O S T A L E K R I V I Č N O P R A V N E N A U K E

https://doi.org/10.7251/CEST1423243D UDK 623.746:343.3/.7

DETEKCIJA I ZAPLJENA DRONOVA KOJI SE KORISTE ZA ILEGALNE AKTIVNOSTI

prof. dr Adnan Duraković

redovni profesor Pravnog fakulteta Univerziteta u Zenici, dadnan07@gmail.com

akademik prof. dr Miodrag N. Simović

redovni član Akademije nauka i umjetnosti Bosne i Hercegovine, redovni član Evropske akademija nauka i umjetnosti, inostrani član Ruske akademije prirodnih nauka, redovni profesor Pravnog fakulteta Univerziteta u Bihaću, profesor emeritus, vlado_s@blic.net.

Apstrakt. *Zahvaljujući nedavnim tehnološkim dostignućima, dostupna je i nova generacija jeftinih, malih, bespilotnih letjelica (UAVs). Te letjelice, koje se često nazivaju dronovima, omogućavaju aplikacije bez presedana, ali se istovremeno pojavljuju nove prijetnje povezane sa njihovom mogućom zloupotrebom (npr. krijumčarenje droge, teroristički napadi, špijunaža).*

Dron je obično male veličine, s mogućnošću vrlo brzog leta u manevru, što čini ove letjelice kategorijom ciljeva koje je mnogo teže otkriti u poređenju s tradicionalnim letjelicama. Ove letjelice se mogukoristiti unutar vazdušnog prostora jedne zemlje ili u pograničnom pojasu, odnosno jurisdikcijama više zemalja. U tom kontekstu, sistemi za detekciju, prepoznavanje i zaustavljanje dronova suočavaju se sa brojnim problemima.

Mnoge policijske i vojne organizacije pokušavaju da izvuku iskustva iz upotrebe i suzbijanja upotrebe dronova iz Iraka, Avganistana i Ukrajine kako bi preduzeli odgovarajuće mjere za suzbijanje njihove zloupotrebe. Pošto upotreba dronova postaje sve popularnija i u privredne, naučne, sportske i privatne svrhe, aktuelizovano je pitanje njihove bezbjednosti i potrebe za donošenjem zakonske regulative kako bi se spriječili mogući incidenti.

U ovom radu razmatraju se glavni izazovi u vezi sa problemom identifikacije dronova, koji uključuju otkrivanje, moguću verifikaciju i klasifikaciju. U fokusu su načini detekcije, verifikacije i zaustavljanja i zapljene dronova koji vrše ilegalne aktivnosti. S tim u vezi, dat je pregled najrelevantnijih tehnologija koje su u savremenim sistemima nadzora stavljene u mrežu prostorno distribuiranih senzora kako bi se obezbijedila potpuna pokrivenost nadgledanog područja. Preciznije, glavni fokus je na ključnim tehnologijama zbog svoje niske cijene i sposobnosti rada na relativno velikim udaljenostima.

Ključne riječi: *dron, detekcija, droge, trgovina, forenzika.*

1. UVOD

Teškoće sa kojima se susreću sadašnji sistemi koji koriste avioni uzrokuju da se dronovikoriste često jer su mnogo manji, lete na malim visinama, velikih su manevarskih sposobnosti, u stanju su da se kreću unutar

urbanog područja gotovo identično kao ptice u radarskim sjenkama visokih objekata. Stoga se njihovo otkrivanje, identifikacija i onesposobljavanje može efikasno vršiti samo na vrlo malim udaljenostima. Sistemi nadzora i odbrane ometani su često slabom vidljivošću, noću, meteorološkim prilikama, topografskim okruženjem sa puno prepreka, a poteškoću predstavlja i korištenje „rojeva“ ovih letjelica od kojih neke služe za odvlačenje pažnje i iscrpljivanje sistema odbrane, dok druge treba da odigraju osnovnu ulogu. Zadatak je da se u realnom i vrlo kratkom vremenskom intervalu detektuje, identifikuje i klasifikuje letjelica i donese ispravna odluka o postupanju prema njima.

Narko-dron je komercijalni mali dron[1] koji nosi razne količine tereta[2]. Gotovo svakodnevno lete takvi dronovi i nose terete i na meksičkoj granici prema SAD[3]. Osim ovih malih dronova, narko-karteli pokazuju inovativnost pa prave ili kupuju *heavy lifter* dronove[4] koji mogu ponijeti i mnogo veće količine

---

1 Dronovi su već godinama jedan od najpopularnijih tehnoloških proizvoda na izuzetno bogatom i zahtjevnom tržištu moderne tehnologije. Svoju popularnost mogu zahvaliti i činjenici da ljudi obožavaju posmatrati svijet iz vazduha, pa se mnogi upravo zbog toga odlučuju na kupovinu drona.

2 Španska policija je krajem jula 2021. godine zaplijenila ogroman dron, do sada najveći upotrebljavan za krijumčarenje droge u Evropi. Riječ je bespilotnoj letjelici francuske bande koja se bavila ilegalnom trgovinom narkoticima „uvezenim” iz Maroka u Španiju, preko šireg područja Gibraltarskog moreuza. U zajedničkoj akciji francuske i španske policije, koja je uslijedila nakon višemjesečnog operativnog rada, osim drona zaplijenjena je i veća količina droge, a četiri osobe su uhapšene – tri u Francuskoj i jedna u Španiji.

Podzemlje je i do sada koristilo male dronove, ali ovaj je bio takvih dimenzija da je ozbiljno ugrožavao vazdušni saobraćaj. Raspon krila mu je bio oko četiri i po metra, a nosivost čak 150 kilograma tereta, u ovom slučaju – droge. Dostiže brzinu od oko 170 kilometara na čas i visinu leta do 2.000 metara. U vazduhu se mogao zadržati čak sedam sati.

Kako navodi španski list „Pais”, dron je mogao da leti automatski, mijenjajući pravac na određenim tačkama leta, ali se ovom bespilotnom letjelicom moglo upravljati i ručno, komandama zadatim sa zemlje. Dron je letio na manjim visinama – da bi se izbjeglo otkrivanje, ali i uštedjelo gorivo. Ovoj letjelici ne treba pista, predviđeno je da polijeće i slijeće vertikalno.

