UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Kristian Hamberger

Kibernetični napadi kot grožnja delovanju avtomatiziranih zračnih bojnih sistemov

Magistrsko delo

Ljubljana, 2016

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Kristian Hamberger

Mentor: izr. prof. dr. Uroš Svete

Kibernetični napadi kot grožnja delovanju avtomatiziranih zračnih bojnih sistemov

Magistrsko delo

Ljubljana, 2016

Iskreno se zahvaljujem svojemu mentorju izr. prof. dr. Svetetu za vse usmeritve ob pisanju magistrskega dela.

Kibernetični napadi – grožnja delovanju avtomatiziranih zračnih bojnih sistemov

Avtomatizirani zračni bojni sistemi iz fikcije prehajajo v realnost, tako kot uporaba kibernetike za bojevanje. V zadnjih letih je tako prvo kot drugo področje doživelo razmah, pri čemer pa se kljub prvotnemu navdušenju nad napredkom na drugi strani porajajo vprašanja o varnosti. Brezpilotni letalniki, ki niso zgolj primerni za bojne naloge, pa postajajo tudi čedalje bolj priljubljeni za dotične storitve, kot je denimo pošta in podobno (ipd.). Poleg tovrstnih institucij pa tovrstni sistemi počasi prehajajo tudi v zasebne roke, kar odpira mnoga vprašanja povezana s pravno podlago za uporabo, varnostjo in tako dalje (itd.). Uporaba tovrstnih letalnikov v zasebne namene pa poraja tudi vprašanje glede zgostitve prometa v zraku, kar poraja spet nov nabor zapletov. Ob vsem tem morebitna ranljivost teh sistemov in njihova neodpornost na raznovrstne vdore končno lahko pripelje do tega, da bo v vsakem trenutku na neki točki nek letalnik odpovedal in strmoglavil. Na drugi strani kibernetska tehnologija, ki jo mnogi enačijo z izrazom informacijsko-komunikacijska tehnologija le da ji dodajo negativen predznak, s svojim hitrim razvojem prav tako odpira tako številne priložnosti kot tudi številna tveganja. Tako že obstajajo primeri, ko so tovrstno tehnologijo izrabili za namene napada na nek sistem. Gre predvsem za to, da že obstajajo primeri vdorov, katerih posledica je bila da je nek letalnik pristal povsem drugje, kot bi prvotno moral. To se zdi precej mila posledica, saj bi v primeru da bi bil letalnik oborožen posledice lahko bile precej hujše.

Ključne besede: avtomatizirani zračni bojni sistemi, brezpilotna bojna letala, informacijsko-komunikacijska tehnologija, kibernetične grožnje, kibernetični napadi.

Cyber attacks – a threat to the functioning of automated aerial combat systems

Automated aerial combat systems are passing from fiction into reality, just like the use of cybernetics as a tool for conducting warfare. In recent years both areas of expertise have seen significant progress, which is accompanied by great enthusiasm on one hand and several security questions on the other hand. Unmanned aerial vehicles, which are not only suitable for combat tasks, are becoming more popular for certain services by the minute such as the post etc. The sole use of such aerial vehicles however also spawns a number of questions about airspace traffic density, which again serves with a wide variety of complications. With that in mind, a potential vulnerability of such systems and its weak resistance agains specific breaches could finally lead to the point , that at some point a certain aerial vehicle could malfunction and crash. On the other hand, cyber technology which some people equal with information-communication technology (except they give it a negative sign) with its fast development also opens numerous opportunities and numerous risks. As it happens, there are already specific cases when this kind of technology was abused for the purpose of attacking a certain system. The fact is, that there have already been cases of breaches, the results of which were that a certain aerial vehicle landed in a completely different location as it was primarily intended. This appears to be a very mild consequence, since in the case that this aerial vehicle would have been armed, the consequences could be much worse.

Key words: automated aerial combat systems, unmanned combat aerial vehicles, information-communication technology, cyber threats, cyber attacks.

Kazalo

1 Uvod

Avtomatizirani zračni bojni sistemi, pri čemer bom pod tem pojmom v magistrskem delu smatral brezpilotne letalnike, so v zadnjem času postali precej razširjen oborožitveni sistem. Na drugi strani se o njih – kljub razširjenosti oziroma razcvetu informacij o njihovi uporabi, o njihovih zmogljivostih ter seveda tudi pomanjkljivostih – še vedno zgolj šepeta. Države se trudijo, da informacije o teh »novih« oborožitvenih sistemih v karseda omejenem obsegu dosegajo splošno javnost. Pravzaprav se v tem trenutku zdi, da informacije o brezpilotnih letalnikih, ne glede na njihovo namembnost, v omejenem obsegu pridejo na plano šele ob kakšnem incidentu. Zaradi omejene količine informacij, ki jih trenutno poseduje splošna javnost o tovrstnih oborožitvenih sistemih, to področje predstavlja tudi nekakšno sivo cono, kar pomeni, da je pravna podlaga za uporabo brezpilotnih letalnikov pomanjkljiva, slednje pa omogoča prostor za subjektivno interpretacijo kar zadeva uporabo tovrstnih oborožitvenih sistemov. Dandanes že veliko držav poseduje vsaj nekatere vrste brezpilotnih letalnikov pa naj bodo le-ti namenjeni za izvidniške, bojne ali civilne naloge (Rogers 2012).

Posledica vedno večjega števila brezpilotnih letalnikov v uporabi na splošno začenja transformacijo načina vojskovanja. Vojskovanje tako postaja čedalje bolj nestično in avtonomno. Posredna uporaba tovrstnih oborožitvenih sistemov pa ustvarja prazen prostor, ki ga potencialni napadalci lahko izkoristijo v svoj prid. Tovrstne zlorabe bi lahko pripeljale do točke, ko bi predstavljale grožnjo širši populaciji. Čedalje večja razširjenost tovrstnih sistemov, poleg novih priložnosti, prinaša tudi nova tveganja. Med priložnostmi, ki jih razširjenost in sama uporaba tovrstnih sistemov prinaša, je nedvomno uporaba za namene storitev, kot je denimo pošta (Samuel 2014) ali za namene izboljšanja sistemov zaščite in reševanja, seveda pa ostaja primarni namen brezpilotnih letalnikov v domeni vojske, ki letalnike uporablja za izvidniške in bojne naloge.

V magistrskem delu se bom ukvarjal predvsem z brezpilotnimi letalniki, ki se uporabljajo za bojne naloge, pri čemer bom v prvem delu analiziral taktično-tehnične značilnosti določenih izbranih letalnikov, medtem ko se bom v drugem delu posvetil kibernetični komponenti tovrstnih oborožitvenih sistemov ter analiziral grožnjo, ki jo kibernetični napadi predstavljajo za tovrstne oborožitvene sisteme.

Čeprav bo magistrsko delo v prvem delu govorilo o brezpilotnih letalnikih, ki se jih uporablja v vojaške namene, je z vidika drugega dela, ki bo govoril o kibernetičnih napadih in grožnji, ki jo predstavljajo za brezpilotne letalnike, potrebno omeniti tudi uporabo brezpilotnih letalnikov v civilne namene in potencialne nevarnosti, ki jih le-ta prinaša. Ne glede na to, da so v Sloveniji brezpilotni letalniki še vedno bolj znanstvena fantastika kot ne (z izjemo v vojski), pa so v nekaterih državah veliko bolj dejavni tudi v civilni sferi, kjer smo v zadnjem času priča številnim primerom uporabe brezpilotnih letalnikov. Ti primeri vključujejo uporabo brezpilotnega letalnika na nogometni tekmi, uporabo za prelete in dostavo pošte (denimo v Franciji) in podobno.

Po poročanju *Mladine* (2015) je v Franciji v mesecu januarju brezpilotni letalnik preletel določena kritična območja. Slednja so bila med drugim Elizejska palača, po nekaterih navajanjih pa tudi Eifflov stolp, določena vojaška območja, jedrske elektrarne ipd. Zaradi nedavnega terorističnega napada na francoski satirični časopis *Charlie Hebdo*, je prelet brezpilotnega letalnika sporočil takojšen odziv s strani francoskih oblasti, ki so primer predale tožilstvu ter izdale izjavo za javnost o varnosti jedrskih elektrarn oz. o nezmožnosti povzročitve škode na tovrsten objekt s strani tovrstnega brezpilotnega letalnika.

Trenutni trend vzpona brezpilotnih letalnikov je zasenčila njihova sposobnost izvajanja bojnih nalog. Le-ta jim nadeva negativen predznak, zaradi česar v družbi (vsaj v Evropi) čedalje bolj prihaja do tega, da slika, ki si jo ustvari družba, prikazuje brezpilotni letalnik, ki je oborožen do zob in prinaša zgolj negativne posledice. Vendar pa v nekaterih državah po svetu že prihaja do pobud ali pa že obstajajo modeli brezpilotnih letalnikov, ki se jih uporablja kot dodatek k človekovim zmogljivostim.

Tako po navedbah vira (Chhabra 2015) brezpilotni letalniki ponekod po svetu zgolj zbirajo informacije na raznovrstnih področjih, in sicer na območjih, ki so za ljudi težko dostopna. V Iranu je tehnološki laboratorij v Teheranu zasnoval brezpilotno letalo, ki deluje kot reševalec iz vode in se ga uporablja za reševanje na Kaspijskem morju. Pri tem avtorica članka kot

prednost brezpilotnega letalnika v primerjavi s človekom navaja, da lahko brezpilotni letalnik utapljajočo se žrtev doseže v tretjini časa, ki bi ga za to nalogo porabil človek. V nekaterih državah brezpilotni letalniki služijo za dostavo nujne medicinske opreme, zdravil, zbiranje podatkov, nadzor, zaščito, reševanje ipd.

Čeprav sem v toku prebiranja podatkov o brezpilotnih letalnikih prišel do spoznanja o njihovi vsestranski uporabnosti, bo v bodoče lahko čedalje večja uporaba ob neustrezni pravni ureditvi na določenih področjih pripeljala do čistega kaosa. Trenutno povečane uporabe brezpilotnih letalnikov ne glede na njihovo namembnost še ne občutimo – vsaj do te mere, ko bi nas to kakorkoli obremenjevalo. Večje število brezpilotnih letalnikov v uporabi na splošno bo pomenilo večjo obremenitev za zračni prostor, pri čemer bo zaradi preprečevanja morebitnih trkov z letali nujno potrebno določiti višino za letenje. Poleg tega iz ZDA že poročajo o prestrezanju telefonskih signalov s strani brezpilotnih letalnikov. Ti so nato posredovali informacije o lokaciji določene osebe, kar bi neka družba lahko izkoristila za manipulacijo s to osebo (Bi 2015a).

Zaradi čedalje večjega števila brezpilotnih letalnikov v uporabi ne glede na njihovo namembnost se ponekod, tudi s strani javnosti (npr. v ZDA), pričakuje, da bodo v naslednjih petih letih brezpilotni letalniki prevzeli dostavo različnih pošiljk. Gre za rezultate ankete, pri kateri sta dve tretjini vprašanih izrekli podporo za dostavo pošiljk s strani brezpilotnih letalnikov (Bi 2015b). Govorim torej o trenutku, ko bo namesto poštarja pred vrati lebdel brezpilotni letalnik, ki bo na sebi imel privezano pošto. Ob tovrstni uporabi, pri čemer imam v mislih uporabo brezpilotnih letalnikov za podobne storitve, kot je pošta, bi to pomenilo drastično povečanje števila brezpilotnih letalnikov, kar bi denimo v nekem mestu povzročilo vrsto negativnih posledic (hrup ipd.).

Z vidika varnosti bi razširjenost brezpilotnih letalnikov za te namene, brez bolj poglobljenega področja varnosti, če na to pogledam z vidika kibernetične varnosti, napadov oz. groženj, pomenilo, da bi v nekem trenutku lahko prišlo do položaja, ko bi sredi mesta letalnik zaradi tehnične okvare ali kibernetičnega napada strmoglavil brez opozorila. Tovrsten scenarij odpre

še mnoge druge razsežnosti varnosti, nevarnost infrastrukturne škode, ogroženost človeških življenj, okoljsko škodo in tako naprej.

1.2 Struktura

Fokus magistrskega dela bo torej na brezpilotnih letalnikih, ki se uporabljajo v vojaške namene. Letalnike bom razdelil v dva sklopa oz. v dve večji skupini. Prvi sklop oz. prvo skupino bodo sestavljali tako imenovani klasični (samostojni) avtomatizirani zračni bojni sistemi oz. brezpilotni letalniki, drugo skupino pa bodo sestavljali avtomatizirani zračni bojni sistemi oz. brezpilotni letalniki, ki so osnovani na principu *fire-and-forget*.

Princip *fire-and-forget* oz. »izstreli in pozabi« se nanaša na to, da tovrstni avtomatizirani zračni (bojni) sistemi niso sposobni vzleteti in pristati samostojno, tj. zgolj s pomočjo vzletne oz. pristajalne steze, temveč za izstrelitev potrebujejo neko posebno izstrelitveno komponento, hkrati pa, v kolikor njihov polet ni enosmeren, potrebujejo za pristajanje posebne mehanizme, kot so npr. padala.

Pri tem je potrebno najprej pojasniti delitev brezpilotnih letalnikov, ki se jih uporablja za bojne naloge, kar bo moja prva naloga v pričujočem delu.

Kaj vse bo torej fokus magistrskega dela? Magistrsko delo se bo osredotočalo na dve raziskovalni vprašanji, in sicer:

- kakšni podsistemi odlikujejo avtomatizirane zračne bojne sisteme in
- kako varni so avtomatizirani zračni bojni sistemi pred kibernetičnimi grožnjami?

Prvi del magistrskega dela bo zajemal analizo izbranih avtomatiziranih zračnih bojnih sistemov, drugi del pa bo zajemal analizo varnosti tovrstnih modelov in avtomatiziranih

zračnih bojnih sistemov na splošno. V prvem delu bom tako analiziral izbrane tri samostojne modele, in sicer ameriški General Atomics MQ-1C Gray Eagle, ruski Mikoyan Skat in kitajski Guizhou WZ-2000 ter njihove podsisteme. Nato bom vse tri izbrane samostojne modele in njihove podsisteme med seboj primerjal. Enako bom analiziral tri avtomatizirane zračne bojne sisteme, ki temeljijo na principu *fire-and-forget*, in sicer izraelski IAI Harpy, francoski SAGEM Sperwer MK II. in ameriški Northrop Grumman Chukar III ter njihove podsisteme, ki jih bom prav tako primerjal med seboj.

Končno nadgradnjo primerjave bom opravil tako, da bom opravil tudi primerjavo med samostojnimi avtomatiziranimi zračnimi bojnimi sistemi in avtomatiziranimi zračnimi bojnimi sistemi, ki temeljijo na principu *fire-and-forget*. Drugi del magistrskega dela pa se bo nanašal na kibernetsko varnost avtomatiziranih zračnih bojnih sistemov. Predvsem bom skušal predstaviti varnostne ukrepe in tehnične značilnosti ter tehnične komponente, ki skušajo zagotavljati kar najvišjo možno stopnjo varnosti avtomatiziranih zračnih bojnih sistemov. Tako kot sem glede na tip avtomatiziranega zračnega bojnega sistema predhodno opravljal analizo in primerjavo, bom podobno razdelavo skušal opraviti tudi v tem delu, in sicer sprva z analizo posameznih varnostnih ukrepov in protiukrepov pri posameznem modelu, nato pa bom poskušal opraviti še nekakšno primerjavo med temi ukrepi – tako med modeli kot tudi med tipi avtomatiziranih zračnih bojnih sistemov.

1.3 Metodologija

Pri raziskovanju se bom opiral na analizo in interpretacijo primarnih in sekundarnih virov, uporabljal študijo primerov, in sicer tako posameznih avtomatiziranih zračnih bojnih sistemov kot tudi primerov njihove uporabe. Nadalje bom uporabljal zgodovinsko analizo za namene analiziranja razvoja in poteka uporabe avtomatiziranih zračnih bojnih sistemov, za medsebojno komparacijo med posameznimi modeli pa bo ključna primerjalna analiza.

Z magistrskim delom želim zagotoviti osnovo za nadaljnje raziskovanje varnosti avtomatiziranih zračnih bojnih sistemov tako kar zadeva same tehnične značilnosti kot tudi

njihovo varnost pred kibernetičnimi grožnjami. Kar zadeva tehnične značilnosti želim predstaviti vsestranskost tovrstnih oborožitvenih sistemov in njihovo primernost za številne vojaške ter nevojaške operacije. Med izbranimi modeli želim izpostaviti prednosti in pomanjkljivosti ter ustvariti grobo sliko o tem, kaj sestavlja oz. bolje rečeno, kakšni podsistemi odlikujejo zares dober avtomatizirani zračni bojni sistem ter kaj pravzaprav definira na tem področju dober avtomatiziran zračni bojni sistem. Na drugi strani želim, kar zadeva področje kibernetske varnosti, analizirati trenutni nivo varnosti oz. zaščite pred kibernetskimi grožnjami, izpostaviti prednosti in pomanjkljivosti ter s tem ustvariti sliko o tem, kje mora v bodoče priti do intenzivnejšega napredka in kje smo že dosegli neko zadovoljivo stopnjo zaščite oz. varnosti.

2 Umestitev v družboslovni kontekst

V uvodnem delu magistrskega dela je že bilo navedenih nekaj dogodkov, ki prikazujejo vsakodnevne implikacije avtomatiziranih zračnih sistemov, ki bi ob širši uporabi tovrstnih sistemov lahko postale del vsakdana, vendar pa je tako za razumevanje tega magistrskega dela kot tudi za razumevanje splošnih varnostnih problemov potrebna umestitev tovrstnih oborožitvenih sistemov v širši družboslovni kontekst. Pri tem bo širši družboslovni kontekst v določenih pogledih še vedno omejen na varnostno področje, hkrati pa nas bo zanimal trenuten »položaj« avtomatiziranih zračnih (tudi bojnih) sistemov.

Sama uporaba avtomatiziranih zračnih bojnih sistemov se je v vojski začela v osemdesetih letih. Prvotno ti sistemi niso posedovali oborožitvene komponente, saj so bili namenjeni za misije opazovanja, nadzorovanja, obveščevalne dejavnosti ipd. Eden izmed prvih tovrstnih avtomatiziranih zračnih bojnih sistemov v uporabi je bil produkt izraelskega podjetja Israel Aerospace Industries z nazivom IAI Scout, ki je bil med drugim udeležen tudi v vojni v Libanonu leta 1982 (Israel Aerospace Industries 2002c).

Širši družboslovni okvir veleva predvsem definicijo uporabe avtomatiziranih zračnih sistemov na drugih področjih ter morebitne varnostne implikacije. Tako se danes avtomatizirani zračni

bojni sistemi uporabljajo za fotografiranje, snemanje, 3D oblikovanje, analize, dela v kmetijstvu ipd., več o tem v nadaljevanju.

Prva izmed možnosti uporabe avtomatiziranih zračnih sistemov je uporaba za fotografiranje. Avtomatizirani zračni sistemi predstavljajo nove načine pridobivanja najboljših in najbolj kakovostnih posnetkov – naj si gre za zajemanje fotografij na nekem dogodku, kot je denimo poroka ali parada, za fotografiranje narave oz. za zajemanje fotografij za namene osnovanja nekega prostora v 3D tako kot to v Sloveniji počne podjetje Modri planet d.o.o., ki avtomatizirane zračne sisteme uporablja na področju geodezije (Pavlin 2014).

Druga možnost uporabe za namene zbiranja podatkov je denimo na področju meteorologije. Tako gre za dotično nalogo prilagojeni avtomatizirani zračni sistem lahko v samo jedro nevihte, orkana, tornada in zbira podatke na licu mesta, brez da bi ob tem bilo ogroženo človeško življenje. Na področju naravnih katastrof bi lahko s pomočjo za to prilagojenimi avtomatiziranimi zračnimi bojnimi sistemi spremljali neko naravno katastrofo, ko je še na točki razvoja, iz česar bi posledično lahko predvidevali, kam bo le-ta udarila ter s preventivnim posredovanjem ublažili tako materialno škodo kot tudi izgubo človeških življenj (Handwerk 2013).

Čedalje večja uporaba avtomatiziranih zračnih sistemov je tudi v kmetijstvu, logistiki in tehničnem vzdrževanju. Tako lahko denimo v kmetijstvu avtomatizirani zračni sistemi pregledujejo in analizirajo rast nekega pridelka, ocenjujejo njegovo zrelost ter na podlagi pridobljenih podatkov podajajo kvalitetne informacije o tem, kdaj je pridelek potrebno pobrati. Poleg tega lahko avtomatizirani zračni sistemi pri analiziranju kmetijskih pridelkov hitreje zasledijo anomalije pri rasti nekega pridelka zaradi neke bolezni ali naravnih dejavnikov (MULTIROTOR GmbH 2016a).

Na področju logistike sta čas in hitrost ključna dejavnika Tako je z avtomatiziranim zračnimi sistemi moč dostavljati tudi manjše pošiljke. Tipičen primer sta hitra pošta ter internetno naročanje, kjer kupec zahteva oz. prosi za dostavo naročenega artikla v istem dnevu. Hkrati je

z vidika transporta določenih dobrin navadno tako, da pomeni mehanska okvara na področju logistike (predvsem na področju dobave nadomestnih delov) finančno izgubo. Avtomatizirani zračni sistemi lahko delež mehanskih okvar na tem področju omilijo do določene točke (ključnega pomena je predvsem to, da naj bi bil sistem do določene mere avtonomen, kar izvzame človeški faktor, tj. zmanjša možnost napak), hkrati pa so časovno ugodnejši (MULTIROTOR GmbH 2016b).

