieinteresēto personu iesaiste.

8. attēls: RASCI matricas piemērs ar C-UAS risinājuma izstrādes procesā iesaistītajām ieinteresētajām pusēm (jāpapildina ar īpašām vajadzībām)

Ieinteresētā persona kategorijā	Ieinteresētās personas	Pirmā fāze Darba sākšana ar C-UAS	Otrā fāze Identifikācija UAS riskus pievienot esošajam riska novērtējums	Trešā fāze C-UAS risinājums dizains	Ceturtā fāze Risinājums īstenošana	Piektā fāze Risinājums īstenošana
Vietne	CI uzņēmuma īpašnieks	A	A	A	A	A
	Vietējā apsardze	R	R	R	R	R
	Vietējā sabiedrība un kaimiņiem	es	Es, C	Es, C	es	es
	Līdzīgas CI vietnes	C	S	C	S	
	Organizācijas regulators	S	C	C	es	S
Iestādes	Likuma izpilde	C	C	es	es	S
	Varas iestādes atļāva izmantot mazināšanas līdzekļus	C	C	C	R	R
	Tehnoloģiju izmantošanu regulējošās iestādes	C	es	C	es	es
valdība entītijām	Varas iestādes ar risku un draudu novērtējums kompetences	C	C	es	es	C
	Regulējošās iestādes	C	C	S	C	es
Privāts entītijām	Telekomunikācijas operatoriem	C	C		S	
	C-UAS risinājumu piegādātāji	S	C	C	C	C
Gaisa telpa	UTM pakalpojumi	C	C	C	R	R
	U-Space pakalpojumu sniedzējs	C	Es, C	es	C	es

R = atbildīgs | A = atbildīgs | S = atbalsta | C = konsultēts | Es = informēts

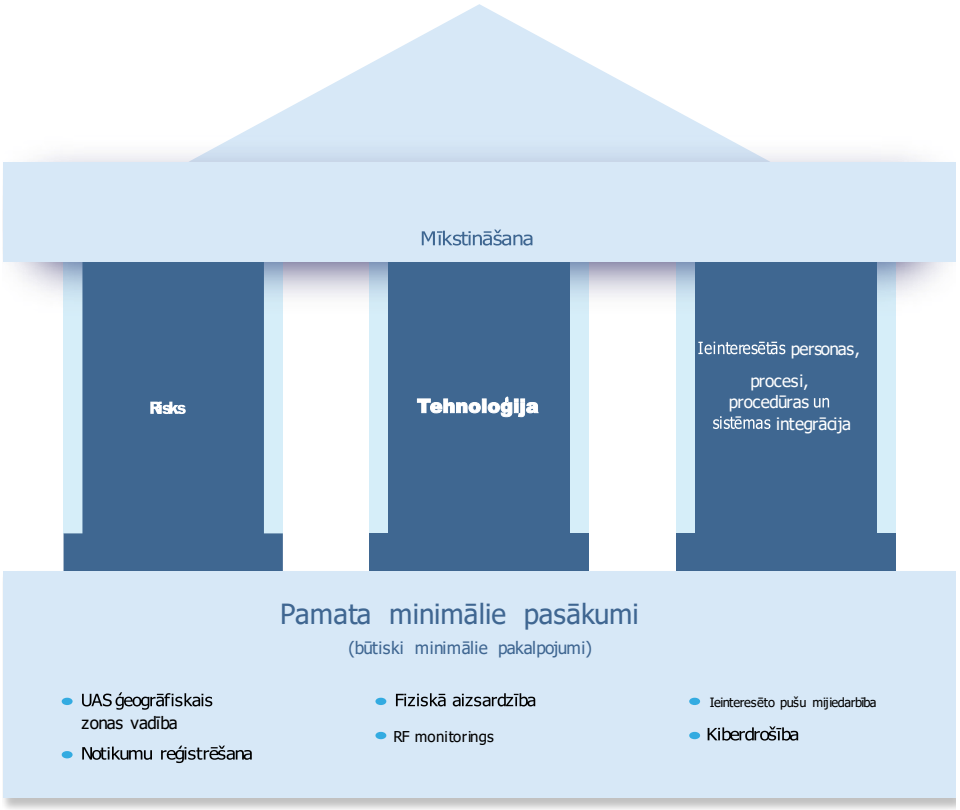
8 Skatīt PM² projektu vadības metodoloģiju

1.6 MINIMĀLIE PAMATPASĀKUMI

Pamatpasākumi ir būtiski un kopīgi visiem risinājumiem, un tie ir jāņem vērā un jāiekļauj lielākajā daļā risinājumu. Šo pasākumu īstenošana ļaus risinājumam attīstīties līdz ar riska līmeņa izmaiņām, kad tiek atjauninātas vai mainītas tehnoloģijas, mainoties procesiem un sagatavotos datu apmaiņai ar ieinteresētajām pusēm.

Tie ir pakalpojumi, kas vienmēr ir nepieciešami un ir jāievieš agrīnā stadijā. Plašāku informāciju par šo pakalpojumu izstrādi skatiet 3.1. sadaļā.

9. attēls: Pamata minimālie pasākumi, kas atbalsta citus C-UAS risinājuma pīlārus



Pamata minimālie pasākumi ir šādi.

- **UAS ģeogrāfiskās zonas pārvaldība** attiecas uz kompetentās iestādes noteikto gaisa telpas pārvaldību, kas atvieglo, ierobežo vai izslēdz UAS darbību, lai novērstu riskus, kas saistīti ar drošību, privātumu, personas datu aizsardzību, drošību vai vidi, kas izriet no UAS darbības [9]. Tas ietver atļaujas darboties UAS, izmantot C-UAS tehnoloģijas un pārbaudīt UAS risinājumu. Izmeklēšana par gaisa telpas pārvaldības rīku izmantošanu, piemēram, UTM izmantošanu un saiknēm ar U-Space pakalpojumiem, jāsāk pēc iespējas ātrāk, jo ir svarīgi integrēt rīkus citos risinājumos, kas tiek ieviesti ap aizsargājamo teritoriju. Tas ietver arī ieinteresēto pušu pārvaldību zonās ap vietu.

9 Komisijas Īstenošanas regula (ES) 2019/947 (2019. gada 24. maijs) par bezpilota gaisa kuģu ekspluatācijas noteikumiem un procedūrām, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0947 .

- **Notikumu reģistrēšanas** mērķis ir izprast, kas notiek jūsu gaisa telpā, reģistrējot visas UAS lietošanas darbības un novērojumus aizsargājamajā vietā un ap to. Reģistrēšanai jāaptver visi datu avoti un novērošanas pasākumi. Reģistrēšanai jābūt pēc iespējas pilnīgākai, lai to varētu izmantot turpmākai risku analīzei un iespējamai kriminālistikai.

- **Fiziskā aizsardzība** ir svarīgs elements, ar ko jāsāk agrīnā stadijā, ņemot vērā riskus, kas tiek radīti ēkām un fiziskajai infrastruktūrai, un to, vai kādām struktūrām ir nepieciešami uzlabojumi vai izmaiņas. Šīs iniciatīvas ir atkarīgas no tā, kāda veida UAS ir jācīnās. Vēlākajos posmos tas ir atkārtoti jāizvērtē, kad riski ir noskaidroti. Plašāku informāciju skatiet JRC rokasgrāmatā par fizisko aizsardzību pret UAS [10].

- **RF monitorings** UAS ir minimālā noteikšana, ar kuru jāsāk visas aizsargātās gaisa telpas. Mērķis ir atklāt pēc iespējas vairāk UAS, taču ir arī skaidrs, ka nav iespējams tos visus atklāt. Šī metode nosaka un nolasa UAS izstaroto komunikāciju un saziņu starp UAS un tās bāzes staciju. Attālinātā ID UAS emitē ietver svarīgus parametrus, kurus var izmantot gaisa telpas pārvaldībai. Pārtverot sakarus starp zemes staciju/pilotu un UAS, tiek pievienota papildu informācija. Šie avoti papildina viens otru un kopā ar atrašanās vietas noteikšanu sniedz ļoti labu pamata gaisa telpas pārskatu. Jāatzīmē, ka tas neatklās tumšās UAS [11], kas ir ieprogrammēti lidošanai bez saziņas ar bāzes vadības staciju. Tas arī neatklās UAS, kas ir modificētas, lai neizstarotu šos signālus vai izmantotu nestandarta frekvences. Lai nodrošinātu maksimālu pārklājumu, ieteicams uzraudzīt frekvences un diapazonu, kas atbilst tiem, ko parasti izmanto UAS, un izvairīties no pārdevēju sistēmām, kas nosaka tikai viņu UAS.

- **Ieinteresēto pušu mijiedarbība** ir viens no galvenajiem risinājuma procesiem, tomēr tas bieži tiek atstāts novārtā un novērtēts par zemu. Visas sistēmas var uzstādīt un darboties atbilstoši specifikācijām, taču bez ieinteresēto pušu iesaistīšanas un integrācijas, kas vajadzīgas, lai ierobežotu apdraudējumu pieejamā laikā, šīs sistēmas var būt bezjēdzīgas. Kā redzams 2. attēlā, procesi, kuros iesaistītas ieinteresētās puses, attiecas uz visām sistēmām un vērtību ķēdes elementiem.

- **Kiberdrošība ir** svarīgs jautājums jebkuram risinājumam, kurā IKT sistēmas ir savienotas ar internetu vai kurā notiek informācijas apmaiņa ar citām sistēmām. C-UAS risinājumi jāizstrādā, izmantojot pieejamos kiberaizsardzības pasākumus. Visiem dizaina elementiem jāspēj darboties bez interneta savienojuma. Ja risks tiek identificēts kā augsts, ja iespējams, ir jābūt liekām sistēmām un sensoriem.

3. SĀKŠANAS POSMA KOPSAVILKUMS

Šīs fāzes beigās jums vajadzētu labāk izprast:

- Biznesa gadījums un skaidri mandātu apraksti.
- Kas ir jāaizsargā pret ko un kur.
- Tehnoloģiju izmantošanas ierobežojumi skaitītāja risinājumā.
- C-UAS risinājuma vajadzības ar noteiktām biznesa vajadzībām un projekta pārvaldību. Tam jāietver skaidra darbības joma, mērķi un rezultāti.
- Vietnes informācija un vides informācija, kas varētu ietekmēt C-UAS risinājumu.
- Ieinteresēto pušu analīze (augsts līmenis).
- Pamatpakalpojumu minimums, kas ļauj sagatavot ieviešanu

10 Aizsardzība pret bezpilota gaisa kuģu sistēmām — Rokasgrāmata par bezpilota gaisa sistēmu riska novērtēšanu un ēku un vietu fiziskās sacietēšanas principiem

11 Tumšie UAS jeb neredzamie UAS ir bezpilota lidaparāti automātiskā lidojuma režīmā, nepārraidot RF signālus gan no tālvadības pults, gan drona.

Otrā fāze / Risks un draudi analīze

Šajā fāzē tiek analizēti aizsargājamās vietnes UAS draudi. Rokasgrāmatā sniegtā pieeja, lai novērtētu riskus, kas saistīti ar UAS izraisītiem uzbrukumiem, ir balstīta uz Starptautiskās standartizācijas organizācijas (ISO) 31000:2018 [12] standarta vispārīgā riska novērtējuma definīcija: "Riska novērtējums ir vispārējs riska identificēšanas, riska analīzes un riska novērtēšanas process". Šāda apraksta mērķis ir riska procesā iekļaut gan dabiskus, gan cilvēka izraisītus apdraudējumus, pat ja pastāv lielas problēmas, novērtējot retu notikumu iespējamību un kvantitatīvi nosakot sekas cilvēka/sociālajā jomā. Ieteicams novērtēt UAS riskus, izmantojot vietnē jau izmantoto riska novērtēšanas metodoloģiju, un atjaunināt risku sarakstu ar identificētajiem UAS riskiem. Jau esošās metodoloģijas izmantošana samazinās dubultošanos un novērsīs divu dažādu riska novērtēšanas metožu nesaderību. Ja ir jāizveido jauns riska novērtēšanas process, KPC riska novērtējums attiecībā uz KI [13] ir labs ceļvedis par to, kā piemērot KPC izstrādāto drošības pieeju [14]. Tāpēc riska novērtējums otrajā posmā ir kopsavilkums no JRC rokasgrāmatas par fizisko aizsardzību pret UAS.

Visos gadījumos riska novērtējumiem būtu jāpalīdz ieinteresētajām personām izprast konkrētajai vietai raksturīgos UAS riskus, lai tās varētu izstrādāt C-UAS risinājumu, kas mazina identificētos riskus.

4. OTRĀ FĀZE – RISKS UN DRAUDI

Tālāk ir norādīti priekšmeti, kas jāsavāc pirms šī posma sākšanas.

- vietas risku reģistrs (no iepriekšējiem un citiem saistītiem riska novērtējumiem);
- likumdošanas izpratne gan vietējā, gan ES[15] [16] noteikumi un noteikumi, kas attiecas uz KI vai publisko telpu, kas jums jāaizsargā;
- augsta līmeņa prasības, kā noteikts pirmajā fāzē "darba sākšana";
- informācija par vietni un vidi.

Šīs fāzes beigās jums vajadzētu būt:

- draudu identificēšana
- vietas apsekošana
- riska un draudu analīze
- draudu un reaģēšanas plāns.

Analizētā UAS ļaunprātīga izmantošana ir viens no līdzekļiem, ko var izmantot vardarbības veicējs, kura mērķis ir indivīds, publiska telpa vai infrastruktūra. Var atšķirt dažādas uzbrukuma taktikas, kas izmanto UAS iespējas. Lai atvieglotu izvērtēšanas procesu, tiek piedāvāta scenāriju izstrāde atkarībā no pārbaudītās KI ievainojamības. 10. attēlā parādīts riska novērtēšanas process.

---

12 Starptautiskā standartizācijas organizācija, ISO 31000:2018, Riska pārvaldība – vadlīnijas, 2018. gads.

13 JRC riska novērtējums kritiskajai infrastruktūrai, https://joint-research-centre.ec.europa.eu/science-activities-z/critical-infrastructure-protection_en.

14 https://home-affairs.ec.europa.eu/news/security-design-protection-public-spaces-terroristattacks-2022-12-14_en.

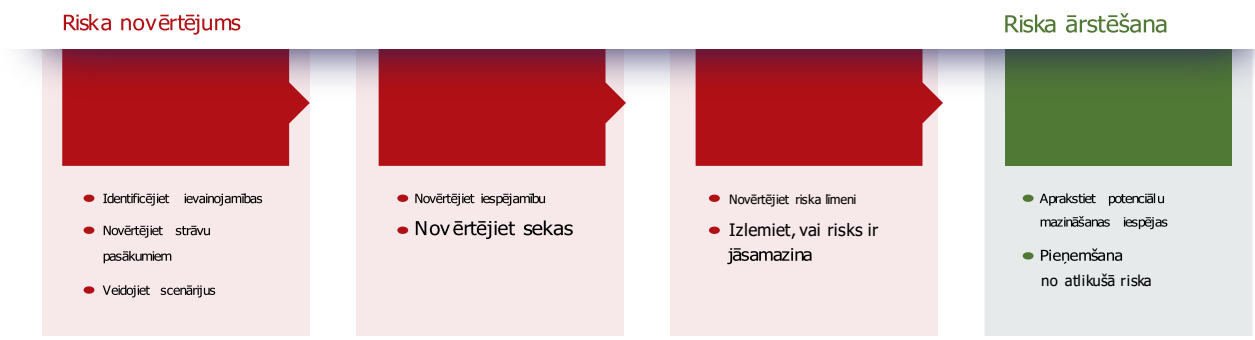
15 Komisijas Deleģētā regula (ES) 2019/945 (2019. gada 12. marts) par bezpilota gaisa kuģu sistēmām un trešo valstu bezpilota gaisa kuģu sistēmu operatoriem, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0945 ;

16 Komisijas Īstenošanas regula (ES) 2019/947 (2019. gada 24. maijs) par bezpilota gaisa kuģu ekspluatācijas noteikumiem un procedūrām, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0947 .

- Draudu identifikācijas process ir potenciālo uzbrukuma līdzekļu un metožu apzināšana, tai skaitā ievainojamību identificēšana pārbaudītajā aktīvā pret aplūkoto UAS uzbrukuma taktiku, pašreizējo (ja tādi ir) aizsardzības pasākumu izvērtēšana un scenāriju izstrāde.
- Riska analīze novērtē katra apdraudējuma iespējamību un ietekmi, kā arī identificē visas ievainojamības vai vājās vietas, kuras varētu izmantot. Riska analīzi var veikt, izmantojot dažādas metodes, tostarp prāta vētru, scenāriju analīzi vai matemātiskos modeļus. Riska analīzes mērķis ir sniegt visaptverošu izpratni par esošajiem riskiem un identificēt nozīmīgākos riskus, kas jārisina.

- Riska novērtējums katram apdraudējumam piešķir riska punktu vai vērtējumu, pamatojoties uz tā iespējamību un iespējamo ietekmi. Riska novērtēšanas mērķis ir noteikt risku prioritāti un noteikt, kuriem no tiem nepieciešama tūlītēja uzmanība. Riski, kuriem ir liela iespējamība un liela ietekme, parasti tiek uzskatīti par viskritiskākajiem, savukārt riskus ar zemu iespējamību un zemu ietekmi var uzskatīt par mazāk svarīgiem.

- Riska mazināšana identificē un ievieš atbilstošus riska kontroles pasākumus, piemēram, drošības protokolu ieviešanu, katastrofu seku novēršanas plānu uzlabošanu vai apdrošināšanas iegādi. Riska mazināšanas mērķis ir samazināt iespējamo apdraudējumu iespējamību un ietekmi, kā arī līdz minimumam samazināt kopējo risku organizācijai. Izvēlētie īpašie riska mazināšanas pasākumi būs atkarīgi no saistīto risku veida, pieejamajiem resursiem un organizācijas riska tolerances.



Riska novērtējuma rezultāts var būtiski atšķirties atkarībā no eksperta pieredzes, kas veic novērtējumu. Ja nav pietiekami daudz datu, lai novērtētu scenārija iespējamību, var būt lietderīgi pieņemt kvalitatīvas metodoloģijas un izmantot spriedumu, lai novērtētu risku. Lai samazinātu neobjektivitāti, vērtētājiem ir jāatbilst noteiktām prasībām, piemēram, iepriekšējai pieredzei terorisma riska novērtējumu veikšanā, interešu konfliktu novēršanai un objektivitātei.

Riska novērtējums būs jādokumentē ar norādījumiem to precīzai interpretācijai pārbaudītā aktīva īpašniekiem/apsaimniekotājiem, kuri ir atbildīgi par pieļaujamā riska līmeņa ierobežojumu noteikšanu un izlemšanu, vai riska novēršana ir nepieciešama.

Rūpīgas draudu un risku analīzes veikšana ir C-UAS risinājuma izstrādes procesa stūrakmens, jo tā nosaka pamatprasības gan nākotnes sistēmai, gan plašākam risinājumam. Draudi un riska analīzes laikā definētie scenāriji ir galvenais ievads testēšanai ieviešanas posmā un regulārai testēšanai, darbojoties C-UAS risinājumā. Ir jābūt skaidram, ka visi risinājumi un draudu aina attīstīsies un ka tas ir jāatkārto regulāri. Analīzē skaidri jādefinē iespējamais kaitējums, ko UAS, kas nesadarbojas, var nodarīt KI vai publiskajai telpai (draudi), un tā iespējamība (risks).

Vairumā gadījumu pati UAS nerada atsevišķu risku, bet tā ir daļa no plašāka riska (ko sauc par "makrorisku"). Tāpēc ir ieteicams risināt UAS risku kā daļu no vietas plašākas riska pārvaldības programmas, nevis kā atsevišķu UAS riska novērtējumu.

2.1 RISKA IDENTIFIKĀCIJA

Pirmais solis riska novērtēšanas procesā ir UAS apdraudējumu identificēšana, kas attiecas uz novērtējamo vietu. Draudu identificēšana koncentrējas uz taktiku noteikšanu, ko var izmantot agresori, un uz iespējamo scenāriju formulēšanu. Cilvēka radītu apdraudējumu un to iespējamības noteikšana ir sarežģīts uzdevums, jo pretēji dabas apdraudējumiem pieejamie dati ir ierobežoti, un tāpēc parasti tiek iesaistīta liela subjektivitāte, mēģinot saistīt konkrētus draudus ar potenciālo mērķi. No izlūkošanas dienestiem un LEA var pieprasīt datus par pašreizējiem un jauniem draudiem, uzbrukuma nolūku un citu saistītu sensitīvu informāciju. Plašāku informāciju par pieejamajiem datu avotiem, kas var atvieglot draudu identificēšanu, var atrast sadaļā Drošība ar izstrādātu: publisko telpu aizsardzība pret teroristu uzbrukumiem [17].