Za polijetanje i slijetanje koristi četiri elektromotora s propelerima, dok je peti motor, motor s unutrašnjim sagorijevanjem koristi benzin i pokretao je potisni propeler za horizontalnilet. U nosu vazduhoplova, gdje su obično kamere, nalazi se prazan prostor za teret.

Utvrđeno je da je ova letjelica proizvedena u Kini, a pretpostavlja se da je za nju plaćeno do 150.000 evra, a možda i znatno manje.

3 Na američko-meksičkoj granici toliko je nedozvoljenih aktivnosti da niko pouzdano ne zna koliko ih je realizovano. Osim toga, narko-karteli koriste dronove i za druge aktivnosti kao što su obavještajne – kojima prate policijske i granične aktivnosti, zatim za obmanjivanje policijskih snaga odvlačeći ih na lažna mjesta dostave – dok se prave isporuke za to vrijeme odvijaju na drugim mjestima.

4 Ovaj dron je potencijalna tačka pogodnosti za ličnu i profesionalnu upotrebu.

droge preko granica[5]. Zabilježeni su slučajevi da su osobe koristile dronove za isporuku droge i u zatvore na tačno određene prozore. U posljednje vrijeme zabilježeni su brojni incidenti izazvani dronovima koji su ljudima padali na glave, udarali u avione, kada su neoprezni vlasnici bespilotnih letjelica ometali gašenje požara ili kada su ljudi puškama obarali dronove misleći da ih neko špijunira[6].

Kada su u pitanju dronovi i autonomna vozila, mnogo veće terete prenose autonomna podvodna vozila[7]. Daljinski upravljani *narco-drones, narco-subs* ili *underwater drones* su izrazi koji se koriste da bi se označila ova plovila i letjelice (Siddiqi et al. 2022: 2.641–2.670). Bilo da su autonomne ili daljinski upravljane, mnogo ih je lakše zaplijeniti nego doći do njihovih operatera ili vlasnika[8] (Klein, McLaughlin 2022).

Narko-dronovi su jedan sasvim novi fenomen[9] za koji čak ni SAD nemaju u potpunosti cjelovitu strategiju iako su vodili ratove protiv švercera

---

Fleksibilnost koju nudi ovaj dron odnosi se na slobodu kretanja od drugih standardnih vozila i sposobnost za podizanje i isporuku teških predmeta. Zamislimo, na primjer, građevinsko okruženje u kojem se određeni alati i zalihe transportuju sa različitih visina bez potrebe da radnici putuju.

5 Održive metode trgovine drogom putem dronova postoje i u slučajevima kolumbijskih operacija trgovine narkoticima, a dokazuje ih otkriće kolumbijske policije narko-drona sa 130 kilograma kokaina u sektoru Bahia Solana u Chocou. Sumnjalo se da je narko-dron angažovan od narko-kartela Clan del Golfo (Schmersahl 2011: 9).

6 Iako je jasno da glavni posao oko letenja obavlja hardverski dio, činjenica je da se u unutrašnjosti drona nalazi vrlo složen sistem koji zapravo omogućava let dronom. Što se tiče hardverskih komponenti, u svojoj osnovi svaki dron ih ima nekoliko, i to važnih. Tijelo drona, s nožicama za sigurno slijetanje, glavni je element drona na koji se vežu razni drugi hardverski dijelovi. Na tijelo drona pričvršćena je jedna (ili više) kamera, čiji je zadatak praćenje leta drona i snimanje događanja ispod linije leta.

Rotori drona sastoje se od motora i propelera. Zavisno od svoje veličine i karakteristika, dronovi imaju različite motore koji pogone različite veličine propelera. Na dronovima se obično nalaze četiri rotora.

Svi dronovi su opremljeni senzorima, među kojima su najvažnija dva (Accelerometer and Altimeter). Prvi je zadužen za praćenje brzine leta, dok drugi senzor korisniku u svakom trenutku otkriva visinu leta, ali i pomaže prilikom spuštanja i podizanja drona. Dronovi mogu biti opremljeni i raznim drugim senzorima koji pomažu u upravljanju dronom.

7 Jedno od takvih vozila je zaplijenila i španska policija i nosilo je 200 kilograma droge (Drug smuggling, 2022).

8 Tako su meksički karteli koristili kako dronove sa fiksnim krilima koji mogu nositi više tereta i letjeti dalje, tako i dronove sa rotorima. Oni ne samo da su koristili komercijalne i uvezene dronove, nego su i izrađivali vlastite.

9 Korištenje dronova u Srbiji takođe doživljava ekspanziju, a dozvole za upravljanje njima izdaje Direktorat civilnog vazduhoplovstva. U suprotnom, za upravljanje dronom bez dozvole, prema Zakonu o vazdušnom saobraćaju, zaprijećene su

droga i imaju iskustvo sa dronovima iz ratova u Iraku, Avganistanu i drugim zemljama. U njihovom iskustvu su bili letovi malih aviona sa drogama preko meksičke granice, kasnije preleti ultralakih letjelica, pa kako su SAD radarski pojačano pokrivale teritoriju pograničnog dijela, tu ulogu su preuzeli dronovi. Naime, policijske snage SAD su osamdesetih godinaprošlog vijeka koristile sofisticirane radare da odgovore na tzv. „Cocaine Cowboys“[10] koji su koristili privatne avione za krijumčarenje droga. Posljedično, krijumčari su mijenjali rute letenja, da bi počeli da kopaju i koriste tunele sa klimatizacijomi poluuronjene čamce na morskoj granici.