Kar zadeva področje tehničnega vzdrževanja so avtomatizirani zračni bojni sistemi uporabni predvsem na težko dostopnih mestih. Ko gre torej za varnostne preglede visokih stavb, industrijskih objektov, težko dostopnih področij ipd., je avtomatizirane zračne bojne sisteme moč uporabljati brez tega, da bi pri tem ogrožali človeška življenja. Hkrati je s pomočjo dodajanja specifičnih komponent, kot so denimo raznovrstne optične naprave ipd., iste sisteme moč uporabljati za več vrst nalog, pri čemer gre zopet za ublažitev finančnih bremen in za zaščito človeških življenj (MULTIROTOR GmbH 2016c).

Ostali primeri širše uporabe avtomatiziranih zračnih bojnih sistemov zajemajo tudi zaščito živalskih vrst, pri čemer ti sistemi skušajo najti določeno (ogroženo) vrsto živali, identificirati naravni habitat, kar omogoča zaščito dotičnega območja itd. Prav tako je ena izmed možnih uporab tovrstnih sistemov uporaba v iskalnih in reševalnih operacijah, saj je hitrost iskanja na težko dostopnih območjih s pomočjo tovrstnih sistemov veliko večja kot zgolj z iskanjem na tleh ali z uporabo helikopterjev. Avtomatizirani zračni sistemi so skupaj s svojimi dodatnimi komponentami pri iskanju in reševanju pogrešanih oseb ter oseb, ki se nahajajo na nekem težko dostopnem območju, veliko bolj učinkoviti, kot pa so denimo človeška posadka s helikopterjem (Handwerk 2013).

Na splošno prihaja zaradi same efektivnosti avtomatiziranih sistemov do namigovanj, da bodo le-ti v bodoče na določenih delovnih mestih pričeli izrinjati človeka. Tako so nekatera področja uporabe farmacevtika, avtomobilska industrija, tovrstni sistemi pa bi lahko pričeli nadomeščati tudi astronavte, vojake, varuške, novinarje itd. (Aquino 2011).

2.1 Varnostne implikacije

Ob širokem naboru možnosti uporabe je torej bistveno vprašanje, kakšni so torej negativni učinki uporabe avtomatiziranih zračnih sistemov. Zakaj so ti sistemi vprašljivi? Kakšne varnostne implikacije povzročajo oz. na kakšen način ti sistemi kompromitirajo varnost?

Eden izmed negativnih učinkov tovrstnih sistemov je ta, da so sicer odličen način zbiranja podatkov, vendar lahko na drugi strani neposredno vdirajo v zasebnost. Medtem ko so bile denimo varnostne kamere in podobni nadzorni sistemi na splošno dobro sprejete oz. v javnosti niso dvigovale toliko prahu, pa nadzorovanje s strani avtomatiziranih zračnih sistemov dviguje precej prahu. Tako je denimo v Avstraliji že določeno za zbiranje kakšnih informacij se avtomatizirane zračne sisteme lahko uporablja, pri čemer je za komercialno uporabo ter za zbiranje občutljivih podatkov potrebno pridobiti soglasje. Prav tako je prepovedano kakršnokoli zasledovanje, nadlegovanje ter oboroževanje avtomatiziranih zračnih sistemov. Ob tem je za uporabo v tovrstne namene strogo določena tudi lokacija ter čas uporabe samega sistema (Wallace 2015).

Ob tem je potrebno poudariti, da na področju vdora v zasebnost s strani avtomatiziranih zračnih sistemov prihaja tudi do razvoja protiukrepov. Tako je ameriško podjetje Domestic drone countermeasures razvilo sistem za detekcijo avtomatiziranih zračnih bojnih sistemov, pri čemer poudarjajo, da sistem omogoča zgolj zaznavo sistemov v uporabi s strani civilistov. Tako je sistem sestavljen iz modula za poveljevanje in nadzor ter iz dveh senzorjev za detekcijo. Sistem deluje tako, da uporabnika obvesti o tem, kdaj je nek avtomatizirani zračni sistem v njegovi bližini (Passary 2014).

Čedalje večja uporaba avtomatiziranih zračnih sistemov – tako s strani organov pregona in vojske kot tudi številnih podjetij ter zasebnih uporabnikov – pomeni na dolgi rok tudi precejšnjo zgostitev zračnega prometa. Če v obzir vzamemo trenutno stanje zračnega prometa, ki zajema vse od vojaške uporabe in potniških prevozov ter civilne oz. zasebne uporabe, bo lahko tovrstna zgostitev brez ustrezne regulacije v bodoče pomenila grožnjo

varnosti. Trenutno se oblasti ukvarjajo z različnimi prepovedmi poletov nad določenimi območji (*no-fly zone* – območje prepovedi letenja), dovoljeno razdaljo do objektov, samoregistracijo uporabnikov ipd. (Merrill in Troen 2014).

Ob zgoraj omenjeni zgostitvi zračnega prometa ter dejstvu, da je sama tehnologija avtomatiziranih zračnih sistemov še v razvoju, kar pomeni, da sama uporaba tovrstnih sistemov še ni tako visoka, je dejstvo, da že na tej točki razvoja prihaja do bližnjih srečanj ter skorajšnjih trčenj med avtomatiziranimi zračnimi sistemi in preostalim zračnim prometom, zaskrbljujoče.

V Veliki Britaniji je na letališčih Heathrow, Stansted, City airport in Manchester že prišlo do tovrstnih bližnjih srečanj z avtomatiziranimi zračnimi sistemi, pri čemer je bilo vedno vpleteno tudi potniško letalo. Ob tem so oblasti pričele s pobudo, da se za imetnike avtomatiziranih zračnih sistemov ustvari nek registracijski sistem, ki bo omogočal izsledite lastnika, ki je avtomatizirani zračni sistem upravljal na nedovoljenem območju ali zagrešil kakšen drug prekršek, pri čemer se ob zgoraj omenjenem registracijskem sistemu snuje tudi sistem sankcioniranja (Topham 2016).

Ob tovrstni umestitvi in varnostnih implikacijah, ki jih povzročajo avtomatizirani zračni sistemi, je moč dobiti nekakšen oris o umestitvi in varnostnih implikacijah, ki zadeva avtomatizirane zračne bojne sisteme. V nadaljevanju magistrskega dela bo moč pridobiti oris o kompleksnosti avtomatiziranih zračnih bojnih sistemov, njihovi umestitvi in varnostnih implikacijah ter grožnjah njihovemu delovanju, začenši z njihovo klasifikacijo.

3 Klasifikacija avtomatiziranih zračnih bojnih sistemov

Kot sem že uvodoma pojasnil bo magistrsko delo osredotočeno na avtomatizirane zračne bojne sisteme (*unmanned aerial combat vehicles*). Za lažjo predstavo oz. razumevanje je potrebno pojasniti pomen zgoraj navedenih besed, in sicer s klasifikacijo avtomatiziranih sistemov. Prva potrebna razmejitev je razmejitev med avtomatiziranimi kopenskimi sistemi (*unmanned ground vehicles*) in avtomatiziranimi zračnimi sistemi (*unmanned aerial vehicles*) oz. vozili. Ker se bo magistrsko delo osredotočalo na slednjo različico, bom zanemaril klasifikacijo kopenske različice ter nadaljnjo klasifikacijo pojasnil zgolj za zračno različico tovrstnih sistemov.

Kako poteka klasifikacija znotraj avtomatiziranih zračnih sistemov? V osnovi poteka med avtomatiziranimi zračnimi sistemi (*unmanned aerial systems* – UAS) in avtomatiziranimi zračnimi bojnimi sistemi (*unmanned combat aerial systems* – UCAS). Meja med obema tipoma oz. med obema oblikama pa je tanka in predstavlja nekakšno sivo cono, saj je po navedbah vira potrebno na avtomatiziran zračni sistem zgolj namestiti »bojno komponento«, da potem le-ta postane avtomatiziran zračni bojni sistem. Sam pojem avtomatiziran zračni sistem definira dejstvo, da nima posadke in leti glede na upravljanje na daljavo, glede na pred-programiran načrt letenja ali glede na nekakšen samostojni sistem razmišljanja (umetna inteligenca). Avtomatizirani zračni sistemi se po navedbah vira od klasičnih raket dolgega dosega razlikujejo po tem, da se vrnejo na mesto vzleta, kar omogoča ponovno uporabo. Vendar pa pri tem ne gre pozabiti, da že obstajajo tudi avtomatizirani zračni sistemi, ki delujejo po principu *fire-and-forget*. Princip je pravzaprav enak principu predhodno omenjenih raket in jih po izstrelitvi ni moč ponovno uporabiti, saj ob uničenju cilja (v kolikor govorimo o bojni različici) pride tudi do njihovega samouničenja (SIPRI 2007).

V splošnem se poraja čedalje več klasifikacij avtomatiziranih zračnih sistemov, ki se med seboj precej razlikujejo. Svoje klasifikacije snujejo različne organizacije, kot je npr. Organizacija severnoatlantske pogodbe (*North atlantic treaty organisation* – NATO), Evropska unija (EU), posamezne države, ki bodisi že posedujejo tovrstne sisteme bodisi

razmišljajo o njihovi uvedbi oz. uporabi. Te klasifikacije se med seboj razlikujejo po tem, da tovrstne sisteme klasificirajo glede na razrede (specifični indikatorji, kot je denimo masa, nosilnost, domet ipd.), glede na velikost (mikro, mini, srednje veliki, veliki) (Ministrstvo za obrambo Velike Britanije 2010). Kot že navedeno se avtomatizirani zračni sistemi v osnovi od avtomatiziranih zračnih bojnih sistemov ločijo po posedovanju »bojne komponente«. Sicer pa se avtomatizirani zračni sistemi v osnovi po navedbah vira ločijo glede na njihovo vlogo, in sicer vloga avtomatiziranih zračnih sistemov, ne glede na zorni kot, vedno predstavlja neko podporno funkcijo samemu boju, ne glede na to, za kakšen boj gre in proti komu poteka. Vloge, po navedbah Stockholmskega mednarodnega mirovnega raziskovalnega inštituta (*Stockholm international peace research institute* – SIPRI), so naslednje: izvidništvo, zbiranje podatkov s pomočjo radarjev, optičnih in/ali elektro-optičnih senzorjev, zbiranje obveščevalnih podatkov, nadzor morja, podpora pri iskanju in reševanju, nadzorovanje in beleženje zbranih podatkov, ne-smrtonosna bojna vloga, elektronski protiukrepi in elektronsko bojevanje, delovanje kot vaba ter nadzor ognja/določanje tarč (SIPRI 2007).

Ena izmed možnih klasifikacij, ki sem jo prav tako že omenil, je klasifikacija, ki izhaja iz Ministrstva za obrambo Velike Britanije. Sicer bo za pričujočo magistrsko nalogo ključna razmejitev glede na »bojno komponento«, torej razmejitev na avtomatizirane zračne sisteme in na avtomatizirane zračne bojne sisteme, bo kljub temu (s perspektive kasnejše primerjave izbranih modelov) relevantna tudi klasifikacija, ki vsebuje razdelitev na posamezne razrede. Kot osnovo za tovrstno razdelitev Ministrstvo za obrambo Velike Britanije (2010) navaja razdelitev glede na težo ob vzletu in glede na operativno višino, ki sicer velja za običajna letala. Prvi razred tako zajema avtomatizirane zračne sisteme oz. brezpilotne letalnike, katerih teža ob vzletu znaša manj kot 150 kilogramov. Gre za najmanjše sisteme, ki se jih zažene z roko in imajo precej kratek domet. Njihova oprema zajema elektro-optične oz. infrardeče sisteme, prav tako pa premorejo nekaj logističnega prostora. Načeloma vedno ostanejo v vidnem polju upravljavca, delujejo pa do višine 5000 čevljev nad površjem. Znotraj tega razreda poteka še dodatna razmejitev, in sicer na mikro, mini in male sisteme, med katerimi potekajo dodatne razmejitve glede teže pri vzletu, dometa, operativne višine in nalog. Drugi razred zajema srednje velike sisteme, ki jih je potrebno izstreliti s pomočjo nekakšnega izstrelitvenega sistema, katerih teža ob vzletu znaša med 150 in 600 kilogrami. Gre za taktične sisteme, ki se gibljejo do višine 10 000 čevljev nad površjem, njihov efektivni domet pa znaša približno 200 kilometrov. Zadnji razred zajema sisteme, katerih teža ob vzletu znaša

več kot 600 kilogramov. Gre za sisteme, ki vzletajo samostojno in se gibljejo v najvišjih pasovih, so operativne, strateške ali bojne narave in katerih domet je praktično neomejen (prav tam).

4 Analiza izbranih modelov

4.1 Samostojni avtomatizirani zračni bojni sistemi

Samostojni avtomatizirani zračni bojni sistemi se od drugega tipa tovrstnih sistemov, ki ga bom predstavil in analiziral v nadaljevanju, razlikujejo v več segmentih. Za namen samega razlikovanja je potrebno sprva definirati, kaj natanko imam v mislih pri samostojnih avtomatiziranih zračnih bojnih sistemih. Za začetek je potrebno obrazložiti razliko, ki jo navaja že predhodno omenjen dokument Ministrstva za obrambo Velike Britanije (2010), in sicer med avtomatiziranim in avtonomnim. Nek avtomatiziran sistem tako zaznamuje dejstvo, da se ravna po vnaprej določenih pravilih in omejitvah. V primeru nekega avtomatiziranega zračnega bojnega sistema to pomeni, da letalnik leti v skladu z vnaprej določeno potjo leta in se odziva glede na ukaze, ki jih pridobiva s strani svojega upravljalca v realnem času. Na drugi strani imamo t. i. avtonomne sisteme, katerih bistvena značilnost in hkrati razlika od predhodno obravnavanih avtomatiziranih sistemov je ta, da so v neki situaciji sami zmožni odreagirati glede na okoliščine. Glede na dokument Ministrstva za obrambo Velike Britanije (2010) naj bi bili tovrstni sistemi sposobni samostojno razumeti višje cilje in usmeritve, samostojno doseči želeni rezultat – pa naj si bo to v vojaški sferi uničenje nekega vojaškega cilja ali zgolj dostava pošiljke, v kolikor se tovrstni sistem uporablja v komercialne namene.

Vendar pa slika ni več tako črno-bela, kot je v primeru zgoraj omenjene razmejitve. Sodobni samostojni avtomatizirani zračni bojni sistemi, ki jih bom v nadaljevanju tudi analiziral, so do neke mere že postali avtonomni. V nadaljevanju sledi ključna obrazložitev besede »samostojni«. Samostojni avtomatizirani zračni bojni sistemi so tako denimo General

Atomics MQ-1C Gray Eagle, Mikoyan Skat ipd. Gre za avtomatizirane zračne bojne sisteme, ki vzletijo »samostojno«. To ne pomeni, da že posedujejo zadostno raven inteligence, da bi samostojno zaznali, kdaj je čas za vzlet, temveč da ročna izstrelitev (s pomočjo človeka) ali izstrelitev oz. vzlet s pomočjo neke izstrelitvene naprave ni več potrebna.

Gre torej za to, da nekemu upravljalcu za vzlet tovrstnega sistema ni potrebno biti fizično prisoten. Razvoj je prišel do te točke, ko se upravljalec lahko nahaja na varnem (denimo nekje v kontrolnem stolpu) in vnaša ukaze v računalnik, ki je povezan s samim avtomatiziranim zračnim sistemom ter tako tovrsten sistem spravi v zrak. Takšen način izstrelitve je na eni strani mogoč in na drugi strani potreben tudi zato, ker navadno ti sistemi, če pogledamo klasifikacijo Ministrstva za obrambo Velike Britanije (2010), spadajo glede na težo v zgornja dva razreda, kar samo izstrelitev v primeru ročne izstrelitve ali v primeru izstrelitve s pomočjo nekega sistema bistveno oteži. Pod samostojnimi avtomatiziranim zračnimi bojnimi sistemi bom tako pojmoval avtomatizirane zračne bojne sisteme, ki so sposobni vzleta s pomočjo zgolj sledenja posredovanim ukazom s strani upravljalca ter vzletno-pristajalne steze.

4.1.1 General Atomics: MQ-1C Gray Eagle

MQ-1C Gray Eagle je produkt ameriškega proizvajalca General Atomics. Gre za podjetje, ki je specializirano v avtomatiziranih zračnih sistemih, nekaterih njihovih posameznih komponentah, kot so denimo radarji in nadzorni sistemi, ter v rokovanju s tovrstnimi sistemi. Poleg snovanja celostnih avtomatiziranih zračnih sistemov proizvajajo tudi različne kopenske nadzorne postaje (*Ground control stations*), različne multifunkcijske radarje in senzorje ter naprave za izvajanje obveščevalne dejavnosti, nadzora in izvidništva (*Intelligence, surveillance and reconaissance – ISR*) (General Atomics 2015).

Sam avtomatiziran zračni sistem MQ-1C Gray Eagle ima t. i. dvojno naravo. Gre za predhodno omenjeno možno razmejitev oz. klasifikacijo nekega sistema na bojnega ali nebojnega. MQ-1C Gray Eagle predstavlja avtomatiziran zračni sistem, ki lahko poseduje bojno komponento ali izvaja zgolj naloge, ki so povezane z obveščevalno dejavnostjo,

nadzorovanjem ali izvidništvom. MQ-1C Gray Eagle je nastal kot posledica želje po nadgradnji modela RQ-5 Hunter. Kot njegovega zadnjega predhodnika se navaja avtomatiziran zračni bojni sistem oz. brezpilotni letalnik, ki deluje pod imenom Predator. Avtomatiziran zračni bojni sistem MQ-1C Gray Eagle predstavlja izredno večnamenski avtomatiziran zračni sistem, saj njegove sposobnosti zajemajo vse od nalog izvidništva, nadzora, določanja tarč, poveljevanja in vodenja, komunikacijske naprave, informacije sredstev za zveze, elektronskega bojevanja, nošenja improviziranih eksplozivnih sredstev oz. naprav ter misije ocenjevanja bojne škode (Army Technology 2015a).

Poleg tega se, podobno kot njegov predhodnik, sistem ponaša s podpornim sistemom, ki zagotavlja, da le-ta v primeru neke okvare ali napake še vedno deluje. Tako imenovani *Triple-redundant avionics system architecture* pravzaprav predstavlja sistem trojnega podvajanja. V osnovi je v vsakem avtomatiziranem sistemu določena programska oprema oz. *software,* ki zagotavlja delovanje tovrstnega sistema. Sistem trojnega podvajanja to osnovno programsko opremo pravzaprav še dvakrat prekopira, s čimer ustvari vzporedni podporni sistem v primeru neke okvare. Glede na to, da ta programska oprema deluje vzporedno, so za namene preprečevanja vmešavanja zdaj enega zdaj drugega programskega sistema med posameznimi sistemi t. i. ključavnice. Tako v primeru programske okvare uporabnik avtomatiziranega sistema preprosto zamenja vmesnik (preklopi na podporni program) ter tako zagotavlja nadaljnje nemoteno delovanje nekega avtomatiziranega sistema (Resch in drugi 2013).

V nadaljevanju sledi analiza posameznih komponent ter tehničnih posebnosti samega avtomatiziranega zračnega bojnega sistema MQ-1C Gray Eagle, in sicer treh osnovnih komponent, kot so pogon oz. motor, oborožitveni podsistemi ter obremenitev oz. nosilnost (pri čemer ne bom govoril zgolj o nosilnosti, ki jo ta sistem premore, temveč tudi o podsistemih, ki prispevajo k tej obremenitvi) in končno tehnične posebnosti, ki zaznamujejo ta avtomatiziran zračni bojni sistem.

MQ-1C Gray Eagle poganja Thielertov dizelski motor z 2000 kubičnimi centimetri delovne prostornine, ki proizvede 155 konjskih moči. Podjetje Continental Motors, čigar lastnik je kitajska družba AVIC, je leta 2006 prevzelo nemško podjetje Thielert. S prevzemom je

prevzelo tudi njihove patente ter produkte in tako nadaljuje s produkcijo predhodno zasnovanih motorjev Centurion, ki se jih uporablja za brezpilotne letalnike. Podjetje Thielert je sprva snovalo motorje, ki so delovali zgolj na dizelsko gorivo (Phelps 2013).

Zakaj so zgoraj omenjeni podatki relevantni? Poleg tehničnih karakteristik in podatkov o delovni prostornini ter moči, ki jo sam motor proizvede, je pomemben tudi prehod iz zgolj dizelskega goriva na kombinacijo oz. mešanico med kerozinom in dizelskim gorivom. Gre za t. i. težko gorivo. V ZDA obstaja več različnih goriv, ki jih uvrščajo med t. i. težka goriva, a je za namene pričujočega magistrskega dela pomemben zgolj podatek, da gre v osnovi za kakršnokoli mešanico med kerozinom in dizelskim gorivom – ne glede na podatek, kolikšen odstotek določene snovi je dejansko v nekem gorivu. Ob tem je uporaba težkega goriva v primerjavi z dizelskim gorivom bolj ugodna z več vidikov, in sicer je v prvi vrsti kerozina kot goriva, kar zadeva svetovne zaloge, absolutno največ. Poleg tega je za vžig težkega goriva potrebna veliko višja temperatura kot za vžig dizelskega goriva, kar pomeni, da je shranjevanje goriva veliko bolj varno. Glede na to, da večino svetovne zaloge goriva predstavlja kerozin, je posledično težje gorivo zaradi večje razpoložljivosti cenejše (Heavy fuel international 2015).