2.2 RISKA ANALĪZE

Konkrētas KI apdraudējumi var ievērojami atšķirties. Vietnes raksturojums (vide, lielums, blakus esošās konstrukcijas, ēkas utt.) ietekmē apdraudējuma ainu. Turklāt katrai vietnei būs atšķirīgas bažas par UAS. Piemēram, cietuma īpašnieks varētu būt vairāk nobažījies par UAS, kas lido ar kontrabandu, savukārt publiska pasākuma organizatori vairāk pievērsīsies UAS draudiem, kas varētu apdraudēt sabiedrisko drošību. Visbiežāk sastopamās draudu kategorijas ir parādītas 5. attēlā.

Ir svarīgi identificēt vietnes elementus, kurus varētu ietekmēt nesadarbīga UAS uzbrukums. Piemēri ir (bet ne tikai) personas, ēkas, aktīvi, drošībai būtiski pakalpojumi, KI pamatdarbības un kontrolēti materiāli.

[17] Coaffee, J. et al., *Dizaina drošība: publisko telpu aizsardzība pret teroristu uzbrukumiem*, Kopīgais pētniecības centrs, Eiropas Savienības Publikāciju birojs, Luksemburga, 2022. gads.

Lai nodrošinātu pilnīgumu, ieteicams veikt vietnes aptauju, kas ietver:

- vietas specifika, tostarp kritisko līdzekļu atrašanās vietas un vietas piekļuves punkti;
- vide ,tostarp trīsdimensiju vietas novietojums, topogrāfija, zemes izmantošana (pilsēta/lauki/mežs) un cilvēka reljefs (pilsētas teritorijas, būves, transporta ceļi);
- virtuāls reljefs, tostarp gaisa telpas ierobežojumi, elektromagnētiskā vai RF spektra izmantošana, iespējamās aklās zonas pārklājuma noteikšanā, izsekošanā un identificēšanā (piemēram, koki, kas traucē radara signālus);
- potenciālās UAS palaišanas vietas un pieejas maršruti atsaucoties uz atsevišķa objekta vidi, tostarp tās ģeogrāfiju, procedūrām un iespējām, kas noteiks situācijas izpratnes aprakstīšanai izmantoto metodoloģju;
- fiziskās ievainojamības, piemēram, būvkonstrukcijas un logi.

Kad vietas apsekojums ir veikts, tas jāizmanto, lai izprastu draudus un iespējamās ievainojamības, kas, visticamāk, tiks vērstas, lai definētu scenārijus. Ieteicams definēt katru scenāriju (definējot iespējas, nolūku, vietnes apsekojuma ievainojamības) un pēc tam detalizētāk aprakstīt katru atsevišķi (parasti atbildot: kas, ko, kur, kad, kāpēc, kā, sekas utt.).

Lai noteiktu šo relatīvo iespējamību, ir jānovērtē apdraudējuma līmenis apgabalā, kas ieskauj pārbaudīto potenciālo mērķi. Tas ir sarežģīts uzdevums, jo parasti attiecīgie dati ir ierobežoti un bieži vien nav pieejami to sensitīvā rakstura dēļ.

Daži izmantojamie indikatori ir šādi.

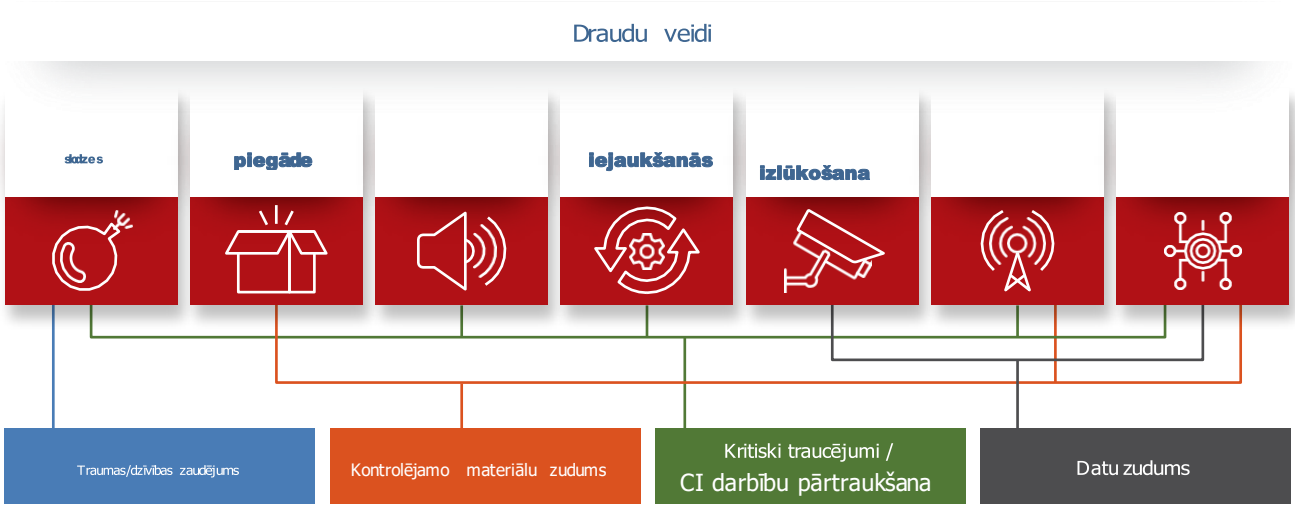
- **Draudi vēsture**. Sniedz informāciju par iepriekš ziņotiem, neveiksmīgiem vai novērstiem uzbrukumiem/draudiem ar katru konkrēto taktiku, kas izmantota, lai mērķētu uz ēku vai tās lietotājiem, vai līdzīgās telpās. Apdraudējumu vēsturē tiek ņemti vērā teroristu grupējumu publiskie izteikumi pret civiliem mērķiem un to motivācija, īpaši, ja priekšroka tiek dota aplūkotajam scenārijam.
- **Uzbrukuma sarežģītība/spēja**. Novērtē praktisko/tehnisko pieredzi, kas agresoram būtu nepieciešama, lai veiktu UAS vadītu uzbrukumu (piemēram, improvizētas sprādzienbīstamas ierīces vai ķīmisku, bioloģisku, radioloģisku un kodolvielu izveidošana), kā arī grūtības iegūt UAS (piemēram, atkarībā no tā izmēra), ieroci vai tā izveides komponentiem. Tajā tiek pārbaudīti finanšu resursi, kas nepieciešami materiālu un citu būtisku elementu iegādei, kas varētu būt nepieciešami (piemēram, atbalsta infrastruktūra, sakaru tīkls un piegādes ķēde).
- **Pievilcība/motivācija.** Atkarīgs no mērķa pievilcības (piemēram, kultūras/ reliģiskā/simboliskā nozīme, cilvēku apmeklējums), kas saistīts ar iespējamo uzbrukuma taktiku. Tā pēta, vai kāds noteikts darbības veids uzbrucējam šķiet pievilcīgāks, jo tam varētu būt lielāka ietekme īpašuma funkciju dēļ (piemēram, savstarpēja atkarība ar citām iekārtām, papildu sekas valstij un sabiedrībai, publisku un/vai sensitīvu datu klātbūtne).

Ja UAS draudi ir integrēti scenārijos, tos var kartēt ar makroriskiem.Makrorisku piemēri, kas ietver UAS, būtu (bet ne tikai) šādi.

- Traumas/dzīvības zaudējums. Tostarp UAS kā ieroču izmantošana fiziskā uzbrukumā.
- Kontrolējamo materiālu zudums. UAS izmantošana noziedzīgu darbību atbalstam (piemēram, intelektuālais īpašums, uzņēmējdarbībai svarīga informācija vai kontrolējamo vielu zādzības).
- Kritiski traucējumi/pārtraukšana CI darbībā. UAS izmantošana sabotāžai vai nu tieši pret KI objektu, vai netieši pret atkarīgu objektu, izmantojot ieroču un/vai atbalsta funkciju (piemēram, izlūkdatu vākšana/kiberuzbrukums).
- Datu zudums. Tostarp UAS kā izlūkošanas platformas izmantošana, lai atbalstītu naidīgas plānošanas darbības, spiegošanu un nelikumīgu informācijas vākšanu.

Katrai KI vietai atšķirsies tas, kā šie makro riski tiek saistīti ar identificētajiem UAS draudu veidiem. Uzņēmumu īpašniekiem ir jāizvērtē, kā makro riski ir saistīti ar viņu vietnes UAS draudu veidiem. Ir skaidrs, ka visi makroriski visās implementācijās tiks saistīti atšķirīgi.

Piemēram, UAS draudu veids "fizisks uzbrukums" var veicināt "dzīvības zaudēšanas" risku. Riska vadītāji var izmantot UAS riska reģistru, lai pārbaudītu scenārijus. Ir svarīgi atzīmēt, ka riska matrica ir jāpielāgo konkrētajam KI vietas kontekstam. To ilustrē piemērs 11. attēlā



UAS incidentu iespējamības un seku novērtējums

Ļaunprātīgas UAS riska līmeņa novērtējums apvieno katra identificētā scenārija iestāšanās iespējamības novērtējumu un iespējamās sekas, ja šis scenārijs īstenosies. Šādā procesā tiek izmantoti draudu un ievainojamības novērtējuma rezultāti. To var ilustrēt riska matricā, kā parādīts 12. attēlā.

12. attēls: Riska matricas piemērs

Ja UAS riski ir identificēti UAS risku reģistrā, UAS riska analīzes ietvaros var noteikt pamata riska rādītāju. Riska analīzes laikā jāņem vērā šādi faktori.

- **Draudu aktieri.** Iespējamie apdraudējuma dalībnieki būtu jānosaka, veicot draudu analīzi. Šis solis ir svarīgs, lai izveidotu iespējamos scenārijus, pret kuriem būtu jāveic riska kontroles pasākumi.
- **Varbūtība.** Kvalitatīvs, relatīvs punktu skaits, kas balstīts uz apdraudējuma dalībnieku motivāciju un spējām. Vērtējums parasti svārstās no 0 līdz 5 (5 ir viskritiskākais drauds) vai no maz ticama, vidēji ticama, ļoti ticama, ticama līdz gandrīz drošam.
- **Ietekme**. Rezultāts, kas balstīts uz apdraudējuma ietekmi uz attiecīgajiem riskiem KI makrorisku reģistrā. Ieteicams veikt kvalitatīvu novērtējumu, izmantojot piemērotu metodiku un vērtēšanas sistēmu, par ko vienojušies atsevišķi KI uzņēmumu īpašnieki [18].

[18] Viens piemērs varētu būt vērtības, kas saistītas ar darbības nepārtraukības plānu (piemēram, atjaunošanas punkta mērķis, atveseļošanās laika mērķi vai darba atjaunošanas laiks).

- Riska rādītājs. Riska rādītāju aprēķina, reizinot iespējamību un ietekmi ar iespējamo svara koeficientu, pamatojoties uz CI vietnes riska pieņemšanas līmeņiem.
  Riska rādītāju var nelineāri svērt, ja notikuma ietekme var būt nesamērīga ar iespējamību (mazas iespējamības notikumi var būt pietiekami katastrofāli, lai prasītu atbilstošu riska mazināšanu). Lai gan šajā rokasgrāmatā ir viena riska aprēķināšanas iespēja, lasītājs var brīvi izvēlēties metodiku un/vai sekot tam, kas viņu vietnē jau ir ieviests.

Uzbrukuma sekas ir saistītas ar īpašuma veidu un apstākļiem incidenta laikā. Iepriekšējie incidenti ir parādījuši, ka uzbrukuma tiešās, tūlītējās sekas ir dažādas, sākot no ietekmes uz cilvēku dzīvību (piemēram, ievainojumiem vai nāves gadījumiem) līdz lieliem ekonomiskiem zaudējumiem (piemēram, remonta izmaksām un pakalpojumu traucējumiem) un vides katastrofām (piemēram, ūdens piesārņojums). Netiešās, ilgtermiņa sekas ir grūtāk novērtēt, jo tās ietver tādus politiskus/sociālus aspektus kā ietekme uz iedzīvotāju psiholoģiju un netiešās ekonomiskās izmaksas (piemēram, ietekme uz tūrisma nozari). Lai atvieglotu šo novērtēšanu, vērtētājam ir jāatbild uz vairākiem jautājumiem, tostarp uz šādiem jautājumiem.

- Cik cilvēku var tikt nogalināti vai ievainoti pēc uzbrukuma ar UAS vadītu taktiku?
- Kādi pakalpojumi var tikt traucēti uzbrukuma gadījumā? Cik ilgi turpināsies traucējumi? Vai ir kādi dublējumi pakalpojumiem un cik maksās remonts?
- Vai starp savienojumiem ar citiem aktīviem vai pakalpojumiem ir kādi kaskādes efekti?
- Kādas ir paredzamās bojājumu novēršanas izmaksas? Vai ir pieejami aizstājēji?
- Vai KI ir ietvertas svarīgas utilītas vai sensitīva informācija, kas var tikt apdraudēta? Kādas ir viņu zaudēšanas vai pakalpojumu pārtraukšanas sekas?
- Vai ir iespējamas kādas politiskas sekas, kaitējums organizācijas/īpašnieka reputācijai un/vai drošības pārkāpumi (piemēram, personas datu pārkāpumi)?
- Kādas ir netiešās ekonomiskās izmaksas (piemēram, tūrisma nozarei) un kādas ir iedzīvotāju psiholoģijas sekas?

2.3 RISKA NOVĒRTĒJUMS

UAS riska novērtēšana notiek pēc UAS riska analīzes. Kad pamata riski ir aprēķināti, pārskatīti un saskaņoti, tie ir jānovērtē attiecībā pret riska pieņemamības līmeni, lai noteiktu, vai ir nepieciešama papildu mazināšana. Katrs risks ir jāapsver, lai noteiktu pieņemamības līmeni attiecībā pret KI uzņēmuma īpašnieka saskaņoto pielaides līmeni. Riska rādītāji, kas pārsniedz šo slieksni, tiek uzskatīti par nepieņemamiem, un ir jārīkojas.

Kā parādīts 13. attēlā, ir jānovērtē riska ārstēšanas risku "pieci T" un katram riskam jāizvēlas iespējamā rīcība. Riski ir jānovērtē, lai izvēlētos kādu no tālāk norādītajām darbībām.

13. attēls

2.4 RISKA APSTRĀDE

Atsaucīga lēmumu pieņemšana C-UAS ir balstīta uz sākotnējās izpratnes, taktiskā līmeņa tehniskās analīzes (UAS uzvedības un/vai UAS konfigurācijas, gan fiziskās, gan elektromagnētiskās) un piemērojamo noteikumu kombinācija.

Runājot par UAS iesaistīšanu, C-UAS risinājumā ir vairāki elementi, kas jāapvieno, lai pieņemtu lēmumu par iesaistīšanos. To vidū ir draudu novērtējums, normatīvie un juridiskie parametri un darba pilnvaras.

Šī šķirošana atspoguļo lēmumu pieņemšanas procesu, ko KI un publisko telpu īpašnieki var izmantot, lai noteiktu pareizo rīcību, ja tiek novērots apdraudējums. Lēmuma pieņemšanas process lielā mērā ir saistīts ar gaidāmajiem draudiem un iespējamiem atbilstošiem pretpasākumiem, kurus var izmantot. Izšķiršana atspoguļo CI reakciju uz UAS iebrukumu un tāpēc ir galvenais ieguldījums C-UAS risinājuma izstrādē.

Detalizētais riska novērtējums ir jādokumentē, lai to varētu izmantot turpmākajos posmos.

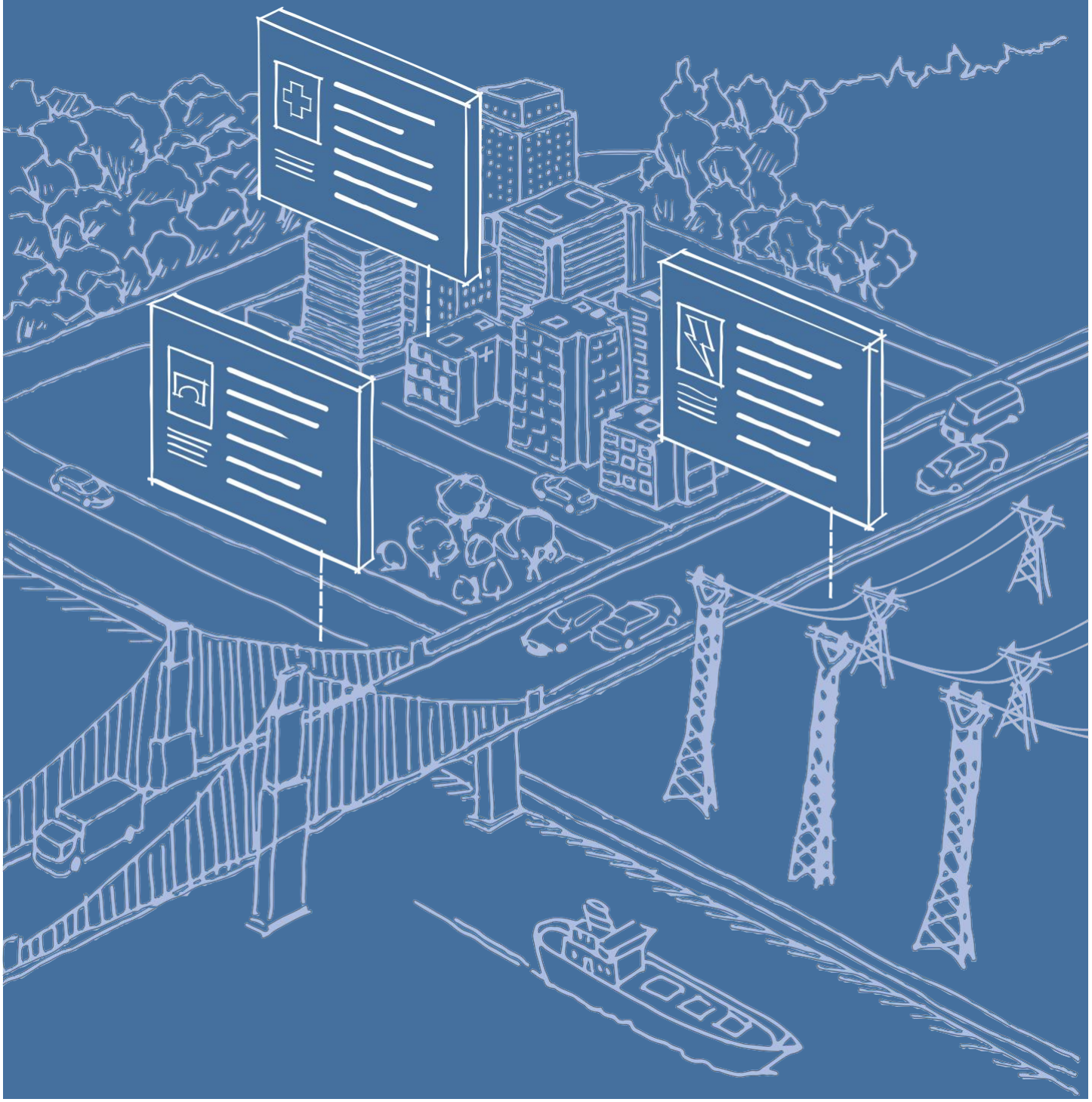
5. RISKA UN DRAUDU ANALĪZES POSMA KOPSAVILKUMS

Šīs fāzes beigās jums vajadzētu labāk izprast:

- izpratne par draudiem;
- izpratne par draudu scenārijiem;
- identificēti konkrēti UAS draudus, kas ir piemērojami vietnei;
- identificētas vietnes ievainojamības;
- vietas apsekojums ar informāciju par to, kur atrodas kritiskie līdzekļi;
- identificēto risku mazināšanas plāns;
- riska matrica;
- vienošanās par riska pieņemšanas līmeņiem;
- draudu un reaģēšanas plāns.

3

Trešā fāze / C-UAS risinājums dizains



"C-UAS risinājuma izstrādes" fāze ietver atbilstošu mazināšanas pasākumu un tehnoloģiju atlases procesu, kas atbilst identificētajiem riskiem un vietnes un ieinteresēto personu vajadzībām.

Visiem risinājumiem kopīgi ir pamata pakalpojumi (skatiet ievada sadaļu), kas atvieglo seku mazināšanas līmeņu mainīšanu uz augšu un uz leju, kad mainās vajadzības (piemēram, VIP apmeklējumi, pagaidu pasākumi, piemēram, Ziemassvētku tirdziņi, lieli sporta pasākumi un koncerti). Pamatpakalpojumu mazināšana ir atkarīga no daudziem faktoriem, kas tiks apskatīti šajā sadaļā. Mērķis ir ieviest pilnīgu risinājumu.

6. TREŠĀ FĀZE – PROJEKTA FĀZE

Šajā posmā nepieciešamā informācija:

- skaidrs izstrādātā risinājuma prasību apraksts (vietnes vajadzības, mērķi un apjoms);
- objektu riska reģistrs;
- skaidrs draudu un reaģēšanas plāns;
- likumdošanas izpratne;
- augsta līmeņa prasības;
- informācija par vietni un vidi.