Za razliku od svih ovih načina krijumčarenja, kod dronova ne postoji fizička veza droge i letjelice sa pošiljaocem, osim da se iz njega forenzičkim putem koriste sofisticirani podaci. Mali komercijalni dronovi, istina, nose male količine droge, ali se oni svakodnevno koriste za prenos pošiljki[11]. Koliko je letova dnevno i koja je njihova uloga, kao i kolika jekoličina droge koja se prenosi – nema pouzdanih podataka. Tome pogoduju organizacioni nedostaci onih koji motre na granice kroz nedostatak isprobane i verifikovane metodologije osmatranja i presretanja, nedostatak osmatrača i raznih senzora za njihovu detekciju, kao i opreme za njihovu pljenidbu.

novčane kazne od 10.000 do 50.000 dinara za fizička, odnosno od 25.000 do milion dinara za pravna lica. Iz Direktorata upozoravaju da dronovi nisu igračke i da je svako ko njima upravlja odgovoran za svoju i tuđu bezbjednost i da je dužan da poštuje propise koji se primjenjuju u Republici Srbiji: zabranjena je upotreba dronova težih od 150 kg; dron može da leti samo danju i da sve vrijeme da bude u vidnom polju onog ko njime upravlja; zabranjeno je izbacivanje predmeta i tečnosti i nošenje spoljnog tereta; nije dozvoljeno upravljati dronom iz vozila u pokretu; najstrože je zabranjen transport ljudi, životinja i opasnih materija; nije dozvoljeno korištenje drona kojim u potpunosti upravlja računar i jedna osoba može upravljati samo jednim dronom.

Iz bezbjednosnih razloga bespilotna letjelica uvijek mora biti na horizontalnoj udaljenosti većoj od 500 metara od infrastrukturnih objekata, državnih i ostalih ustanova i saobraćajnih sredstava i mora biti udaljena najmanje 30 metara od ljudi koji se nalaze u rejonu letenja.

Iako su dronovi odavno postali popularni, predviđanja kažu da tokom sljedećih godina možemo očekivati još veću potražnju za ovim uređajima i da će se njihova prodaja brojati u milionima. S druge strane, nesavjesno upravljanje njima otvara mogućnosti za ugrožavanje bezbjednosti na različite načine.

[10] Kokainski kauboji: Kraljevi Majamija (engl. Cocaine Cowboys: The Kings of Miami) je šestodijelna dokumentarna serija iz 2021. godine koja prati uspon i pad narko-bosova u Majamiju – Sala Magluta i Vilija Falkona. Njih dvojica su na kraju optuženi u jednom od najvećih slučajeva droge u istoriji SAD, optuženi za ilegalno krijumčarenje 75 tona kokaina u zemlju.

[11] Tipični dron je sa četiri ili šest rotora sa vrijednošću od nekoliko stotina do nekoliko hiljada dolara, koji nose do 35 funti tereta (Wright 2020).

2. SPORNA PITANJA

Pitanja koja se postavljaju kod narko-kriminala i korištenja dronovasvode sena tri problema: (1) prijetnja i rizik transnacionalnih kriminalnih organizacija koje koriste dronove; (2) razvoj vazdušne trgovine narkoticima i nedostatak strategije za otkrivanje, praćenje i sprečavanje i (3) korištenje vojnih sposobnosti u obliku aktivne i pasivne protivmjere za podršku„operativne kontrole" niskog vazdušnog prostora iznad granice (Schmersahl 2011:3).

Zapadni vojni izvještaji i istrage otkrili su i proširenu upotrebu lažnih dronova u ratu u Avganistanu, Iraku, Siriji i Ukrajini. Uz to, sve veći broj napada modifikovanim dronovima pokazuje ograničenje postojeće tehnologije za njihovo zaustavljanje i neutralisanje (npr. RF ometač[12], ometač ručne puške, dresirani orao) (Chaari, Al-Maadeed 2020).

Tehnologija borbe protiv dronova odnosi se na sisteme koji se koriste za njihovo otkrivanje i onesposobljavanje. Postojeće tehnologije ne mogu kontrolisati i neutralizovati autonomne pilotske dronove bez njihovog uništenja i imaju mnogo nedostataka. Džemer uređaj[13] može prekinuti radio-frekvencijske veze s dronovima, ali ne može uništiti autonomne pilotske dronove.Pored toga, radar ne može otkriti dronove na malim visinama izaustaviti dronove koji rade s komunikacijom frekvencijske veze većom od 6 GHz. Laserski snop za karbonizovanje i uništavanje svih vrsta dronova, uključujući programabilni dronjedno je od novih i perspektivnih rješenja. Tehnologija za zaustavljanje ilegalnog drona nije ni izbliza visoko efikasna, a na sadašnjem nivou je i vrlo skupa (Schmersahl 2011:3).

3. DRON KAO IZVOR VAŽNIH FORENZIČKIH PODATAKA

Jednom kada je zaplijenjen, dron je izvor važnih forenzičkih podataka.

Forenzička ispitivanja dronova su usmjerena na ispitivanje hardvera, odnosno tijela drona, serijskih brojeva, motora, propelera, baterija, tereta i senzora, softvera i sadržaja koje je dron generisao u obliku datoteka, GPS podataka. Sve to sa ciljem da bi se identifikovao dron ako je registrovan, njegov vlasnik ili osoba koja je uzurpirala dron – da bi se nedvosmisleno utvrdio način upotrebe drona (npr. nagib drona, nagib kamere i smjer leta ukazuju na to da li je na toj lokaciji samo prelijetao ili snimao), odnosno potrošnja baterija, uz

[12] To je ometač radio-frekvencija, kao posebno dizajniran uređaj koji pomaže u zaštiti uređaja od prisluškivanja. Štiti sve vrste alarma, kontrolne ploče itd.

[13] Profesionalni džemer (engl. jammer) – ometač je uređaj koji se godinama uspješno koristi u svijetu. Za razliku od dosadašnjih modela, ovaj model džemer aparata dizajniran je da bez problema može raditi 24 sati dnevno, sedam dana sedmično, 365 dana u godini. Ometač (džemer) ometa rad svih mobilnih mreža od 850MHz do 2500MHz. Prednost ovih aparata je što su rađeni po licenci vojne tehnologije (*https://www.cis.hr/www.lexis/pojmovi_view.php?l=J).*

procjenu da li je dron nosio teret i koje težine – ako on nije nađen. Od značaja su grafički prikazi, uz rekonstrukciju putanje leta sa značajnim tačkama polijetanja i slijetanja.