Prav tako se uporaba težkega goriva za uporabo tudi pri brezpilotnih letalnikih sklada z načrtom ZDA o konceptu uporabe enotnega goriva (*Single fuel concept*). Gre za koncept, ki so ga uradno vpeljali z letom 1988. Koncept v osnovi veleva, da ameriške sile v primeru mobilizacije (*deployment*) uporabljajo zgolj eno vrsto goriva. Po navedbah pristojne oblasti ob vsaki napotitvi na neko misijo poudarijo, ali bo prišlo do uveljavitve tega koncepta ali ne. Pri brezpilotnih letalnikih lahko na drugi strani vidimo, da ko gre za uveljavitev neke nove tehnologije, snovalci že ob izdelavi predvidevajo uporabo tega koncepta, saj uporabljajo motorje, ki so kompatibilni z nekim težkim gorivom. Primer je denimo analizirani brezpilotni letalnik Gray Eagle (Le Pera 2005).

Kar zadeva oborožitev brezpilotnega letalnika lahko v skladu s celotno dovoljeno obtežitvijo na 17 metrov dolga krila namestimo številne sisteme za določanje tarč – tako v zraku kot tudi na tleh, radarje, komunikacijske komponente in štiri rakete tipa Hellfire (Army Technology

2015a). Vrste možnih zunanjih komponent bom razdelal nekoliko kasneje, na tej točki se bom osredotočil zgolj na oborožitev v smislu raket tipa Hellfire.

Pri raketah tipa Hellfire je potrebno izpostaviti, da ne gre zgolj za tip oz. model rakete. Beseda Hellfire predstavlja sinonim za skupino raket, ki se jih ne uporablja zgolj v zračnih silah. Podjetje Orbital ATK, ki proizvaja rakete tipa Hellfire, poleg samih raket proizvaja tudi izstrelitveno komponento za rakete pod istim imenom (Orbital ATK Inc 2015a).

Izstrelitvena komponenta za rakete, tj. motor, predstavlja visoko zmogljivo izstrelitveno komponento, ki izstrelek izstreli z minimalno količino dima, kar rezultira v težko zaznavo izstrelitve. Hkrati to pomeni tudi boljšo vidljivost v primeru, da gre za oborožitveni sistem s posadko, obenem pa sama zasnova izstrelitvene komponente ne moti signala vodenja izstrelka. Celotna izstrelitvena komponenta je po navedbah proizvajalca cenovno ugodna in zanesljiva. S samo proizvodnjo je podjetje pričelo leta 1989. Do danes je v uporabi preko 80 000 tovrstnih izstrelitvenih komponent. Sama komponenta tehta 14,2 kilogramov, v dolžino meri 59,3 centimetrov, njena debelina pa znaša 17,7 centimetrov. Naj zgolj kot zanimivost navedem, da je sama komponenta operativna v temperaturnem razponu od -43^{o} C pa do +63^{o} C, njena pričakovana življenjska doba pa znaša 20 let (Orbital ATK Inc 2015b).

Kot že navedeno gre pri raketah tipa Hellfire za skupino raket, ki jih je mogoče izstreliti z več vrst platform. Tako se rakete tipa Hellfire uporablja v zračnih silah (helikopterji, letala, brezpilotna letala), kopenskih silah (predvsem na vozilih, poznanih pod imenom Hummer) in pomorskih silah (priobalne bojne ladje). Zasnova in razvoj raket tipa Hellfire sega v leto 1974, proizvodnja pa se je začela leta 1982, in sicer z modelom AGM-114A. Po tem modelu je prišlo še do nadgradnje modela na AGM-114B in do proizvodnje različnih testnih modelov. Danes je v uporabi 5 modelov raket tipa Hellfire, in sicer:

- AGM-114K (gre za raketo zasnovano za uničevanje bojnih vozil);
- AGM-114L (gre za raketo, ki deluje po principu *fire-and-forget* tudi v težkih vremenskih pogojih);
- AGM-114M (gre za raketo, ki ob kontaktu razpade na več delcev);

- AGM-114N (gre za precizno raketo, namenjeno za uničevanje stavb, ki povzroča malo postranske škode);
- AGM-114R (gre za raketo, ki združuje vse lastnosti predhodno omenjenih modelov raket in vsebuje pol-aktiven laserski sistem za določanje tarč, kar ji omogoča širok nabor tarč) (Army Technology 2015b).

Rakete tipa Hellfire tehtajo med 45,4 in 49 kilogramov, imajo doseg od 7,1 do 11 kilometrov, njihov pogonski sitem pa jim mogoča, da ob izstrelitvi dosegajo pospešek tudi do 10G (prav tam).

Poleg oborožitve samostojni avtomatiziran zračni bojni sistem MQ-1C Gray Eagle odlikujejo tudi drugi podsistemi, kot so denimo:

- elektro-optičen oz. infrardeč podsistem za določanje in identifikacijo tarč podjetja Raytheon z oznako MTS (CSP) (Raytheon 2013);
- taktični radar STARLite z oznako AN/ZPY-1 podjetja Northrop Grumman (Northrop Grumman 2015);
- podsistem za komunikacijo (Army Technology 2015b).

MQ-1C Gray Eagle se ponaša tudi z nekaj specifičnimi lastnostmi, kot so denimo upravljanje s premične nadzorne postaje, ki se nahaja na tleh, krila in rep so zasnovani tako, da so odporni proti zmrzali, prav tako pa je mogoče sam sistem transportirati v letalu tipa C-130 (General Atomics 2015b).

4.1.2 Mikoyan Skat

Rusija je leta 2007 na salonu MAKS pod nazivom Mikoyan Skat predstavila svojo različico samostojnega avtomatiziranega zračnega bojnega sistema oz. oboroženega brezpilotnega letalnika. Kljub visokim ciljem – nosilnost do 10 ton in doseg do 4000 metrov – se projekt sprva ni realiziral. Rusija je po začetnem neuspehu namenila 5 milijard rubljev za razvoj ruskih avtomatiziranih zračnih bojnih sistemov, a le-to ni imelo željenega učinka. Posledično je Rusija za zapolnitev vrzeli odkupila načrte in dele izraelskih avtomatiziranih zračnih sistemov IAI Searcher Mk II in IAI Bird Eye 400, razvila pa je tudi nekatere svoje prototipe. Ker so bili rezultati testiranj pod pričakovanji, še vedno ni preizkušenega modela, ki bi bil operativen (Russia & India report 2015).

Leta 2013 so v javnost prišle informacije, da ideja iz 2007 le ni zamrla in da Rusija vendarle razvija svojo različico avtomatiziranega zračnega bojnega sistema, ki temelji na prototipu Mikoyan Skat iz leta 2007. Kljub temu, da je proizvodnja po letu 2008 zamrla, naj bi bilo v celoti izdelanih 17 prvotnih modelov. Leta 2013 je na osnovi tega modela prišlo do razvoja dogodkov, saj naj bi podjetji MiG in Sukhoi združila moči in izdelovala tovrsten sistem na osnovi prvotnega modela. Pogonski agregat naj bi predstavljal agregat pod oznako Klimov RD 5000B (derivat motorja Klimov RD-93), kar naj bi novemu modelu omogočalo hitrost 800 kilometrov na uro in doseg do 2000 metrov. Največja višina, ki naj bi jo novi model dosegal, naj ne bi presegala 12 000 metrov. Kar zadeva samo oborožitev ni specificirano, kakšne vrste oborožitev naj bi sam avtomatizirani zračni bojni sistem posedoval, znan je le podatek, da naj bi teža same oborožitve segala vse do 2 ton (Immortal today 2014).

Trenutno je novi model Skata še vedno v eksperimentalni fazi, zato se Rusija še naprej zanaša na tovrstne oborožitvene sisteme, ki jih je kupila od Izraela. V nadaljevanju bom analiziral ta dva modela in s tem ustvaril nekakšno sliko, kakšna oborožitev v smislu avtomatiziranih zračnih sistemov trenutno dopolnjuje ruske zračne sile.

Na začetku je potrebno poudariti, da nakupljeni izraelski avtomatizirani zračni sistemi ne posedujejo t. i. bojne komponente, kar pomeni, da avtomatizirana zračna sistema (tako IAI Searcher Mk II kot tudi IAI Bird eye 400) nista oborožena. IAI Searcher Mk II predstavlja večnamenski avtomatizirani zračni sistem, ki ga je moč uporabiti v raznovrstnih misijah za namene izvidništva, ocenjevanja škode, nadzorovanja ipd.

IAI Searcher Mk II tako poseduje:

- elektro-optičen oz. infrardeč podsistem za določanje in prepoznavo tarč;
- taktični radar;
- podsistem za komunikacijo;
- sposobnost letenja v težkih vremenskih pogojih;
- nizko zvočni motor, ki ga naredi težko zaznavnega (Unmanned 2015).

Celoten sistem je hkrati zgrajen iz kompozitnih materialov, kar ga naredi težko zaznavnega (prav tam).

Na drugi strani IAI Bird eye 400, ki se ga uporablja za namene obveščevalne dejavnosti, izvidništva in nadzorovanja, prav tako predstavlja avtomatiziran zračni sistem, ki ne poseduje orožja. Slednje mu omejujejo tudi tehnično-taktične lastnosti, saj sistem ne preseže 304 metrov višine, njegov operativni doseg pa znaša prib. do 10 kilometrov. Gre pravzaprav za mini-različico avtomatiziranega zračnega sistema (Airforce technology 2015).

IAI Bird eye 400 poseduje sledeče tehnične komponente:

- prenosno nadzorno kopensko postajo;
- podsistem infrardečih senzorjev;
- elektro-optični podsistem za opazovanje (prav tam).

Na tem področju je Rusija v primerjavi z drugimi velesilami očitno v velikem zaostanku. Kaj kljub zaostanku pomenijo trenutne zmogljivosti ruskih avtomatiziranih zračnih sistemov pa bo ob primerjavi posameznih modelov moč videti kasneje. Kot zanimivost naj navedem, da kljub nakupu izraelskih avtomatiziranih zračnih sistemov, le-ti niso bili kupljeni kot zaključena celota in nato pripeljani v Rusijo, temveč je (če poenostavim) Rusija kupila zgolj načrte in dele, na svojem ozemlju sestavila te avtomatizirane zračne sisteme in jih predstavila pod drugimi imeni. Ti imeni sta Zastava in Forpost (Lugansk news today 2015).

Ker so podatki za oba avtomatizirana zračna sistema skopi (kar sem do določene mere tudi pričakoval), sem na podlagi navedb, da je Rusija načrte za ta dva avtomatizirana zračna sistema odkupila od Izraela, nadaljnje informacije glede tehnično-taktičnih značilnosti črpal iz vira, tj. Israel Aerospace Industries.

Podatki, ki sem jih pridobil od prvotnega proizvajalca »ruskih« avtomatiziranih zračnih sistemov, tj. Israel Aerospace Industries, govorijo o avtomatiziranih zračnih sistemih IAI Searcher Mk III in IAI Bird eye 400. Pri prvem modelu je moč opaziti razliko pri oznaki. Razlog za to je posodobitev oz. nadgradnja modela IAI Searcher Mk II. V nadaljevanju bom zgolj za predstavo o zmogljivostih IAI Searcher Mk II predstavil posodobljeno različico, torej model IAI Searcher Mk III.

Tehnično-taktične karakteristike IAI Searcher Mk III zajemajo:

- elektro-optičen oz. infrardeč podsistem za določanje in identifikacijo tarč;
- taktični radar;
- sistem za prestrezanje informacij SIGINT[1];
- specifičen sistem, ki mu omogoča operativnost tudi izven vidnega polja upravljalca;
- dvojni sistem za avtomatsko vzletanje in pristajanje (v primeru odpovedi prvotnega, upravljanje prevzame dvojnik);

[1] Gre za obveščevalni sistem prestrezanja in zbiranja informacij iz komunikacij in/ali informacijskih sistemov (National security agency 2009).

- vgrajen 4-taktni motor, ki povzroča minimalen hrup;
- največji doseg sistema (radij) znaša 250 kilometrov;
- vzdržljivost sistema do 18 ur;
- razpon kril znaša 8,55 metrov;
- meja za nosilnost zunanjega tovora znaša 120 kilogramov (Israel Aerospace Industries 2015a).

Drugi avtomatiziran zračni sistem, ki ga bom v nadaljevanju predstavil na osnovi podatkov pridobljenih pri Israel Aerospace Industries, je IAI Bird eye 400. Gre za specifičen avtomatiziran zračni sistem. IAI Bird eye 400 izhaja iz skupine mini avtomatiziranih zračnih sistemov. Za razliko od vseh predhodno omenjenih avtomatiziranih zračnih sistemov je zasnovan na električni pogon. Nabor operacij oz. misij, ki jih ta avtomatiziran zračni sistem lahko izvaja, zajema izvidništvo, nadzorovanje, ocenjevanje škode in urbane operacije

Tehnično-taktične lastnosti:

- celoten avtomatiziran zračni sistem je moč prenašati v dveh nahrbtnikih;
- kamera z visoko ločljivostjo za dnevne in nočne operacije se zaradi boljšega zajemanja slik nahaja na spodnjem delu trupa;
- vzlet s pomočjo nekakšne elastike (bungee launch) in optimiziran koncept pristajanja (ob pristajanju se sproži posebno padalo);
- avtomatiziran način letenja, ki vključuje vzletanje in pristajanje;
- električni pogon, ki zagotavlja minimalno avdio sled;
- razpon kril znaša 2, 2 metra;
- največja nosilnost zunanjih sistemov znaša 1, 2 kilograma;
- vzdržljivost sistema do 90 minut (Israel Aerospace Industries 2015b).

Z vidika bojne komponente avtomatiziranih zračnih sistemov je torej jasno, da Rusija na tem področju še nima ustrezne rešitve in tovrstno podhranjenost rešuje oz. bolje rečeno kompenzira z uporabo svojih lovskih letal v proporcionalno večjem obsegu. Koliko pa trenutno obstoječi sistemi že prispevajo k obrambi pa kasneje v primerjalnem delu, ki bo

sledil analizi avtomatiziranega zračnega bojnega sistema kitajskega izvora z oznako Guizhou WZ - 2000.

4.1.3 Guizhou WZ - 2000

Avtomatiziran zračni sistem Guizhou WZ - 2000 (poznan tudi pod oznako WZ-9 in WuZhen 2000) je plod dela številnih različnih institucij na Kitajskem in predstavlja preboj te države na področju tehnologije avtomatiziranih zračnih bojnih sistemov. Podobno kot pri modelu Grey Eagle ima ta avtomatiziran zračni sistem dvojno naravo. Tako obstajata dve različici, in sicer bojna ter nebojna. Prvi polet je ta avtomatiziran zračni bojni sistem zabeležil leta 2003 (MilitaryFactory 2015). Sama ideja o začetku raziskav v smeri avtomatiziranih zračnih (bojnih) sistemov je bila, po navedbah vira, rezultat udejstvovanj tovrstnih sistemov na Balkanu v devetdesetih letih 20. stoletja. V začetku raziskovanja je bil GAIC (*Guizhou Aviation Industry Group*) zgolj eno izmed številnih podjetij, ki je poskušalo ustvariti nek napredek na tem področju. Skupaj s še tremi univerzami je podjetju leta 2003 uspelo narediti preboj na tem področju, leta 2008 pa je avtomatiziran zračni bojni sistem z oznako Guizhou WZ - 2000 uradno postal tudi prvi avtomatiziran zračni bojni sistem Kitajske (Boyuan 2014).

V nadaljevanju sledi analiza tehnično-taktičnih značilnosti dotičnega avtomatiziranega zračnega bojnega sistema, in sicer po enakih parametrih kot pri predhodno omenjenih modelih.

Gonilo kitajskega avtomatiziranega zračnega bojnega sistema je pogonski agregat z oznako AI-25. Gre za turbo-propelerski agregat podjetja Ivchenko Progress iz Ukrajine (MilitaryFactory 2015). Sam agregat AI-25 se uporablja za pogon številnih letal, tudi lažjih modelov letal, za namene uporabe v avtomatiziranih zračnih sistemih pa se uporablja posebej prirejen agregat z oznako AI-25TL 300.11, ki pravzaprav predstavlja derivat prvotnega agregata z oznako AI-25. Prvotni pogonski derivat AI-25 je podjetje Ivchenko Progress začelo proizvajati v komercialne namene leta 1967, prvi derivat AI-25TL pa je v produkcijo prišel leta 1973 (Ivchenko Progress 2015a). Vseh pogonskih agregatov, torej tako prvotnega AI-25 kot tudi vseh derivatov, je bilo izdelanih preko 5100. Po navedbah podjetja Ivchenko Progress se danes agregati zgolj tega tipa uporabljajo v več kot 37 državah. Zgolj kot zanimivost naj navedem, da v navedbah podjetja ni moč zaslediti podatka o številu izdelanih derivatov

prvotnega pogonskega agregata z oznako AI-25TL 300.11, ki naj bi se uporabljal zgolj za pogon avtomatiziranih zračnih sistemov (Ivchenko Progress 2015b).

Ob vseh zgoraj naštetih derivatih je potrebno podrobneje opredeliti oz. navesti nekaj podatkov o posameznih derivatih in o prvotnem modelu pogonskega agregata AI-25. Prvotni pogonski agregat z oznako AI-25 je bil zaradi same zmogljivosti namenjen za uporabo v potniških letalih, in sicer v nižjem razredu (do nekje 40 potnikov). Tipičen model, pri katerem je bil uporabljen oz. vgrajen tovrstni agregat, je letalo Yak 40. Specifične karakteristike, ki jih navaja podjetje Ivchenko Progress so, da pogonski agregat tehta 312 kilogramov, ob vzletu pa proizvede do 1500 kilogramov na funt potiska. Pričakovana življenjska doba tega prvotnega modela pogonskega agregata je do 20 000 ur (Ivchenko Progress 2015a).

Derivat in hkrati posodobljena verzija prvotnega pogonskega agregata (z oznako AI-25) AI-25TL se od prvotnega razlikuje po tem, da ob vzletu proizvede večjo silo potiska (1720 kilogramov na funt), da tehta 38 kilogramov več ter da njegova pričakovana življenjska doba dosega zgolj petino življenjske dobe prvotnega modela (AI-25), tj. nekje do 4000 ur. Predhodno omenjeni podatki so ključni za predstavo o ne toliko sami zmogljivosti kot samem izvoru pogonskih agregatov, ki poganjajo avtomatizirane zračne sisteme. Zadnji predstavljeni derivat (AI-25TL) je namreč osnovni model, iz katerega je nato nastal že omenjeni AI-25TL 300.11., ki se, po navedbah podjetja Ivchenko Progress, uporablja tako za pogon avtomatiziranih zračnih sistemov na splošno kot tudi pogon samega avtomatiziranega zračnega bojnega sistema Guizhou WZ-2000 (Ivchenko Progress 2015c).

Kar zadeva tako samo oborožitev kot tudi vse preostale komponente so podatki izredno skopi. Eden izmed problemov pri preučevanju avtomatiziranih zračnih (bojnih) sistemov kitajskega porekla je tudi ta, da obstaja na Kitajskem ogromno avtomatiziranih zračnih (bojnih) sistemov s svojevrstnimi oznakami (Chengdu, Tian-ji, WuZhen, Sky Wing, Long Eagle, Divine Eagle itd.) (Fisher 2011). Večina teh avtomatiziranih zračnih bojnih sistemov, v kolikor ne vsi, predstavljajo prototipe. Tako pride ob prebiranju literature, ko želimo pridobiti podatke o točno določenem tipu oz. modelu avtomatiziranega zračnega (bojnega) sistema, zaradi poplave različnih oznak, do ogromne zmešnjave. Hkrati je na splošno za avtomatizirane

zračne (bojne) sisteme kitajskega porekla na voljo izredno omejeno število podatkov. Posledično lahko analiza nekega izbranega avtomatiziranega zračnega (bojnega) sistema hitro postane stvar špekulacij.

Če se vrnem k izbranemu modelu avtomatiziranega zračnega (bojnega) sistema in iz danih podatkov poskušam opredeliti oborožitev in dodatne komponente ter morebitne sistemske posebnosti samega avtomatiziranega zračnega sistema, lahko navedem, da ima ta avtomatiziran zračni (bojni) sistem:

- taktični radar;
- sistem za prestrezanje informacij SIGINT ter
- elektro-optičen oz. infrardeč podsistem za določanje in identifikacijo tarč (Aviations Militaires 2015).

Sama komunikacija oz. posredovanje podatkov upravljalcu avtomatiziranega zračnega (bojnega) sistema poteka preko povezave s satelitom. Druge relevantne tehnično-taktične lastnosti poleg zgoraj omenjenih pa so še:

- vzdržljivost sistema do 3 ur;
- razpon kril do 9,8 metrov;
- operativen radij delovanja do 800 kilometrov;
- domet do 2400 kilometrov;
- hitrost do 800 kilometrov na uro;
- največja operativna višina 17983 metrov (prav tam).

Kar zadeva bojno komponento tega avtomatiziranega zračnega bojnega sistema izrecnega podatka, ki bi navajal točno določen tip ali znamko ter naravo same komponente ni. Po nekaterih navedbah naj bi bil ta avtomatiziran zračni bojni sistem opremljen z raketami tipa zemlja-zrak ali z vodenimi izstrelki (prav tam). Oziraje na druge avtomatizirane zračne bojne sisteme kitajskega porekla, kot so denimo Pterodactyl-1, CH-3 in pa avtomatiziran zračni bojni sistem podjetja LOEC (*Luoyang Opto-Electronics*), lahko do neke mere vsaj domnevamo, kaj bi izbrani avtomatizirani zračni bojni sistem Guizhou WZ-2000 lahko posedoval v kontekstu bojne komponente. Pterodactyl-1 tako uporablja optično voden

izstrelek z oznako Norinco BA-7, CH-3 uporablja prav tako optično voden izstrelek z oznako AR-1 ter manjši satelitsko voden izstrelek z oznako FT-5 in končno avtomatiziran zračni bojni sistem podjetja LOEC uporablja izstrelek tipa zrak-zrak z oznako TY-90 (Fisher 2011).