Šīs fāzes beigās jums ir jābūt:

- vietnes vajadzībām atbilstošs dizains;
- augsta līmeņa risinājumu arhitektūra;
- atjaunināta objekta aptauja;
- risinājuma ieviešanas specifikācijas;
- atjaunināta ieinteresēto pušu analīze ar skaidrām lomām un pienākumiem.

Risinājuma izstrāde ir sarežģīts posms, un tas būs pamats ieviešanas un darbības fāzēm. Ja C-UAS risinājumiem var būt kopīgi daudzi faktori, katrs elements un iestatījums ir jāpielāgo riska pieņemamības līmeņiem, vietas specifikai, pieejamajam budžetam utt. Būs vajadzīgs skaidrs augstākā hierarhijas līmeņa, iestāžu un KI regulatoru pilnvarojums. Labs dizains un metodika palīdzēs atvieglot izmaiņas, kad tas būs nepieciešams. Labs dizains arī palīdzēs iesaistīt un pārvaldīt procesus un procedūras no daudzām iesaistītajām pusēm visos līmeņos.

PADOMS

C-UAS risinājuma mērķis ir mazināt UAS risku objektam, veicot atbilstošus pasākumus juridiskajās, tehniskajās robežās un iesaistot pareizās ieinteresētās personas.

Vienkāršota procesa ceļa kartes risinājuma izstrādi var apkopot četros galvenajos posmos, skatiet 14. attēlu.

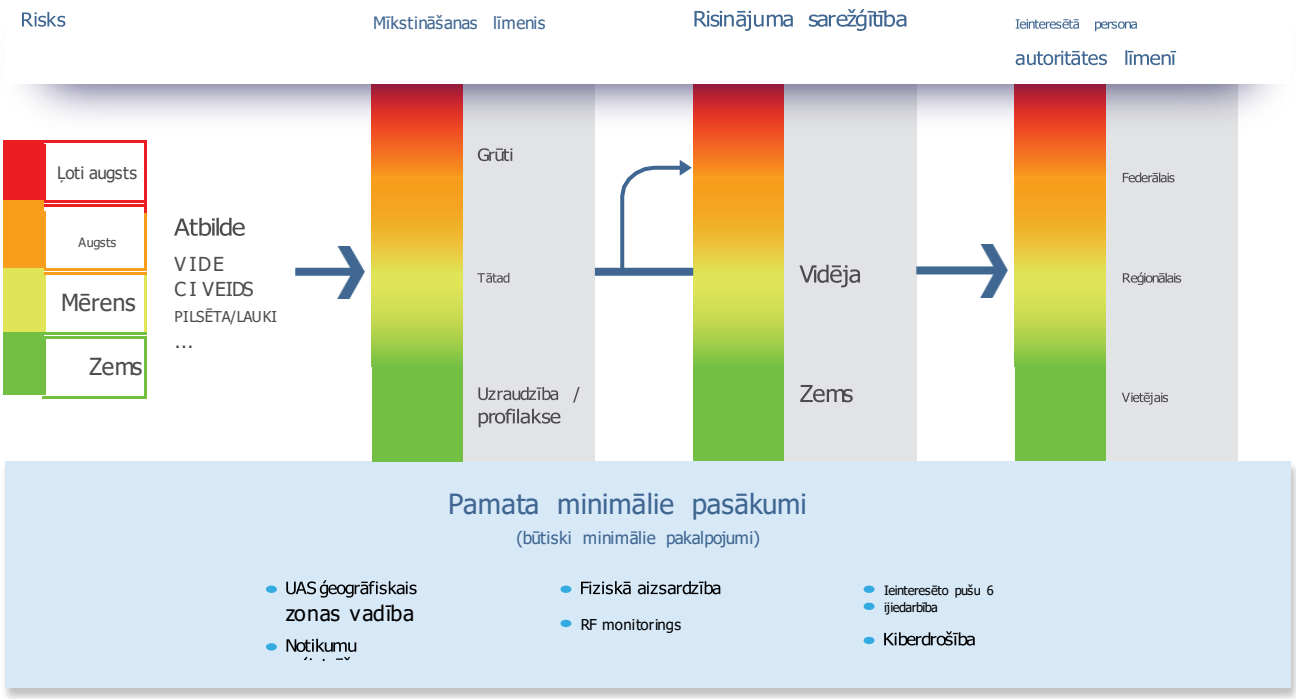
1. Riska novērtējuma veikšana un vides ierobežojumu un uzņēmējdarbības vajadzību apkopošana.

2. Izvēloties problēmu mazināšanas līmeni, kas atbilst problēmai un nepārsniedz juridiskos ierobežojumus.

3. Izvēlētajam seku mazināšanai atbilstošu tehnoloģiju un risinājumu izvēle.

4. Procesu un procedūru noteikšana ar iesaistītajām pusēm un to ieviešana. Tas ietvers ieinteresētās personas visos līmeņos.

14. attēls: C-UAS projektēšanas procesa ceļvedis



Projektēšanas fāzes beigās vietnei ir risinājuma prasību specifikācija, kas ir paredzētā risinājuma apraksts ar to saistītajām procedūrām un procesiem. Tas var būt par pamatu risinājumu iepirkuma procesam.

Daži svarīgi elementi, kas jāņem vērā un jāizlemj projektēšanas fāzē, ir šādi.

- **Investīciju pieeja** .Šajā posmā būtu jāpieņem lēmums par to, kā finansēt projektēšanas pirmo posmu. Lielākajai daļai risinājumu, iespējams, būs nepieciešamas C-UAS zināšanas. Daudzos gadījumos būtu lietderīgi nošķirt konsultantus no tehnoloģiju nodrošinātājiem, lai samazinātu aizspriedumus pret risinājumiem, ko tehnoloģiju uzņēmums jau ir ieviesis. Labam projektam jābūt pietiekami detalizētam, lai to varētu izmantot kā iepirkuma procedūras tehnisko dokumentu. Jādomā, vai risinājums būs sagādāts, īrēts vai arī tas tiks iegūts kā pakalpojums. Turklāt izmaksu tāme ir ieteicama ar pārskatu par dažādiem izmaksu faktoriem (tostarp izmaksu aplēsēm iekšējām un ārējām pusēm), kā arī to, kā risinājums tiks izmantots un finansēts tā darbības laikā.

- **Juridiskie apsvērumi.** Tas ietver atļaujas izmantot tehnoloģijas atklāšanai un mazināšanai. Tāpat būtu jāizpēta, kādas ir iespējas iejaukties vietas perimetrā un ap to. Tam būs jāiesaista daudzas ieinteresētās puses, piemēram, LEA, iestādes, kaimiņi, citu risinājumu operatori, gaisa telpas pārvaldība, UTM, gaisa satiksmes pārvaldība un U-Space operatori. Galu galā projektam ir jānodrošina, lai visi risinājuma juridiskie aspekti tiktu izskatīti un dokumentēti, tostarp viss nepieciešamais atļaujas un licences par risinājumu.

- **Risinājuma apjoms un mērķis**. Jebkurā projektā ir svarīgi definēt darbības jomu un mērķus, lai izvairītos no neskaidrībām, pārpratumiem un darbības joma. Tas tiek darīts, lai izvairītos no izdevumu pieauguma un iespējamas neefektīvas ieviešanas, kas neatbilst attiecīgajām vajadzībām, vai lai izvairītos no risinājuma, ko nevar mainīt vai integrēt, kad nepieciešamas izmaiņas.

- **KI, sabiedriskās telpas un apkārtne**. Izstrādājot, jāņem vērā vietnes un tās apkārtnes attīstības plāni. Tas ietvers instalācijas citās vietnēs, kas varētu ietekmēt noteikšanas sistēmas.

- **Informācijas apmaiņa.** Ieinteresētajām pusēm būtu jāapspriež un jāvienojas par informācijas apmaiņu. Tas ir svarīgi izmēģinājuma lidojumiem, kurus varētu noteikt apkārtējās implementācijas, pārklājošās UAS ģeogrāfiskās zonas un brīdinājuma zonas, uztveršanas sistēmu traucējumi (piemēram, radaru frekvences), UAS darbības attīstība un iniciatīvas gaisa telpas pārvaldībai (U-Space pakalpojumi un UTM sistēmu ieviešana) utt.

- **Blakusparādību novērtējums**. Tas ir ļoti svarīgs punkts, kuru nevajadzētu novērtēt par zemu. Jāpārbauda, kādu ietekmi izvēlētās noteikšanas un neitralizācijas tehnoloģijas atstās uz objektu, tās vidi, citām iekārtām, apkārtējām iekārtām utt. Pārbaudēs īpaši jāaptver ietekmes mazināšanas pasākumu izmantošana. Frekvences, ko izmanto saziņai starp zemes stacijām un bezpilota lidaparātiem, vairumā gadījumu ir tās pašas frekvences, ko bezvadu sakariem izmanto parastās rūpniecības un sadzīves tehnikas. Turklāt globālās navigācijas satelītu sistēmas signālu traucēšana vai viltošana var radīt nevēlamas blakusparādības.

- **Vietnes aptauja**. Projektēšanai ir nepieciešams skaidrs un pilnīgs vietass un apkārtnes pārskats. Nepieciešama visaptveroša izpēte, kas satur ēku augstumu, kokus, ainavu utt. To var izmantot, lai modelētu, atlasītu un plānotu izvietojuma noteikšanas sensorus un neitralizācijas sistēmas. Otrajā fāzē (risku un draudu analīze) izmantotā vietas apsekošana ir saistīta ar risku sarakstu ceturtajā posmā (zonu izmēru noteikšanas risinājuma īstenošana). Šai aptaujai jābūt pietiekami skaidrai un detalizētai, lai trešās puses to varētu izmantot risinājuma ieviešanai.

3.1 MINIMĀLIE PAMATPASĀKUMI

Visu risinājumu pamatā ir jābūt minimālajiem pamata pasākumiem. Kā aprakstīts ievaddaļā, tie būs visu pārējo pakalpojumu pamatā un atvieglos izmaiņas, kad tās būs vajadzīgas. Dažus no tiem jau varētu ieviest kā daļu no parastajiem drošības procesiem, kas pēc tam būs vienkārši jāatjaunina ar C- UAS elementiem. Nākamajās sadaļās ir aprakstīti šie pakalpojumi un sniegti padomi, kā tos ieviest.

UAS ģeogrāfiskās zonas pārvaldība

Ap aizsargājamo vietu ir lietderīgi noteikt dažādas zonas, kurās tiek veiktas dažādas darbības. Aizsargājamās teritorijas vide, atrašanās vieta un veids ir svarīgi faktori šo zonu projektēšanā un noteikšanā. Lielumam un platībai, kas jāuzrauga, jābūt balstītai uz apdraudējumu, pret kuru ir jāaizsargā. Rezultāti būs svarīgi faktori, lai noteiktu zonu lielumu, kur novietot sensorus un kādas darbības jāveic un kur. Jo lielākas ir zonas, jo grūtāk un dārgāk tās ir aizsargāt. Konfigurācija un zonu skaits var atšķirties atkarībā no ieviešanas.
Galu galā tiem jābūt veidotiem tā, lai sniegtu laiku, kas nepieciešams reakcijai un neitralizācijai, radot vismazāko papildu bojājumu. Tas jāplāno tā, lai visas vai jutīgākās vietnes daļas būtu aizsargātas. Nosakot šīs zonas, ir jāņem vērā, kādas iestādes ir nepieciešamas draudu neitralizācijai un kam ir šīs tiesības. Daudzos gadījumos atkarībā no zonas ir dažādi dalībnieki. Tāpēc procesu un procedūru izstrādē būtu jāiekļauj visi dalībnieki. Šī iemesla dēļ ir nepieciešams rūpīgi analizēt vajadzības un skaidri definēt procesus un procedūras ap un iekšpusē C-UAS drošības zonās.

Ieteicams izveidot daudzslāņu zonas, kā redzams 15. attēlā. Definīcijas un izmēri ir jāsaskaņo ar pasākumiem, kas nepieciešami riska mazināšanai, kādiem mazināšanas pasākumiem ir atļauts, kā arī ar risinājumā iesaistītajām ieinteresētajām personām. Sensoru izvietojums ir cieši saistīts ar definīcijas lielumu un darbību definīcijām zonās (skatiet 3.2. sadaļu apsvērumus par sensoru izvietojumu un to, kas jāņem vērā, lai iegūtu pareizu pārklājumu visās zonās).

Zonu lielums un ar tiem saistītās darbības būtu jānosaka tā, lai visiem iesaistītajiem dalībniekiem būtu laiks saskaņotā veidā mazināt UAS incidentu. Seku mazināšanas vietai jābūt pēc iespējas drošākai un drošai, ar minimālu papildu bojājumu un ievērojot noteikumus un noteikumus.

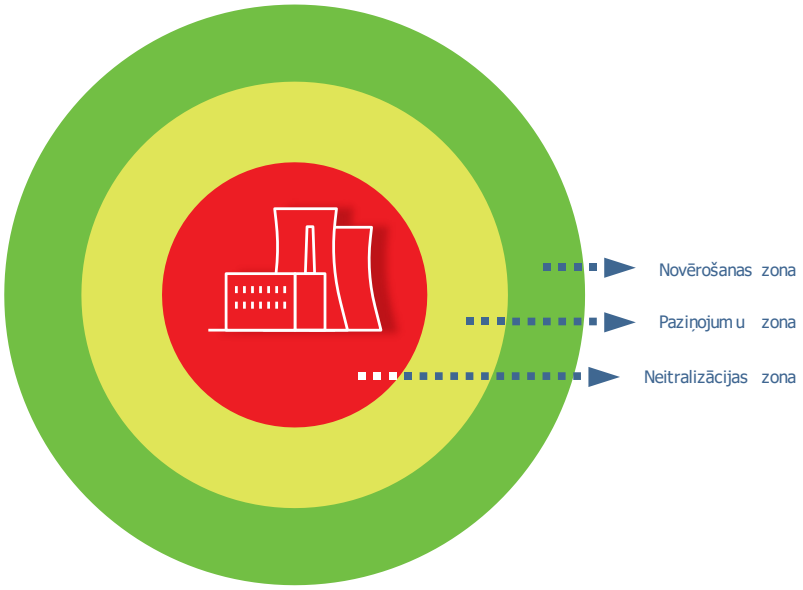
UAS ģeogrāfiskā zona ir gaisa telpa, ko valsts civilās aviācijas iestāde var piešķirt objekta īpašniekam, lai varētu noteikt noteikumus UAS darbībai [19]. Tas var būt UAS minimālo specifikāciju, paziņojumu, laika ierobežojumu, darbības vietas utt. veidā. Tā ir arī zona, kurā zonas pārvaldniekam būs noteiktas pilnvaras iejaukties atklātu lidojumu gadījumā. Atkarībā no valsts un vietējiem noteikumiem tas var ietvert seku mazināšanas pasākumu izmantošanu. Tāpēc ir ļoti svarīgi iekļaut regulējošās iestādes to darbību izstrādē un definēšanā, kuras vēlas īstenot.

[19] Komisijas Īstenošanas regula (ES) 2019/947 (2019. gada 24. maijs) par bezpilota gaisa kuģu ekspluatācijas noteikumiem un procedūrām .

Slāņainā C-UAS zonu modelī:

- iekšējais slānis ir neitralizācijas zona. Tā ir UAS ģeogrāfiskās zonas trīsdimensiju zona, kurā KI vai publiskās telpas īpašnieks vēlas neitralizēt jebkuru neatļautu UAS, izmantojot pasākumus, kas noteikti identificēto risku mazināšanai. Ir svarīgi, lai šīs zonas lielums tiktu definēts pareizi, lai neitralizācijas dalībniekiem būtu atbilstošas juridiskās pilnvaras un laiks reaģēt, kad tas ir nepieciešams. Šī zona ir pilnībā jānosedz ar noteikšanas sistēmām.
- Paziņojumu zona ir vieta, kur draudi tiek rūpīgi uzraudzīti, un, kad tie rodas, visi dalībnieki ir gatavi to mazināšanai, ievērojot noteiktos procesus un procedūras. Tās lielums ir atkarīgs no laika, kas nepieciešams, lai mobilizētu resursus un sagatavotos ielaušanās zonās, kur nepieciešama neitralizācija.
- Novērojumu zona ir zona ap paziņojumu zonu. Šī zona tiek izmantota, lai novērotu darbības, kuras var izmantot, lai optimizētu risinājumu un izpratni. Šo zonu var daļēji segt ar noteikšanas sistēmām.

15. attēls: Slāņainā C-UAS zonu modeļa piemērs



Daži svarīgi apsvērumi saistībā ar šīm zonām ir šādi.

- Integrācija un UTM sistēmas izmantošana ir svarīgs instruments gaisa telpas pārvaldībai un integrācijai ar U-telpu un apkārtni. Izmantojot parasto UTM pakalpojumu (piemēram, no mākoņa), jebkuram risinājumam tiek pievienota vērtīga informācija, bet UTM nav C-UAS risinājums.
- Ja objektā vai aizsargājamās zonās ir paredzēta UAS izmantošana, ir jāizpēta un jāplāno, kā to pārvaldīt un integrēt C-UAS risinājumā.
- Pieprasīt UAS ģeogrāfiskās zonas un gaisa telpas pārvaldību atbildīgajai valsts civilās aviācijas iestādei risinājuma izstrādes agrīnā stadijā.
- Informēt ieinteresētās puses un apkārtni par šīs UAS ģeogrāfiskās zonas ieviešanu.

- Pārliecinieties, ka visas vietnes apdrošināšanas ir atjauninātas, iekļaujot visu veidu UAS izmantošanu aizsargājamajā vietā un tās tuvumā. Tas ir nepieciešams vietas apsekošanai, sensoru pārbaudei, iespiešanās testiem, apmācībai utt.
- Vairumā gadījumu būs ļoti noderīgi reģistrēties kā UAS operatoram (kā noteikts ES tiesību aktos [20] [21]),
- lai atļautu izmantot lidojumus pārbaudēm, apmācībām, apsekojumiem utt.
- C-UAS sistēmas veiktspējas verifikācijas un validācijas testi ir jāizstrādā tā, lai tie atbilstu draudu scenārijiem un atbilstu tam, pret ko ir jāaizsargā. Piemēram, nav jēgas veikt augsta līmeņa teroristu uzbrukumu testu risinājumam, kas paredzēts aizsardzībai pret privātuma problēmām, uzraudzība nav neitralizācijas metode.
- Izkārtņu izlikšana ap objektu saskaņā ar vienošanos ar iestādēm un apkārtni. To varētu saistīt ar informācijas kampaņu, lai informētu apkārtējās ieinteresētās personas, ka šī teritorija ir teritorija, kurā UAS nav lidots.
- Ieviest pārvaldības procesus un procedūras iekšēji un kopā ar ārējām ieinteresētajām personām (piemēram, UTM, vietējām ieinteresētajām personām, LEA, iestādēm).

Notikumu reģistrēšana

Notikumu reģistrēšana ir svarīga, lai risinājums būtu efektīvs un iedarbīgs. Dizainam jābūt pietiekami elastīgam, lai reģistrētu manuālus novērojumus, sensoru noteikšanu un informāciju, kas saņemta no ārējiem avotiem, piemēram, UTM vai no kaimiņiem. Žurnālu saglabāšanas laiks ir jādefinē tā, lai to varētu izmantot modeļu noteikšanai. Žurnālu analīze jāveic ar regulāriem intervāliem un jāizmanto risinājuma atjaunināšanai/ jaunināšanai.

Iekļautajai informācijai jābūt pietiekamai, lai noteiktu tendences un identificētu iespējamos jaunus draudus (piemēram, ja kāds mēģina noskaidrot, vai ir UAS aizsardzība). Tas varētu ietvert konstatējumus, kas nav pārbaudīti kā UAS vai klasificēti kā viltus pozitīvi. Mežizstrādei jābūt centralizētai no visiem avotiem ar pēc iespējas pilnīgāku informāciju, piemēri ir šādi.

- Tiešais un tīkla attālais ID, kā noteikts Komisijas Deleģētajā regulā (ES) 2019/945 (UAS operatora reģistrācijas numurs un verifikācijas kods, bezpilota gaisa kuģa unikālais sērijas numurs, laika zīmogs, UAS ģeogrāfiskā atrašanās vieta, ātrums, maršruts, pilota pozīcija, pacelšanās pozīcija un avārijas stāvoklis).
- UAS informācija un visa pieejamā informācija (mediju piekļuves kontroles adrese, bezpilota lidaparāta tips, sērijas numurs utt.).
- Konstatēts, pēc kādiem detektoriem, personām, metodei utt.
- Tiesu ekspertīzē izmantojamie attēli, video un signālu informācija. Ieejas avots (piemēram, ārējā novērošana, UTM, cits C-UAS risinājums, sensors un detektors). Informācija par laiku un atrašanās vietu.
- Lidojuma informācija un īpašības.
- Apstiprinātie un neapstiprinātie lidojumi.

---

[20] Komisijas Deleģētā regula (ES) 2019/945 (2019. gada 12. marts) par bezpilota gaisa kuģu sistēmām un trešo valstu bezpilota gaisa kuģu sistēmu operatoriem .