Za pristup podacima potrebni su portovi[14] na dronu, kartice, pristup podacima bez mjera ili sa mjerama kojima se neutrališu antiforenzičke mjere onoga ko je koristio dron. Na samom dronu mogu biti instalirani softveri koji onemogućavaju pristup podacima bez lozinke ili koji brišu podatke nakon nekog vremena ili daljinski aktiviraju brisanje podataka. Mnogo tehnologija je u igri s obzirom na način kako se dronovi zaustavljaju u letu – fizičkim ili elektronskim mjerama.

Pametni telefoni igraju važnu ulogu u procesu upravljanja dronovima. Oni imaju dvije svrhe u interakciji telefon–dron, gdje se korisnici mogu prebacivati između ručnih i automatskih/autonomnih načina upravljanja. Dronovi preko pametnih telefona šalju podatke o statusu drona, kao i slike i video putem vaj-faj komunikacijskih kanala. Pametni telefon može izdati skup unaprijed definisanih naredbi koje mijenjajurad rotora drona za promjenu položaja. Alternativno, algoritmi za obradu mogu se realizovati na pametnom telefonu klijenta i generisati naredbe koje dron vraćaju u autonomne načine letenja.

Za veće udaljenosti prenosa podataka između dronova i pametnih telefona koristise radio-komunikacijski kanal od 2,4 GHz. Prenos podataka vrši se između odašiljača i kontrolora prijemnika spojenog na pametni telefon putem USB kabela i montiranog na prijemniku na sklopu drona. Autonomna navigacija drona može se postići na osnovu proračuna letai obrade vizije leta koja se realizuje na pametnom telefonu. Lažni agent može koristiti lažnu adresu elektronske pošte i prijaviti se u mobilnu pametnu aplikaciju drona i sakriti svoj identitet dok dron leti, te počiniti neke krivične radnje kao što je „povreda vazdušnog prostora“ ili sprovođenje nezakonitih aktivnosti kao što je fotografisanje strateških ili osjetljivih lokacija kod onih letjelica koje imaju male ili nikakve sigurnosne kontrole (Baig et al. 2022).

U slučaju da je dron upleten u kriminalne aktivnosti, njegovo oduzimanje i naknadna analiza u laboratoriji za digitalno forenzičko istraživanje ključni je dio postupka prikupljanja i analize dokaza. Izazovi povezani s forenzikom drona uključuju dekompoziciju drona i dijelovakoji se nalaze rasuti unaokolo, što zahtijeva skupljanje materijala i njegovo povezivanje. Oni digitalni forenzički alati koji su upotrebljivi na određenim dronovima i komponentama neće moći biti upotrijebljeni na drugim tipovima dronova i drugim komponentama, tako da je za potpun forenzički postupak potrebno mnoštvo softvera i hardvera. Pored toga, pojedini dronovi nemaju određenih portova i moguć je samo bežični prenos slika, što predstavlja ozbiljan problem.

[14] Portovi (ulazi) su neophodni za spajanje periferije na računar, odnosno služe kao sredstvo preko kojeg računar komunicira s periferijom ili obrnuto – periferija s računarom.

Pristup podacima sa drona može biti onemogućen jer su forenzičari blokirani nemogućnošću pristupa usljed mehanizama zaštite koje je instalirao ili sam proizvođač ili je to učinjeno naknadno manipulacijom visokotehnološki edukovanog vlasnika ili korisnika. Ako je vlasnik i identifikovan, on možda neće biti voljan da omogući pristup podacima, čak i pod prijetnjom zakonske kazne.

3.1. Fleš memorija i RAM

Fleš memorija[15] i RAM[16] mogu izgubiti podatke nakon pada, ako se baterija drona isprazni. Podaci mogu biti enkriptovani, što otežava ili onemogućava očitanje. Poznato je da komponente drona imaju različite identifikacione brojeve. Takve informacije mogu sadržavati serijske brojeve drona (dodijelio ih proizvođač), njegovih propelera, motora, kamera i ugrađenih GPS uređaja. Zavisno od vrste drona, takve informacije mogu, ali i ne moraju biti dostupne istražiteljima, ali ako su dostupne– korisno je utvrditi vezu između drona i njegovog potencijalnog korisnika (Baig et al. 2022).

Tokom samog leta dron u svojim datotekama bilježi podatke koji su generisani tokom leta, a kada se skinu sa drona– moguće je rekonstruisati različite aspekte kretanja i operacija drona, kao što su: vremenske odrednice, trajanje leta, brzina, snage, skretanje, nagib, kotrljanje i visina. Ako su podaci čitljivi, moguć je i grafički prikaz leta drona, što sliku čini preglednom i daje jasne okvire za zaključke o prirodi leta i aktivnostima. Forenzika dronova je dakle usmjerena na preuzimanje i korištenje podataka o mrežnom prometu između drona i kontrolora, preuzimanje zapisnika iz dnevnika koje automatski vodi dron u odgovarajućim datotekama, analizu sistema datoteka i skidanje i pregledavanje produkata kao što su fotografije i video-snimci.

[15] Fleš memorija ili Fleš EEPROM (engl. Electrically-Erasable Programmable Read-Only Memory) je vrsta EEPROM elektronske memorije koja čuva podatke kada je isključen napon i gdje se pisanje, mijenjanje i brisanje vrši elektronskim putem. Za razliku od „uobičajene“ EEPROM memorije, u Fleš EEPROM memoriji se bajtovi ne mogu pojedinačno brisati. Fleš memorija se koristi tamo gdje je bitno da su podaci pohranjeni na fizički što manjem mediju (MP3 plejeri, USB stikovi itd.)(*https://hr.wikipedia.org/wiki/Flash_memorija).*

[16] RAM (engl. Random Access Memory – memorija s nasumičnim pristupom) je oblik primarne računarske memorije čijem se sadržaju može direktno pristupiti, za razliku od sekvencijskih memorijskih uređaja kao što su magnetne vrpce, CD i DVD diskovi, te tvrdi diskovi, u kojima pristup određenom sadržaju zavisi od položaja čitača. RAM omogućava upisivanje i čitanje podataka, za razliku od ROM-a iz kojeg se podaci mogu samo čitati (*https://hr.wikipedia.org/wiki/RAM*).