Za kakšno oborožitev torej gre? V nadaljevanju sledi nekaj podrobnosti predhodno omenjenih izstrelkov drugih avtomatiziranih zračnih bojnih sistemov kitajskega porekla:

- Norinco BA-7 ali Blue Arrow 7 predstavlja pravzaprav helikopterski izstrelek zrak-zemlja z laserskim sistemom za določanje tarč in se lahko s 47 kilogrami primerja z raketo ameriškega porekla tipa Hellfire. Lahko bi rekli, da so izstrelek prilagodili zgolj za aplikacijo na avtomatizirane zračne bojne sisteme, in sicer so proizvedli manjši izstrelek, ki s podobnimi lastnostmi (26,5 kilogrami ter dometom do 6 kilometrov) nosi naziv Blue Arrow 9 (Fisher 2015);
- AR-1 predstavlja izstrelek tipa zrak-zemlja (*air to surface missile*), z laserskim vodenjem in skupno težo 45 kilogramov (Hsiao 2010);
- FT-5 predstavlja manjši satelitsko voden izstrelek – za razliko od drugih izstrelkov, ki predstavljajo rakete, gre pri tem izstrelku za vodeno bombo;
- TY-90 predstavlja primarno izstrelek v obliki rakete, namenjen za uporabo na helikopterjih. V osnovi gre za raketo tipa zrak-zrak, ki tehta 20 kilogramov in ima doseg do 6 kilometrov, vendar pa ima ta izstrelek določeno posebnost, in sicer, da je nameščen na poseben sistem za izstreljevanje, ki omogoča prenašanje štirih izstrelkov naenkrat (China national aero-technology import & export corporation 2011).

V kontekstu z zgornjo analizo izstrelkov drugih avtomatiziranih zračnih bojnih sistemov kitajskega porekla pa je potrebno omeniti še, da naj bi po navedbah Fisherja (2011) avtomatizirani zračni bojni sistem Guizhou WZ-2000 ponazarjal oz. bil v določeni meri podoben avtomatiziranemu zračnemu bojnemu sistemu ameriškega proizvajalca Northrop Grumman z nazivom Global Hawk.

Za boljši oris, kakšen avtomatiziran zračni bojni sistem naj bi »upodobil« avtomatiziran zračni bojni sistem Guizhou WZ-2000, v nadaljevanju sledi groba analiza avtomatiziranega

zračnega bojnega sistema ameriškega proizvajalca Northrop Grumman z nazivom Global Hawk. Sam naziv Global Hawk predstavlja sinonim za ogromen avtomatiziran zračni bojni sistem, katerega zasnova sega v leto 1995.

Gre za avtomatiziran zračni bojni sistem, ki se uporablja predvsem za namene nadzorovanja, opazovanja, izvidništva ipd. Po velikosti se lahko primerja s prvotno analiziranim modelom ameriškega proizvajalca General Atomics z nazivom MQ-1C Gray Eagle. Njegov razpon kril tako meri 39, 9 metrov, medtem ko dolžina celotnega avtomatiziranega zračnega bojnega sistema znaša 14, 4 metrov. Sam sistem je lahko operativen 32 ur, medtem ko podrobnejših podatkov o samem pogonskem agregatu, ki torej omogoča tovrstno vzdržljivost samega sistema, ni. Prav tako ta avtomatiziran zračni bojni sistem nima bojne komponente v smislu nekega orožja. Sam naziv avtomatiziranega zračnega bojnega sistema mu pripisujejo na podlagi upravljanja z informacijami v realnem času na nekem bojnem območju (Northrop Grumman 2016b).

Kaj je torej tisto, kar dela ta avtomatiziran zračni bojni sistem kljub temu, da nima nobene klasične oborožitve, zanimiv? Northrop Grumman Global Hawk se ponaša z dvema ključnima visoko sofisticiranima komponentama, in sicer z večplatformnim radarjem, ki ga je moč prilagajati glede na vstavljen program, ter z vozliščem za bojne komunikacije v zraku. Večplatformni radar oz. program, ki zaznamuje ta radar (*Multi-platform radar technology insertion program MP-RTIP*), predstavlja aktiven taktičen radar z visoko ločljivostjo, indikator premičnih tarč na tleh ter sistem za sledenje zračnih tarč. Vse to na samem bojišču v realnem času omogoča hitrejši odziv bojnih sil, prav tako pa sama modularna zasnova tega radarja omogoča, da je radar moč vgraditi tudi v druge bojne sisteme (Northrop Grumman 2016c).

Poleg zgoraj omenjenega visoko sofisticiranega radarja pa je druga posebnost oz. izstopajoča karakteristika tega avtomatiziranega zračnega bojnega sistema vozlišče za bojne komunikacije v zraku (*Battlefield airborne communications node - BACN*). Gre za sistem komunikacij, ki sprejema, prestreza in posreduje komunikacije v zraku v realnem času. Tako služi kot nekakšna visoko zmogljiva premična radarska postaja. Po navedbah vira je v preteklosti

zaradi morebitnega težavnega območja bojevanja (hribovit, gorski svet ipd.) prihajalo do težav s komunikacijo. Zaradi integracije sistema komunikacij v avtomatiziran zračni bojni sistem so tovrstne težave odpravljene, poleg tega pa, v kolikor je avtomatiziran zračni bojni sistem kot komunikacijsko vozlišče izven vidnega polja (*line of sight*), poteka sama komunikacija med različnimi akterji še vedno nemoteno. Prav tako komunikacija med podobnimi akterji oz. med akterji s podobnimi komunikacijskimi značilnostmi poteka preko IP povezave – gre torej za podobno komunikacijo, kot je ta, ki se dogaja med strežniki pri uporabi računalnikov (Northrop Grumman 2016b).

4.1.4 Primerjava izbranih samostojnih avtomatiziranih zračnih bojnih sistemov

Eden izmed ciljev pričujočega magistrskega dela je tudi primerjava med izbranimi modeli, kjer pa ne bo šlo zgolj za primerjavo med posameznimi modeli temveč tudi za primerjavo med posameznimi tipi avtomatiziranih zračnih bojnih sistemov. Povedano drugače – ena izmed primerjav bo tudi med tipoma avtomatiziranih zračnih bojnih sistemov, tj. med samostojnimi avtomatiziranimi zračnimi bojnimi sistemi in med avtomatiziranimi zračnimi bojnimi sistemi, ki temeljijo na principu *fire and forget*. Pri tem bo ključno to, da izpostavim tako prednosti kot tudi slabosti obeh tipov avtomatiziranih zračnih bojnih sistemov.

Na tej točki sledi primerjava prvih treh analiziranih avtomatiziranih zračnih bojnih sistemov, ki spadajo pod tip samostojnih avtomatiziranih zračnih bojnih sistemov, in sicer ameriški model Gray Eagle, ruski model Mikoyan Skat ter kitajski model Guizhou WZ-2000. Ker gre hkrati za primerjavo med modeli in primerjavo med državami proizvajalkami teh modelov, bom predstavil tudi alternative tovrstnim modelom, ki sem jih že predhodno omenil in analiziral. Vse skupaj bo tako sestavljalo primerjavo med samimi analiziranimi modeli avtomatiziranih zračnih bojnih sistemov in med zmogljivostmi izbranih treh držav v nekem omejenem obsegu. Sprva bom naredil primerjavo med analiziranimi modeli, kasneje jo bom razdelil v segmente, po katerih je potekala sama analiza teh modelov. Segmente bodo predstavljali pogonski agregati, oborožitev, druge komponente, namenjene npr. izvidništvu ter morebitne posebnosti nekega modela.

Primerjava pogonskih agregatov vseh treh analiziranih modelov avtomatiziranih zračnih bojnih sistemov bo v grobem potekala med pogonskim agregatom Thielert z 2000 kubičnimi centimetri delovne prostornine in 155 konjskimi močmi, pogonskim agregatom Klimov 5000B ter pogonskim agregatom Ivchenko AI-25TL 300.11. Primerjalni parametri bodo hitrost, ki jo nek avtomatiziran zračni bojni sistem doseže, vzdržljivost in doseg samega sistema ter največja višina, ki jo avtomatiziran zračni bojni sistem lahko doseže. Hitrost, ki jo pogonski agregati lahko omogočijo samim avtomatiziranim zračnim bojnim sistemom, pri ameriškem modelu Gary Earle znaša največ 309 kilometrov na uro, pri ruskem modelu Mikana Skat naj bi znašala največ 80 kilometrov na uro, največ 800 kilometrov na uro pa

znaša pri kitajskem modelu W-2000. Ker ruski model Mikana Skat uradno še ni v uporabi, bi bilo smiselno predstaviti edino hitrost nadomestnih dveh modelov izraelskega proizvajalca Izrael Aerostate Industrije, vendar je ta s hitrostjo drugih dveh modelov neprimerljiva. Kar zadeva samo vzdržljivost vseh treh modelov ima daleč najdaljšo vzdržljivost ameriški model Gary Earle, in sicer do 24 ur.

Za ruski model Mikana Skat podatka o vzdržljivosti ni, je pa novejša različica modela, s katerim kompenzira Rusija, MK Sacher III (Rusija uporablja starejši model MK Sacher II), spodobno vzdržljiva, in sicer do 18 ur. Kitajski model Guizhou WZ-2000 se s samo vzdržljivostjo ne ponaša, saj le-ta znaša zgolj tri ure.

Naslednji podatek za primerjavo je sam doseg nekega avtomatiziranega zračnega bojnega sistema. Za ameriški model Gray Eagle tega podatka ni, a je pri vzdržljivosti do 24 ur kljub temu moč sklepati, da gre za precej velik doseg. Za samo primerjavo naj bi imel ruski model Mikoyan Skat doseg do 2000 metrov, kitajski model Guizhou WZ-2000 pa do 2400 metrov. Pomemben podatek za primerjavo je tudi največja višina, ki jo nek avtomatiziran zračni bojni sistem lahko doseže. Tako le-ta pri ameriškem modelu Gray Eagle znaša največ 8839 metrov, pri ruskem modelu Mikoyan Skat naj ne bi presegala 12000 metrov, pri kitajskem modelu pa znaša največ 17983 metrov.

Naslednji parameter za primerjavo med analiziranimi modeli je oborožitev. Ta parameter bo okrnjen, saj pri ruskem modelu Mikoyan Skat podatka o oborožitvi ni, prav tako podatka o oborožitvi ni pri izbranih dveh alternativah izraelskega proizvajalca Israel Aerospace Industries oz. gre za modela, ki sta namenjena zgolj za naloge izvidništva. Posledično bo sama primerjava v tem segmentu potekala zgolj med ameriškim modelom Gray Eagle in kitajskim Guizhou WZ-2000. Oborožitev pri ameriškem modelu Gray Eagle predstavljajo rakete tipa Hellfire. Gre za celo družino raket, ki imajo vsaka zase svoje posebnosti. Različice segajo od raket za uničevanje oklepnih vozil, raket ki ob zadetku razpadejo na več delcev (princip šrapnela), preciznih raket, ki ob zadetku povzročijo zelo malo postranske škode, do raket, kot je denimo Hellfire AGM-114R (Romeo), ki predstavlja nekakšno kombinacijo naštetih. Rakete tipa Hellfire imajo istoimenski lastni izstrelitveni sistem, ki omogoča izstrelitev z minimalno količino dima, kar posledično med drugim pomeni težko zaznaven

izstrelek. Poleg tega posebne lastnosti rakete tipa Hellfire predstavljajo še operativnost v temperaturah od -43ºC do +63ºC, doseg do 11 kilometrov ter življenjska doba do 20 let.

Na drugi strani je oborožitev kitajskega modela Guizhou WZ-2000 večinoma stvar špekulacij. Ker izrecnega podatka za model Guizhou WZ-2000 ni, hkrati pa obstaja širok nabor oborožitve za druge avtomatizirane zračne bojne sisteme kitajskega porekla, je edino logično, da se kot morebitno oborožitev za primerjavo jemlje oborožitev iz že obstoječega nabora drugih avtomatiziranih zračnih bojnih sistemov kitajskega porekla. Nabor tako predstavljajo raketa tipa zrak-zemlja Norinco BA-7 (Blue Arrow 7), raketa tipa zrak-zemlja AR-1, voden izstrelek (bomba) FT-5 in helikopterska raketa tipa zrak-zrak TY-90 z lastnim istoimenskim tipom izstrelitvene komponente, ki omogoča simultano nošenje štirih raket na izstrelitveno komponento.

Prav tako so parameter za primerjavo tudi dodatne komponente, ki jih poseduje določen avtomatiziran zračni bojni sistem. Po opravljeni analizi vseh treh modelov so v osnovi te dodatne komponente vsaj tri, in sicer nekakšen podsistem za določanje tarč, taktični radar in nekakšen podsistem za komunikacijo. Dodatne komponente pri ameriškem modelu gray Eagle predstavljajo elektro-optični oz. infrardeč podsistem za določanje tarč podjetja Raytheon z oznako MTS (CSP), taktični radar podjetja Northrop Grumman z oznako STARLite AN-ZPY ter sistem za komunikacijo.

Pri ruskem modelu Mikoyan Skat o dodatnih komponentah ni podatka, kar pa zadeva alternativi, ki naj bi ta model nadomeščali, imata obe elektro-optični oz. infrardeč podsistem za določanje tarč, taktični radar, podsistem za komunikacijo pa ima zgolj IAI Searcher MK II. Kar se tiče elektro-optičnega oz. infrardečega podsistema za določanje tarč in taktičnega radarja za kitajski model Guizhou WZ-2000 zasledimo zgolj podatek, da ga ima, prav tako pa ima prav poseben podsistem za komunikacijo, tj. sistem z oznako SIGINT (*signals intelligence*).

Zadnji parameter, ki je relevanten za primerjavo med posameznimi analiziranimi modeli, so t. i. posebnosti. Gre za specifične karakteristike, ki so značilne za vsak model posebej. Ameriški model Gray Eagle zaznamuje to, da uporablja težko gorivo. Gre za posebno gorivo, čigar uporaba sovpada z ameriškim konceptom o uporabi enotnega goriva za vse akterje. Druga posebnost, ki ga zaznamuje, je upravljanje s premične nadzorne kopenske postaje. Sama krila in rep avtomatiziranega zračnega bojnega sistema so odporna na zmrzal, prav tako pa je sam model možno transportirati v letalu tipa C-130. Hkrati je posebnost tega modela opcijska uporaba oborožitve – obstaja tako bojna kot tudi nebojna različica modela Gray Eagle.

Same posebnost ruskega modela Mikyan Skat zaradi razvojne faze samega modela niso znane, alternativi izraelskega proizvajalca Israel Aerospace Industries pa sta sestavljeni iz kompozitnih materialov, zaradi česar sta težko zaznavni. Poleg tega model IAI Bird Eye 400 zaznamuje tudi delovanje na električni pogon ter podatek, da ga je moč prenašati v dveh nahrbtnikih. Guizhou WZ-2000 – prav tako kot ameriški model Gray Eagle – zaznamuje dvojna narava, kot zanimivost pa naj navedem, da naj bi sam model »upodabljal« model ameriškega proizvajalca Northrop Grumman z nazivom Global Hawk.

4.2 Avtomatizirani zračni bojni sistemi (*fire and forget*)

Za avtomatizirane zračne bojne sisteme, ki temeljijo na principu *fire and forget*, bi lahko rekli, da izhajajo iz drugačnega koncepta kot predhodno analizirani samostojni avtomatizirani zračni bojni sistemi. Za trenutek si predstavljajmo, da je iz strani lovskih letal prišlo do ideje o podobnem tipu udeleženca v zračnih silah, in sicer o takem, ki ne bi ogrožal življenja pilota, saj bi le-ta lahko z »letalom« upravljal od daleč, hkrati pa pri tem ne bi zanemarili ognjene moči in drugih sposobnosti oz. karakteristik tipičnega letala. Potemtakem iz »navadnih« lovskih letal izvirajo samostojni avtomatiziranih zračni bojni in nebojni sistemi, medtem ko je pri avtomatiziranih zračnih bojnih sistemih, ki temeljijo na principu *fire and forget*, ideja v ozadju nekoliko drugačna. Če gre pri samostojnih avtomatiziranih zračnih bojnih sistemih za »poosebljanje« lovskih in izvidniških letal, gre pri avtomatiziranih zračnih bojnih sistemih bolj za idejo o razširjeni uporabi raket.

Splošna predstava o raketnih izstrelkih oz. raketah je ta, da gre za izstrelek, ki se ga tako ali drugače izstreli in usmeri v nek cilj. Ena in edina naloga rakete oz. nekega izstrelka je bila do danes zgolj in samo uničenje identificiranega cilja. Tako je tudi v definicijah rakete oz. raketnega izstrelka navedeno, da gre za kakršnokoli oborožitev, ki s pomočjo raketnega pogona na nek zastavljeni cilj dostavi neko eksplozivno telo oz. konico (Encyclopaedia Britannica). Z razvojem avtomatiziranih zračnih bojnih sistemov, ki temeljijo na principu *fire and forget*, se očitno spreminja tako samo pojmovanje kot tudi same naloge oz. namen raket ter raketnih izstrelkov.

Novodobni tip raket oz. raketnih izstrelkov ter hkrati avtomatiziranih zračnih bojnih sistemov, ki temeljijo na principu *fire and forget*, tovrstne oborožitve, kot so denimo *loitering weapons* (postopajoča orožja), *low cost autonomous attack systems* (nizko-cenovni avtonomni napadni sistemi), *surveilling miniature attack cruise missiles* (miniaturni vodeni izstrelki z možnostjo opazovanja), *inteligent munitions systems* (inteligentni sistemi streliva) ipd. danes uvrščajo v več novih pojmovanj. Pri t. i. *loitering weapons* (postopajoča orožja) gre za princip, da neka raketa oz. izstrelek nič več ne služi zgolj za namene uničevanja tarč, ampak nek določen čas kroži v določenem območju in tako služi za namene opazovanja, izvidništva ipd. Šele takrat,

ko s pomočjo komponent zazna neko tarčo, se vrnemo k začetnemu konceptu oz. ideji o raketi (Dictionary.com 2016).

Tipičen primer enega od prvih tovrstnih orožij je raketa izraelskega porekla z nazivom Delilah. Šlo je za prvo raketo oz. avtomatiziran zračni bojni sistem, ki ni bila namenjena zgolj za uničenja ali za nošenje kamere, posledično torej za opazovanje in izvidništvo, temveč kot sredstvo za preslepitev nasprotnika. Tako je bila naloga te oborožitve, da preusmeri sovražni ogenj na sebe in s tem razbremeni dejanske zračne enote (Israeli Air Force 2016).

Drug način pojmovanja avtomatiziranih zračnih bojnih sistemov, ki temeljijo na principu *fire and forget*, je *low cost autonomous attack system* (nizko-cenovni avtonomni napadni sistemi). Eno izmed vodilnih podjetij, ki se ukvarja s tovrstnim pojmovanjem in z izdelovanjem tovrstnih oborožitvenih sistemov, je ameriško podjetje Lockheed Martin. Porodilo se je glavno vprašanje, in sicer od kod pobuda za izdelavo praktično novega tipa orožja ob že obstoječem. Za čas prve in druge svetovne vojne je bilo značilno t. i. frontno oz. pozicijsko bojevanje. V osnovi gre za to, da sta se obe strani ustalili na neki poziciji, na nekem območju, kjer je nato potekalo samo bojevanje. V veliki meri je šlo za zelo statično vojskovanje, kar je skorajda popolno nasprotje temu, kar se dogaja danes. Zaradi napredka v vojaški industriji je vojskovanje postalo veliko bolj mobilno in posledično – z vidika zračnih napadov – veliko bolj izmuzljivo.

Če z vidika zračnih napadov za časa prve in druge svetovne vojne plastično predstavim sliko: v kolikor je ena od strani v spopadu imela informacijo, kje se nahaja nasprotnik in je na lokacijo usmerila nek izstrelek, je v večini primerov sovražnika tudi zadela. Danes je to »zagotovilo« za zadetek – ob vsem napredku v vojaški industriji, v strategiji vojskovanja/bojevanja in v sredstvih, ki preprečujejo odkritje pozicije nekega akterja v boju – veliko manjše, če ne praktično ničelno. Če se vrnem k samemu tipu oborožitve LOCAAS (*low cost autonomous attack system*). Sam tip oborožitve je nastal v devetdesetih letih 20. stoletja in je sprva predstavljal na videz popolnoma enostaven raketni izstrelek. Slednjega je bilo moč programirati tako, da je nekaj časa na videz brezciljno krožil na nekem območju, iskal ter zaznal morebitne tarče, o njih poročal in jih (v kolikor je bilo potrebno) tudi uničil.

Za ta namen je oborožitveni sistem uporabljal poseben radar s kratico LADAR (*laser-radar sensor*). Njegovo modificirano verzijo danes uporabljajo v prototipih vozil, ki vozijo sama. Sama začetna vzdržljivost teh sistemov je znašala do 30 minut, kasnejša analiza avtomatiziranih zračnih bojnih sistemov, ki temeljijo na principu *fire and forget*, pa bo spodoben indikator, kako velik napredek je vojaška industrija dosegla do danes (Haddick 2015).