[21] Komisijas Īstenošanas regula (ES) 2019/947 (2019. gada 24. maijs) par bezpilota gaisa kuģu ekspluatācijas noteikumiem un procedūrām.

- Mazināšanas darbības: ja sistēma veic kādas darbības, lai mazinātu atklātos draudus, piemēram, UAS traucē vai novirza, šīs darbības ir jāreģistrē, ieskaitot veiktās darbības laiku un veidu.
- Viltus trauksmes: visas sistēmas iedarbinātās viltus trauksmes ir jāreģistrē kopā ar viltus trauksmes iemeslu un jebkādām korektīvajām darbībām, kas veiktas, lai novērstu viltus trauksmes nākotnē.
- Sistēmas veiktspēja: sistēmas veiktspējas rādītāji, piemēram, noteikšanas biežums un reakcijas laiks, ir jāreģistrē, lai uzraudzītu sistēmas efektivitāti laika gaitā.
- Lietotāja darbības: visas darbības, ko veic C-UAS risinājuma autorizētie lietotāji, ir jāreģistrē, ieskaitot darbības laiku un veidu, kā arī lietotāja identitāti.
- Sistēmas kļūdas: visas sistēmas kļūdas vai darbības traucējumi ir jāreģistrē kopā ar visu diagnostikas informāciju, ko var izmantot, lai novērstu un atrisinātu problēmu.
- Operatora darbības.

Visai reģistrētai informācijai jābūt eksportējamai, lai attiecīgās iestādes to varētu izmantot kriminālistikā.

Fiziskā aizsardzība

Fiziskā aizsardzība [22] ir svarīgs mazināšanas pasākums pret daudziem UAS draudiem, tomēr tas bieži tiek ignorēts un tas ir rūpīgi jāizvērtē. Fiziskās aizsardzības pasākumi dažos gadījumos var būt vieglāk, lētāki un ātrāk īstenojami nekā dārgās C-UAS sistēmas.

Daži piemēri:

- folijas uz logiem, lai novērstu draudus no maziem UAS taranēšanas logiem;
- folijas uz atraitnēm, lai izvairītos no filmēšanas no ārpuses;
- tīklus virs cilvēkiem, lai izvairītos no traumām;
- ārējās žalūzijas, lai izvairītos no taranēšanas;
- sprādzienizturīgs stikls un fiziska aizsardzība pret mazām sprāgstvielām;
- cilvēku pārvietošana prom no logiem un monitoru novietošana tā, lai tos nevarētu redzēt no ārpuses.

RF monitorings

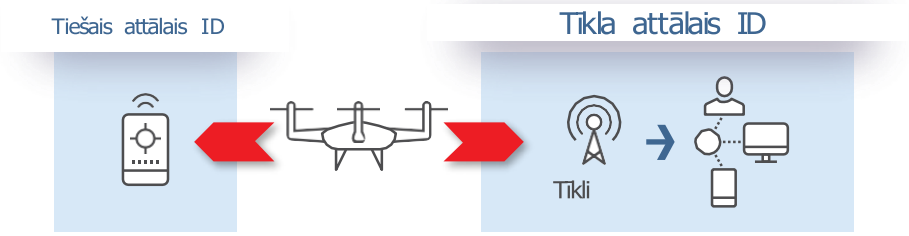
UAS savai darbībai izmanto dažādas sakaru frekvences. UAS izmantotā frekvenču josla ir atkarīga no konkrētā lietojuma, UAS veida un darbības reģiona. Parasti UAS izmanto gan licencētas, gan nelicencētas frekvenču joslas saziņai ar zemes vadības stacijām, citiem bezpilota lidaparātiem un satelītu sakariem.

[22] Aizsardzība pret bezpilota gaisa kuģu sistēmām — Rokasgrāmata par bezpilota gaisa sistēmu riska novērtēšanu un ēku un vietu fiziskās sacietēšanas principiem

Tiešā attālinātā identifikācija ID [23] ir atvērtā protokola signāls, kas tiek pārraidīts reāllaikā visa lidojuma laikā. Šo tiešo periodisko apraidi no bezpilota gaisa kuģa, izmantojot atklātu un dokumentētu pārraides protokolu, var uztvert tieši, izmantojot esošās mobilās ierīces apraides diapazonā. Tajā ir vismaz šādi dati.

- UAS operatora reģistrācijas numurs un verifikācijas kods, ko reģistrācijas procesa laikā norādījusi reģistrācijas dalībvalsts.
- Unikāls bezpilota gaisa kuģa sērijas numurs.
- Laika zīmogs, bezpilota gaisa kuģa ģeogrāfiskais novietojums un augstums virs virsmas vai pacelšanās punkta.
- . Peilējums, mērīts pulksteņrādītāja virzienā no patiesajiem ziemeļiem, un bezpilota lidaparāta ātrums uz zemes
- Pilota ģeogrāfiskā atrašanās vieta vai, ja tas nav pieejams, pacelšanās punkts.

To pašu informāciju var iegūt, izmantojot tīkla attālo ID. Kamēr tiešā attālinātā ID tiek pārsūtīts tieši no bezpilota lidaparāta uz uztvērēju, tīkla attālā ID informācija tiek pārsūtīta no bezpilota lidaparāta uz mobilajiem tīkliem (Global System for Mobile Bands), no kurienes tā tiek izplatīta. Tas ir parādīts 17. attēlā. Integrējot risinājumu ar ārējiem pakalpojumiem, kuriem ir pieejama tīkla attālā ID informācija, ir vēlams šo informāciju integrēt, taču tas netiek uzskatīts par būtisku pakalpojumu minimumu.



Lai gan ir svarīgi saņemt ID no UAS, jāpieņem, ka daudzi UAS un jo īpaši UAS, kas nav korporatīvi, tos nepārsūtīs. Tāpēc ir svarīgi uzraudzīt arī UAS saziņai visbiežāk izmantotās frekvenču joslas, kā norādīts 18. attēlā.

Komerciālo UAS daudzējādā ziņā var salīdzināt ar Wi-Fi maršrutētāju, kas pilotam nosūta video kadrus un lidojuma datus. Lielākā daļa komerciālo UAS izmanto 2,4 GHz un 5,8 GHz, kas arī ir standarta Wi-Fi savienojuma frekvences. UAS tālvadības signālu informācijas noteikšana un interpretācija var sniegt vērtīgu papildu informāciju, piemēram, UAS modeli un ražotāju, GNSS pozīciju, pacelšanās pozīciju (parasti saistīta ar pilota pozīciju), akumulatora procentuālo daudzumu, multivides piekļuves kontroles adresi, UAS vadības komandu veidu un lidojuma režīmus.

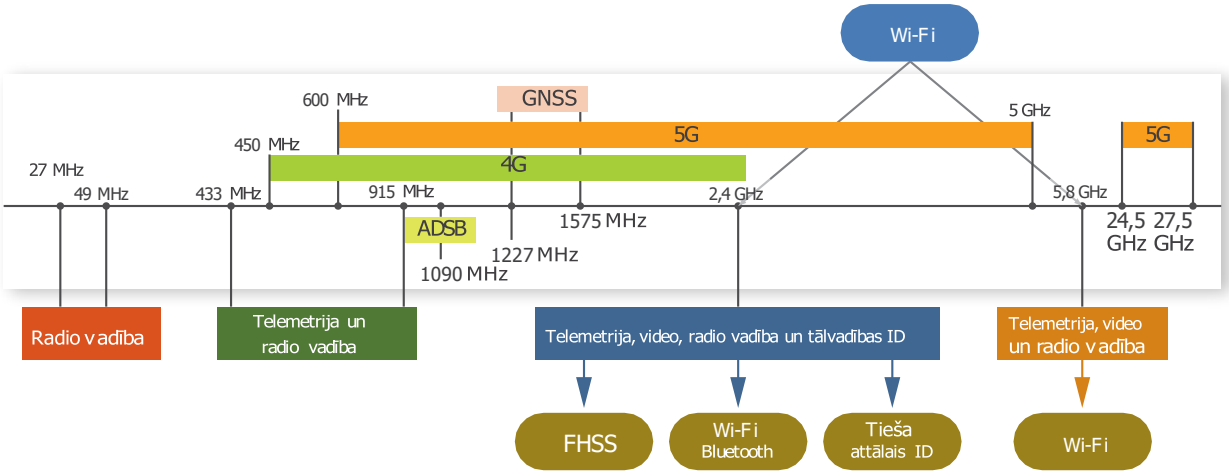
[23] https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easyaccess-rules-unmanned-aircraft-systems?page=19 .

UAS var darboties arī licencētās frekvencēs, piemēram, L joslā (1–2 GHz) un S joslā (2–4 GHz), ko parasti izmanto satelītu sakariem. Šīs frekvences nodrošina uzticamu un drošu saziņu lielos attālumos, padarot tās piemērotas darbībām ārpus redzes līnijas. Papildus šīm joslām UAS izmanto arī citas frekvenču joslas, piemēram, C joslu (4–8 GHz) un Ku joslu (12–18 GHz) satelītu sakariem un īpaši augstas frekvences joslu (300–400 MHz) aizsardzības lietojumiem.

Noteiktu frekvenču joslu izmantošanai var būt nepieciešams normatīvais apstiprinājums, un dažādās valstīs var būt atšķirīgi noteikumi attiecībā uz UAS sakaru frekvencēm. Tāpēc ir būtiski izprast darbības reģiona normatīvo regulējumu, lai nodrošinātu atbilstību vietējiem likumiem un noteikumiem.

Neskatoties uz to, ka tehnoloģija tiek uzskatīta par "viegli uzstādāmu" (pasīvā RF antena), veiktspēja ir tieši saistīta ar uzstādīšanas vidi, piemēram, attālumu no ēkām un kokiem. Turklāt RF tehnoloģijas noteikšanas diapazons ir atkarīgs no uztvērēja jutības un UAS raidītāja RF signāla jaudas.

17. attēls:UAS izmantotās frekvences



Ieinteresēto pušu mijiedarbība

Ieinteresēto pušu mijiedarbība ir viens no būtiskākajiem obligātajiem pakalpojumiem, kas būtu jāveic ikviena risinājuma izstrādē, jo, iesaistot ieinteresētās puses procesos un procedūrās, tās veicina efektīvu un produktīvu ieviešanu. Visās C-UAS risinājuma fāzēs tiks iesaistītas dažādas ieinteresētās puses. C-UAS risinājumā jāiesaista precīzas ieinteresētās personas katrai vietnei un tās pieņemtajam eskalācijas līmenim. Ieinteresētajām personām būtu jāpanāk kopīga vienošanās par to, kas ko, kur un kad dara.

Kiberdrošība

Jebkurai ieviešanai, kurā tiek izmantota IKT, IKT drošības nostiprināšana ir obligāta. Tā kā C-UAS sistēmas ir drošības informācijas sistēmas un tās ir potenciāli integrētas citās drošības sistēmās, visus tīkla savienojumus var izmantot, lai ievadītu un mainītu konfigurācijas vai samazinātu sistēmas. Ja C-UAS risinājums ir savienots ar internetu, šie savienojumi ir rūpīgi jāanalizē, lai noteiktu drošības riskus. Pilnīgajam risinājumam jābūt iekļautam vietnes darbības nepārtrauktības plānā, kiberdrošības politikā, drošības procedūrās un procesos, kā arī pieņemtajā riska līmenī.

3.2 MAZINĀŠANAS LĪMEŅA IZVĒLE UN ATKLĀŠANAS TEHNOLOĢIJU ATBILSTĪŠANA

C-UAS risinājuma izstrādē ietilpst atbilstošas reakcijas uz draudiem atlase CI vietnei vai publiskajai telpai un pēc tam to saskaņošana ar atbilstošiem pasākumiem. Ņemot vērā šo pasākumu ietekmi uz to mērķiem, vidi, kurā tie tiek darbināti, un nodomu izmantot šīs ierīces civilā vidē, šādu pasākumu likumība būtu jānosaka pirms lēmuma pieņemšanas par to pieņemšanu. Tiesību akti par tehnoloģiju izmantošanu dažādās dalībvalstīs ir atšķirīgi. Tāpēc katrai KI vietnei vai publiskai telpai ir ieteicams noskaidrot piemērojamos noteikumus savas valsts un vietējās iestādēs.

Sākotnējais vietas novērtējums un apsekojums palīdzēs noteikt labāko tehnoloģiju, kas atbilst noteiktajām vajadzībām. Vietnes apsekojuma laikā ir jāizmanto sākotnējā modelēšana, un tā jāpapildina ar testiem.

14. attēlā parādīta saikne starp mazināšanas līmeņiem un tehnoloģijām. Seku mazināšanas līmeņa noteikšanas, tehnoloģiju izvēles un ieinteresēto pušu iesaistīšanas process risinājuma izstrādē ir jāatkārto vairākas reizes. Neatkarīgi no reaģēšanas uz draudiem būs vairāki pamata pasākumi, kas KI vietnei vai publiskai telpai būtu jāīsteno.

Šī metodoloģija ņem vērā uzraudzību, mīkstos un stingros mazināšanas pasākumus, taču bez skaidras nodalīšanas, skatīt 19. attēlu. Tie ir papildinoši un papildina ieguvumus, ko sniedz pamata pasākumi.

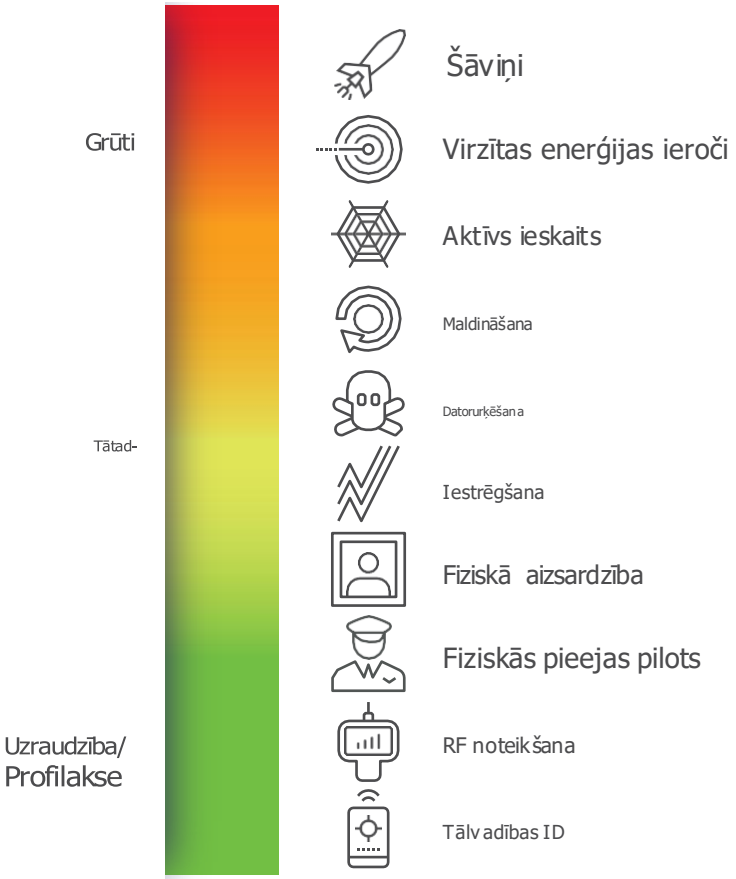
Uzraudzība/profilakse zemākais mazināšanas līmenis. Šis apdraudējuma-reakcijas līmenis attiecas uz UAS satiksmes noteikšanu un uzraudzību noteiktajās zonās un tuvojas UAS pilotiem. Tas ietver neuzbāzīgu darbību veikšanu, ja tiek pārkāptas noteiktās robežas vai noteikumi. Šī zemākā aizsardzības līmeņa mērķis ir radīt situācijas izpratni par UAS izmantošanu, atklājot UAS trafiku aizsargājamās vietnes apgabalā.

Mīksta mazināšana koncentrējas uz pašreizējo notikumu apturēšanu ar salīdzinoši nekaitīgiem pasākumiem, kas varētu ietvert tuvošanos pilotam(-iem) un nekinētisku pasākumu izmantošanu.

Cieta mazināšana ir augstākais mazināšanas līmenis no trim. Šajā līmenī tiks izmantoti visi pieejamie pasākumi, lai apturētu UAS draudus zonās, kas noteiktas ar minimālu papildu bojājumu. To varētu panākt, kombinējot pasākumus, piemēram, tuvojoties pilotam(-iem), izmantojot kinētiskos un nekinētiskos pasākumus. Visas procedūras būs pareizi jāīsteno ar iestāžu apstiprinājumu. Seku mazināšanas dalībnieki varētu būt iekšējās un ārējās drošības kombinācija, piemēram, LEA vai aizsardzības nozare.

Visi pasākumi un darbības būs jāreģistrē, lai uzlabotu reaģēšanas spēju.

19. attēls



Ir svarīgi, lai šajā jomā būtu labi definēts mazināšanas process un procedūras. To izmantos gūtajām atziņām un salīdzināšanai ar citiem risinājumiem. Var būt arī izdevīgi izmantot metodoloģiju, ko atpazīst un izmanto ieinteresētās personas, kas veic līdzīgas tuvumā esošās implementācijas, un tā palīdzēs izvairīties no pārpratumiem un neskaidrībām informācijas apmaiņas laikā. Jāuzsver, ka nav tiešas saiknes starp riska mazināšanas līmeni un izmantojamo tehnoloģiju. Sliekšņi, kas attiecina riska rādītājus ar eskalācijas līmeņiem, ir jānosaka katram risinājumam atsevišķi.

Tie ir jāpapildina ar papildu dizaina apsvērumiem, kas saistīti ar mazināšanu, kas nepieciešama, lai novērstu UAS risku. Pārsvarā seku mazināšanas pasākumus uzskata par kinētiskiem vai nekinētiskiem. Kinētiskie pasākumi ietver fiziska spēka izmantošanu, lai atspējotu vai iznīcinātu UAS, savukārt nekinētiskie pasākumi ietver elektronisku vai citu līdzekļu izmantošanu, lai traucētu vai atspējotu UAS. Pasākumu izvēle būs atkarīga no konkrētajiem UAS radītajiem draudiem un darbības vides, kurā C-UAS sistēma tiek izvietota. Šo seku mazināšanas pasākumu izmantošana un personas, kuras var veikt, ir jāīsteno saskaņā ar valsts un reģionālajiem noteikumiem un noteikumiem.

Tālāk ir aprakstīti visizplatītākie [24] un pieejamie pasākumi.

[24] https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf.

Kinētiskie pasākumi ietver fiziska spēka izmantošanu, lai atspējotu vai iznīcinātu UAS. Šie pasākumi ietver šādus pasākumus.

- Virzītas enerģijas ieroči (DEW) izmanto augstas enerģijas starus, piemēram, lāzerus vai mikroviļņus, lai atspējotu vai iznīcinātu UAS. Parasti tiek uzskatīts, ka DEW nav nāvējošs, taču tas joprojām var sabojāt UAS sastāvdaļas.

- Lādiņi vai raķetes: pret-UAS raķetes izmanto sprāgstvielas vai citus līdzekļus, lai fiziski iznīcinātu UAS. Šīs raķetes var būt vadāmas vai nevadāmas, un tās var palaist no dažādām platformām, tostarp no zemes palaišanas ierīcēm vai gaisa platformām.

- Kājnieku ieroči, piemēram, šautenes vai bises, var izmantot, lai notriektu UAS. Tomēr šī pieeja var būt sarežģīta un bīstama, jo tai nepieciešama precīza mērķauditorijas atlase un tā var izraisīt citu objektu netīšus bojājumus vai iznīcināšanu.

- Tīkls ietver specializēta aprīkojuma izmantošanu, lai uztvertu un imobilizētu UAS gaisā, neļaujot tai lidot tālāk.

Nekinētiski (elektroniski) mēri, no otras puses, ietver elektronisku vai citu līdzekļu izmantošanu, lai atspējotu vai traucētu UAS darbību. Šie pasākumi ietver šādus pasākumus.

- RF traucēšana var izmantot, lai traucētu saziņu starp UAS un tā pilotu, izraisot UAS kontroles zaudēšanu un, iespējams, avāriju[25].

- Maldināšana ietver viltus signālu radīšanu, lai UAS liktu domāt, ka tā saņem likumīgas komandas no pilota. Tas var izraisīt UAS mainīt kursu vai atgriezties savā sākuma punktā.

- Datorurķēšana ietver nesankcionētas piekļuves iegūšanu UAS vadības sistēmai, lai pārņemtu kontroli vai traucētu tās darbību.

Izstrādājot C-UAS risinājumu, kurā ņemts vērā seku mazināšanas līmenis, ir jāņem vērā vairāki faktori, lai nodrošinātu, ka tiek izvēlēti atbilstoši pasākumi, lai efektīvi cīnītos pret specifiskajiem UAS radītajiem draudiem, sk. 14. attēlu. Tie jāņem vērā papildus pamata minimuma pakalpojumiem, kas vienmēr būtu jāievieš.

Daži svarīgi faktori, kas jāņem vērā, ir šādi.