3.2. Hardverska forenzika

Kao i kod svakog uviđaja hardverska forenzika uključuje pregled drona i njegovog tereta (npr. eksploziv, droga i oružja koje je instalirano na njemu), te obradu drona – da bi se skinuli otisci prstiju sa njega i komponenti. Zatim, potrebna je analiza tehničkih karakteristika drona: vrsta, opis nosivosti, maksimala udaljenost, maksimalno vrijemei visina leta, radna frekvencija, vrsta veze između drona i kontrolora, putanja leta, moguće tačke polijetanja i dovođenje u vezu drona sa osobom i mobilnim telefonom ili kontrolorom. Sve to je vrlo složeno s obzirom na to da postoji veliki broj dronova i da njihov hardver i softver nije isti, kao ni količina i vrsta podataka koje oni generišu i čuvaju.

Ukratko, rad je fokusiran na vraćanje svih podataka drona na siguran način i da se mogu nedvosmisleno povezati s podacima na nečijem mobilnom telefonu. Neki od alata usvojenih za forenzičku istragu uključivali su 2D i 3D rendgenske uređaje, DataCon, CsvView, EnCase/FTK Imager i Compact Forensic Imaging Device (CFID). Preuzimanje hardvera uključuje pažljivo rastavljanje matične ploče drona i fleš memorijskog čipa. Ako je model drona poznat kroz registraciju njegovog korisnika, lakše je prepoznati pravu tehničku tablicu za referencu koja zauzvrat pomaže u razumijevanju usvojene tehnike pohrane podataka.

Mogu se koristiti i rendgenski aparati za traganje strujnih krugova i pinova/tačaka u čipu, te za čitanje podataka ako nisu bili dostupni za čitanje direktno s memorijskog čipa preko čitača čipa.Forenzički ispravne i održive stavke podataka uključuju mapu crne kutije (informacije o letu), mapu sistema (informacije o operativnom sistemu i procesu), nadogradnju mape (informacije o firmveru[17]), datoteku dnevnika (pojedinosti o sistemu, disku i procesu), FTP datoteku[18](naredbe, vrijeme početka i podaci za prijavu), serijski broj ploče i kamera i serijski broj senzora.

Enkripcija podataka opterećuje forenzičare i istražni proces, a istraga će se stoga morati oslanjati na one podatke koji se izdvajaju u formatu otvorenog teksta. Podaci se mogu prikupljati putem USB veze i vaj-faj veze, odnosno pristupne tačke koju uspostavlja dron tokom pokretanja. Daljinski upravljač se takođe može koristiti za prikupljanje podataka o putanji leta.

Slike i video-zapisi pohranjeni su u unutrašnjoj fleš memoriji uređaja i mogu se preuzeti putem FTP-a. GPS koordinate uključene su samo kada su bile dostupne tokom leta. Analiza različitih tehnika služi za pronalaženje slike i podataka o snimanju videa iz drona. Koriste se bežične veze FTP, Telnet[19] i

[17] Firmver (engl. Firmware) je posebna vrsta računarskog softvera koji obezbjeđuje kontrolu niskog nivoa (engl. low-level control) za određene tipove uređaja.

[18] File Transfer Protocol (FTP) je standardni mrežni protokol koji se koristi za premještanje datoteka s jednog hosta na drugi putem mreže zasnovane na TCP-u, kao što je internet (*https://hr.wikipedia.org/wiki/FTP*).

[19] Telnet je mrežni protokol unutar IP grupe protokola koji se koristi na internetu ili u

žičane veze putem USB priključka ili serijskog (UART[20]) priključka. Serijska UART veza je donijela prednost u pogledu količine dostupnih podataka, odnosno medija datoteke, kao i datoteke sistema bespilotne letjelice i podatke sa drona. Koriste se različiti operativni sistemi –kako oni licencirani, tako i *open source*[21] (Baig et al. 2022; Duraković, Simović 2020).

3.3. Identifikacija drona

Identifikacija drona se sprovodi kroz tri faze koje su prilično zahtjevne. Prva fazaje detekcija mete koja ukazuje na njenu prisutnost. U drugoj fazi se vršiprovjera da li se zaista radi o prisustvu mete –kako bi se isključio ili smanjio broj lažnih alarma. Provjera se vrši i drugim autonomnim sistemima radi potvrde prisustva mete – kombinovanjem radara i kamera ili akustičnih senzora ili putem osmatrača, uz korištenje akustičnih senzora (multispektralnih), kamera s video-analitikom, LIDAR-a (svjetlosna detekcija i domet) i radio-frekvencijskih (RF) senzora za detekciju (bilo da su pasivni ili aktivni). Nakon potvrde ide se u sljedeću, treću fazu klasifikacije drona u određene kategorije. Kategorizacija se vrši prema tipu letjelice, npr. fiksna krila, broj rotora, veličina, postojanje tereta itd. (Coluccia 2020).

Složenost problema otkrivanja i praćenja kretanja letjelice povećava nesigurnosti u ishod procesa i donošenja odluka o djelovanju na letjelicu. Fokus je na razvijanju tehnika koje pokrivaju određeni uži geografski prostor od značaja, uz upotrebu različitih senzora koji iz suštinski različitih podataka potvrđuju prisustvo letjelice i omogućavaju praćenje kretanja i aktivnosti drona, kao i određenih tereta na dronovima. Zaključak treba biti holistički[22], bez greške u uslovima slabe vidljivosti, raznih ometanja ili u uslovima urbanog ambijenta sa brojnim preprekama i smetnjama.

3.4. Korištenje senzora

Uključene tehnologije su 3D LIDAR senzor[23], pasivni radio-detektori, video-analitika i pasivni akustični senzori. Sve ove tehnologije treba da

lokalnim mrežama. Namjena ovog protokola je uspostavljanje dvosmjernog 8-bitnog komunikacijskog kanala između dva umrežena računara (*https://hr.wikipedia.org/wiki/Telnet).*

20 *Universal asynchronous receiver – transmitter*.

21 Open source je izvorni kod koji je slobodno dostupan za eventualne modifikacije i ponovnu distribuciju.

22 Holistički pristup stavlja pojedinca u centar zbivanja, te uključuje njegovo tijelo, um (emocije i misli) i duh, a u svojim terapijama i pristupu teži prirodnim rješenjima (*https://adhara.hr/holisticka-metoda*).