Tretji način za pojmovanje avtomatiziranih zračnih bojnih sistemov, ki temeljijo na principu *fire and forget*, je *surveilling miniature attack cruise missiles* – SMACM (miniaturni vodeni izstrelki z možnostjo opazovanja). Gre za na videz enostavni raketni izstrelek, ki lahko s pomočjo dodatnih komponent (radar, infrardeč senzor ter laserski sistem za iskanje in določanje tarč) opravlja naloge obveščevalnih dejavnosti, opazovanja in izvidništva tudi do dveh ur. Po navedbah virov lahko tovrstni tip oborožitve v zraku kroži oz. bdi tudi do dve uri in šele nato začne z napadanjem sovražnika. Hkrati lahko tovrstni tip oborožitvenega sistema služi kot sredstvo za transport oz. kot izstrelitvena komponenta, saj je na sam oborožitveni sistem tega tipa moč dodajati druge manjše tipe oborožitve. Poenostavljen in zelo plastičen prevod napisanega bi bil, da gre za izstrelek, na katerega so dodani drugi izstrelki, ki delujejo povsem neodvisno drug od drugega. Govorimo torej o izstrelitveni komponenti z izstrelki, pri čemer tudi izstrelitvena komponenta sama po sebi predstavlja izstrelek (Robinson 2006).

Četrti način pojmovanja avtomatiziranih zračnih bojnih sistemov, ki temeljijo na principu *fire and forget*, je *inteligent munitions systems* – IMS (inteligentni sistemi streliva). Sam oborožitveni sistem navadno sestoji iz modula, integriranega sistema senzorjev, streliva (pa naj bo to ubojno ali neubojno) ter neke nadzorne postaje (Globalsecurity.org 2016). Eden vodilnih proizvajalcev teh oborožitvenih sistemov je ameriško podjetje Textron systems. Tako bi lahko v skladu z njihovimi podatki ta tip oborožitvenega sistema razdelili na obrambne oz. zaščitne sisteme, kot sta denimo *Spider* in *Scorpion*, ter na napadne sisteme, kot sta denimo BLU-108 ter CSS ali *Common smart submunition* (osnovno pametno strelivo). Sam *Spider* predstavlja nadgrajen tip pehotne mine, pri kateri gre za več malih eksplozivnih teles, ki se izstrelijo iz glavnega dela in tako ustvarijo neko varno območje oz. vzpostavijo nek perimeter. Zaradi posebnih karakteristik in senzorja gre za »pehotno mino«, ki sama zazna in opozori na

pristnost sovražnika in jo je moč opremiti z ubojnimi in nebojnimi sredstvi (Textron systems 2015a).

Na podobni osnovi deluje tudi sistem *Scorpion*, pri katerem gre za bolj robustno različico, ki je odporna na različne konfiguracije terena in na vse vrste vremena, prav tako pa je moč izbirati med ubojnimi in neubojnimi sredstvi. Prednost tega sistema je nenehna možnost interveniranja operaterja (Textron systems 2015b). Kar zadeva napadne sisteme, ki nas v kontekstu avtomatiziranih zračnih bojnih sistemov, ki temeljijo na principu *fire and forget*, bolj zanimajo, so pri podjetju Textron system zasnovali oborožitvena sistema BLU-108 in CSS (*Common smart submunition*). BLU-108 predstavlja izstrelek, ki ustvarja škodo predvidoma na širšem območju (princip šrapnela – *large area damage*). Sam izstrelek je moč izstreliti iz praktično kateregakoli nosilca in je efektiven tako na kopnem kot tudi na morju (Textron systems 2015c).

Drugi izstrelek pa predstavlja CSS, ki ga je prav tako moč izstreliti s katerekoli platforme in z več vrst vozil, dodatne komponente pa temu izstrelku omogočajo visoko natančnost pri določanju in uničevanju tarč. Prav tako se vsi produkti podjetja Textron systems ponašajo z varnostno komponento, ki po morebitnem neuspešnem samouničenju preprečuje kakršnokoli spontano delovanje teh produktov (Textron systems 2015d). Na podlagi predhodno predstavljene teorije in morebitnega idejnega ozadja avtomatiziranih zračnih bojnih sistemov, ki temeljijo na principu *fire and forget,* v nadaljevanju sledi analiza treh izbranih modelov. Analiza bo narejena po enakih parametrih kot pri predhodnih analiziranih modelih tovrstnih oborožitvenih sistemov, zajemala pa bo modela izraelskega proizvajalca Israel Aerospace Industries, IAI Harpy, model francoskega proizvajalca SAGEM, Sperwer MK II. in model ameriškega proizvajalca Northrop Grumman, Chukar III.

4.2.1 Israel Aerospace Industries IAI Harpy / IAI Harop

Prvi model, ki ga bom analiziral, bo produkt izraelskega proizvajalca Israel Aerospace Industries, z oznako IAI Harpy. Potrebno je povedati, da bo pod tovrstnim imenom predstavljenih zgolj nekaj osnovnih podatkov, medtem ko bo analiza po prvotno izbranih parametrih potekala na nadgradnji tega modela, in sicer pod oznako IAI Harop oz. IAI Harpy NG (*New generation* – nova generacija). Model IAI Harpy je bil zasnovan v devetdesetih letih 20. stoletja, in sicer pod predhodno pojasnjeno idejo o oborožitvenih sistemih tipa *loitering weapon*. Model je bil zasnovan z namenom, da leti nad nekim območjem in se ob detekciji tarče samouniči, in sicer tako, da se vanjo zaleti. Model se še danes uporablja večinoma za uničevanje nasprotnikovih radarjev ter zračne obrambe. Ob tem sta pomembni dve značilnosti, in sicer, da je bil napad tega modela izveden vertikalno, s čimer je bil še bolj učinkovit in pa da je bilo napad po izstrelitvi mogoče tudi preklicati (Israel Aerospace Industries 2013a).

IAI Harop je nadgradnja modela IAI Harpy. Poznan je tudi pod imenom IAI Harpy 2. Gre za avtomatiziran zračni bojni sistem tipa *fire and forget*, ki temelji na ideji *loitering weapon*. IAI Harop uporablja princip rakete tako, da tarčo uniči s samouničenjem. Le-to mu omogoča dnevno-nočni elektro-optični iskalec tarč, hkrati pa je model IAI Harop moč izstreliti iz raznovrstnih premičnih lanserjev. Podrobnejša analiza posameznih komponent sledi v nadaljevanju.

Kar zadeva pogon samega modela IAI Harop in kasnejšo nadgradnjo IAI Harpy NG je potrebno le-to razdeliti na dve komponenti. Prva komponenta predstavlja t. i. *Container launch unit*, ki predstavlja izstrelitveno komponento navadno dodano k nekemu oborožitvenemu ali transportnemu sistemu – naj gre za uporabo na kopnem, vodi ali v zraku. Prav zaradi tovrstne možnosti uporabe več različnih tipov izstrelitvenih sistemov so avtomatizirani zračni bojni sistemi, ki temeljijo na principu *fire and forget*, v primerjavi s samostojnimi avtomatiziranimi zračnimi bojnimi sistemi bolj fleksibilni. Pri samostojnih avtomatiziranih zračnih bojnih sistemih je za vzlet sistema potrebno neko vzletišče, kar pomeni, da je uporabnik tovrstnega sistema konstantno (vsaj za čas vzleta sistema) vezan na

neko območje, iz česar sledi, da je konstantno vezan na neko območje na kopnem (edina potencialna izjema je uporaba letalonosilk za namene izstreljevanja samostojnih avtomatiziranih zračnih bojnih sistemov).

Kaj torej pri tovrstnih oborožitvenih sistemih, ki temeljijo na principu *fire and forget*, predstavlja t. i. *Container launch unit*? Gre za tip izstrelitvenega sistema, ki ga je moč namestiti tako na plovila (predvsem na priobalne ladje) kot tudi na vrsto kopenskih vozil. Sam izstrelitveni sistem predstavlja napredek na področju izstrelitvenih sistemov oz. komponent, saj gre za izstrelitveni sistem, za katerega ni nujno, da se nahaja v vidnem polju upravljalca (gre za nov tip izstrelitvenih komponent – *Non line of sight launch systems*). Gre za izstrelitveno komponento, ki se razvija v okviru ameriškega principa *Future combat systems* oz. bojnih sistemov prihodnosti.

Sam *Container launch unit* se ponaša z lastnim napajanjem in s programsko opremo, kar omogoča tako upravljanje na daljavo kot tudi brezpilotno delovanje (postopno ukinjanje principa *Man in the loop* oz. posredovanje človeka). Prav tako se vsak tovrstni izstrelitveni sistem ponaša s sistemom za komunikacijo, sama kapaciteta pa zaleže za 15 raketnih izstrelkov, med katere se uvršča tudi tiste z avtonomnim delovanjem in samostojnim iskanjem tarč, kar pomeni, da lahko med te raketne izstrelke uvrščamo tudi avtomatizirane zračne bojne sisteme, ki temeljijo na principu *fire and forget* (The office of Operational test and evaluaton director 2012).

Kar zadeva preostale tipe izstrelitvenih sistemov oz. komponent, lahko le-te razdelimo v tri večje skupine, in sicer izstrelitvene komponente za plovila oz. mornarico (*navy launch platforms*), izstrelitvene komponente za vozila (*vehicle launch platforms*) ter druge izstrelitvene sisteme oz. komponente, kamor spada tudi predhodno omenjen *Container launch unit* (Save the Royal navy 2015). Vodilni podjetji na tem področju predstavljata ameriški podjetji Raytheon in Lockheed Martin.

Če se vrnem nazaj k pogonskemu agregau modela IAI Harpy, se je tip pogona skozi razvoj modela razlikoval. Med možnimi različicami pogonskega agregata se tako omenja tudi električni pogon, a po zadnjih podatkih pogonski agregat IAI Harpy predstavlja produkt podjetja UAV Engines ltd. iz Velike Britanije, z oznako AR 731 – 38 BHP (UAV Engines ltd 2016a). Ta agregat naj bi predstavljal gonilo tako za model IAI Harop kot tudi za novejši model IAI Harpy NG. Kakšen agregat se torej skriva v avtomatiziranem zračnem bojnem sistemu tipa *fire and forget*, ki nosi oznako IAI Harpy NG? Pogonski agregat AR 731 – 38 BHP se ponaša z življenjsko dobo, ki znaša med desetimi in petdesetimi urami. Edinstvena zasnova agregata, ki temelji na principu Wanklovega motorja, mu omogoča zelo ugodno razmerje med proizvedeno močjo in težo samega agregata. Same specifične karakteristike Wanklovega motorja bom zaradi boljše predstave podal nekoliko kasneje.

Med zmogljivosti pogonskega agregata AR 731 – 38 BHP spadajo tudi:

- 208 kubičnih centimetrov delovne prostornine;
- za ta model specifičnih 38 konjskih moči (gre za način označevanja pogonskih agregatov s strani proizvajalca) in
- možnost uporabe goriva MoGas ali Avgas (UAV Engines ltd 2016b).

Kar zadeva možnost različne uporabe goriv predstavlja gorivo MoGas nekakšen tip goriva s podobnimi lastnostmi kot avtomobilsko gorivo (glavno razliko med obemi gorivi predstavlja vsebnost oktanov). Po navedbah virov naj bi gorivo MoGas imelo vrednost oz. vsebnost oktanov nekje približno 88 (sama merska lestvica se giblje med 0 in 100), alternativno gorivo Avgas, ki predstavlja veliko bolj kvalitetno in stabilno oz. zanesljivo gorivo, pa nekje 99,6 oz. 100 (BP p.l.c. 2016).

Za boljši oris naj navedem še nekaj značilnosti, prednosti in slabosti Wanklovega oz. rotacijskega pogonskega agregata. Sam pogonski agregat je nastal leta 1919 s strani njegovega izumitelja Felixa Wankla. Gre za lahek pogonski agregat, ki v primerjavi z alternativami proizvede manj tresljajev, kar je priročno pri uporabi v avtomatiziranih zračnih bojnih sistemih, hkrati pa motor proizvede ogromno moči. Pomanjkljivosti tega tipa

pogonskega agregata predstavljajo pregrevanje, visoka obraba in posledično kratka življenjska doba, kar je moč razbrati tudi iz navedb britanskega proizvajalca UAV Engines ltd, ki mu pripisuje življenjsko dobo med desetimi in petdesetimi urami (Delta expo 2006). Tovrstne karakteristike so ustrezne predvsem za oborožitvene sisteme tipa *fire and forget*.

Naslednja karakteristika in hkrati parameter za kasnejšo primerjavo med avtomatiziranimi zračnimi bojnimi sistemi tipa *fire and forget* je oborožitev, ki se je v toku razvoja samega oborožitvenega sistema do določene mere spreminjala. Kar zadeva sam tip bojne konice nameščene na oborožitveni sistem naj povem, da gre za fragmentacijsko eksplozivno bojno konico (*explosive fragmentation warhead*). Predhodno omenjene spremembe bojne konice gredo predvsem v smeri teže same bojne konice.

Tako naj bi po nekaterih navedbah bojna konica pri modelu IAI Harop (oz. t. i. Harpy 2) tehtala 21 kilogramov, prav tako pa je v kontekstu bojne konice pomemben tudi faktor vzdržljivosti samega oborožitvenega sistema, ki ob predpostavki, da bojna konica tehta 21 kilogramov, znaša do 6 ur (Airforce technology 2016). Po drugih navedbah pa konica pri novejšem modelu, tj. IAI Harpy NG (*New generation* – nova generacija) tehta 15 kilogramov, ob čemer je potrebno dodati, da gre za isti tip bojne konice. S tovrstno bojno konico tako celoten oborožitveni sistem tehta 160 kilogramov, sama vzdržljivost oborožitvenega sistema pa znaša do 9 ur (Zitun 2016).

Kakšno konico torej predstavlja eksplozivna fragmentacijska bojna konica? Gre za eksplozivno telo, katerega zunanja površina je navadno prevlečena s krhkim materialom, kar rezultira v fragmentaciji samega izstrelka. Ena izmed ključnih lastnosti tovrstne bojne konice je, da je njena fragmentacija in posledično škoda drugačna od tiste pri tipičnem fragmentacijskem strelivu. Pri slednjemu je velikost delcev določena pred samo izstrelitvijo oz. pred samim zadetkom, medtem ko velikost samih delcev oz. fragmentov pri eksplozivnih fragmentacijskih bojnih konicah ni določena vnaprej, zato so delci »nepravilne velikosti« in »nepravilne oblike«. Sama hitrost in oblika oz. vzorec fragmentacije je pri eksplozivni fragmentacijski bojni konici drugačen kot pri tipičnem fragmentacijskem strelivu. Posledično

je hitrost delcev oz. fragmentov večja, sam vzorec razpršenosti pa je drugačen kot pri običajnem fragmentacijskem strelivu (Moxnes in drugi 2014).

Tretji parameter primerjave so t. i. dodatne komponente, in sicer visoko kvalitetni, nočno-dnevni, elektro-optični radar, sistem za obrambo proti sovražnim radarjem oz. proti sovražnikovi zaznavi, naprej usmerjena infrardeča barvna kamera ter podsistem za komunikacijo. Podrobnejši podatki za ta model kažejo na to, da se kot visoko kvalitetni, nočno-dnevni, elektro-optični radar uporablja kar model proizvajalca Israel Aerospace Industries z oznako IAI Tamam POP-200.

IAI Tamam POP sistemi predstavljajo podsisteme, ki združujejo t. i. *thermal imaging* (kamera identificira toploto posameznih objektov in subjektov), visoko kakovostno CCD (*charged-couple device*) kamero različnih ločljivosti glede na model, lasersko tehniko za iskanje, določanje in usmerjanje na tarčo ter lasersko tehniko za ocenjevanje razdalje. Ti podsistemi so zasnovani za tako nočne kot tudi dnevne operacije, namestiti jih je moč na katerokoli platformo (tako avtomatizirane zračne bojne sisteme kot tudi nekatere kopenske sisteme, helikopterje ipd.). Glede na različico in komponente posamezne različice se njihova cena giblje med 220 in 260 tisoč dolarji (Israel Aerospace Industries 2002a). Sam IAI Tamam POP-200 predstavlja naprej usmerjeno infrardečo kamero – gre za tip kamere, za katerega se uporablja oznaka FLIR (*forward looking infrared camera* – naprej usmerjena infrardeča kamera), integriran sistem DTV (*day TV*), avtomatski sledilec videa (AVT) ter laserski sistem za določanje oz. usmerjevanje (*laser pointer*) in laserski sistem za merjenje oz. ocenjevanje razdalj (*laser range finder*). Sam podsistem IAI Tamam POP-200 v celoti tehta 16, 3 kilogramov (Israel Aerospace Industries 2002b). Kar zadeva sistem za obrambo pred sovražnikovimi radarji oz. pred samo zaznavo sovražnika ni točnejših podatkov.

Specifična karakteristika avtomatiziranega zračnega bojnega sistema IAI Harpy, ki se je razvijala tudi s samim razvojem sistema oz. njegovo nadgradnjo, je tudi zasnova kril v obliki grške črke delta. Tako je v grobem celoten avtomatiziran zračni bojni sistem IAI Harpy izgledal kot trikotnik. Z razvojem modela IAI Harpy NG in spremembo oznake je prišlo tudi do spremembe zasnove kril, ki sicer še vedno izhaja iz prvotne zasnove tipa *delta-wing*,

vendar pa se pri modelu IAI Harpy NG del kril nahaja že spredaj pri nosu samega avtomatiziranega zračnega bojnega sistema, medtem ko se del zadnjih kril zloži pod večji del krila. S to prerazporeditvijo in spremembo koncepta »enega krila« se je v določeni meri spremenil tudi hrbtni del avtomatiziranega zračnega bojnega sistema, kar pripomore k večjemu dosegu, doseganju višine in vzdržljivosti, ki naj bi po navedbah vira znašala do 9 ur (Hughes 2016).

4.2.2 SAFRAN SAGEM Sperwer Mk. II

Drugi model, ki ga bom analiziral, spada med avtomatizirane zračne bojne sisteme tipa *fire and forget*. Model je produkt evropskega podjetja SAGEM, ki deluje znotraj strukture z imenom SAFRAN, ki predstavlja pravzaprav konzorcij podjetij. Samo podjetje ima sedež v Franciji, podružnice pa ima tako v Evropi, Aziji kot tudi v Ameriki. Nastanek samega podjetja sega v leto 1925 (SAGEM 2016a).

Sam model Sperwer Mk. II spada med tiste avtomatizirane zračne bojne sisteme tipa *fire and forget*, ki opcijsko posedujejo t. i. bojno komponento. V primerjavi s predhodno analiziranim modelom IAI Harpy je ena izmed prednosti modela Sperwer Mk. II v tem, da je model Sperwer Mk. II po končani nalogi zaradi dodelanega »sistema za ponovno uporabo«, ki vključuje padalo ter set zračnih blazin, ki preprečujejo poškodbe ob pristanku, moč ponovno uporabiti (SAGEM 2016b).

Več o sistemu pozneje. Kar želim izpostaviti ta trenutek je, z ozirom na predhodno omenjeni sistem, samo pojmovanje oz. uvrščanje tega avtomatiziranega zračnega bojnega sistema med sisteme tipa *fire and forget*. Sama kategorija oz. tip teh sistemov nekako narekuje oz. daje občutek, da po izstrelitvi tovrstnih sistemov le-teh, zaradi narave njihove zasnove oz. njihovega delovanja, ni moč ponovno uporabiti. Več o samem delovanju modela Sperwer Mk. II v nadaljevanju, ko sledi analiza po segmentih.

Kar zadeva sam pogonski agregat bo analiza potekala podobno kot pri predhodno analiziranem modelu IAI Harpy, in sicer bo ta segment vključeval tako analizo samega sistema izstrelitve, ki pri modelu Sperwer Mk. II deluje na osnovi katapulta, ter analize samega pogonskega agregata, ki ga model uporablja po izstrelitvi. Pri sistemu izstrelitve gre (kot že rečeno) za princip katapulta. Sistem temelji na stisnjenem zraku – izstrelitev omogoča sam pritisk. Pogodbeni partner tako podjetja SAGEM kot tudi celotne skupine SAFRAN je finsko podjetje Robonic (Robonic 2016a).

Sam model katapultne izstrelitve, na katerem so testirali tudi izstrelitev preučevanega modela SAGEM Sperwer Mk. II, nosi oznako Robonic Kontio MC 2555LLR. Gre za superioren model katapultne izstrelitve, katerega lastnost je njegova univerzalnost oz. vsestranska uporaba. Model deluje na sistemu visokega pritiska oz. kompresije zraka. Kot tak lahko služi kot izstrelitvena komponenta tako za avtomatizirane zračne bojne sisteme tipa *fire and forget*, ki za pogonski agregat uporabljajo propelerske motorje, kot tudi tiste, katerim pogonski agregat predstavlja turbina. Sam model izstrelitve ima svoj napajalni sistem, kar mu omogoča neodvisno delovanje.

Pomembne lastnosti tega modela med drugim predstavljajo čas postavitve, ki je manjši od 15 minut in sam čas za ponovno izstrelitev, ki znaša nekje 5 minut. Model je moč transportirati v posebnih kontejnerjih, kar omogoča njegovo uporabo tako na kopnem kot tudi na različnih plovilih, hkrati pa ga je moč prevažati tudi v letalih tipa C-130 (Robonic 2016b).

Na drugi strani pogonski agregat avtomatiziranega zračnega bojnega sistema tipa *fire and forget* predstavlja dvotaktni pogonski agregat, ki proizvede do 70 konjskih moči (Armada international 2013). Dvotaktni pogonski agregat tako omogoča vzdržljivost oz. operativnost samega modela Sperwer Mk. II preko 6 ur, pri čemer je oborožitveni sistem sposoben avtonomno delovati 4 ure. Kar zadeva doseg omejitev predstavlja sama povezava s kopensko nadzorno postajo, ki uspešno deluje do oddaljenosti 200 kilometrov. Omenjeni pogonski agregat omogoča doseganje višine do 4572 metrov (SAGEM 2016c).