- draudu novērtējums. Ir svarīgi pastāvīgi novērtēt konkrētos UAS radītos draudus. Tas ietver izpratni par UAS iespējām, lidojuma īpašībām, kravnesību, kā arī potenciālajiem mērķiem un paredzēto uzbrukuma efektu.

- Jāņem vērā arī darbības vide, kurā C-UAS pasākumi tiks izvietoti. Daži faktori (piemēram, laika apstākļi, reljefs, lauku vai pilsētas teritorija, troksnis, kur uzstādīti sensori, šķēršļi, piemēram, augstas ēkas) ietekmēs C-UAS sistēmas veiktspēju.
  Piemēram, tuksneša instalācijai izmantotais risinājums atšķirsies no tā, ko izmanto aizsardzībai pilsētas teritorijā, Ziemassvētku tirdziņā, ūdens attīrīšanas iekārtā vai cietumā.

- Zonām un to lielums, piemēram, ir jebkura no zonu daļām, kas ir kopīga ar citām aizsargājamām zonām.

[25] Tā kā pieejamās ierīces tiek traucētas UAS saziņai apstiprinātajās frekvencēs, tās būs neefektīvas UAS ar modificētām frekvencēm (skatiet 3.1. sadaļu).


NO DRONES

- Fiziskā aizsardzība īstenotajiem pasākumiem vai plāniem to darīt.
- UAS satiksmes informācija no atklāšanas sistēmas un dati, kas pieejami no citiem avotiem ,piemēram, gaisa telpas pārvaldības iniciatīvas (UTM un U-Space).
- Pieejamība dalībniekiem un ieinteresētajām pusēm kuriem ir tiesības veikt riska mazināšanas pasākumus. Vai tie ir pieejami nekavējoties vai ar viņiem ir jāsazinās? Piemēram, LEA vai aizsardzības nozare.
- Laiks, kas vajadzīgs, lai beigās rīkoties, iespējams, ir vissvarīgākais faktors.
- Izmaksas C-UAS pasākumiem. Tas ietver pašu pasākumu izmaksas, kā arī personāla apmācības un aprīkojuma uzturēšanas izmaksas.
- Traucējumi un kļūdaini pozitīvi rezultāti var samazināt, pievienojot papildu sensorus vai strādājot ar vairāku veidu sensoriem un apvienojot datus, lai iegūtu labāku situācijas izpratni. Tomēr par to būs jāmaksā.
- Juridiskie un ētiskie apsvērumi C-UAS pasākumu izmantošana var radīt juridiskus un ētiskus apsvērumus. Ir svarīgi nodrošināt, lai visi izvēlētie pasākumi atbilstu attiecīgajiem likumiem un noteikumiem un neradītu risku neiesaistītajām pusēm.

Rūpīgi apsverot šos faktorus, var noteikt atbilstošu seku mazināšanas līmeni. Ir svarīgi regulāri pārskatīt visus šos faktorus, lai nodrošinātu, ka risinājums tiek atjaunināts atbilstoši pašreizējiem draudiem un atjauninātām tehnoloģiju specifikācijām, skatiet 14. attēlu.

C-UAS sistēmās tiek izmantotas daudzas noteikšanas un izsekošanas tehnoloģijas, un to attīstība ir ļoti ātra. Tālāk ir aprakstīti visbiežāk lietotie.

- Radars ir elektroniska ierīce, kas objektu noteikšanai un atrašanās vietas noteikšanai izmanto radioviļņus. Tas izstaro radioviļņus, kas atstaro objektus to ceļā, un radara sistēma pēc tam nosaka atstarotos viļņus, lai noteiktu objekta atrašanās vietu, ātrumu un citas īpašības. Radari var būt noderīgi, lai atklātu bezpilota lidaparātus lielā augstumā un lielos attālumos. Tomēr radara viļņi var neizkļūt cauri šķēršļiem, piemēram, ēkām vai kokiem, un tie var nebūt tik efektīvi, lai atklātu mazākus bezpilota lidaparātus zemākos augstumos vai pilsētas vidē, kur ir daudz jucekli.
- RF analīze noteikt RF signālus, ko izstaro bezpilota gaisa kuģa vadības sistēma. Tā kā UAS izmanto radio signālus, lai sazinātos ar tālvadības pultīm, RF sensori var noteikt bezpilota lidaparāta un tā kontroliera izstarotos signālus. RF sensori ir noderīgi mazāku UAS noteikšanai zemākā augstumā. Tomēr tie var nebūt tik efektīvi, lai noteiktu UAS, kas izmanto frekvences lēcienu vai citas metodes, kas apgrūtina noteikšanu.
- Akustiskie sensori noteikt bezpilota gaisa kuģa rotoru radīto skaņu. Lidojot UAS, tie izstaro atšķirīgu skaņas signālu, ko var uztvert akustiskie sensori. Akustiskie sensori ir noderīgi, lai noteiktu zema augstuma UAS, un tos var izmantot pilsētvidē, kur citas tehnoloģijas var nebūt tik efektīvas. Tomēr akustiskajiem sensoriem var būt ierobežojumi bezpilota lidaparātu noteikšanā ar klusākiem rotoriem vai trokšņainā vidē.
- Elektrooptiskie / infrasarkanie (EO/IR) sensori izmantojiet vizuālo un termisko attēlveidošanu, lai noteiktu un izsekotu UAS. Šie sensori var noteikt bezpilota gaisa kuģa dzinēju radīto siltumu vai paša bezpilota lidaparāta vizuālo parakstu. EO/IR sensori var noteikt bezpilota lidaparātus vāja apgaismojuma apstākļos un var būt noderīgi UAS veida identificēšanai. Tomēr tiem var būt ierobežojumi bezpilota gaisa kuģu noteikšanā lielos attālumos vai apstākļos, kad bezpilota gaisa kuģa karstuma zīmi maskē citi vides faktori.

Sensoru saplūšanas programmatūra izmanto, lai apvienotu signālus no dažādiem sensoriem. To var izmantot, lai papildinātu sensoru signālus un apvienotu tos kopējā attēlā. Tas nodrošinās labāku atklāšanas pārklājumu un nodrošinās, ka tiek izmantotas visu pieejamo noteikšanas tehnoloģiju labākās daļas. Piemēram, sensoru saplūšanas programmatūra var izmantot datorredzes un mašīnmācīšanās algoritmus, lai noteiktu UAS, analizējot video plūsmas no kamerām un apvienojot tās ar radara informāciju. Tas ļautu atklāt un izsekot UAS reāllaikā un uzlabot lielu platību uzraudzību.

Lai gan iepriekš minētās tehnoloģijas ir efektīvas UAS noteikšanā un izsekošanā, ir jāņem vērā, izvēloties tehnoloģiju vai tehnoloģiju kombināciju UAS noteikšanai. Šos mainīgos ietekmē tas, pret kādu UAS vietne cenšas aizsargāties. Tas attiecas uz iepriekšējās fāzes riska un draudu analīzes draudu novērtējumu. Turklāt ir jāpārbauda, vai tehnoloģijas ir piemērotas vietai un vai ir nepieciešami pasīvie RF sensori vai aktīvā radara tehnoloģija, pēdējā, ja tas ir likumīgi atļauts. Aktīvos pasākumus bieži ir sarežģītāk īstenot, jo uz to izmantošanu attiecas vairāk regulējumu (piemēram, spektra licences un jaudas ierobežojumi radaru lietošanai).

Tālāk ir minēti svarīgi elementi, kas jāņem vērā, izstrādājot risinājuma tehnisko daļu.

- Diapazons. Dažām tehnoloģijām ir lielāks diapazons, un tās var noteikt UAS lielākos attālumos, savukārt citām tehnoloģijām var būt mazāks diapazons, un tās var nebūt tik efektīvas UAS noteikšanā lielos attālumos.
- Vide. Vide, kurā tiek izvietota UAS noteikšanas sistēma, var būtiski ietekmēt tehnoloģijas efektivitāti. Piemēram, radars var nebūt tik efektīvs UAS noteikšanā pilsētvidē, kur ir daudz jucekli vai apgabalos ar augstām ēkām vai kokiem, kas var traucēt radara signālu.
- Izmaksas. Svarīgs apsvērums ir arī tehnoloģijas izmaksas. Dažu tehnoloģiju, piemēram, radara, uzstādīšana un uzturēšana var būt dārga, savukārt citas, piemēram, RF sensori vai akustiskie sensori, var būt rentablākas.
- Viltus pozitīvi. UAS noteikšanas sistēmām var būt arī kļūdaini pozitīvi rezultāti, kas var samazināt sistēmas efektivitāti. Piemēram, RF sensori var uztvert signālus no citām ierīcēm vai avotiem, un akustiskie sensori var uztvert skaņas no citiem avotiem, piemēram, putniem vai lidmašīnām.
- Pretpasākumi. Dažas UAS noteikšanas tehnoloģijas pašas par sevi var būt pakļautas pretpasākumiem, piemēram, signāla traucēšanai vai viltošanai. Tas var padarīt noteikšanas sistēmu mazāk efektīvu vai pat pilnīgi neefektīvu.

Daži svarīgi UAS faktori, kas jāņem vērā, ir šādi.

- UAS lielums. UAS lielums var ietekmēt arī noteikšanas tehnoloģijas efektivitāti. Dažas tehnoloģijas var būt labāk piemērotas lielāku UAS noteikšanai, savukārt citas var būt labākas mazāku UAS noteikšanai.
- Ātrums .Bezpilota lidaparāta ātrums nosaka laiku, kurā jāreaģē uz draudiem. Ņemot vērā, ka UAS, kas lido ar ātrumu 60 km/h, var nobraukt 2 km 120 sekundēs, kā parādīts 21. attēlā, šajā 2 minūšu laikā C-UAS risinājumam ir jāatklāj, jāseko, jāidentificē un jāmazina draudi.
- Lidojuma veids. Ja vainīgais izmanto automatizētu lidojumu, RF signāls netiks uztverts.

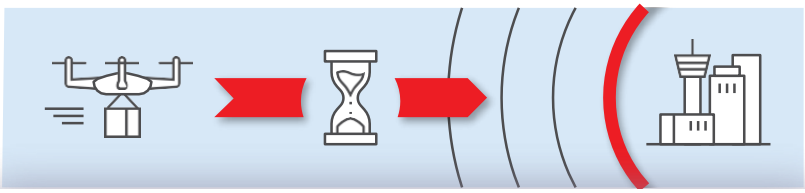
- Pilota amats. Ja pilota atrašanās vietas noteikšana ir svarīgs faktors, tad jāpatur prātā sekojošais.
  - » Daudzas noteikšanas sistēmas nolasa pilota atrašanās vietu no signāliem starp UAS un tālvadības pulti. Tos var mainīt vai izslēgt.
  - » Tālvadības pults RF noteikšana ir atkarīga no signāla saņemšanas pārsūtīja tālvadības pulti. Vide to var padarīt ļoti sarežģītu vai neiespējamu.
  - » Automatizēta lidojuma gadījumā nav cilvēka pilota, kas kontrolētu lidojums.

Blakusparādības

Seku mazināšanas tehnoloģiju blakusparādības ir svarīgas, un tās rūpīgi jāanalizē, īpaši attiecībā uz turpmāk minētajiem neitralizācijas pasākumiem.

- Vadības signālu traucēšana var ietekmēt arī citas iekārtas, kas izmanto to pašu RF joslu.
- Maldināšana un uzlaušana var ietekmēt UAS lidojumu, izraisot iespējamu avāriju vai ielidošanu citās zonās, kur tas rada bojājumus.
- Šāviņš vai raķetes pārvietojas tālāk par mērķi un var sabojāt infrastruktūru un cilvēkus.
- DEW sabojās UAS, bet var ietekmēt arī citas ierīces.

20. attēls: UAS laiks, kas nepieciešams, lai sasniegtu mērķi



Pie 60 km/h (maks. 0. kategorija) 2 km = 120 sek

Jo vairāk laika vajadzēs reaģēšanai un incidentu mazināšanai, jo lielākai būs jābūt paziņojumu zonai. Ātrāka UAS ir jāatrod tālāk, lai nodrošinātu, ka ir laiks uzsākt seku mazināšanas pasākumus.

PADOMS

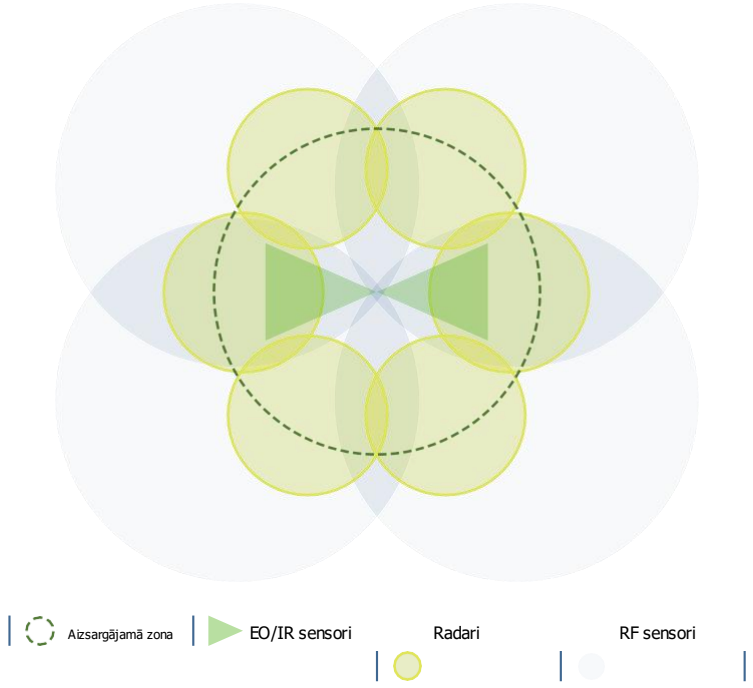
Kad potenciālais apdraudējums ir atklāts un identificēts, risinājumam ātri jāreaģē, lai mazinātu draudus. Tas ietver tādus pretpasākumus kā tuvošanās pilotam, traucēšana vai cita veida pārtveršana.

Sensoru izvietojums

Šī daļa apstrādā to sensoru izvietošanu, kuri ir izvēlēti UAS noteikšanai. Lai nodrošinātu vislabāko noteikšanas pārklājumu, jāanalizē darbības vide un potenciālie draudi saistībā ar sensoriem. To var paveikt, izmantojot modelēšanas un simulācijas rīkus, kā arī veicot testēšanu un novērtēšanu uz vietas. Visi modeļi un simulācijas ir jāpārbauda praksē, lai nodrošinātu pareizu noteikšanu un izvairītos no aklo zonu.

Jāapsver slāņveida drošības izveide, izmantojot vairākas noteikšanas sistēmas, piemēram, radaru, kameras un akustiskos sensorus, lai nodrošinātu pārklājumu un dublēšanu (piemēram, Šveices siera modelis [26]).

21. attēls: Zonas aizsardzības piemērs ar vairākiem dažādiem sensoriem



Ieviešot atklāšanas sistēmas, ir ļoti svarīgi ņemt vērā darbības vidi. Reljefs, laika apstākļi un iespējamie šķēršļi lielā mērā ietekmēs to, cik labi risinājumi darbosies. Nākamreiz, lemjot par risinājumam nepieciešamo noteikšanas sistēmu izvietošanu, svarīgi ir vairāki faktori, un tie jāņem vērā, lai nodrošinātu optimālu aizsardzības pārklājumu.

Šie faktori ietver šādus faktorus.

- Izpratne par konkrēto bezpilota gaisa kuģa radīto apdraudējumu, kā aprakstīts draudu scenārijā, apgabalā, kurā tiks izvietots C-UAS risinājums. Tas ietver iespējamo bezpilota gaisa kuģa veidu, gaisa kuģa ekspluatācijas augstumu un ātrumu, kā arī pārvadājamo kravu.

[26] Šveices siera negadījumu cēloņsakarības modelis parāda, ka, lai gan daudzi aizsardzības slāņi atrodas starp apdraudējumiem un negadījumiem, katrā slānī ir trūkumi, kas, ja tie ir saskaņoti, var ļaut notikt negadījumam.

- Lemjot par izvietojumu, jāņem vērā noteikšanas diapazons un sistēmas iespējas. Iespēja noteikt dažāda veida bezpilota lidaparātus, kā arī tā darbības rādiusu, precizitāti un reakcijas laiku. Sistēmas ar lielāku diapazonu un augstākām noteikšanas iespējām spēj noteikt UAS no tālākas attāluma un ar lielāku precizitāti, kas var nodrošināt vairāk laika reakcijai.

- Apvidus reljefs un šķēršļi var ietekmēt atklāšanas sistēmu efektivitāti. Piemēram, kā parādīts 23. un 24. attēlā, ēkas, koki vai citas konstrukcijas var bloķēt vai atstarot signālus, savukārt pakalni vai kalni var ierobežot redzes līnijas noteikšanas diapazonu.

- Izvietojums, kas novērš vājināšanos vai atstarošanu no avotiem, piemēram, ēkām, lapotnēm un ūdens.

- Jāņem vērā arī atklāšanas sistēmas izvietošanas loģistika. Tas ietver strāvas un tīkla savienojamības pieejamību, kā arī apgabala pieejamību, kurā sistēma tiks instalēta.

- Pieņemot lēmumu par atklāšanas sistēmu izvietojumu, jāņem vērā darbības vide, tostarp reljefs, laika apstākļi un iespējamie šķēršļi. Tas ietver iespējamo ievainojamības apgabalu noteikšanu un noteikšanas sistēmu izvietošanu stratēģiskās vietās, lai nodrošinātu vislabāko pārklājumu. Pieņemot lēmumu par sensora uzstādīšanu, videi un atrašanās vietai būs būtiska ietekme.

- Lai palielinātu noteikšanas diapazonu, varētu apsvērt sensoru uzstādīšanu infrastruktūrā, mastos vai torņos. Turklāt var apsvērt sadalītu sensoru sistēmu, skatiet 24. attēlu.

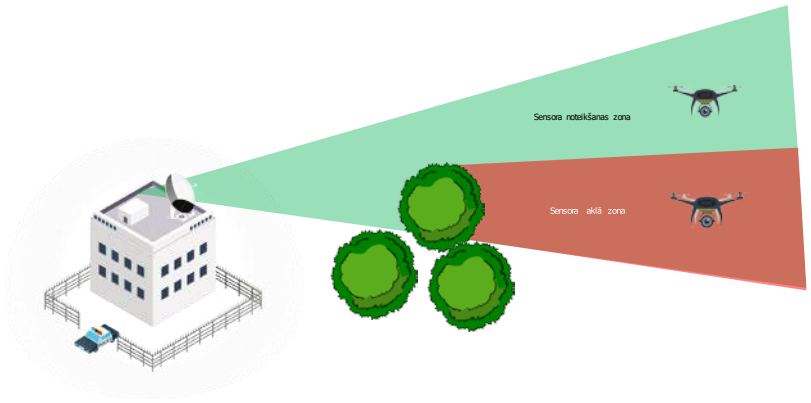
- Integrācija ar citiem C-UAS pasākumiem. Atklāšanas sistēmu izvietošana jāapsver arī saistībā ar citiem C-UAS pasākumiem, piemēram, kinētiskiem vai nekinētiskiem pasākumiem. Atklāšanas sistēmu izvietošana stratēģiskās vietās var uzlabot citu C-UAS pasākumu efektivitāti.

Lemjot par sensoru izvietojumu, jāpārbauda arī elektromagnētiskie traucējumi. To sauc arī par RF traucējumiem RF spektrā. Elektromagnētiskie traucējumi ir ārēja avota radīti traucējumi, kas ietekmē elektrisko ķēdi, izraisot elektromagnētisko indukciju, elektrostatisko savienojumu vai vadītspēju. Piemēram, radara izmantošana mobilitātē (piemēram, ātruma kameras, automašīnu radaru sistēmas) var radīt traucējumu avotus ar C-UAS radaru sistēmām vai otrādi, ietekmējot sensoru datu kvalitāti un, iespējams, radot viltus pozitīvus rezultātus. Citi iespējamie avoti varētu būt mobilie tālruņi, kosmiskais troksnis, zibens vai elektrības kabeļi.