23 To je metod za određivanje dometa ciljanjem objekta ili površine laserom i mjerenjem vremena vraćanja reflektovane svjetlosti na prijemnik. Ponekad se naziva 3D lasersko skeniranje – posebna kombinacija 3D skeniranja i laserskog skeniranja.

onemoguće zamjenu drona za ptice i obrnuto. Cilj je za svaku od primijenjenih tehnika izdvojiti neke karakteristike za različite vrste letjelica: kategorija bespilotnih letjelica (s fiksnim krilima, s jednim rotorom ili više rotora); razlika između dronova i pticakoje su najsličnije po veličini i radarskom presjeku (RCS) i evaluacija prisustva bilo kakvog korisnog tereta koji utiče na RCS cijele mete (Coluccia 2020).

Neke tehnike su korisnije u prvoj fazi otkrivanja, dok su druge korisnije radi potvrde prisustva i klasifikacije vrste letjelice. U prvoj fazi se obično koriste različiti radari, dok udrugoj fazi dominira upotreba kamera i algoritama za identifikaciju dronova, uz aktivnu ulogu operatera. Kamere su limitirane efektima svjetlosti, refleksija i sjena, a u noćnim uslovima korištenja infracrvene kamere. Povoljni uslovi vidljivosti i pozicija letjelice na manjim udaljenostima, uzimajući u obzir rezoluciju i domete, kao i cjenovne raspone opreme – prilično su pouzdani. Jasno je da se za bolje i kvalitetnije rezultate koriste skuplji i precizniji sistemi.

Od značaja su i elektrooptički (EO) senzori u obliku kamera koje su osjetljive na vidljivo svjetlo ili infracrveno zračenje. Infracrveni EO senzori identifikuju toplotu motora ili baterija dronova i omogućavaju razlikovanje od ptica. Ovo je jedno od najisplativijih i na sadašnjem nivou razvoja tehnologije vrlo praktično rješenje, mada nema podataka o nekim već izgrađenim komercijalnim umreženim sistemima (Humphreys 2015).

Audio - senzori detektuju zvuk motora i propelera i služe za njihovu potvrdu i zarazlikovanje dronova od ptica. Njihov domet je vrlo ograničen zbog šumova i buke iz okruženja. Oni služi za razlikovanje letjelice sa fiksnim krilima od one sa više rotora i veličine letjelice. Mogu biti beskorisni ukoliko se radi o letu letjelice koja je ugasila motore i kreće se kao jedrilica u završnoj fazi leta, naročito kod samoubilačkih misija ili kod spuštanja sa teretom u završnim fazama leta.

Senzori za analizu radio-spektra otkrivaju bespilotne letjelice kada postoje *uplink/downlink* prenosi između drona i njegovog radio-upravljača. To je važno i sa stanovišta identifikacije osobe koja stoji iza drona.

Senzori radijskih emisija su korisni kod bespilotne letjelice jer obično šalju podatke nazad svom pilotu putem bežične veze, kao i datoteke. Radio-emisija otkriva i locira letjelicu pod uslovom da su signali snažni i konstantni (Humphreys 2015).

Pored direktne radio-veze, postoji i mogućnost autonomnog kretanja letjelice po unaprijed zadatom planu letenja. Autonomni način se zasniva na GPS lociranju i ometanju ovih signala, kao i radio-signala i stvara ogromne probleme za funkcionisanje građana, privrede, industrije i javnih službi, tako da se ove mjere samo izuzetno primjenjuju u urbanom prostoru (Coluccia 2020).

3.5. Elektronska odbrana dronova

Elektronska odbrana dronova sposobnih za autonomni let oslanja se na dvije vitalne bežične veze: veza s operaterom i (pasivna) navigaciona signalna veza s nadzemnom GPS[24]/GNSS[25] letjelicom. Ova veza se može pokušati prekinuti ili se poslati lažni signali. Još uvijek se koriste tradicionalni RC kontrolori kao rezervno sredstvo upravljanja, čak i za bespilotne letjelice s visokim stepenom autonomije. Za kontrolu na višem nivou, kontrolna stanica može komunicirati nezavisno od RC kontrolora. Poput RC kontrolora, ova se veza često uspostavlja unutar nelicenciranih pojaseva. Da bi se preuzela komunikacija, potrebno je utvrditi koji protokol se koristi, a zatimodabrati jedan od mogućih brojeva kanala za komunikaciju, te potom utvrditi da li je veza šifrovana.

GPS/GNSS signali omogućavaju autonomiju dronova signalima iz satelita, nisu šifrovani i autentifikovani. Stalno i snažno ometanje GNSS-a uzrokovalo bi znatnu štetu, onemogućavajući korištenje civilnog GNSS-a na širokom području oko zaštićenog područja, remeteći civilni život i navigaciju vozilima, a ometan bi bio i vazduhoplovni saobraćaj i rad vazdušnih luka. Poređenja radi, onemogućavanje ovog signala dronu u dometu jednog kilometra od štićenog objekta ometa se vazdušni saobraćaj u istoj liniji od pet kilometara (Humphreys 2015).

U normalnim vremenskim uslovima LIDAR (laserski skener) može biti vrlo efikasan za detekciju dronova i osnovnu klasifikaciju. Međutim, mete slične veličine, posebno dronovi i ptice, ne mogu se razlikovati. Stoga se LIDAR može smatrati komplementarnom tehnologijom s obzirom na RF senzore.RF signali su otporni na vremenske uslove i uslove osvjetljenja, te mogu pružiti srednje i dugotrajne signale pokrivenosti i raspona. Oni su prikladan alat za rukovanje primarnom fazom otkrivanja koja pokreće cijeli proces identifikacije. Najvažniji uređaj za aktivnu RF detekciju dronova je radarski senzor, ali su relevantne i pasivne tehnologije. Radari s frekvencijskim moduliranim kontinuiranim talasom (FMCW–*Frequency Modulated Continuous Wave*[26]) i kontinuiranim talasom (CW[27]) trenutno predstavljaju

[24] *Global Positioning System*. GPS koncept se zasniva na vremenu i poznatoj poziciji GPS specijalizovanih satelita. Sateliti nose veoma stabilne atomske satove koji su sinhronizovani jedni sa drugima i sa zemaljskim satovima.