Drugi segment se bo, kot pri predhodno preučevanih modelih, osredotočal na samo oborožitev. Oborožitev pri modelu Sperwer Mk. II je opcijska, kar pomeni, da v kolikor okoliščine narekujejo oborožen spopad, je na model moč namestiti oborožitev. Zaradi zasnove kril v obliki grške črke delta (gre za enako zasnovo, kot pri predhodno analiziranem modelu IAI Harpy, le da so pri tem modelu krila dvojna) je na spodnjo stran le-teh moč namestiti posebne stebričke, ki omogočajo namestitev izstrelkov.

Na posameznem krilu lahko oborožitev skupaj z omenjenim stebričkom, ki služi kot izstrelitvena komponenta, tehta največ 30 kilogramov. Med potencialne izstrelke spadata izstrelek podjetja Rafael advanced defense systems ltd. z oznako Spike ER ter izstrelek 155 BONUS, ki je produkt sodelovanja med francoskim podjetjem Nexter ter švedskim podjetjem BAE Systems (Army Technology 2016). Kar zadeva prvi izstrelek, tj. izstrelek podjetja Rafael advanced defense systems ltd. z oznako Spike ER, gre za protitankovski vodeni izstrelek. Gre za izredno prilagodljiv izstrelek, ki ga je moč namestiti tako na kopenska vozila, plovila kot tudi denimo na helikopterje. Sam doseg izstrelka znaša do 8 kilometrov. Ta izstrelek zaradi svojih dodatnih komponent spada pod t. i. pametno strelivo, saj izstrelek vsebuje dnevni ali dnevno-nočni iskalec tarč ter dvojni *modus operandi*, pri čemer prvi predstavlja operacijo navadnega izstrelka, tj. izstrelitev in uničenje tarče, medtem ko predstavlja drugi princip pametnega streliva, in sicer s tem, da nenehno posreduje nove podatke o svoji tarči, s čimer pa omogoča spremembo tarče tudi po sami izstrelitvi. Prav tako izstrelku drugi *modus operandi* omogoča opravljanje operacij ocenjevanja škode ter obveščevalne dejavnosti (Rafael advanced defense systems ltd 2010).

Kar zadeva drugi izstrelek, tj. izstrelek 155 BONUS, se le-ta od prvega izstrelka razlikuje po tem, da gre primarno za artilerijsko strelivo. Zopet gre za posebno strelivo, saj vsebuje tulec, ki predstavlja izstrelek, dve bojni konici ter vrsto programske in druge opreme, ki ob izstrelitvi išče tarče. Izstrelek vsebuje infrardeč senzor, ki ob sprostitvi konic iz zunanjega ovoja oz. tulca prične z iskanjem in identifikacijo tarč, ki jih nato nevtralizirata bojni konici, pri čemer ena bojna konica služi za uničenje ene tarče. Ena izmed ključnih lastnosti tega izstrelka oz. izstrelkov je ta, da je zaradi same zasnove dveh bojnih konic v enem ovoju oz. tulcu težko zaznati, da gre pravzaprav za dve bojni konici (BAE Systems 2016).

Tretji segment bo predstavljal skupek dodatnih komponent, ki jih poseduje model Sperwer Mk. II in ki mu omogočajo opravljanje nalog, kot so denimo obveščevalna dejavnost, opazovanje, določanje tarč ter izvidništvo. Poleg dodatnih komponent model Sperwer Mk. II odlikuje tudi uporaba sistema ISTAR (*intelligent system for telemetry analysis in real time*), ki predstavlja edinstven sistem za analizo telemetrije ter skrbi za popoln grafični pregled in tako upravljalcu z oborožitvenim sistemom Sperwer Mk. II olajša pregled nad dogajanjem (NASA technical reports server 1994).

Komponente, ki dopolnjujejo oborožitveni sistem Sperwer Mk. II so:

- elektro-optičen oz. infrardeč podsistem za določanje in identifikacijo tarč z oznako Euroflir 350 (gre za produkt podjetja SAGEM), ki predstavlja skupek toplotne kamere, visokoločljivostne kamere, laserskega telemetra ter laserskega namerilnika (SAGEM 2016d);
- taktični radar;
- podsistem za komunikacije;
- podsistem za prestrezanje in analizo nasprotnikovih komunikacij ELINT in COMINT, ki ju združena poznamo pod okrajšavo SIGINT (*signals intelligence*). Medtem ko COMINT prestreza in analizira tipične komunikacijske signale, ELINT prestreza in analizira ne-komunikacijske signale, kot so denimo signali radarskih oddajnikov (Adamy 2013).

Posebnost modela Sperwer Mk. II je njegova lastnost, ki samo opredelitev, da gre za avtomatiziran zračni bojni sistem tipa *fire and forget*, postavlja pod vprašanje. Model Sperwer Mk. II ima poseben sistem za pristajanje, ki ga sestavljata padalo in set blazin, ki ublažijo pristanek. Sam postopek pristajanja poteka tako, da sam oborožitveni sistem kroži na območju pristanka, ustavi delovanje pogonskega agregata, ki smo ga analizirali v prvem segmentu, sproži zračne blazine, ki ublažijo pristanek, in aktivira padalo (Canadian american strategic review 2008).

4.2.3 Northrop Grumman Chukar III

Avtomatizirani zračni bojni sistem tipa *fire and forget* z oznako Chukar III ameriškega proizvajalca Northrop Grumman ima podobno kot nekateri predhodno analizirani modeli avtomatiziranih zračnih bojnih sistemov dvojno naravo. A ne gre zgolj za razmejitev na bojno in nebojno različico, temveč bolj za to, da lahko sam model služi ali kot oborožitveni sistem ali kot sredstvo za usposabljanje. Kot sredstvo za usposabljanje model služi tako, da posnema vodene izstrelke ali celo bojna letala. Gre za izredno vsestranski sistem, ki omogoča vrsto razširitev, s čimer se dodobra približa realnim situacijam, prav tako pa je izredno logistično ugoden, saj ga je moč uporabljati tako na kopnem, na vodi kot tudi v zraku, k čemur nedvomno prispeva tudi izredno prilagodljiva nadzorna postaja (*ground control station*) (Northrop Grumman 2016č).

Northrop Grummanov model Chukar III trenutno predstavlja aktualni model na področju tovrstnih oborožitvenih sistemov. Gre za poseben tip avtomatiziranih zračnih bojnih sistemov tipa *fire and forget,* ki odpira povsem novo dimenzijo tovrstnih oborožitvenih sistemov. Pri predhodno analiziranih tovrstnih oborožitvenih sistemih, neglede na to ali je šlo za samostojne oborožitvene sisteme ali oborožitvene sisteme tipa *fire and forget*, smo nekako pričakovali, da bodo njihove naloge uničenje sovražnika (enot, infrastrukture ipd.) ali pa odkrivanje in analiziranje sovražnikovih kapacitet, s čimer pojmujemo obveščevalno dejavnost, nadzorovanje, opazovanje itd.

Model Chukar III ter njegovi sovrstniki, o katerih več v nadaljevanju, predstavljajo novo dimenzijo, saj je njihova primarna naloga zavajanje sovražnika. Sam model poseduje ogromno dodatnih komponent, ki modelu omogočajo opravljanje tudi nalog izvidništva ipd., a je kljub temu primarna naloga tovrstnih modelov zavajanje sovražnika. Ti modeli dejansko ne posedujejo oborožitve kot take, kar njihovo pozicijo na bojišču najbolje opredeli kot vabo. Kar zadeva mirnodobne dejavnosti pa tovrstni modeli služijo za vadbeno dejavnost kot aktivni simulatorji v potencialnih situacijah. Podobno kot pri predhodno analiziranem modelu Sperwer Mk II predstavlja način pristajanja za tovrstne modele večinoma pristanek s padalom.

Kot možen način pristajanja se omenja tudi posebna naprava za plovnost, a ne gre za preverjeno informacijo (Northrop Grumman 2016d).

Podjetje Northrop Grumman je s proizvajanjem tovrstnih modelov začelo leta 1935. Danes sovrstnike modela Chukar III predstavljajo modeli BQM-34 Firebee, BQM-74E in BQM-74F. Vsi modeli, vključno z modelom Chukar III, se med seboj razlikujejo po vzdržljivosti, ki se giblje med 78 minutami in 120 minutami. Kar zadeva doseganje višine je model BQM-34 Firebee daleč najboljši, saj lahko doseže do 18 300 metrov nadmorske višine, medtem ko se pri preostalih modelih meja nahaja pri 12 200 metrih. Prav tako je vsem modelom skupno ogromno število možnih razširitev oz. dodatnih komponent ter možnost zelo nizkega letenja, pri modelu BQM-74E celo zgolj 2, 1 metra nad tlemi. Kar zadeva pogonske agregate so le-ti od modela do modela različni, vsem pa je skupni imenovalec njihov proizvajalec, tj. podjetje Williams oz. Rolls-Royce (Northrop Grumman 2016e).

Pri samem pogonu modela Chukar III je potrebno obravnavati dve komponenti. Prva komponenta je sam pogonski agregat z oznako J400-WR-404. Gre za produkt sodelovanja med podjetjema Williams international in Rolls-Royce. Gre za turbopropelerski pogonski agregat, ki deluje na letalsko gorivo, modelu Chukar III pa v skladu z njegovo konfiguracijo zagotavlja vzdržljivost do 78 minut (Naval air systems command 2016).

Druga komponenta pri pogonu modela Chukar III je odvisna od načina oz. lokacije izstrelitve. Tako je v primeru izstrelitve z nekega letala sam način oz. potek izstrelitve dokaj očiten, medem ko je pri izstrelitvi s tal zopet specifičen sistem. Sam model namreč ne uporablja metod, ki jih uporabljajo drugi modeli, kot je denimo katapultna izstrelitev, temveč uporablja t. i. sistem JATO (*jet assisted take-off*) oz. RATO (*rocket assisted take-off*). V osnovi gre za to, da model Chukar III za pomoč pri vzletu uporablja dve pomožni raketi, ki sam model dvigneta dovolj visoko, da se vključi pogonski agregat (prav tam).

Kot že navedeno v uvodni predstavitvi modela Chukar III gre za neoborožen avtomatizirani zračni bojni sistem tipa *fire and forget*, zato bom v nadaljevanju analiziral dodatne komponente oz. možne razširitve modela Chukar III.

Same možne razširitve na modelu Chukar III so naslednje:

- okrepitev aktivnega ali pasivnega radarja, pri čemer imata oba svoj nabor zmogljivosti. Tako okrepitev aktivnega radarja lahko pomeni dvoje: ojačitev pridobljenega signala in vrnitev v okrepljenem stanju ali okrepitev oddajnika, ki rezultira v aktiviranju določenega zračnega oddajnika (Federal aviation administration 1975);
- simulator iskalnih naprav, ki omogoča simulacijo izračunov v realnem času in s tem omogoča predvidevanje obnašanja nekega drugega oborožitvenega sistema (denimo vodenega raketnega izstrelka) v realnem boju. Prav tako omogoča simulator nadaljnji razvoj tovrstnih iskalnih naprav, naprav za vodenje izstrelkov in pa zasnovo protiukrepov, ki tovrstne oborožitvene sisteme, kot je denimo Chukar III, skrijejo pred sovražnikovo zaznavo (MI technologies 2014);
- okrepitev infrardečih komponent, pri čemer je najbolj pomembna karakteristika možnost zaznave. Ameriška mornarica pozna napravo pod imenom *Thermic pot*, ki predstavlja posebno oblikovano kupolo, v kateri steče kemijska reakcija, kar omogoča zaznavo s pomočjo infrardeče tehnologije (Naval air systems command 2016b);
- vlečni sistem za vabe, ki v primeru modela Chukar III pomeni vleko manjšega plovila približno 8 metrov za sabo, kar v primeru poskusa sestrelitve deluje kot »magnet« za izstrelke, s čimer povečuje možnosti za preživetje samega modela Chukar III. Zaradi električnega napajanja znaša življenjska doba posamezne tovrstne vabe približno 60 minut (Naval air systems command 2016c);
- sistem za ocenjevanje zgrešene razdalje (*Scoring system*), ki predstavlja poseben računalnik, ki tekom leta denimo modela Chukar III ali nekega vodenega izstrelka preračunava oz. ocenjuje, za kakšno razdaljo bo sam oborožitveni sistem zgrešil tarčo. Informacijo nato posreduje upravljalcu z oborožitvenim sistemom, ki lahko pripravi korekcijo in poskrbi za večjo natančnost pri samem zadetku (Naval air systems command 2016d);

- dispenzerji za izstrelitev svetlobnih signalov in drugih vab, ki v primeru približujočega se sovražnega izstrelka lahko izstrelijo bakle, različne svetlobne signale in druge objekte, ki delujejo kot vaba za sovražnika. Tovrstni dispenzerji imajo navadno tudi več načinov praznjenja oz. izstreljevanja, kot je to značilno denimo za sistem z oznako AN/ALE 44 (Naval air systems command 2016e).

4.2.4 Primerjava izbranih avtomatiziranih zračnih bojnih sistemov tipa *fire and forget*

V nadaljevanju sledi primerjava med analiziranimi modeli avtomatiziranih zračnih bojnih sistemov tipa *fire and forget*. Končne analize avtomatiziranih zračnih bojnih sistemov – tako samostojnih kot tudi tistih, ki temeljijo na principu *fire and forget*, zaključujejo prvi del tega magistrskega dela. Primerjavi znotraj zadnje preučevane in analizirane skupine avtomatiziranih zračnih bojnih sistemov tipa *fire and forget* bo sledila primerjava med obema skupinama oz. tipoma preučevanih modelov, in sicer z namenom ugotovitve podobnosti in razlik, s čimer bo prišlo do izpostavitve področij, kjer je možen napredek. Sama primerjava bo potekala po ustaljenih parametrih, ki jih sestavljajo pogon, oborožitev, dodatne komponente oz. razširitve ter posebnosti posameznega modela.

Prvi parameter primerjave predstavlja pogon. Sam koncept slednjega je pri zadnji preučevani skupini zaradi različnih tehnik vzletanja oz. različnih pomagal pri vzletu nekoliko širši. Tako so ta sredstva različna pri vseh treh preučevanih modelih. Pri modelu IAI Harpy oz. IAI Harop za samo pomoč pri vzletu skrbi t. i. *container launch unit*, in sicer v različnih konfiguracijah glede na uporabo na kopenskih vozilih ali plovilih. Pri modelu SAFRAN SAGEM Sperwer Mk. II za pomoč pri vzletu skrbi poseben mehanizem, ki deluje na osnovi stisnjenega zraka po principu katapulta z oznako Robonic Kontio MC 2555LLR, pri modelu Northrop Grumman Chukar III pa za pomoč pri vzletu skrbi sistem JATO (*jet assisted take-off* – vzlet s pomočjo goriva) oz. RATO (*rocket assisted take-off* – vzlet s pomočjo raket).

Pri vseh treh modelih so različni tudi pogonski agregati. Tako za pogon IAI Harpy oz. IAI Harop skrbi pogonski agregat UAV Engines ltd. z oznako AR731 – 38 BHP, model SAFRAN SAGEM Sperwer Mk. II poganja dvotaktni pogonski agregat, model Northrop Grumman Chukar III pa poganja plod sodelovanja med podjetjem Williams international in podjetjem Rolls-Royce z oznako J400-WR-404. Same zmogljivosti med posameznimi agregati se medsebojno razlikujejo. Pogonski agregat prvega in drugega modela se med drugim razlikujeta tudi v proizvedenih konjskih močeh, ki se pri prvem gibljejo okrog številke 38, pri drugem pa okrog številke 70.

Medtem ko o samih konjskih močeh za tretji pogonski agregat ni podatka, je podatek o sami vzdržljivosti sila zanimiv. IAI Harpy oz. IAI Harop se ponašata s šestimi do devetimi urami vzdržljivosti, kar je nedvomno povezano s težo bojne konice. Model SAFRAN SAGEM Sperwer Mk. II se prav tako ponaša s 6 urami vzdržljivosti, medtem ko model Northrop Grumman Chukar III lahko v zraku ostane največ 78 minut. Anomalija oz. odklon se poraja tudi pri informacijah o sposobnosti doseganja višin, pri čemer za prvi model ni točnega podatka, drugi model lahko doseže višino 4572 metrov, tretji model pa z najmanjšo vzdržljivostjo doseže osupljivih 12 000 metrov. Izstopajoči karakteristiki se pojavljata pri pogonskih agregatih prvega in drugega modela. Pogonski agregat prvega modela lahko koristi dve vrsti goriva, in sicer MoGas ali AvGas (karakteristike so podane pri sami analizi modela). Izstopajoča karakteristika drugega modela je sam doseg modela, ki ne presega 200 kilometrov.

Drugi parameter primerjave predstavlja oborožitev, pri kateri zaradi same zasnove in posledično spremenjene namembnosti samega modela v celoti izpade tretji analizirani model, tj. Northrop Grumman Chukar III. Tako bosta predmet primerjave zgolj oborožitveni komponenti modela IAI Harpy oz. IAI Harop ter model SAFRAN SAGEM Sperwer Mk. II. Bojno komponento prvega modela predstavlja eksplozivna fragmentacijska bojna konica (*explosive fragmentation warhead*), pri čemer je potrebno izpostaviti dejstvo, da pri preučevanem modelu le-ta tehta 21 kilogramov, medtem ko pri modelu IAI Harpy NG (*new generation* – nova generacija) tehta 15 kilogramov, od koder tudi izhaja odklon pri sami vzdržljivosti.

Pri drugem modelu lahko bojno komponento predstavlja izstrelek Spike ER ali izstrelek 155 BONUS. Ob tem je pomembno dodati, da izstrelek pri drugem modelu ne sme tehtati več kot 30 kilogramov. Kar zadeva samo primerjavo med vsemi tremi tipi oborožitve gre pri eksplozivni fragmentacijski bojni konici in pri izstrelku 155 BONUS za oborožitev, ki povzroča škodo na nekem določenem območju (*area damage*), pri čemer lažjo predstavo nedvomno omogoča dejstvo, da spada izstrelek 155 BONUS pravzaprav med artilerijsko strelivo. Ta podatek je pomemben v kontekstu narave drugega možnega izstrelka pri drugem

modelu, tj. izstrelka podjetja Rafael advanced defense system, z oznako Spike ER, ki pravzaprav predstavlja voden raketni izstrelek (*precision guided missile*).

Tretji parameter primerjave so dodatne komponente oz. v primeru analiziranih modelov razširitve. Same razširitve pri modelu Northrop Grumman Chukar III bodo imele tokom te analize pomembno vlogo, saj bodo predstavljale povsem nov kriterij za vrednotenje dodatnih komponent, ob tem pa ne bodo predstavljale nekaj kontradiktornega, temveč bodo nadgradile samo idejo o dodatnih komponentah, jim dale neko dodano vrednost in z vidika uporabe avtomatiziranih zračnih bojnih sistemov kot vabe za sovražnika odprle novo perspektivo – tako o sami zasnovi tovrstnih oborožitvenih sistemov kot tudi o njihovi opremljenosti.

Naj začnem s primerjavo dodatnih komponent med prvima dvema analiziranima modeloma. Vsak od prvih dveh modelov ima neke vrste elektro-optični oz. infrardeč sistem, ki deluje kot radar oz. kot nek sistem za določanje tarč. Pri prvem modelu le-tega predstavlja IAI Tamam POP-200, medtem ko pri drugem le-tega predstavlja podsistem z oznako Euroflir 350. Tako IAI Tamam POP-200 kot tudi Eurofli 350 predstavljata celoto oz. skupek številnih komponent, kot so toplotna kamera, visokoločljivostna kamera, laserski telemeter in laserski namerilnik, ki so integrirani v zaokroženo celoto. Model Northrop Grumman Chukar III to zaokroženo celoto predstavlja kot več ločenih razširitev.

Prva izmed razširitev je okrepitev radarja, pri čemer obstaja možnost izbire med pasivnim in aktivnim radarjem. Druga razširitev predstavlja simulator iskalnih naprav, ki bi jo okvirno lahko pojmovali z laserskim telemetrom in laserskim namerilnikom, tretja razširitev pa predstavlja sistem za ocenjevanje zgrešene razdalje, ki bi jo lahko pojmovali z laserskim telemetrom in laserskim namerilnikom. Zadnja, četrta razširitev pa predstavlja okrepitev infrardeče komponente.

Vsak od treh preučevanih modelov ima podsistem za komunikacijo, pri čemer gre model SAFRAN SAGEM Sperwer Mk. II s sistemoma za prestrezanje in analizo nasprotnikovih

komunikacij COMINT in ELINT, ki jih večinoma poznamo kot »nadpomenko« SIGINT, še korak dlje.

Isti model se hkrati ponaša z uporabo sistema ISTAR, ki skrbi za analizo telemetrije. Poleg omenjenih razširitev modela Northrop Grumman Chukar III ima sam oborožitveni sistem na voljo še dve razširitvi, ki ju predstavljata vlečni sistem za vabe (*tow system*) ter dispenzerji za izstreljevanje svetlobnih signalov in drugih motilcev. Ocena samih dodatnih komponent ter primerjava med njimi kaže na to, da so pri modelu Northrop Grumman Chukar III vse dodatne komponente razvili še korak dlje in kljub široki paleti možnih razširitev še vedno uspeli vse skupaj združiti v avtomatiziran zračni bojni sistem tipa *fire and forget*. Samo razmišljanje o uporabi tovrstnih oborožitvenih sistemov kot sredstvo za zavajanje nasprotnika ter kot sredstvo za usposabljanje je pripeljalo do večjega napredka kot zgolj uporaba za napad ter naloge izvidništva, opazovanja itd. Integracija številnih sicer kompatibilnih komponent se ni izkazala za nujno najboljšo rešitev.