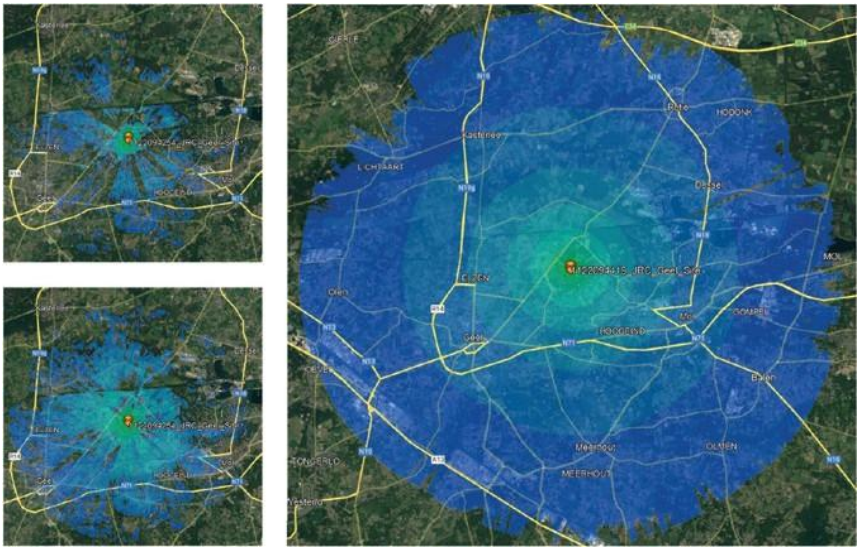
Sensoriem var būt nepieciešama redzamības līnija, un noteikšanu var tieši ietekmēt šķēršļi. Signāla vājināšanās vai atstarošanas avoti, kas jāņem vērā, ietver būves (augstu ēku, vēja turbīnu, ūdenstorņu un rūpniecisko iekārtu tuvumā), mežus (blīvu lapotni un potenciālu koku augšanu) un ūdeni (pienācīga kopšana jārūpējas par upēm, jūru, ezeriem utt.). Turklāt augstākas frekvenču joslas bieži ietekmē meteoroloģiskas parādības, piemēram, migla, lietusgāzes un sniega uzkrāšanās sensoros.

Tāpēc, lemjot par atklāšanas sistēmu izvietošanu, rūpīgi jāapsver darbības vide, tostarp reljefs, laikapstākļi un iespējamie šķēršļi. Noteikšanas diapazons, fiziskie šķēršļi un elektromagnētiskie traucējumi ir rūpīgi jāizvērtē, lai nodrošinātu precīzu noteikšanu un samazinātu viltus pozitīvus rezultātus.

22. attēls: Sensoru aklo zonu piemērs (oranža zona)



23. attēls: Zilā zona parāda noteikšanas pārklājumu – mainot sensora novietojumu, tika panākts atšķirīgs pārklājums



3.3 RISINĀJUMS ARHITEKTŪRAS PROJEKTĒŠANA — TO VISU SAVIENOŠANA

Risinājuma dizains nosaka tā turpmāko spēju palikt aktuālam un atjauninātam paredzētā kalpošanas laikā. Risinājuma arhitektūra ir galvenais elements, kas parasti ietver procesu, procedūru, aparatūras, programmatūras un tīkla komponentu kombināciju.

Daži galvenie komponenti, kas varētu būt iekļauti tipiskā C-UAS risinājuma arhitektūrā, ir šādi.

- Sensori. Tie var ietvert dažāda veida sensorus, piemēram, radaru, EO/IR un akustiskos sensorus, ko izmanto, lai noteiktu un izsekotu potenciālos UAS draudus.

- Sakaru sistēmas un tīklu infrastruktūra. Tos izmanto, lai nosūtītu sensoru datus uz centrālo vadības un kontroles (C2) centru, kur datus var analizēt un izmantot, lai pieņemtu lēmumus par to, kā reaģēt uz draudiem. C-UAS risinājums var ietvert virkni tīkla komponentu, tostarp serverus, maršrutētājus un slēdžus, kas tiek izmantoti datu pārsūtīšanai starp dažādiem sistēmas komponentiem.

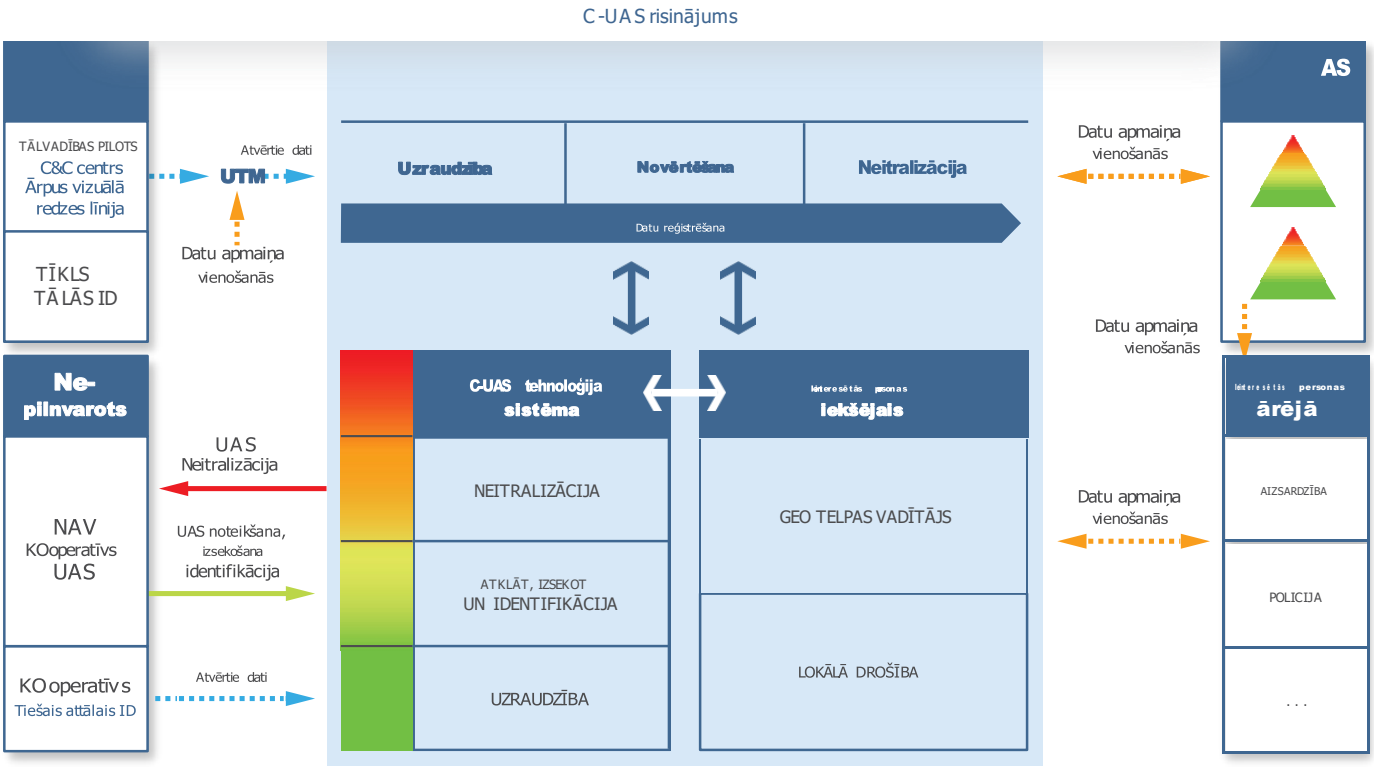
- C2 centrs un grafiskā lietotāja saskarne. Šis ir C-UAS risinājuma nervu centrs, kurā tiek saņemti, analizēti un izmantoti visi sensoru dati, lai pieņemtu lēmumus par to, kā reaģēt uz iespējamiem UAS draudiem. C2 centrā varētu būt iekļauti dažādi programmatūras rīki datu analīzei, vizualizācijai un lēmumu pieņemšanai.

- Efektori. Šie ir rīki, ko izmanto, lai mazinātu UAS draudus. Tie var ietvert traucēšanas sistēmas, kas traucē UAS sakarus vai navigācijas sistēmas, vai citus rīkus, piemēram, lāzerus, ko izmanto, lai atspējotu vai iznīcinātu UAS.

- Lietotāja saskarnes ar citām ieinteresētajām pusēm. Šīs ir saskarnes, kas ieinteresētajām personām jāizmanto, lai mijiedarbotos ar C-UAS sistēmu. Tie var ietvert grafiskas lietotāja saskarnes datu vizualizācijai un lēmumu pieņemšanai vai specializētākas saskarnes informācijas vai datu paziņošanai un efektoru kontrolei, ko izmanto UAS draudu mazināšanai.

Kopumā C-UAS risinājuma arhitektūra ir izstrādāta, lai noteiktu iespējamos draudus, analizētu datus, lai noteiktu atbilstošu reakciju, un pēc tam izvietotu efektorus, lai neitralizētu draudus. Risinājuma arhitektūras īpašie komponenti atšķirsies atkarībā no sistēmas īpašajām prasībām un draudu veidiem, kuriem tā ir paredzēta.

24. attēls: Risinājuma arhitektūras piemērs



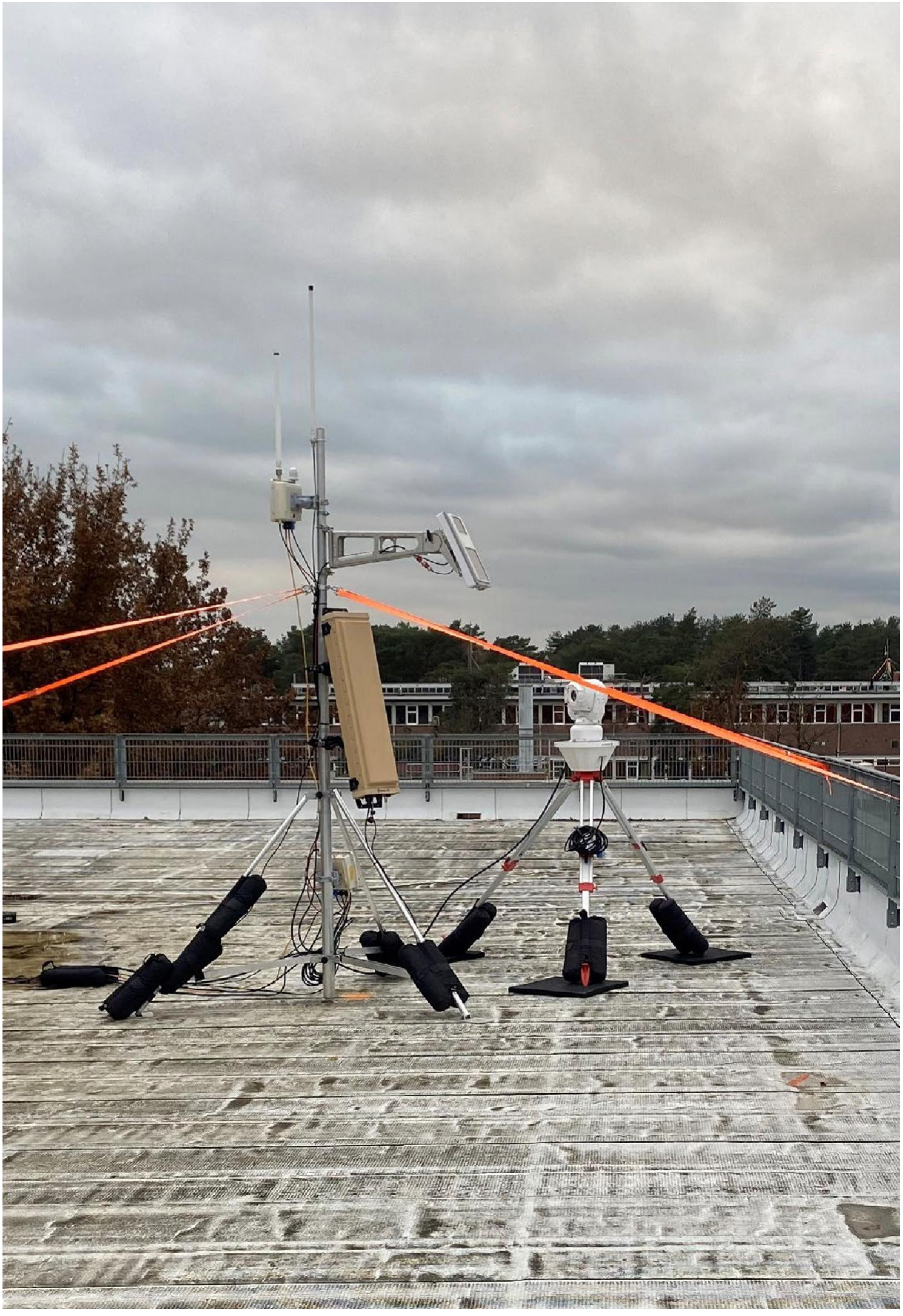
Šajā rokasgrāmatā ir ieteikts izstrādāt C-UAS risinājumu ar atvērtu arhitektūru, kas ļauj integrēt aparatūru, programmatūru un komponentus, izmantojot vienotus standartus. Tas atvieglo citu uzņēmumu izstrādāto komponentu pievienošanu, mainīšanu un nomaiņu.

Tehnoloģijai neizbēgami progresējot un attīstoties, C-UAS tirgū kļūst pieejamas papildu iespējas, un vietnes situācijas izmaiņas un no tiem izrietošie riski radīs nepieciešamību pielāgot tā risinājuma konfigurāciju. Līdz ar to, ja risinājums būtu izveidots, izmantojot atvērtas arhitektūras pieeju, risinājuma izmaiņu gadījumā samazināsies sarežģītība un izmaksas.

Atvērtās arhitektūras sistēmas dažkārt savos projektos iesaka šādus kvalitātes atribūtus.

- Pielāgošanās spēja. Piemērojamība dažādu platformu prasībām.
- Modularitāte. Sastāvdaļām jābūt neatkarīgi no sistēmas atdalāmām.
- Pārnesamība. Risinājumam jābūt pārnesamam no vienas sistēmas uz citu.
- Mērogojamība. Risinājumam ir jābūt lielākam vai mazākam atkarībā no vajadzības.

- Sadarbspēja. Efektīva datu koplietošana ar citām sistēmām.



Papildus šiem parametriem sistēmas izmaksas būs papildu virzītājspēks projektēšanas lēmumu pieņemšanai. Tas galu galā būs C-UAS pieejamā budžeta funkcija. Šajā rokasgrāmatā ir ieteikts meklēt nozares un arhitektūras standartus un vispārīgus protokolus, kas plaši pieņemti C-UAS nozarē, lai nodrošinātu to risinājumus, lai nodrošinātu savietojamību.

8. PROJEKTA POSMA KOPSAVILKUMS

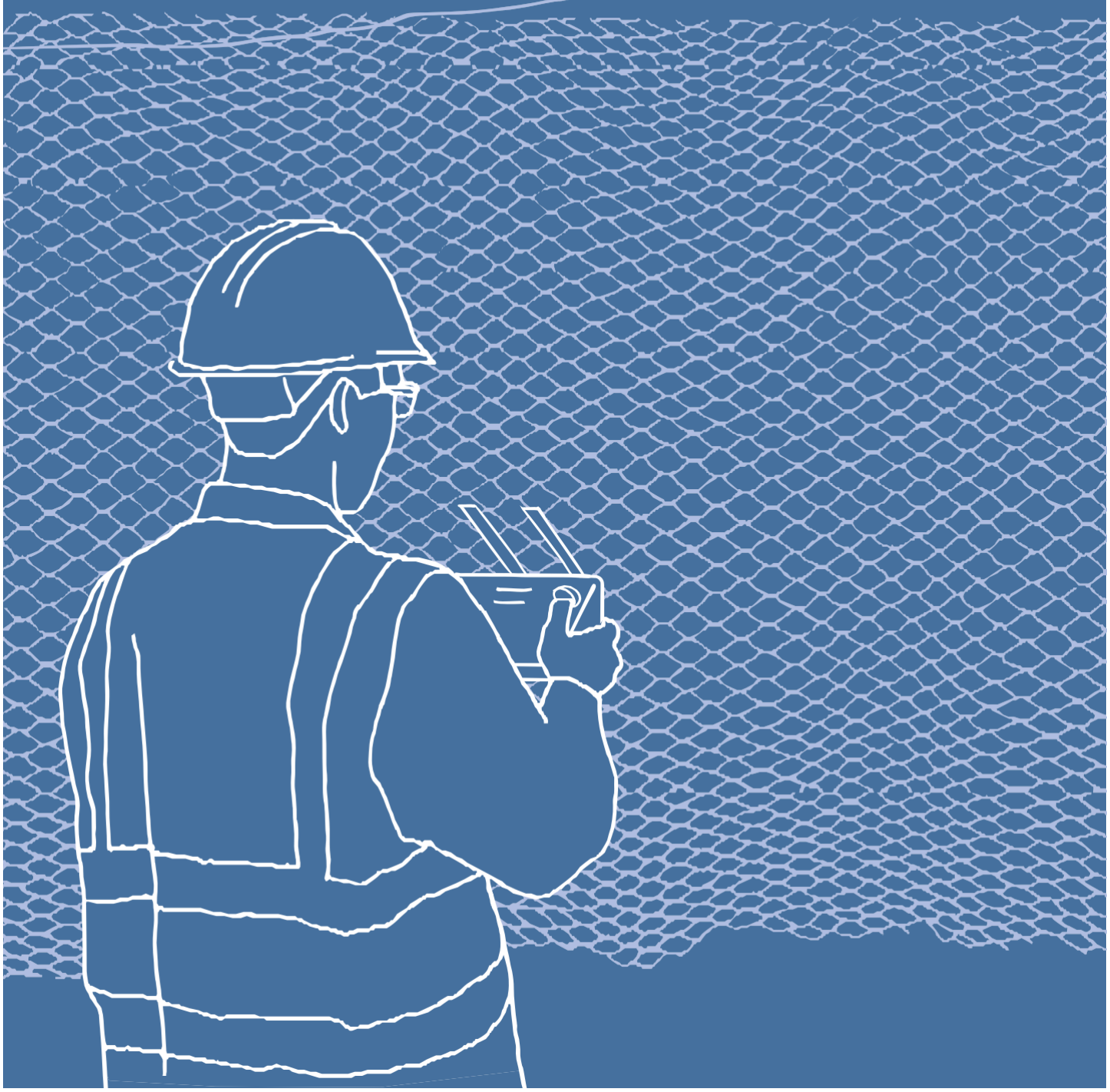
Projektēšanas fāzes beigās bija jāsavāc informācija un jāizstrādā plāni. Tie ietvers vajadzības saistībā ar vietu, atrašanās vietu, vidi, ieinteresētajām personām, noteikumiem, iestādēm (valsts un reģionālajām) utt.

Šo dokumentu un plānu formāts un informācija var atšķirties, un tie ir jāatjaunina, ja nepieciešams. Daži dokumentu piemēri ir:

- objektu riska reģistrs;
- draudu izpratne;
- likumdošanas izpratne;
- atjaunināta objekta aptauja;
- objekta vajadzībām atbilstošs risinājuma dizains;
- risinājumu arhitektūra un specifikācijas;
- informācija par vietu un vidi;
- procesi, procedūras un darbības plāni;
- atjaunināta ieinteresēto pušu analīze ar skaidrām lomām un pienākumiem;
- riska un draudu izpratne un draudu scenāriji, kas jāmazina un pret kuriem ir jāaizsargā;
- skaidra visu ieinteresēto pušu lomu un atbildības noteikšana;
- augsta līmeņa risinājumu arhitektūra;
- risinājuma prasību specifikācijas.