[25] *Global navigation satellite system* (GNSS) je opšti termin koji opisuje bilo koju satelitsku konstelaciju koja pruža usluge pozicioniranja, navigacije i tajminga (PNT) na globalnoj ili regionalnoj osnovi.

[26] Automobilski radarski sistemi rade pomoću tzv. frekventnog modulisanog kontinuiranog talasa (FMCW). Sistem prenosi kontinuirani talas na određenoj frekvenciji, koji se zatim moduliše tokom vremenskog perioda. To daje prenesenom signalu „vremensku oznaku“.

[27] CW Television Network (obično se naziva samo The CW) je američka komercijalna televizijska mreža na engleskom jeziku koju preko The CW Network, LLC,

najprivlačnije i najisplativije rješenje za rješavanje ovog problema (Coluccia 2020:4).

Proizvođači komercijalnih bespilotnih letjelica mogu odigrati ključnu ulogu, i to implementacijom geofencinga[28] koje provodi GPS unutar njihovih sistema autopilota. Oni sprečavaju let njihovih UAV-ova[29] unutar zabranjenih zona, vazdušnih luka, sportskih stadiona, vladinih zgrada i drugih bezbjednosno osjetljivih mjesta. Pred senzorima za detekciju i zaustavljanje mogu se koristiti snažne i brzebespilotne letjelice – presretači, koji bi mogli djelovati kao tim i zarobiti i odnijeti mali broj istovremenih „uljeza".

Upadima bespilotnih letjelica novije generacije biće se mnogo teže suprotstaviti jer bi sofisticirani napadač mogao izvesti napad u stilu kamikaze protiv osjetljive mete. Uz samo manje izmjene na softveru, dron može da radiu „radio-tišini", ignorišući vanjske radio-upravljačke naredbe i ne emitujući vlastite radio-signale. UAV bi stoga bilo teško otkriti i bio bi nepropusan za ometanje naredbene veze. Za posebno kritična mjesta sistemi detekcije i praćenja,zasnovani na elektrooptičkim senzorima, biće najefikasniji, posebno oni koji primjenjuju prepoznavanje uzoraka infracrvenog senzora.

Kinetička odbrana[30] drona obuhvata sve tehnike koje uključuju mehanički kontakt s UAV „uljezom", kao npr. bespilotne letjelice presretači, gumeni meci, sačma, rakete ili mreže (Humphreys 2015). Razvijene su nove radarske postavke koje pokušavaju iskoristiti za procjenu, povratnodejstvo raspršenja radarskih zraka rotirajućih dijelova, poput propelera i rotora. Mikrodoplerska analizamožeposebno pružiti korisne informacije o broju propelera i rotora. Takođe, u slučaju lažne uzbune zbog ptica, vremensko-frekvencijska analiza može omogućiti tačnu identifikaciju. Problem je i kod stacioniranih ciljeva koji ne stvaraju Doplerov efekat[31]. Uglavnom, u literaturi se predlaže postavljanje mreže jeftinih radarskih senzora, što omogućava otkrivanje i razlikovanje dronova od drugih letećih objekata.

---

kontroliše Nexstar Media Group sa 75 odsto svojinskog udjela.

[28] Geofencing je upotreba satelitske mreže Global Positioning System (GPS) i/ili lokalnih radio-frekventnih identifikatora (kao što su vaj-faj čvorovi ili blutut svjetionici) za stvaranje virtuelnih granica oko lokacije (https://www.howtogeek.com/221077/htg-explains …).

[29] Termin UAV (engl. *Unmanned Aerial Vehicle*) označava bespilotnu letjelicu i odnosi se na bilo koji leteći avion kojim upravlja softver ili daljinski upravljač i (što je najvažnije) koji je sposoban za ponovnu upotrebu (https://www.dronesvilla.com/drones-vs-uavs).

[30] Ova odbrana se prebacuje u električnu, fizičku, digitalnu.

[31] Doplerov efekat je promjena posmatrane talasne dužine talasa zbog međusobnog približavanja ili udaljavanja izvora i posmatrača. Ovaj efekat otkrio je Kristijan Dopler 1842. godine na osnovu proučavanja promjene frekvencije svjetlosti koju emituju zvijezde u dvojnom sistemu (dvije zvijezde koje se okreću jedna oko druge). Efekat je eksperimentalno potvrdio Buys Ballot 1845. godine na Utrehtskoj željezničkoj stanici upoređujući zvuk trubača koji stoje na jednom mjestu i trubača koji se kreću (*https://sh.wikipedia.org/wiki/Do pplerov_efekat*).

Laserski sistemisu jeftiniji i efikasniji od drugih tehnologija za onesposobljavanje drona. Visokoenergetski fiksni laserski topovi mogu probušiti rupe u bespilotnoj letjelici i uništiti autonomno programirani dron. Izazov je držati laser fokusiran na fiksnu tačku na tijelu drona (Chaari, Al-Maadeed 2020).

4. ZAKLJUČAK

Automatska identifikacija malih bespilotnih letjelica je pravovremen i važan problem. Rasprostranjenost dronova nesporno omogućava aplikacije bez presedana, ali se istovremeno pojavljuju nove prijetnje povezane sa njihovom mogućom zloupotrebom (npr. krijumčarenje droge, teroristički napadi, špijunaža). Još uvijek postoji dilema u sistemima nadzora za suočavanje sa ovim problemom, a glavni izazovi su povezani sa zadacima detekcije, moguće verifikacije i klasifikacije. Savremeni sistemi nadzora sastavljeni od mreže prostorno distribuiranih senzora najperspektivniji su pristup kako bi se osigurala potpuna pokrivenost nadgledanog područja i iskoristile prednosti različitih tehnologija. Ovi sistemise posebno fokusiraju na radarske senzore, što je ključna tehnologija i zbog niske cijene i sposobnosti rada na relativno velikim udaljenostima.

U svakom slučaju, potrebna je mješavina različitih rješenja za suočavanje sa ovim izazovnim problemom. Istovremeno, potrebni su sofisticiraniji algoritmi za obradu signala kako bi se poboljšale performanse detekcije i klasifikacije.