Četrti parameter primerjave med analiziranimi modeli predstavljajo specifične karakteristike, ki načeloma od modela do modela variirajo. Tako je prva specifična karakteristika pri modelu IAI Harpy oz. IAI Harop lastnost, da gre za *loitering weapon* ter da model napad izvede vertikalno. Skupno karakteristiko predstavlja možnost preklica napada tarče po sami izstrelitvi, a s to razliko, da pri modelu IAI Harpy oz. IAI Harop s tem pride do samouničenja. Pri drugih dveh obstaja sistem za pristajanje, in sicer padalo, ki je skupno obema preostalima modeloma, pri čemer ima model SAFRAN SAGEM Sperwer Mk. II na voljo še set zračnih blazin za ublažitev pristanka.

Preostale specifične karakteristike pri modelu SAFRAN SAGEM Sperwer Mk. II predstavljajo opcijsko posedovanje bojne komponente, medtem ko ima model Northrop Grumman Chukar III t. i. dvojno naravo, vendar ne kot razdelitev na bojno in nebojno različico, temveč gre ali za oborožitveni sistem (katerega primarna naloga je zavajanje sovražnika) ali za sredstvo za usposabljanje.

4.3 Primerjava med tipoma avtomatiziranih zračnih bojnih sistemov

Primerjava med obema tipoma avtomatiziranih zračnih bojnih sistemov bo potegnila ločnico med enimi in drugimi ter izpostavila točke, na katerih se njihove karakteristike križajo. Tako bo z izpostavljenimi podobnostmi in razlikami prvotno predstavljena kategorizacija avtomatiziranih zračnih bojnih sistemov dobila ustrezen kontekst. Sama primerjava bo potekala po parametrih, ki jih predstavljajo pogon, oborožitev, dodatne komponente ter posebnosti oz. specifične karakteristike modelov.

Pred samo primerjavo dejanskih pogonskih agregatov in njihovih zmogljivosti je potrebno izpostaviti ključno razliko, in sicer da samostojni avtomatizirani zračni bojni sistemi zaradi zmogljivosti samih pogonskih agregatov, svoje velikosti ter posledično potrebe po ustrezni vzletni in pristajalni površini, ne potrebujejo pomožnih sredstev za vzlet, kot je praksa pri avtomatiziranih zračnih bojnih sistemih tipa *fire and forget*. Če nadaljujem s primerjavo samih karakteristik pogonskih agregatov, je prvi ključni podatek ta, da samostojni avtomatizirani zračni bojni sistemi uporabljajo veliko močnejše pogonske agregate. Tako denimo model Northrop Grumman MQ-1C Gray eagle uporablja pogonski agregat z 2000 kubičnimi centimetri delovne prostornine, ki proizvede kar 155 konjskih moči, medtem ko na drugi strani model IAI Harpy oz. IAI Harop uporablja pogonski agregat z 208 kubičnimi centimetri delovne prostornine, ki proizvede 38 konjskih moči, kar se odraža tudi na sami vzdržljivosti. Slednja se pri avtomatiziranih zračnih bojnih sistemih tipa *fire and forget* giblje med oseminsedemdesetimi minutami in devetimi urami, medtem ko se pri samostojnih avtomatiziranih zračnih bojnih sistemih le-ta nahaja nekje med tremi in štiriindvajsetimi urami.

Kar zadeva doseganje višin se pri avtomatiziranih zračnih bojnih sistemih tipa *fire and forget* doseganje giblje nekje do 12 000 metrov višine, medtem ko je najvišja meja pri analiziranih samostojnih zračnih bojnih sistemih 17983 metrov.

Oborožitveni parameter primerjave presenetljivo ne predstavlja edine razlike v kvantiteti. Tako ni edina razlika med tipoma avtomatiziranih zračnih bojnih sistemov količina oborožitve, ki jo lahko nosi posamezen tip ali posamezen model, temveč so tudi same karakteristike oborožitve. Medtem ko gre pri oborožitvi avtomatiziranih zračnih bojnih sistemov tipa *fire and forget* za oborožitev, ki cilja na tarče nekako v vidnem polju oborožitvenega sistema, se na drugi strani določena oborožitev pri samostojnih avtomatiziranih zračnih bojnih sistemi, kot je denimo oborožitev tipa Hellfire pri modelu Northrop Grumman MQ-1C Gray Eagle, ponaša z dosegom po izstrelitvi v razponu od 7,1 do 11 kilometrov.

Sam nabor oborožitve pri obeh tipih avtomatiziranih zračnih bojnih sistemov obsega tako vodene bombe, vodene raketne izstrelke kot tudi artilerijsko strelivo. Pri avtomatiziranih zračnih bojnih sistemih tipa *fire and forget* gre za posebej prilagojeno oz. skrbno izbrano oborožitev, saj denimo v primeru modela SAFRAN SAGEM Sperwer Mk. II sama oborožitev ne sme tehtati več kot 30 kilogramov. Tako raketni izstrelek tipa Hellfire za ta oborožitveni sistem ni primeren.

Tretji parameter, ki zajema primerjavo dodatnih komponent, prikazuje določeno omejenost pri samostojnih avtomatiziranih bojnih sistemih. Vsem trem modelom skupine je skupno, da imajo elektro-optičen oz. infrardeč podsistem za določanje tarč oz. radar, taktični radar ter podsistem za komunikacijo. Kar zadeva prvi dve komponenti se Northrop Grumman Gray Eagle ponaša s podsistemoma, in sicer podsistem Raytheon MTS (CSP), ki predstavlja elektro-optični oz. infrardeč podsistem za določanje tarč, STARLite AN-ZPY pa predstavlja taktični radar. Model Guizhou WZ-2000 kot podsistem za komunikacijo uporablja sistem SIGINT.

Na drugi strani so avtomatizirani zračni bojni sistemi tipa *fire and forget* veliko bolj naklonjeni razvoju ter širjenju svojih kapacitet. Tovrstni predhodno predstavljeni »osnovni paket« ima tudi model IAI Harpy oz. IAI Harop. Model SAFRAN SAGEM Sperwer Mk. II pa gre korak dlje, in sicer razdeli podsistem za komunikacije na COMINT in ELINT ter s tem več pozornosti posveča posameznemu, hkrati pa uporablja tudi sistem ISTAR, ki predstavlja

poseben sistem za analizo telemetrije. Model Northrop Grumman Chukar III s široko paleto možnih razširitev z vidika vsestranskosti (v kolikor ne z vidika napredovanja) na področju posamezne komponente predstavlja najmanjši standard.

Četrti parameter, ki zajema posebnosti oz. specifične karakteristike posameznega modela, daje vtis, da ga ni moč vključiti v primerjavo, a se pri več modelih pojavi več t. i. posebnosti, ki izhajajo bodisi iz ene bodisi iz druge skupine. Tako je denimo modelom MQ-1C Gray Eagle, Guizhou WZ-2000, Sperwer Mk. II ter Chukar III skupna t. i. dvojna narava oz. posedovanje bojne in/ali nebojne komponente oz. uporabe kot sistem za vabo. Modelu MQ-1C Gray Eagle ter modelu Sperwer Mk. II je prav tako skupna možnost transporta v letalu tipa C-130. Razlike pa predstavljajo predvsem pristajalni mehanizmi, zasnova kril (delta ipd.), sprememba načina napada (vertikalen napad na tarčo) ter sprememba namembnosti oborožitvenega sistema (*loitering weapon*). Prav tako so določeni modeli drugačni, saj jih je po terenu moč prenašati v nahrbtnikih (IAI Bird eye 400), spet drugi so sestavljeni iz drugačnih materialov (IAI Bird eye 400 ter IAI Searcher Mk. II sta sestavljena iz kompozitnih materialov).

5 Kibernetične grožnje in protiukrepi v kontekstu delovanja avtomatiziranih zračnih bojnih sistemov

Z analizo posameznih tipov in posameznih modelov avtomatiziranih zračnih bojnih sistemov ter njihovih podsistemov sem omogočil celosten vpogled v zmogljivosti tovrstnih oborožitvenih sistemov. V drugem delu magistrskega dela se bom osredotočil na koncept kibernetičnih groženj in njihov vpliv na delovanje avtomatiziranih zračnih bojnih sistemov, neglede na tip samega oborožitvenega sistema ter na možne protiukrepe tem grožnjam, neodvisno od njihove preventivne ali kurativne narave. Ob tem je potrebno poudariti, da so osrednji akter pri tej analizi sami avtomatizirani zračni bojni sistemi, kljub temu pa je potrebno določen del pozornosti nameniti tudi njihovim nadzorovalnim postajam.

Zaradi dvosmerne komunikacije med avtomatiziranimi zračnimi bojnimi sistemi sta oba akterja pri analiziranju kibernetskih groženj in samih protiukrepov pomembna, hkrati pa oba akterja predstavljata morebitno točko napada. Ena izmed pogosto spregledanih predpostavk je tudi ta, da ni nujno, da je napad izveden »od zunaj«. Prepogosto imamo ob omembi nekega napada v glavah sliko, da gre za boj med dvema sovražnikoma, ki se med seboj ne poznata in sta drug od drugega oddaljena. Ena izmed možnosti na tovrstnih področjih je uporaba koncepta notranjega sovražnika (*inside man*), kjer neka oseba na podlagi takšnih ali drugačnih razlogov (izsiljevanje, grožnje, podkupnina, osebni razlogi ipd.) sabotira svoje delo oz. svojega delodajalca.

V nadaljevanju bo analiza groženj potekala v skladu s klasifikacijo groženj, ki pretijo dotično samemu oborožitvenemu sistemu ter groženj, ki pretijo dotično sami nadzorni postaji tovrstnih sistemov. Ob tem bo ob analizi posameznih groženj, kjer obstaja večja možnost uporabe izrecno enega ali izrecno drugega koncepta, koncept notranjega oz. zunanjega sovražnika dodatno poudarjen.

Sama analiza groženj in morebitnih protiukrepov bo sprva predstavljena na splošno, natančneje pa bodo protiukrepi podrobneje predstavljeni tudi v skladu s perspektivo nekaterih proizvajalcev (predhodno) analiziranih modelov avtomatiziranih zračnih bojnih sistemov. Tako bo sprva v skladu z običajno strukturo in podsistemi predstavljena ranljivost nekega avtomatiziranega zračnega bojnega sistema. Sledila ji bo analiza možnih napadov oz. groženj, in sicer tako, da bo najprej opravljena osnovna klasifikacija, razmejitev na možne napade oz. grožnje na tiste, ki pretijo samim avtomatiziranim zračnim bojnim sistemom, in tiste, ki pretijo kopenskim nadzornim postajam.

Ob tem bo predstavljenih več perspektiv oz. zornih kotov teh napadov, sledila bo navedba možnih napadov oz. groženj ter njihova kratka analiza. Po analizi samih groženj bo predstavljeno tudi delovanje različnih proizvodnih podjetij analiziranih avtomatiziranih zračnih bojnih sistemov na področju kibernetičnih napadov kot groženj delovanju avtomatiziranim zračnim bojnim sistemom.

Preden začnem s samo analizo ranljivosti nekega avtomatiziranega zračnega bojnega sistema v skladu z običajno strukturo in podsistemi, je potreben manjši *intermezzo* glede razlogov za sam napad na tovrstne oborožitvene sisteme. Ne glede na to, kaj je trenutno popularno ali kaj je bilo popularno v preteklosti, danes moč predstavlja informacija. Avtomatizirani zračni bojni sistemi zaradi svoje vsestranskosti in sposobnosti opravljanja številnih predhodno omenjenih nalog predstavljajo odlično zalogo informacij, ki v tem trenutku še ni tako dobro zaščitena. Medtem ko je napredek zaželen, pa je potrebno na avtomatizirane zračne bojne sisteme gledati kot na visoko izpostavljeno, večstransko povezano strojno opremo z visoko ekonomsko in strateško vrednostjo (Hartmann in Steup 2013).

Za lažje razumevanje nadaljnje analize možnih napadov oz. groženj je potrebno imeti pregled nad strukturo in podsistemi nekega avtomatiziranega zračnega bojnega sistema. Strukturo samega oborožitvenega sistema sestavljajo osnovni operacijski sistem, komunikacijske povezave, senzorji ter naprave, potrebne za letenje. Poleg teh komponent sta možni komponenti tudi podsistem oborožitve in podsistem, ki oborožitvenemu sistemu omogoča določeno stopnjo avtonomnosti. Na drugi strani strukturo kopenske nadzorne postaje

oborožitvenega sistema predstavljajo operaterji ter komunikacijske povezave (prav tam). Sama omemba strukture kopenske nadzorne postaje je pri tem pomembna zato, ker bi v danih okoliščinah sam kibernetični napad lahko izviral tudi iz kopenske nadzorne postaje samega oborožitvenega sistema.

Kot bo razvidno v nadaljevanju, sama narava avtomatiziranih zračnih bojnih sistemov ter njihov sistem komunikacij predstavlja odlično tarčo za napad. Gre predvsem za to, da je povezava med samim oborožitvenim sistemom ter kopensko nadzorno postajo brezžična. Pri tem je le-ta mogoča ali preko sistema za komunikacijo, pri katerem je oborožitveni sistem konstantno v polju vidljivosti (*line-of-sight*), ali preko sistema, ki uporablja satelit. Sama komunikacija ter prenos informacij med oborožitvenim sistemom ter kopensko nadzorno postajo predstavlja prvi šibek člen kar zadeva varnost, medtem ko drugi šibek člen predstavlja izmenjava informacij znotraj samega oborožitvenega sistema med dodatnimi komponentami (senzorji) ter operacijskim sistemom.

Ker so dodatne komponente (senzorji) za nemoteno delovanje oborožitvenega sistema esencialnega pomena, predstavljajo odlično tarčo za napad (prav tam). Kritične točke avtomatiziranih zračnih bojnih sistemov so torej povezave s kopensko nadzorno postajo, ki omogočajo izmenjavo informacij tako zunaj kot tudi znotraj samega oborožitvenega sistema.

Kako je mogoče, da se tako sodobna tehnologija na področju avtomatizacije in avtonomnosti, ki sta pravzaprav koncepta v razvoju, ni sposobna kosati z že nekaj časa uveljavljenimi metodami kibernetskih napadov? Odgovor leži v zasnovi avtopilota za zračne sisteme s posadko. Avtomatizirani zračni bojni (kot tudi nebojni) sistemi temeljijo na principu avtopilota, ki je vgrajen v zračne sisteme s posadko. Ob zasnovi tovrstnega sistema avtopilota zaradi vgrajevanja v sisteme s posadko kibernetična varnost ni bila prioriteta, saj naj bi bil sam sistem avtopilota pomožne narave, hkrati pa bi lahko posadka v primeru odklanjanja od definiranih standardov prevzela vajeti nazaj v svoje roke (Kim in drugi 2012).

Za samo analizo možnih napadov oz. samih groženj ter za lažje razumevanje je potrebno narediti razmejitev oz. klasifikacijo samih napadov. Tako je kibernetične napade moč opredeliti s pomočjo treh kategorij, in sicer prvo skupino kibernetičnih napadov predstavljajo napadi na strojno opremo (*hardware attack*), pri čemer ima napadalec neposreden dostop do komponent nekega avtomatiziranega zračnega bojnega sistema (Kim in drugi 2012).

Prav pri tem napadu je pomemben predhodno omenjeni koncept notranjega sovražnika (*inside man*), ki lahko deluje v najmanj dveh razsežnostih. Prvo razsežnost tako predstavlja nek zlonameren posameznik, ki »sodeluje« pri sami zasnovi določenega avtomatiziranega zračnega sistema in ga tako namerno naredi še bolj ranljivega kot sicer. Drugo razsežnost pa predstavlja nek zlonameren posameznik, ki prisostvuje v sami kopenski nadzorni postaji in upravlja s samim oborožitvenim sistemom.

Drugo skupino kibernetičnih napadov predstavljajo napadi na brezžične povezave (*wireless attack*), ki navadno predstavljajo ali napad na povezavo med kopensko postajo in avtomatiziranim zračnim sistemom ali na povezavo med satelitom in samim oborožitvenim sistemom, od česar je odvisen način komunikacije med oborožitvenim sistemom ter kopensko nadzorno postajo. Tretjo skupino kibernetičnih napadov predstavljajo napadi na senzorje oz. dodatne komponente (*sensor spoofing*), ki ciljajo denimo na navigacijski vmesnik, naprave za telemetrijo itd. (prav tam). En način klasifikacije kibernetičnih napadov tako predstavlja zgornja razmejitev, medtem ko bi same kibernetične napade lahko klasificirali tudi glede na tarčo napada. V primeru preučevanih oborožitvenih sistemov sta tarči dve, in sicer eno predstavlja sam avtomatizirani zračni bojni sistem, drugo tarčo pa predstavlja kopenska nadzorna postaja.

Drugi način klasifikacije bi glede na tarčo in glede na dosedanjo analizo bil sledeč.

Kibernetične grožnje za avtomatizirani zračni bojni sistem:

- odvzem, sprememba ali injiciranje skorumpiranih podatkov skozi osnovno programsko opremo;

- odvzem, sprememba ali injiciranje skorumpiranih podatkov skozi senzorje oz. dodatne komponente;
- odvzem, sprememba ali injiciranje skorumpiranih podatkov v naprave potrebne za samo letenje in s tem morebitno spreminjanje načrtovane poti;
- prenos vseh zbranih podatkov oborožitvenega sistema;
- vdor v povezavo med oborožitvenim sistemom in kopensko nadzorno postajo z namenom prevzema nadzora s pomočjo blokiranja ali prevar navigacijskih naprav (*GPS jamming, GPS spoofing*);
- vstavljanje virusa v osnovno programsko opremo in morebitna uporaba tehnike *spear fishing* – ustvarjanje posebnega dostopa v osnovno programsko opremo.

Kibernetične grožnje za kopensko nadzorno postajo:

- vdor v programsko opremo kopenske nadzorne postaje (vstavljanje virusov, vdor v komunikacijo z oborožitvenim sistemom ipd.);
- fizičen vdor v kopensko nadzorno postajo in prevzem nadzora ter izvajanje kibernetičnih napadov s prevzemom nadzora, vstavljanjem virusov itd.

Ob zgoraj omenjenih kategorizacijah kibernetičnih napadov obstaja še tretja »različica« oz. še dodaten način klasifikacije, in sicer glede na to, česar varnost ogrožajo kibernetični napadi znotraj samega avtomatiziranega zračnega bojnega sistema. Gre torej za pravzaprav poglabljanje prvega načina klasifikacije, in sicer za poglabljanje prve in tretje skupine kibernetičnih napadov (tj. *hardware attack* in *sensor spoofing*).

Dodatni tretji način klasifikacije tako zgoraj navedeni skupini kibernetičnih napadov redefinira in loči na varnost nadzornega sistema (*control system security*), kar v osnovi pomeni manipulacijo osnovnih programskih funkcij do točke, ko le-te podivjajo oz. so preprosto neodzivne ter na varnost programske logike (*application logic security*), ki v grobem pomeni manipulacijo različnih senzorjev oz. dodatnih komponent, med katere spadajo podsistem za komunikacijo, navigacijo ipd. Zanimiv je tudi sam odnos v primeru, da gre za napad na varnost programske logike.

Medtem ko korupcija varnosti nadzornega sistema povzroči resno škodo, ki načeloma rezultira najmanj v izgubi nadzora nad avtomatiziranim zračnim bojnim sistemom, če ne kar v izgubi celotnega oborožitvenega sistema, pa na drugi strani napad na varnost programske logike povzroči škodi na dotični tarči (senzorju oz. dodatni komponenti), s čimer pa ne škodi osnovnim funkcijam, ki jih vsebuje nadzorni sistem. Sam avtomatizirani zračni bojni sistem tako še naprej deluje in je še vedno v rokah primarnega upravljalca, pri čemer je okrnjen za prizadete dodatne komponente oz. senzorje, kar glede na tarčo, kar se tiče letenja, rezultira v odklonu letenja (Kim in drugi 2012).