4

Ceturtā fāze / C-UAS risinājums īstenošana

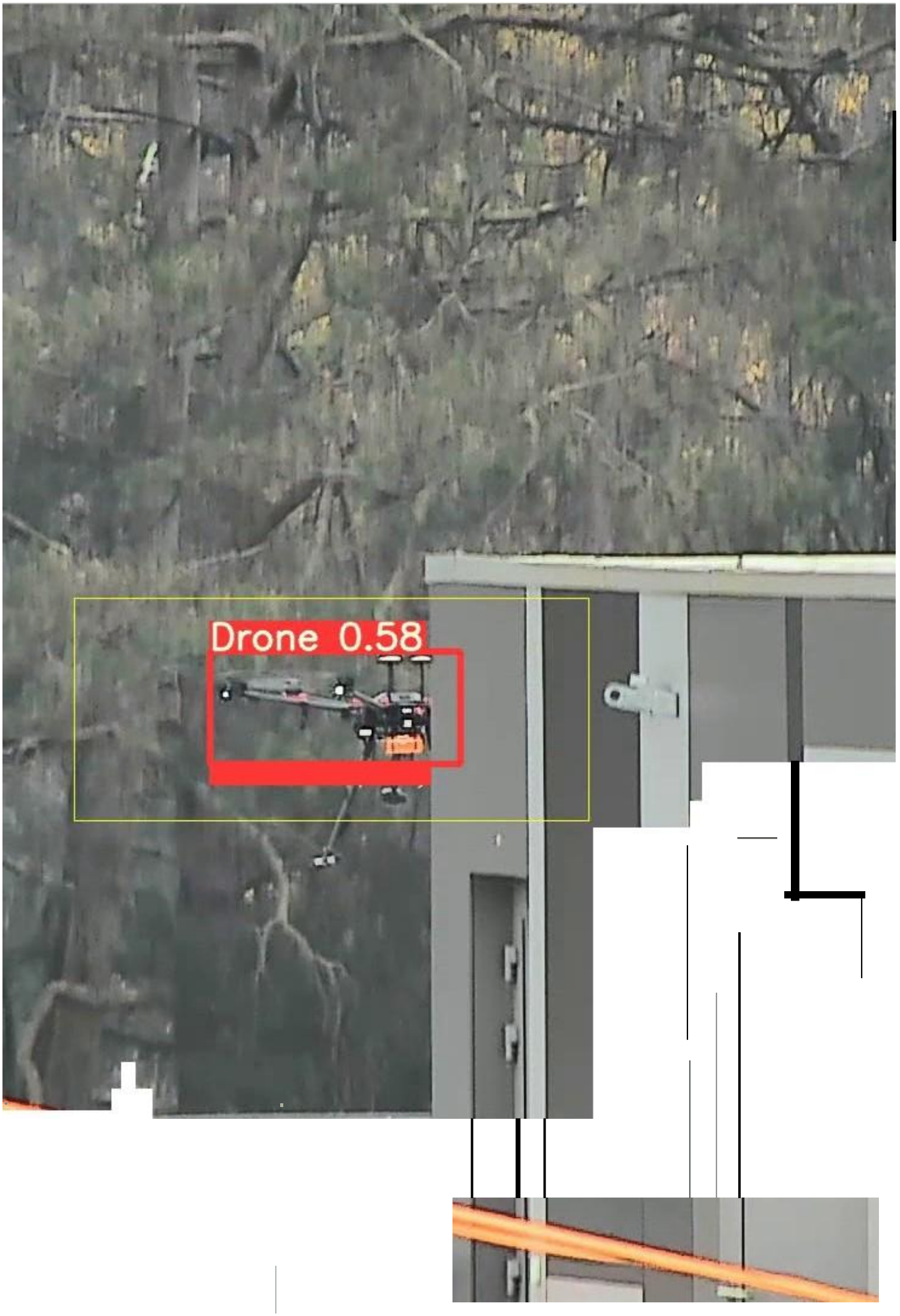


Kad visas prasības ir skaidri definētas, izstrādāts risinājums, izvēlēts(-i) integrators(-i) un definētas sistēmas specifikācijas, ir jāizstrādā risinājuma ieviešanas plāns. Tas būs jāizstrādā sadarbībā ar visām ieinteresētajām pusēm. Atkarībā no prasībām var būt nepieciešams izmantot vairākus integratorus ar papildu iespējām. Piemēram, uz UTM vai UAS orientēts programmatūras nodrošinātājs, kas apstrādā un vizualizē C-UAS aparatūras nodrošinātāja ģenerētos datus. Ja tas attiecas uz vietni, ieteicams apsvērt iespēju strādāt ar integratoriem, kuriem jau ir regulārs partneru kopums.
Tas uzlabos iespējas, ka risinājums tiks pilnībā integrēts un pārbaudīts un pierādīts. Darbs ar vairākiem piegādātājiem un viņu darba koordinēšana, lai nonāktu pie kopīga risinājuma, var būt sarežģīts uzdevums. Būtisks ir labs projektu vadītājs ar pieredzi attiecīgajā jomā. Turklāt līgumiem ar piegādātājiem jābūt detalizētiem un konkrētiem, lai skaidri noteiktu visu ieinteresēto pušu pienākumus un jo īpaši procesu saskarnes. Daudzos gadījumos var būt izdevīgi izmantot pakalpojumu modeļus ar īpašiem un detalizētiem pakalpojumu līmeņa līgumiem (SLA). Lai sāktu īstenošanu uz vietas, visām ieinteresētajām personām, iekārtām un infrastruktūrai jābūt gatavai. Ir svarīgi, lai C-UAS risinājumu nodrošinātājs(-i) pēc iespējas ātrāk saprastu šos ieviešanas priekšnosacījumus, lai samazinātu problēmas un izvairītos no ilgstošas kavēšanās. Īstenošanas posms ietvers uzstādīšanas, testēšanas un kalibrēšanas prasību laika plānošanu, operatoru apmācību pirms pieņemšanas un nodošanas operatīvajam personālam. Ja priekšnoteikumi netiek noteikti, tas var atspoguļot ievērojamu kavēšanos, pēdējā brīža darba slodzi un budžeta palielinājumu.

Šādu priekšnosacījumu piemēri ir:

- tehnoloģiju izmantošanas atļaujas (piemēram, frekvenču izmantošanas licencēšana);
- normatīvie apstiprinājumi;
- īpašas ēkas vai infrastruktūras izmaiņas;
- izmaiņas vidē, piemēram, veģetācijas likvidēšana, topoloģijas un vietas apkārtnes izmaiņas;
- vietas infrastruktūrā, kur var uzstādīt sensorus;
- kabeļu un tīkla infrastruktūra, tostarp tīkla savienojamība un telekomunikāciju vajadzības;
- elektrības pieejamība, kur tiks uzstādīti sensori.

Šajā sadaļā sniegtie padomi jāizmanto kā ceļvedis, lai integrētu C-UAS risinājumu parastā vietnes drošībā un darbībā.


Drone 0.58

9. CETURTĀ FĀZE – RISINĀJUMA ĪSTENOŠANA

Tālāk ir norādīti punkti, kas jāapkopo pirms ieviešanas posma sākšanas.

•risinājumu projektēšana;

•objekta apsekošana;

• skaidrs ieviešamā risinājuma prasību apraksts;

• draudu scenāriji;

• risinājums un sistēmas specifikācijas;

•arhitektūras projektēšana;

• ieviešanas prasības;

• ieinteresēto pušu procesi un plāni (kas, ko dara, kur un kad?).

Šīs fāzes beigās jums ir jābūt:

• ieviests risinājums, kas atbilst organizācijas un risku mazināšanas vajadzībām;

• atjauninātas darbības rokasgrāmatas ar procesiem un procedūrām;

•testu un kalibrēšanas atskaites;

• risinājuma pārejas plāns;

•atjaunināti ieinteresēto personu saraksti;

• pabeigtas apmācības un atjaunināti apmācību plāni;

• integrēt C-UAS risinājumu normālā darbībā;

• pilns fails, kas nodrošina pāreju no instalēšanas uz darbību.

4.1 KALIBRĒŠANA, SISTĒMAS UN C-UAS SISTĒMAS DARBĪBAS VERIFIKĀCIJA UN VALIDĀCIJA

Tehniskie un kalibrēšanas testi ir svarīgs posms ieviešanas posmā. Šie testi ir jāizstrādā un jāveic tā, lai parādītu visa risinājuma pareizu darbību. Šos testus varētu sadalīt mazākos testos, taču galu galā vajadzēja pārbaudīt visus elementus. Jāveic galīgā risinājuma pārbaude, kas aptver visas procedūras un procesus, kā arī visas sistēmas.

Pārbaudes procedūras un protokoli ir skaidri jādokumentē, lai testus varētu atkārtot ar regulāriem intervāliem. Rezultāti, visi sensoru dati un mijiedarbība jādokumentē pārskatos. Bieži vien to veic risinājuma piegādātājs, taču ir jāapsver neatkarīgas puses iesaistīšana gan šo testu izstrādē, gan izpildē.

Ārējie eksperti varētu būt noderīgi, jo īpaši iespiešanās testos. Iespiešanās testiem jābūt reprezentatīviem attiecībā uz identificētajiem riskiem, draudiem un scenārijiem konkrētajam risinājumam. Ārējais "sarkanās komandas" tests varētu nodrošināt, ka tie ir visaptverošāki.

Visos šajos testos ir jāpiedalās visām ieinteresētajām personām, kurām nākotnē būs nozīme risinājuma izmantošanā. Viņu ievade un apstiprināšana ir būtiska. Testi ir arī laba iespēja apmācīt ieinteresētās puses un demonstrēt risinājumu biznesam.

4.2 INTEGRĒŠANA AR ESOŠAJIEM PROCESIEM

Ieviestā risinājuma un sistēmas integrācija ar esošajiem procesiem (piemēram, drošības un drošības telpām), potenciāli rada nepieciešamību pēc jauniem procesiem. Atkarībā no draudu reaģēšanas līmeņa un atbilstošās tehnoloģijas izvēles šīs vajadzības būs atšķirīgas. Ietekmes un integrācijas analīze jāveic savlaicīgi, lai nodrošinātu vienmērīgu pāreju uz darbību, īpaši, ja šīm procesa izmaiņām ir nepieciešami iekšēji vai ārēji apstiprinājumi. Šīs analīzes galvenie rezultāti būtu jāatspoguļo pārejas, apmācības, darbības un apkopes plānos.

4.3 IZGLĪT UN APMĀCĪT OPERATORUS UN IEINTERESĒTĀS PERSONAS

Jauni vai atjaunināti procesi, papildu sistēmas un procesi, darba veidi un darbības izmaiņas radīs nepieciešamību apmācīt jaunus vai pārkvalificēt darbiniekus un ieinteresētās personas. Jaunu cilvēka un mašīnas saskarņu, uzraudzības rīku vai aparatūras lietošanas un apkopes lietotāji ir attiecīgi jāapmāca.

Ieteicama rūpīga analīze un apmācības plāni. Tajos būtu jāņem vērā tādi galvenie faktori kā personāla pieejamība un apmācības atkārtošanās. Misijai kritiskā personāla apmācībai parasti ir nepieciešama ilgāka iepriekšēja resursu plānošana, un tas rada problēmas kapacitātes plānošanā. Apmācību plāni, visticamāk, tiks sākti izstrādes posmā.

Ieinteresēto pušu apmācībai par C-UAS risinājumu jābūt prioritātei, lai nodrošinātu optimālu risinājuma darbību. Apmācībā jāiekļauj noteikumu (ES un vietējo) interpretācija un piemērošana.

Tā kā darbības vietas var mainīties no objekta robežas uz darbību zonās ap objektu, tas jāņem vērā apmācībā. Noteikumi un procedūras šajās zonās būs atšķirīgi, un apmācība palīdzēs komandām optimāli izmantot risinājumu. Kur iespējams, varētu būt lietderīgi apmācībās iesaistīt vietējās varas iestādes, LEA, kaimiņvalstis, lidostas, lidlaukus un UAS klubus. Tas varētu pārbaudīt vairāk C-UAS vērtību ķēdes elementu.

4.4 PIEŅEMŠANA UN NODOŠANA EKSPLUATĀCIJAI

Projekta pieņemšana un nodošana servisa režīmam attiecas uz pabeigta projekta pārsūtīšanu no projekta komandas uz operatīvo komandu, kas būs atbildīga par risinājuma aizsardzības uzturēšanu, darbību un piegādi vietnei. Nodošanas process ir būtisks solis, lai nodrošinātu, ka projekta mērķi ir sasniegti un galīgā aizsardzība tiek nodrošināta atbilstoši riska, dizaina un biznesa vajadzībām. Kad uzstādīšana, testēšana un apmācība ir pabeigta, risinājums ir jānodod operatīvajai komandai. Šis svarīgais solis bieži tiek ignorēts un novērtēts par zemu, kā rezultātā nodošana ir slikta, un ieviešanas posms pakāpeniski beidzas ar ražošanu. Tas var novest pie neskaidrām lomām un pienākumiem, kā arī pasliktināt vispārējo risinājumu efektivitāti.

Tāpēc projekta pieņemšanai un nodošanai ražošanai jāietver šādas darbības.

- Projekta komandai ir jāveic projekta galīgā pārbaude, lai pārliecinātos, ka tas atbilst noteiktajām risinājuma prasībām, tam nav defektu un atbilst kvalitātes standartiem.
- Projekta komandai jādokumentē risinājums, iekļaujot visus attiecīgos dokumentus, piemēram, projektēšanas dokumentus, testu rezultātus un plānus. Šī dokumentācija kalpos kā atsauce operatīvajai grupai.
- Nodošanas sanāksmes jāveic starp risinājuma ieviešanas komandu, operatīvo komandu un uzņēmuma īpašnieku, lai apspriestu procesus un prasības nodošanas procesam.
- Skaidri definējiet katra nodošanas procesā iesaistītā komandas locekļa lomas un pienākumus. Tas nodrošinās, ka ikviens apzinās savus pienākumus un var tos efektīvi pildīt.
- Ieviešanas komandai ir jānodod visas zināšanas un zināšanas operatīvajai komandai, lai tā varētu efektīvi uzturēt un izmantot risinājumu.
- Testa rezultāti jādokumentē.
- Visa pieeja sistēmām (IKT, paroles, piekļuves tiesības utt.) ir jāpārskata un jāmaina saskaņā ar vietējām drošības politikām un procedūrām.
- Jānoslēdz skaidra nodošanas dokumentācija un vienošanās starp īstenotāju un uzņēmuma īpašnieku.

10. ĪSTENOŠANAS POSMA KOPSAVILKUMS

Šīs fāzes beigās jums ir jāpabeidz risinājuma ieviešana saskaņā ar projektēšanas dokumentiem un jāpabeidz:

- organizācijai un risku mazināšanas vajadzībām atbilstoša risinājuma ieviešana;
- darbības rokasgrāmatu atjaunināšana ar procesiem un procedūrām;
- testēšana un kalibrēšana ar atskaitēm;
- apmācības un atjaunināti apmācību plāni;
- ieinteresēto personu sarakstu atjauninājumus;
- C-UAS risinājuma integrēšana normālā darbībā;
- risinājuma pārejas fails, kas nodrošina pāreju no instalācijas uz darbību;
- uzstādīšana un nodošana uzņēmuma īpašniekam.

5

Piektā fāze / darbojas

C-UAS risinājums

Pēc veiksmīgas riska analīzes, izstrādes un ieviešanas risinājums pāriet darba režīmā. Risinājums tagad ir jāintegrē projketsun jāpārvalda komandai, kas ir atbildīga par vietnes drošību. Procedūrās ir iekļauta visa informācija, kas nepieciešama, lai mazinātu riskus, pret kuriem risinājums ir izstrādāts, lai aizsargātu. Visi risinājumi, iespējams, būs unikāli, jo risinājuma sarežģītība un integrācija būs atšķirīga.

Šajā rokasgrāmatas pēdējā sadaļā ir papildu faktori, kas jāņem vērā, darbojoties ar ieviesto C-UAS risinājumu. C-UAS risinājums tagad ir jāintegrē parastajos drošības procesos un jāpārvalda saskaņā ar tās vietnes noteikumiem un noteikumiem, kurā tas tiek ieviests.

11. PIEKTĀ FĀZE – RISINĀJUMA DARBĪBA

Šajā posmā nepieciešamā informācija:

- ekspluatācijas rokasgrāmatas un procedūras;
- apmācīti un informēti operatori, kuri ir informēti par noteikumiem un procedūrām;
- testēšana un pārbaude, vai risinājums darbojas atbilstoši prasībām;

galveno darbības rādītāju (KPI) un SLA uzraudzība un iespējamā pielāgošana, kas jāievēro.

Risinājuma darbības laikā ir jāreģistrē tālāk norādītais, lai to varētu izmantot nepārtrauktai risinājuma atjaunināšanai.

- incidentu reģistrēšana (manuāla un automātiska sistēmas reģistrēšana),
- gūtās atziņas un problēmu saraksts,
- ziņojumi par incidentiem,
- atgriezeniskā saite no tiesībaizsardzības iestādēm un ārējām ieinteresētajām personām.

5.1 IESAISTĪTI UN INFORMĒTS IEINTERESĒTAS PERSONAS

Ieinteresēto pušu iesaistīšana un informēšana ir ļoti svarīga jebkura projekta vai darbības panākumiem. Drošības apsvērumu dēļ tas, protams, dažkārt var būt sarežģīti, un koplietotajai informācijai ir jāsastāv tikai no nepieciešamās informācijas, neapdraudot vispārējo drošību. Tālāk ir sniegti daži apsvērumi par to, kā iesaistīt un informēt ieinteresētās personas.

- Skaidri identificējiet ieinteresētās puses, to intereses un to, kas viņiem jāzina. Tas palīdzēs jums pielāgot komunikācijas un iesaistīšanās aktivitātes viņu vajadzībām. Tas ietver gan iekšējās ieinteresētās puses (darbiniekus, vadību), gan ārējās ieinteresētās puses (LEA, klientus, pārdevējus, partnerus).
- Izstrādājiet komunikācijas plānu, kurā izklāstīts, kā jūs sazināsities ar ieinteresētajām pusēm, ar kādu informāciju varat un ar kādu informāciju dalīsities un cik bieži. Rūpīgi analizējiet, kurus kanālus izmantot (e-pasti, sociālie mediji, informatīvie izdevumi un sanāksmes ir labākais veids, kā sasniegt ieinteresētās personas).
- Sniedziet regulārus atjauninājumus par projekta gaitu un visām izmaiņām, kas var ietekmēt ieinteresētās puses. Noteikti izceliet projekta pozitīvo ietekmi uz organizāciju un tās ieinteresētajām personām.
- Lūdziet atsauksmes no ieinteresētajām pusēm, lai izprastu viņu bažas un ieteikumus. Iekļaujiet viņu atsauksmes sava projekta plānošanā un izpildē.

- Ja iespējams, iesaistiet ieinteresētās puses, aicinot tās piedalīties sanāksmēs, semināros vai citās aktivitātēs.
- Esiet pēc iespējas pārredzamāks par projekta mērķiem, izaicinājumiem un riskiem. Tas palīdzēs veidot uzticēšanos ieinteresētajām personām un palielināt viņu uzticību risinājuma aizsardzībai.

Tāpēc ir ļoti svarīgi skaidri noteikt ieinteresēto pušu lomu, pienākumus un iesaistīšanos, un tā ir labi jāpārvalda. 26. attēlā ir RASCI tabulas piemērs, ko var izmantot ieinteresēto personu kartēšanai. Šāda tabula var būt tik plaša, cik nepieciešams, un tai jābūt pielāgotai risinājuma vajadzībām.

25. attēls: Ieinteresēto personu RASCI tabulas piemērs, kuru pēc vajadzības var paplašināt

Uzdevums	Ieinteresētā persona												
	Uzņēmuma īpašnieks	Vietējā apsardze	Risinājuma operators	Mīkstināšanas aktieri	Likuma izpilde	C-UAS risinājums piegādātājs(-i)	U-space pakalpojums pakalpojumu sniedzējs	UTM pakalpojums piegādātājs	Iestādes	Vietējā kopiena	Kaimiņi	Telecom operatoriem	valdība entitijām
Incidentu vadība													
Ieraksts un reģistrēšana	A	R	R	es	es	es	es	es	es	-	-	-	es
Komunikācija ar ieinteresētajām pusēm													
Informēt iestādes													
Kriminālistikas kolekcija													
Atjaunināt risku reģistru													
Mīkstināt													
Pieeja pilotiem, lai panāktu vieglu mazināšanu	R	R		R	A	A	R			es		R	R
Sniedziet informāciju par 4G-5G lidojumiem	R	R		R	A	R	R			S		S	S
UAS lidojumi													
Apstiprināt lidojumus	A	R		es	-	-	es	es	-	-	-	-	-
Integrēt lidojumu plānus													
Atjauniniet lidojumu žurnālus	A	A		A	S	C	A			es		A	A
Atjauniniet un apkalpojiet UAS													
Risinājuma darbība													
C2 vadība	A	A		A	R	C	A			es		S	R
Servisa līmeņa veiktspējas pārbaudes													
Operatoru grafiki													
Negadījumu reģistrēšana	A	A		A	S	C	A			es		es	es
Pievienojiet žurnālam incidentus, par kuriem ziņots no cita avota	C	C		C	A	C	A			C		C	A
Novērot un sniegt lidojuma datus	S	S		S	S	S	S			S		es	S
Operatoru apmācība													
Komunikācija ar ieinteresētajām pusēm													
Komunikācija ar uzņēmuma īpašnieku													

Uzdevums	Ieinteresētā persona												
	Uzņēmuma īpašnieks	Vietējā apsardze	Risinājuma operators	Mīkstināšanas aktieri	Likuma izpilde	C-UAS risinājums piegādātājs (-i)	U-space pakalpojums pakalpojumu sniedzējs	UTM pakalpojums piegādātājs	Iestādes	Vietējā kopiena	Kaimiņi	Telecom operatoriem	valdība entitijām
Iespiešanās testi													
Plānojiet testus													
Izpildi testus													
Baļķu pārbaude													
Sazinieties un ziņojiet par rezultātiem													
Risinājuma veiktspēja													
Plānojiet testus													
Pārbaudiet rezultātus													
Atjauniniet pārbaudes plānu													
Kalibrēšana													
Serviss un remonts													
Tehniskās apkopes grafiki													
Pakalpojumu līgumi													

R = atbildīgs | A = atbildīgs | S = atbalsta | C = konsultēts | Es = informēts | - = Nav piemērojams

5.2 C-UAS RISINĀJUMA ATJAUNOŠANA

Paredzams, ka jebkurš C-UAS risinājums visā tā darbības laikā tiks pakļauts vairākām izmaiņām: tas var saskarties ar tādām problēmām kā tehnoloģiskie sasniegumi, izmaiņas tiesiskajā regulējumā, iekšējās politikas vai procesa izmaiņas, vai arī tas var tikt pakļauts izmaiņām vietnes riska līmeņa pieņemšanā. Visos gadījumos ir ieteicams rūpīgi uzraudzīt faktorus, kas varētu ietekmēt konkrētu KI vietu vai publisko telpu. Izstrādājot risinājumu ceļvedi, kas tiek uzraudzīts un atjaunināts, tiek nodrošināts, ka CI vietnes vai publiskās telpas C-UAS risinājums atbilst vajadzībām un attiecīgi aizsargā vietni.