Literatura

Baig, Z., Khan, M.A., Mohammad, N.,Brahim, G.B. (2022). „Drone Forensics and Machine Learning: Sustaining the Investigation Process“, *Sustainability.*

Cavalry, C. (2014). *Drones fleet to help rescuers operations over disasters scenarios*, Proceedings of the 2014 IEEE Conference on Antenna Measurements Applications (CAMA); Antibes, France, 16–19 November 2014.

Chaari, M.Z., Al-Maadeed, S. (2020). „Testing the efficiency of laser technology to destroy the rogue drones“, *Security and Defence Quarterly*, 32(5): 31–38.

Coluccia, A., Parisi, G., Fascista, A. (2020). *Detection and Classification of MultirotorDrones in Radar Sensor Networks: A Review*.

Drug smuggling: Underwater drones seized by Spanish police, Published, 4 July 2022, *https://www.bbc.com/news/world-europe-62040790.*

Digulescu, A., Despina-Stoian, C., Popescu, F., Stanescu, D., Nastasiu, D., Sburlan,D. (2023). „UWB Sensing for UAV and Human Comparative Movement Characterization“,*Sensors* Basel, 23(4):1956.

Duraković, A., Simović, M.N., Duraković, S. (2022). „Upotreba dokaza prikupljenih dronovima u kriminalističkim istraživanjima“, *Zbornik radova* „Digitalizacija u kaznenom pravu i pravosuđu“, Beograd.

Elloumi, M., Dhaou, R., Escrig, B., Idoudi, H., Saidane, L.A. (2018). „Monitoring road traffic with a UAV-based system“, *Proceedings of the 2018* IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain. 15–18 April 2018.

Humphreys, T. (2015). *Statement on the security threat posed by unmanned aerial systems and possible countermeasures*, The University of Texas at Austin, Submitted to the

Subcommittee on Oversight and Management Efficiency of the House Committee on Homeland Security, March 16.
Khawaja, W., Semkin, V., Ratyal, N.I., Yaqoob, Q., Gul, J., Guvenc, I. (2022). „Threats from and Countermeasures for Unmanned Aerial and Underwater Vehicles“, *Sensors*, Basel,20, 22(10):3896.
Klaer, P., Huang, A., Sévigny, P., Rajan, S., Pant, S., Patnaik, P., Balaji, B. (2020). „Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations“, Sensors, Basel, 21, 20(20): 5940.
Klein, N., McLaughlin, R. (2022). *Narco-drones' are the newest form of drug trafficking*,Our laws aren't yet ready to combat them Published: July 25, 2022 5.08am CEST, *https://phys.org/news/2022-07-narco-drones-drug-trafficking-laws-ready.html.*
Lagkas, T., Argyriou, V,. Bibi, S., Sarigiannidis, P.(2018). „UAV IoT Framework Views and Challenges: Towards Protecting Drones as *Things",Sensors*, Basel, 18(11): 4015.
Schmersahl, A.R. (2011).*Fifty feet above the wall: cartel drones in the U.S. –Mexico Border Zone Irspace, and what to do about them*, United States Navy B.S., Southern Polytechnic State University.
Siddiqi, M.A., Iwendi, C.J., Anumbe, K.N.(2022). „Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations“,*Math Biosci Eng*., 19(3): 2641–2670.
Svanström, F., Alonso-Fernandez, F, Englund, C. (2021).„A dataset for multi-sensor drone detection“, *Data Brief*, 27, 39: 107521.
Tokekar, P., Hook, J.V., Mulla, D., Isler, V. (2016). „*Sensor Planning for a Symbiotic UAV and UGV System for Precision Agriculture*“, IEEE Trans. Robot,32:1498–1511.
Turkmen, Z., Kuloglu, M. (2018). *A new era for drug trafficking: drones*, Institute of Forensic Sciences, Istanbul University, Turkey, Crimsion Publishers, *https:// crimsonpublishers.com/fsar/pdf/FSAR.000539.pdf.*
Wright,T. (2020). „How Many Drones Are Smuggling Drugs Across the U.S. Southern Border?“,*Air & Space magazine*, *https://www.smithsonianmag.com/air-space-magazine/narcodrones-180974934/.*

DETECTION AND SEIZURE OF DRONES USED FOR ILLEGAL ACTIVITIES

Prof. dr Adnan Duraković

Full Professor at the Faculty of Law, University of Zenica

Academician prof. dr Miodrag N. Simović

full member of the Academy of Sciences and Arts of Bosnia and Herzegovina, full member of the European Academy of Sciences and Arts, foreign member of the Russian Academy of Natural Sciences, full professor of the Faculty of Law, University of Bihac, professor emeritus

Abstract: *Thanks to recent technological achievements, a new generation of cheap, small, unmanned aerial vehicles (UAVs) is available. These aircrafts, which are often called drones, enable unprecedented applications, but at the same time new threats related to their possible misuse (e.g. drug smuggling, terrorist attacks, espionage) are emerging.*

The drone is usually small, with the ability to fly very quickly in a maneuver, which makes these aircrafts a category of targets that are much more difficult to detect compared to traditional aircrafts. These aircrafts can be used within the airspace of one country or in the border zone, that is, in the areas under the jurisdictions of several countries. In this context, systems for detecting, recognizing and stopping drones face numerous problems.

Many police and military organizations are trying to draw experience from the use and suppression of the use of drones from Iraq, Afghanistan and Ukraine in order to take appropriate measures to combat their abuse. Since the use of drones is becoming more and more popular for economic, scientific, sports and private purposes, the issue of their safety and the need for adopting legal regulations to prevent possible incidents has become an actual issue.

This paper discusses the main challenges related to the problem of drone identification, which include detection, possible verification and classification. The focus is on methods of detection, verification and stopping and confiscation of drones that perform illegal activities. In this regard, an overview of the most relevant technologies, which in modern surveillance systems are placed in a network of spatially distributed sensors, is given in order to ensure complete coverage of the monitored area. More precisely, the main focus is on key technologies due to their low cost and ability to operate over relatively long distances.

Key words: *drone, detection, drugs, trade, forensics.*