PADOMS

Risinājums ir paredzēts aizsardzībai pret konkrētu apdraudējumu un to mazināšanai. Ja mainās kāds elements, piemēram, drauds, vide, biznesa vajadzības vai drošības līmenis, visi posmi ir jāpārskata. Būtiski minimālie pasākumi ir jebkura risinājuma pamatā, un to izmantošana ar projektēšanas principiem un atvērtu arhitektūru atvieglos atjauninājumus un izmaiņas.

KPI var būt efektīva metode, lai noteiktu risinājuma veiktspēju laika gaitā un uzraudzītu, vai tā mērķi tiek sasniegti. To definēšana vai atlase var izrādīties sarežģīta, un KPI nevajadzētu beigties ar tehnisko detaļu identificēšanu, bet gan mērīt aizsardzības līmeni, kura sasniegšanai risinājums bija paredzēts. Precīzi definēti KPI atspoguļos piegādātāju un integratoru izmantoto sistēmu veiktspēju, un tos var izmantot, lai salīdzinātu risinājumu ar citu salīdzināmu ieviešanu.

Saskaroties ar tehnoloģiskām izmaiņām, var būt izaicinājums, jo ne tikai noteikšanas iekārtas un programmatūra ir pakļauta attīstībai, bet arī UAS, no kurām ir jāaizsargā. Piemēram, propelleru konstrukcijas izmaiņas un lidaparātu izgatavošanai izmantotais materiāls var padarīt UAS arvien grūtāk pamanāmu. Regulāru sistēmas testu un iespiešanās testu veikšana palīdzēs nodrošināt, ka risinājums joprojām ir labi pielāgots un atbilst pašreizējām vajadzībām.

Izvairīšanās no pārdevēja bloķēšanas ir vēl viena vispārpieņemta paraugprakse. Pārliecinoties, ka sistēmu pamatinfrastruktūra ir pēc iespējas agnostiska pārdevējam, ļaus dažādiem piegādātājiem vajadzības gadījumā veikt pakalpojumus, apkopi un atjauninājumus.

Strādājot gan ar aparatūras, gan programmatūras integratoriem, ir vērts izpētīt "pakalpojuma" pieeju risinājumam, nevis iegūt to savā īpašumā. Galvenā "pakalpojuma" modeļa priekšrocība ir tā, ka KI vietne vai publiskā telpa mazina tehnoloģiskās novecošanas risku. Protams, šādiem ieviešanas modeļiem ir nepieciešama vietai specifiska analīze, ņemot vērā citus faktorus, piemēram, tiesisko regulējumu, datu atrašanās vietu, datu īpašumtiesības, darbības izmaksas, sistēmas uzraudzību un SLA, iekšējās jaudas, zinātību un apmācības prasības.

Ir svarīgi rūpīgi apsvērt un savstarpēji vienoties par SLA ar pārdevēju vai integratoriem. Tie ir jānoformē detalizētā pakalpojumu līgumā, kurā ir aprakstīti savstarpējie pienākumi, kā arī C-UAS risinājumu mazināšanas stratēģijas. Arī šeit stabila sistēmas specifikācija un dizains, kas izriet no visaptverošas prasību analīzes, palīdz izvairīties no kļūmēm un turpmākām diskusijām, piemēram, saistībā ar viltus pozitīvu vai viltus negatīvu atklāšanu.

Piedāvātā piektā posma metodika šeit neapstājas. Kā norādīts rokasgrāmatas sākumā, šis ir apļveida process, kurā īstenošanas un darbības fāzēs gūtās atziņas, kā arī strauji mainīgais draudu attēls un iesaistītās tehnoloģijas novedīs pie nepārtrauktas izmantotā risinājuma pārskatīšanas.

12. DARBĪBAS POSMA KOPSAVILKUMS

Šis ir nepārtraukts risinājuma darbības process. Šajā posmā jums vajadzētu:

- uzraudzīt, vai risinājums atbilst specifikācijai un aizsargā pret identificēto risku;
- informēt ieinteresētās personas;
- nepārtraukti atjaunināt procesus un procedūras;
- ekspluatēt risinājumu atbilstoši biznesa vajadzībām, noteikumiem un noteikumiem;
- pārraudzīt izmaiņas biznesa vajadzībām, tehnoloģijām, ieinteresētajām personām, vidē, draudu attēliem utt. un, kad nepieciešamas izmaiņas, restartējiet visas šīs rokasgrāmatas fāzes – visa informācija un izmaiņas ir jāreģistrē un jāatjaunina.

Secinājums

Pēdējos gados UAS izmantošana, ko parasti dēvē par droniem, ir ieguvusi apgriezienus. Eiropā un pārējā pasaulē ir vērojams milzīgs UAS izmantošanas pieaugums dažādiem mērķiem. UAS pielietojums ir no civilām vajadzībām līdz komerciālai lietošanai ar jauniem uzņēmējdarbības modeļiem un izmantošanai aizsardzībā.

Šī rokasgrāmata piedāvā piecu posmu metodika KI īpašniekiem un tiem, kas ir atbildīgi par publisko telpu aizsardzību, par to, kā izstrādāt risinājumu UAS draudu mazināšanai. Šī metodoloģija sniedz plašu skatījumu uz problēmām, ko UAS rada KI un publiskajām telpām. Tas parāda, cik svarīgi ir izstrādāt risinājumus, kas ietver visu vērtību ķēdi – ieinteresēto pušu procesu integrāciju ar tehnoloģiskajām C-UAS sistēmām. Ja C-UAS sistēmas koncentrējas uz UAS noteikšanas, izsekošanas un identificēšanas tehnisko sarežģītību, C-UAS risinājums ietver visus aspektus un attiecīgās ieinteresētās puses, lai mazinātu no UAS radītos draudus. Metodikā ir aprakstītas darbības, kas jāņem vērā, veidojot C-UAS risinājumu.

Pirmā fāze Metodikas daļa ir padoms par to, kā sākt, iegūstot skaidru biznesa mandātu un skaidri definējot mērķus, ko un kur aizsargāt un pret ko. Tajā ir aprakstīti skaidri izstrādes principi un tas, kuras ieinteresētās personas jāiesaista procedūru un procesu izstrādē. Šajā fāzē ir aprakstīti būtiskie minimālie pasākumi, uz kuriem būtu jābalstās visiem C-UAS risinājumiem.

Otrā fāze aptver UAS riskus, kas jāpievieno pašreizējam risku reģistram, un to, kā definēt attiecīgos īpašos UAS draudu scenārijus atkarībā no tā, kura KI vai publiskā telpa ir jāaizsargā.

Pamatojoties uz šo analīzi, trešā fāze apraksta, kā izstrādāt risinājumu, kas atbilst biznesa vajadzībām un identificētajiem riskiem. Tajā ir aprakstīti svarīgi apsvērumi, ieviešot pamata minimālos pasākumus un kā tos izmantot, izvēloties pareizo mazināšanas līmeni un saskaņojot nepieciešamās tehnoloģijas. Projektēšanas fāzes noslēgumā tiks izstrādāta arhitektūra, ko var izmantot diskusijās ar piegādātājiem (kuri ieviesīs risinājumu) un ieinteresētajām pusēm (kas mazinās riskus).

Ceturtā fāze īstenošana. Tas izceļ nepieciešamību pēc sistēmas testēšanas un iespiešanās testiem, pirms ieinteresētās personas var tikt apmācītas un risinājums var pāriet servisa režīmā. Pareizo ieinteresēto personu identificēšana un to iesaistīšana ir būtiska, lai nodrošinātu, ka risinājums ir efektīvs un noteiktajā termiņā var veikt seku mazināšanu. Tā kā C-UAS, iespējams, būs vajadzīgas papildu ieinteresētās puses, salīdzinot ar parasto drošību, ir svarīgi sazināties un iesaistīt ar tām agrīnā stadijā un kopīgi izstrādāt risinājumu, procedūras un procesus.

Piektā fāze ietver risinājuma darbību, vajadzību informēt ieinteresētās personas un risinājuma atjaunināšanu. Nepārtraukta uzraudzība, precīzi definēti KPI, uzturēšana un atjauninājumi nodrošina, ka tiek pievienotas pašreizējās un jaunas vajadzības, kā arī papildu ieinteresētās personas.

Ir labi jāsaprot C-UAS biznesa vajadzības. Plašā un sarežģītā C-UAS pasākumu tehnoloģiskā ainava dažkārt var novirzīt uzmanību no sākotnējās biznesa problēmas, kas izraisīja nepieciešamību pēc C-UAS. Tas var novest pie neefektīvas resursu izmantošanas un sliktas tehnoloģiju izvēles, kas nespēs nodrošināt vajadzīgo risinājumu.

Visos risinājumos ir jāievieš pamata minimuma pasākumi. Tie veido pamatu, kas ļauj risinājumam attīstīties, mainoties riskiem un biznesa vajadzībām.
Turklāt var savienot specifiskās tehnoloģijas, kas nepieciešamas risku mazināšanai, un, ja nepieciešams, risinājumu var modificēt, lai aptvertu vides un risku izmaiņas.

Nav viena risinājuma, kas atbilstu visām ieviešanām. Izmantojot stabilus dizaina principus, būs vieglāk integrēt C-UAS risinājumu vietnes drošības darbībās, padarot to efektīvāku. Katrs metodoloģijas posms ir jāpielāgo konkrētajai videi un riskiem. Visas vietnes darbojas atšķirīgā vidē, ar dažādām attiecīgajām ieinteresētajām personām, dažādiem tirgiem, dažādām kopienām un tā tālāk.

Jāvelta pietiekami daudz laika, lai izpētītu vidi no UAS viedokļa. Izpratnes veidošana, runājot ar blakus esošajām KI vietām, vietējām iestādēm un pilsoniskajām kopienām, atvieglos C-UAS risinājumu.

Visbeidzot, C-UAS risinājuma izveides process nebeidzas ar šīs metodoloģijas pēdējo posmu. Attīstoties videi, mainās arī draudu ainava un tehnoloģiskā ainava. Tāpēc piecu fāzu metodika ir jāatkārto iteratīvi, lai C-UAS risinājums attiecīgi attīstītos.

Saīsinājumu saraksts un definīcijas

Saīsinājums vai termiņš	Apraksts
Aktīvie pasākumi	Pasākumi, kas paredzēti, lai fiziski apturētu atklāto UAS.
'uzmanīgs' UAS operators klasifikācija	UAS operatori, kuri apzinās un ievēro noteikumus, dronu kontroles pasākumus un drošu dronu darbību.
'neuzmanīgs' UAS operators klasifikācija	UAS operatori, kuri, iespējams, zina, bet var neievērot noteikumus, dronu kontroles pasākumus un kuru nodomi tiek uzskatīti par neapdomīgiem.
KI	Kritiskā infrastruktūra Aktīvs vai sistēma, kas ir būtiska vitāli svarīgu sabiedrības funkciju uzturēšanai.
'nezinošs' UAS operators klasifikācija	UAS operatori, kuri nezina un neievēro noteikumus, UAS kontroles pasākumus, drošu UAS darbību, bet kuru nolūki nav uzskatāmi par ļaunprātīgiem.
'noziedznieks' UAS operators klasifikācija	UAS operatori, kuri var zināt, bet neievēro noteikumus, UAS kontroles pasākumus un kuru nodomi tiek uzskatīti par naidīgiem.
C-UAS	Pretdarbība pret UAS ir likumīgi un droši atklāt, izsekot, identificēt un mazināt bezpilota gaisa kuģu sistēmu riskus.
C-UAS sistēma	C-UAS sistēma ir risinājuma sastāvdaļa, kas paredzēta C-UAS veikšanai
C-UAS risinājums	C-UAS risinājums ir C-UAS sistēmu, ieinteresēto pušu un procesu kopums, kas iesaistīts to darbībā
RASA	Virzītie enerģijas ieroči
Tiešais attālais ID	"Tieša attālināta identifikācija" ir sistēma, kas nodrošina lokālu informācijas apraidi par ekspluatācijā esošu bezpilota gaisa kuģi, tostarp bezpilota gaisa kuģa marķēšanu, lai šo informāciju varētu iegūt bez fiziskas piekļuves bezpilota gaisa kuģim.
EO/IR	Elektrooptiskais / infrasarkanais

Saīsinājums vai termiņš	Apraksts
Eskalācijas līmenis	Pastāvīgā un pieaugošā risku līmeņa apraksti. Eskalācijas līmeņu piešķiršanu katram riska rādītājam nosaka vietne, pamatojoties uz riska un draudu analīzes uztverto bīstamību.
GNSS	Globālās satelītu navigācijas sistēmas
Datorurķēšana	Datorurķēšana pārņem UAS operētājsistēmas saknes privilēģijas un izdod atbilstošas darbības. Šīs metodes trūkums ir tāds, ka tā attiecas tikai uz konkrētām operētājsistēmām un tīkla protokoliem, un, tāpat kā RF traucēšanas gadījumā, tā traucē citām rūpnieciskajām, zinātniskajām un medicīnas joslas ierīcēm.
IKT	Informācijas un komunikāciju tehnoloģija
ISO	Starptautiskā standartizācijas organizācija
JRC	Kopīgais pētniecības centrs
Kinētiskie pasākumi	Kinētiskās mazināšanas metodes bieži ietver kādu tiešu fizisku darbību, lai novērstu vai samazinātu UAS radīto risku.
KPI	Galvenais veiktspējas indikators
LEA	Tiesībaizsardzības aģentūra
Tīkla tālvadības pults ID	Tīkla attālā ID izmanto saziņu, izmantojot internetu no tīkla attālās ID pakalpojumu sniedzēja, kas tieši vai netieši saskaras ar UAS vai citiem avotiem, ja tīkla dalībnieki nav aprīkoti.
RASCI	Atbildīgs, atbildīgs, atbalstošs, konsultēts, informēts RASCI ir matrica (ti, diagramma, modelis vai ietvars), ko izmanto, lai palīdzētu identificēt visas projektā iesaistītās puses visas lomas un pienākumus. Tas skaidri nosaka, kurš strādā pie konkrēta projekta apakšuzdevuma.
RF	Radio frekvence
RF traucēšana	RF traucēšana izjauc RF savienojumu starp dronu un tā operatoru, radot lielu RF traucējumu apjomu. Kad RF saite (kas var ietvert Wi-Fi saites) ir pārtraukta, drons parasti vai nu nolaižas uz zemes, vai sāks manevru "atgriezties mājās". Tomēr šis paņēmiens neietekmē dronus, kas darbojas bez aktīvas RF saites. Daudziem signālu traucētājiem ir arī ierobežots efektīvais darbības diapazons — daži simti metru, kas nozīmē, ka sistēmai ir jāatrodas ļoti tuvu iebrūkošajai UAS, lai veiksmīgi mazinātu tās draudus, un tie nav efektīvi bez tiešas redzamības līnijas uz UAS. Jammeriem, kas spēj darboties lielos attālumos un ārpus redzamības līnijas, jābūt ievērojami jaudīgākiem, taču jaudīgāki traucētājierīces arī rada lielāku traucējumu risku likumīgai saziņai.

Saīsinājums vai termiņš	Apraksts
Riska vadība	UAS draudu procesa elements, kas izmanto draudu integrācijas un draudu analīzes konstatējumus, lai padziļināti novērtētu KI vietnes specifiskos riskus un atbilstošos mazināšanas pasākumus.
Riska rādītājs	Aprēķināts, iespējamību reizinot ar ietekmi.
SLA	Pakalpojuma līmeņa līgums
Maldināšana	Ļauj pārņemt kontroli pār vai nepareizi novirzīt mērķa UAS, ievadot tai viltus saziņas vai navigācijas saiti. Tomēr viltošanas sistēmas ir tehniski ļoti grūti izveidot un ieviest, un tās var nebūt universālas pret visām UAS. Piemēram, bezpilota lidaparāti, kas ir būvēti ar aizsargātām sakaru saitēm, varētu būt izturīgi pret viltošanas uzbrukumiem.
Draudu analīze	UAS draudu procesa elements, kura mērķis ir izprast UAS ekosistēmu.
Draudu gaita darbības analīze	Draudi integrācijas elements, kas sastāv no visas izpratnes par draudiem sapludināšanas ar vietnes un iespējamo ievainojamību apsekojuma analīzi, lai noteiktu visticamākos draudus un visietekmīgāko draudu scenāriju.
Draudu integrācija	UAS draudu procesa elements, kas izmanto draudu analīzes rezultātus, lai izceltu visticamākos un bīstamākos UAS draudus.
Draudu šķirošana	Fāze tūlīt pēc UAS draudu procesa. Tajā aprakstīts taktiskā līmeņa lēmumu pieņemšanas process, kas veidos sistēmas reakciju uz UAS iebrukumu. Šī fāze atspoguļo pamata saikni starp riska novērtējumu un C-UAS pasākumu īstenošanu.
UAS	Bezpilota lidaparātu sistēmas Bezpilota lidaparāts un aprīkojums tā attālinātai vadībai.
UAS ģeogrāfiskais zonā	Kompetentās iestādes izveidota gaisa telpas daļa, kas atvieglo, ierobežo vai izslēdz UAS darbību, lai novērstu riskus, kas saistīti ar drošību, privātumu un personas datu, drošības vai vides aizsardzību, ko rada UAS darbība.
UAS operators	Jebkura fiziska vai organizācija, kurai pieder vai nomā UAS.
UAS risku reģistrs	Identificēto risku saraksts, sadalot problēmu, kas noteikta pēc draudu veida.

Saīsinājums vai termiņš	Apraksts
UAS draudi process	Sniedz vadlīnijas CI operatoriem, lai palīdzētu izprast un efektīvi pārvaldīt UAS riskus.
UTM	Bezpilota gaisa kuģu sistēmas Gaisa satiksmes pārvaldība Visplašākajā nozīmē Starptautiskā civilās aviācijas iestāde UTM definē kā "īpašu gaisa satiksmes pārvaldības aspektu, kas droši, ekonomiski un efektīvi pārvalda UAS darbību, nodrošinot aprīkojumu un nevainojamu pakalpojumu kopumu sadarbībā ar visām pusēm un ietverot gaisa un zemes funkcijas." Līdz ar to UTM sistēma "nodrošina UTM, sadarbojoties cilvēku, informācijas, tehnoloģiju, iekārtu un pakalpojumu integrācijai, ko atbalsta gaisa, zemes vai kosmosa sakari, navigācija un novērošana".
VIP	Ļoti svarīga persona Persona ar ievērojamu nozīmi vai ietekmi, kurai nepieciešama īpaša attieksme.

Kastīšu saraksts

Attēlu saraksts

SAZINĀŠANA AR ES

PERSONĪGI

Visā Eiropas Savienībā ir simtiem Europe Direct centru. Jūs varat atrast sev tuvākā centra adresi tiešsaistē (european-union.europa.eu/contact-eu/meet-us_en).

PA TELEFONI VAI RAKSTI

Europe Direct ir pakalpojums, kas atbild uz jūsu jautājumiem par Eiropas Savienību. Jūs varat sazināties ar šo pakalpojumu:

- pa bezmaksas tālruni:00 800 6 7 8 9 10 11 (noteikti operatori var iekasēt maksu par šiem zvaniem),
- ar šādu standarta numuru: +32 22999696,
- izmantojot šādu veidlapu:european-union.europa.eu/contact-eu/write-us_en.

INFORMĀCIJAS MEKLĒŠANA PAR ES

ONLINE

Informācija par Eiropas Savienību visās oficiālajās ES valodās ir pieejama tīmekļa vietnē Europa (european-union.europa.eu).

ES PUBLIKĀCIJAS

ES publikācijas varat apskatīt vai pasūtīt vietnēop.europa.eu/en/publications . Vairākas bezmaksas publikāciju kopijas var iegūt, sazinoties ar Europe Direct vai vietējo dokumentācijas centru (european-union.europa.eu/contact-eu/meet-us_en).

ES TIESĪBU AKTI UN SAISTĪTIE DOKUMENTI

Lai piekļūtu juridiskai informācijai no ES, tostarp visiem ES tiesību aktiem kopš 1951. gada visās oficiālajās valodu versijās, apmeklējiet vietni EUR-Lex (eur-lex.europa.eu).

ATKLĀTI DATI NO ES

Portāls data.europa.eu nodrošina piekļuvi ES iestāžu, struktūru un aģentūru atvērtajām datu kopām. Tos var lejupielādēt un atkārtoti izmantot bez maksas gan komerciāliem, gan nekomerciāliem nolūkiem. Portāls nodrošina arī piekļuvi daudzām datu kopām no Eiropas valstīm.

Eiropas Komisijas zinātnes un zināšanu dienests

Kopīgais pētniecības centrs

JRC misija

Kā Eiropas Komisijas zinātnes un zināšanu dienestam Kopīgā pētniecības centra misija ir atbalstīt ES politiku ar neatkarīgiem pierādījumiem visā politikas ciklā.

ES zinātnes centrs
joint-research-centre.ec.europa.eu

@EU_ScienceHub

ES Zinātnes centrs – Kopīgais pētniecības centrs

ES zinātne, pētniecība un inovācijas

ES zinātnes centrs

ES zinātne

Publications Office
of the European Union