Znotraj varnosti programske logike je (zaradi same širine nabora tarč) širok tudi nabor možnih kibernetičnih napadov:

- usklajevanje kanalov (*gain scheduling*) predstavlja kompleksnost samega nadzornega sistema v avtomatiziranih zračnih bojnih sistemih. Usklajevanje kanalov temelji na tem, da se sam osnovni operacijski sistem v danem trenutku lahko povezuje z eno dodatno komponento, kar pomeni en odprt kanal. Ker sam oborožitveni sistem poseduje več dodatnih komponent, mora za optimalno delovanje samega oborožitvenega sistema med komunikacijo prihajati do natančnega usklajevanja med kanali. Tovrstno usklajevanje je navadno preračunano vnaprej in računalniško vodeno, posledično upravljalec le-temu ne posveča veliko pozornost, kar predstavlja odlično tarčo za kibernetični napad, ki bi bil v določeni meri tudi precej neopazen. Kibernetični napad bi tako bil lahko izveden ali z namenom spremembe določenega kanala v določenem trenutku ali kot neprestano menjavanje med samim kanali izven računalniško določenih okvirjev izračunov menjavanja kanalov. Prav tako bi lahko v tem primeru metoda kibernetičnega napada bila omejitev ali blokada dostopa do nekega kanala. Tovrstne manipulacije bi rezultirale v slabšem delovanju ali hudi nestabilnosti samega oborožitvenega sistema;

- prožilec/senzor (*actuator/sensor*) predstavlja pravzaprav komponento, ki konstantno posodablja podatke o tem, kje se nek avtomatizirani zračni bojni sistem nahaja, njegovo oddaljenost od cilja, tarče ali pristajališča. Posledično bi kibernetični napad v obliki prevare, zaobitja te komponente ali prirejanje podatkov, ki jih ta komponenta

posreduje naprej, lahko rezultiral v nestabilnosti samega oborožitvenega sistema, njegovemu prevzemu ali spremembi cilja, tarče ipd.;

- navigacijski podsistem: napad na navigacijski podsistem bi pomenil, da bi oborožitveni sistem pristal na napačnem kraju ali se zaradi napačne ocene trenutne lokacije samouničil ob predpostavki določenih okoljskih dejavnikov (gorovje ipd.). Sam kibernetični napad bi tako lahko bil zgolj blokiranje samega navigacijskega signala (*GPS jamming*) ali na drugi strani prevara navigacijske komponente ter posredovanje napačnih navigacijskih informacij (*GPS spoofing*);

- samodejno odvisno nadzorovanje – difuzija (*Automatic dependent surveillance – broadcast*) predstavlja pravzaprav podatkovni promet oz. podatkovno komunikacijo tako med samim avtomatiziranim zračnim bojnim sistemom in nadzorno postajo kot tudi med omenjenima akterjema, drugimi letali, letališči itd. Gre za način komunikacije, ki vsem vključenim akterjem razkriva lokacijo dotičnega zračnega sistema, s čimer se preprečuje nesreče v zraku, komunicira in identificira. Morebitni kibernetični napad na to komponento bi tako lahko rezultiral v trčenju avtomatiziranega zračnega bojnega sistema z nekim drugim zračnim sistemom oz. v primeru identifikacije v tem, da bi določene oborožene sile sestrelile lastni avtomatizirani zračni bojni sistem;

- preizkušanje z naključnimi podatki (*fuzzing*) predstavlja kibernetični napad, ki poskuša vplivati na kvaliteto podatkov oz. informacij, ki se gibljejo tako znotraj osnovnega operacijskega sistema kot tudi med številnimi dodatnimi komponentami ter osnovnim operacijskim sistemom. Kibernetični napad bi z vnosi naključnih podatkov in vrednosti te podatke »pokvaril«, kar bi lahko, zaradi preobremenitve z injeciranjem skorumpiranih podatkov ter nestabilnosti celotnega avtomatiziranega zračnega bojnega sistema, pripeljalo do odpovedi oz. blokade določene komponente;

- hitrost osveževanja podatkov (*digital update rate*) predstavlja hitrost prenosa podatkov oz. informacij v avtomatiziranem zračnem bojnem sistemu med posameznimi komponentami in osnovnim operacijskim sistemom. Podobno kot pri usklajevanju

kanalov gre pri hitrosti osveževanja podatkov za podoben princip. V kolikor ena od komponent prične zaostajati in vrednost hitrosti osveževanja podatkov ni več konstantna, postane celoten oborožitveni sistem nestabilen. Kibernetični napad, ki bi eno komponento pretirano zasičil z nekoristnimi informacijami oz. podatki ali pa blokiral delovanje ene od komponent oz. zgolj onemogočil prenos podatkov, bi vplival na hitrost osveževanja podatkov in posledično škodoval samemu avtomatiziranemu zračnemu bojnemu sistemu (Kim in drugi 2012).

Možnosti kibernetičnih napadov so številne, njihova razlikovanja pa izvirajo (kot že predhodno omenjeno) iz razlogov za napad, tarče in konec koncev tudi ciljev. Zgoraj predstavljeni možni kibernetični napadi so dober uvid v to, kako zelo proste roke ima napadalec ter kakšne so lahko posledice tovrstnih napadov na avtomatizirane zračne bojne sisteme.

Na podlagi povedanega je z vidika kibernetičnih napadov preostalo še eno vprašanje, in sicer kako se braniti pred kibernetičnimi napadi oz. kakšna so sredstva za zaščito avtomatiziranih zračnih bojnih sistemov. Kar zadeva sredstva za zaščito avtomatiziranih zračnih bojnih sistemov pred kibernetičnimi napadi je pri modelu ameriškega proizvajala Northrop Grumman z oznako MQ-1C Gray Eagle že predstavljen model t. i. trojnega podvajanja oz. *triple-redundant avionics system architecture*, ki pomeni, da se poleg osnovnega operacijskega sistema v oborožitvenem modelu nahajata še dve kopiji operacijskega sistema, ki lahko v primeru okvare prevzameta upravljanje (Resch in drugi 2013).

Podjetje Northrop grumman je aktivno na področju obrambe pred kibernetičnimi napadi. Njihov *modus operandi* izgleda kot predvidevanje in analiziranje čim širših možnosti kibernetičnih napadov. Za ta namen so ustvarili posebno integrirano omrežje za kibernetično bojevanje (*Cyber warfare integration network*), ki pravzaprav predstavlja široko platformo za zbiranje, analiziranje, simuliranje in tudi izvajanje kibernetičnih napadov v virtualni razsežnosti z namenom analiziranja učinkov dejanskih kibernetičnih napadov, s čimer lahko posledično pride do oblikovanja varnostnih ukrepov. Omrežje deluje že od leta 2002 in

vključuje tako podružnice podjetja Northrop Grumman povsod po svetu kot tudi zunanje partnerje podjetja.

Same analize kibernetičnih napadov pa ne potekajo na podlagi nekih naključnih podatkov, temveč se v omenjeno virtualno okolje delovanja vključuje modele pravih zračnih sistemov s posadko ali brez, realistične konfiguracije terena (bojišča), realistično programsko opremo, ki bi jo v principu lahko združili pod okrajšavo C4ISR.

Tako na podlagi realističnih podatkov podjetje skupaj s partnerji ustvari realno sliko nekega napada, na podlagi katerega lahko gradi sistem zaščite tudi za avtomatizirane zračne bojne sisteme (Northrop Grumman 2016f). Hkrati je podjetje Northrop Grumman ustanovilo še Raziskovalni konzorcij za kibernetsko varnost (*Cybersecurity research consortium*) ter Center za napredno kibernetsko tehnologijo (*Advanced cyber technology center*). Poleg ustvarjanja platform za preučevanje možnih kibernetičnih napadov je podjetje Northrop Grumman razvilo tudi nov koncept, pod imenom *continuous trust restoration* – neprekinjeno vzpostavljanje zaupanja, ki temelji na tem, da napadalcu skrajšajo čas, ki ga preživi na njihovem omrežju (Boyle 2015a).

Gre za koncept oz. strategijo, pri kateri se sam programski del nekega avtomatiziranega zračnega bojnega sistema konstanto obnavlja. Pri dotedanjih sistemih se je sistem obnavljal šele po detekciji in začetku protiukrepov, pri čemer se je izgubilo ogromno časa. Strategija *continuous trust restoration* pa predvideva konstantno obnavljanje samega sistema, kar bo skrajšalo čas, ki ga nek napadalec lahko »preživi« v nekem določenem avtomatiziranem zračnem bojnem sistemu, ko enkrat vanj vdre, hkrati pa mu bo lahko onemogočilo dostop do nadaljnjega zlorabljanja sistema oz. mu bo onemogočilo dostop do drugih komponent (Boyle 2015b).

Izraelsko podjetje Rafael advanced defense systems ltd. je na nevarnost kibernetičnih napadov ustvarilo svojevrsten odgovor. Gre za protiukrep, ki nosi ime Drone Dome in je zasnovano tako, da zazna, identificira, sledi in nevtralizira sovražnikove avtomatizirane zračne (bojne)

sisteme, ki naj bi predstavljali glavno grožnjo kar zadeva zračne napade, zbiranje informacij ipd. Sama naprava deluje kot neke vrst senzor oz. radar za zaznavanje, ki naj bi bil sposoben operativnega delovanja v vseh vremenskih okoliščinah.

Gre za sistem, ki je opremljen z radarjem in elektro-optičnimi oz. infrardečimi senzorji, s katerimi zazna nek sovražnikov avtomatizirani zračni (bojni) sistem in opozori upravljavca domnevno sovražnega avtomatiziranega zračnega (bojnega) sistema. Ob tem naj bi bile določene meje oz. območja, ki bi določevala, v kolikor posredovanje ostane pri samem opozarjanju oz. ali gre zadeva tako daleč, da je potrebna nevtralizacija. V kolikor bi se nek nepooblaščen avtomatiziran zračni (bojni) sistem preveč približal denimo nekemu varovanemu območju, bi sama nevtralizacija potekala s pomočjo blokiranja povezave med nepooblaščenim sistemom ter povezanim navigacijskim sistemom oz. s pomočjo prekinitve signala s satelitom. Specifičen protiukrep je prekinitev povezave za navigacijo, kar navadno pomeni izgubo nadzora primarnega upravljavca oz. uničenje samega sistema (iHLS 2016).

Israel Aerospace Industries je še eno izraelsko podjetje, ki ustvarja svojo različico protiukrepov proti kibernetičnim napadom. Podjetje je, podobno kot ameriško podjetje Northrop Grumman, pod imenom TAME Cyber defense suite, ustvarilo svojo platformo za detekcijo, analizo in obrambo pred napadi. Sama filozofija podjetja je, da kibernetičnih napadov ni moč v celoti preprečiti, a jih je možno nekoliko ukrotiti.

Tako zgoraj omenjena platforma (TAME Cyber defense suite) ponuja celostno platformo, ki nudi možnosti urjenja, analize sistema in posledično v določeni meri predvidevanja narave kibernetičnega napada, odkrivanje napadov, do določene mere pa ima tudi forenzične prvine, ki služijo sledenju napada oz. dotično samemu napadalcu. Sama platforma sestoji iz dela za urjenje (TAME Range), delov za detekcijo za (TAME Guard in TAME Neptune), dela za širjenje ozaveščenosti med partnerji (TAME iShare) ter obnovitvenega sistema (TAME Respond) (Israel Aerospace Industries 2013b).

Ena izmed možnosti, ki se jo prav tako navaja kot ustrezen protiukrep proti kibernetičnim napadom, je uvedba t. i. nadzornika (*supervisor* oz. *hypervisor*), ki služi znotraj avtomatiziranega zračnega bojnega sistema kot antivirusni program z določenimi dodatnimi funkcijami.

Prvi tovrstni sistem z imenom *Supervisor* omenjajo Kim in drugi (2012) in predstavlja pravzaprav nadzorni sistem, ki deluje sicer neodvisno, a hkrati vzporedno z osnovnim operacijskim sistemom in spremlja morebitne spremembe v obnašanju same programske opreme oz. išče anomalije. V primeru zaznave neke anomalije oz. nenavadnega obnašanja programske opreme, le-te sporoči upravljalcu samega avtomatiziranega zračnega bojnega sistema. Pri tem je potek komunikacije enosmeren, kar pomeni, da *Supervisor* poroča upravljalcu oborožitvenega sistema, medtem ko mu upravljalec zaradi nevarnosti vdora v to povezavo povratne informacije ne more sporočiti. V primeru zaznave je postopek tak, da v kolikor upravljalec ne more odpraviti anomalije in oborožitvenega sistema vrniti v optimalno delujoče stanje, to nalogo prevzame *Supervisor*, ki s konstantnim posodabljanjem sistema poskuša napako oz. anomalijo odpraviti. V kolikor je pri tem neuspešen pa lahko v celoti prevzame nadzor nad samim oborožitvenim sistemom ter ga v skladu z njegovo operativno sposobnostjo koordinira (nadaljuje z misijo, se vrne v bazo ali se na varen način odstrani z naloge).

Drugi tovrstni sistem, ki je izredno podoben sistemu *Supervisor*, je sistem za zaščito pod imenom *Hypervisor*. Gre za produkt podjetja Lynx Software Technologies Inc., pri katerem je način delovanja izredno podoben sistemu *Supervisor*, a s to razliko, da ni nikjer omenjen sam prevzem nadzora nad denimo nekim avtomatiziranim zračnim (bojnim) sistemom. Prav tako sistem *Hypervisor* deluje na osnovi detekcije neke anomalije, ki jo v primeru odkritja izolira od ostalih komponent z namenom, da prepreči širjenje »okužbe«. Gre bolj za osamitev neke grožnje ter blokiranje dostopa do nje s strani denimo osnovnega operacijskega sistem ter drugih komponent, za samo posodabljanje oz. odpravo anomalije oz. nadaljevanje neke misije oz. naloge brez te dotične komponente. Dodatna prednosti, ki jo prinaša sistem *Hypervisor*, je ta, da ima svoj način šifriranja programske opreme, kar nudi višjo stopnjo zaščite pred kibernetičnimi napadi (Lynx Software Technologies Inc 2016).

5.1 Študije primerov kibernetičnih napadov ter izvedenih protiukrepov

V nadaljevanju sledijo študije primerov izvedenih kibernetičnih napadov na avtomatizirane zračne (bojne) sisteme ter morebitnih protiukrepov, pri čemer napadi ne bodo omejeni glede na državo ali napadalca, prav tako pa ne bodo omejeni glede na čas izvedbe (preventivni, v času napada, po napadu).

5.1.1 Kibernetični napad – Irak

Eden izmed primerov izvedenih kibernetičnih napadov predstavlja kibernetični napad leta 2008, ko je v Iraku prišlo do vdora v modele ameriških avtomatiziranih zračnih (bojnih) sistemov z oznako Predator. Pri napadu ni šlo za prevzem nadzora nad samim oborožitvenim sistemom, temveč za vdor v prenos videa med samim oborožitvenim sistemom ter satelitom, kar je napadalcem omogočalo spremljanje video prenosa v realnem času skozi »oči« samega oborožitvenega sistema (Mount in Quijano 2009). Podrobnosti napada razkrivajo, da naj bi posredovanje podatkov več udeležencem oteževalo samo povezavo med oborožitvenim sistemom ter drugimi udeleženci, zaradi česar je bila višja stopnja zaščite pri večini tovrstnih prenosov video vsebin odstranjena. Le-to je posledično povečalo možnost kibernetičnih vdorov, saj je olajšalo delo napadalcem (prav tam).

Ob tem je na zanimiv način predstavljen tudi način odkritja samega kibernetičnega napada. Ameriške sile naj bi leta 2008 po napadu prijele pripadnika Šiitov v Iraku ter pri tem pridobile njegov prenosni računalnik, na katerem naj bi se nahajali video prenosi iz avtomatiziranega zračnega (bojnega) sistema. Le-to pomeni, da v času kibernetičnega napada ameriške sile niso zaznale samega vdora in ni bilo izvedenih nobenih protiukrepov, kar samo odkritje kibernetičnega napada prikazuje kot golo naključje. Po kasnejših analizah samega kibernetičnega napada so ugotovili, da je bil za prestrezanje video signala uporabljen program SkyGrabber. Gre za program, ki dejansko ni namenjen prestrezanju video vsebin avtomatiziranih zračnih (bojnih) sistemov, temveč prestrezanju video vsebine, ki so namenjene splošni javnosti (Gorman in drugi 2009).

Kar zadeva same protiukrepe, je le-te na danem primeru težko definirati. Tako se tekom samega napada uporabniki oborožitvenega sistema niso zavedali, da je dejansko prišlo do vdora in zato ni bilo nikakršnih protiukrepov. Kot sam protiukrep je moč navesti kodiranje video signalov, katerih primarno pomanjkanje je omogočilo oz. najmanj olajšalo sam kibernetični napad. Pomanjkanje kodiranja je bilo utemeljeno kot sicer varnostni ukrep, ki bi otežil prenos video vsebin med oborožitvenim sistemom ter preostalimi akterji, prav tako pa bi zaradi nujnih dodatnih nadgradenj samih operativnih sistemov tovrstnih oborožitvenih sistemov le-to pomenilo finančne stroške (Gorman in drugi 2009).

5.1.2 Kibernetični napad – Izrael

Pri kibernetičnem napadu sta britanska in ameriška obveščevalna služba leta 2009 domnevno vdrli v avtomatizirani zračni (bojni) sistem, in sicer z namenom spremljanja trenutnega dogajanja iz perspektive tega oborožitvenega sistema. Razlogi za tovrstno delovanje (sicer zaveznic) naj bi bili predvsem izvidništvo za morebitne napade na Iran in hkrati spremljanje razvoja avtomatiziranih zračnih (bojnih) sistemov Izraela (Currier in Moltke 2016).

Tako naj bi ameriške in britanske sile s Cipra s pomočjo tajne programske kode Anarhist vdrle v izraelski avtomatizirani zračni bojni sistem ter pridobile tako načrt poleta kot tudi posnetke s kamere, hkrati pa naj bi bile sposobne spremljati dogajanje iz samega oborožitvenega sistema. Tako naj bi bil predmet interesa tudi posnetek samega avtomatiziranega zračnega bojnega sistema, ki je v letu 2008 prvič prikazoval oborožen model izraelskega avtomatiziranega zračnega bojnega sistema (prav tam).

Ob tem je dogajanje, ki ga je zajela video oprema dotičnega sistema, vsebovalo dogajanje v Gazi, višavju Golan, na Palestinskem ozemlju ter mejah Izraela z Libanonom in Sirijo. Kvaliteta video posnetkov je, zaradi kodiranih signalov med samim oborožitvenim sistemom ter njegovo kopensko nadzorno postajo, slaba, saj je sama slika večkrat popačena (prav tam).

Kar zadeva sam vidik izvedenih protiukrepov ob kibernetičnem napadu je predhodno nastavljen varnostni sistem bil le delno uspešen, saj je kljub kodiranemu signalu prišlo do vdora v sistem. Ker pa je kvaliteta odvzete vsebine slaba, lahko napadalcu služi le v omejenem obsegu.

Prav tako se ob tem napadu poraja še druga plat zgodbe. Mesec dni po objavljeni novici, da ZDA in Velika Britanija že leta spremljata dogajanje s pomočjo vdiranja v avtomatizirane zračne bojne sisteme Izraela, je neki neimenovani izraelski uradnik le-to zanikal ter dejal, da gre za določeno količino informacij, ki so bile že podane v javnost (Times of Israel 2016).

5.1.3 Kibernetični napad – Nemčija

Nemčija določen del operacij s pomočjo avtomatiziranih zračnih bojnih sistemov izvaja tudi v Afganistanu. Tako je leta 2010 in 2013 že prišlo do nesreč s tovrstnimi oborožitvenimi sistemi. Leta 2010 se je tovrstni oborožitveni sistem modela Heron proizvajalca Israel Aerospace Industries zaletel v tovorno letalo tipa C-160, leta 2013 pa je strmoglavil v gorah v Afganistanu (Cenciotti 2013).

Za to magistrsko delo je pomembna predvsem druga nesreča, tj. strmoglavljenje v afganistanskih gorah, kjer za pripetljaj naj ne bi bila nujno kriva okvara. Podatki so skopi, saj se kibernetični napad omenja zgolj kot eno izmed možnosti. Ena izmed možnih teorij je, da je prišlo do vdora v navigacijsko povezavo oz. navigacijski sistem na samem avtomatiziranem zračnem bojnem sistemu modela Heron. Vdor naj bi izpeljali Talibani, dotični oborožitveni sistem pa naj bi namerno strmoglavili v gorah. Po navedbah naj bi za to dejanje potrebno znanje in oprema prihajala iz Irana. Samo teorijo v določeni meri podpira tudi dejstvo, da so izraelske zračne sile po odkritju nesreče s pomočjo enega od svojih lovskih letal sam oborožitveni sistem uničile (prav tam).

5.1.4 Kibernetični napad (vaja) – ZDA

Pri tem primeru kibernetičnega napada gre pravzaprav za vajo oz. prikaz situacije v trenutku, ko pride do kibernetičnega napada na nek avtomatizirani zračni bojni sistem. Tako so raziskovalci Univerze v Teksasu leta 2012 na varovanem območju s pomočjo prevare navigacijske komponente ter posredovanja napačnih navigacijskih informacij (*GPS spoofing*) vdrli v oborožitveni sistem ter prikazali ranljivost samega sistema (BBC 2012).

Kot že predhodno omenjeno je eden izmed najbolj učinkovitih načinov kibernetičnega napada napad na navigacijsko napravo. Predhodno analizirani napadi so prav tako pokazali posledice oz. rezultate napada, v kolikor ima oborožitveni sistem kodirane povezave z drugimi akterji ali ne.

Pri tem kibernetičnem napadu so raziskovalci napadli avtomatiziran zračni sistem, ki ni imel kodiranih povezav, kar po navedbah velja za večino civilnih uporabnikov avtomatiziranih zračnih sistemov. Raziskovalci so tako ocenili, da bi vsakdo z zadostnim tehničnim znanjem in pravo opremo, ki jo je moč kupiti s približno 1000 euri, bil sposoben vdreti v nezaščiten avtomatizirani zračni sistem. Sam način napada avtomatizirani zračni (bojni) sistem zmede do te mere, da sistem ne ve več točno, kje se nahaja, kar bi ob pravilnem rokovanju napadalca lahko rezultiralo v strmoglavljenju, namernem strmoglavljenju v določeno tarčo ali kraji samega sistema (BBC 2012).

Ob tem se raziskovalci soočajo s še večjim problemom. Na podlagi izsledkov izvedenega kibernetičnega napada na civilni avtomatizirani zračni sistem domnevajo, da dotičnemu visoko izobraženemu posamezniku prav tako ne bi predstavljalo ovir niti vojaško kodiranje, kar bi zopet lahko rezultiralo v predhodno navedenih posledicah. Ob tem je potrebno dodati, da bi v primeru oborožitve lahko le-ta bila končno usmerjena proti svojemu primarnemu upravljalcu (prav tam).

5.1.5 Kibernetični napad – ZDA (Iran)

Analizirani kibernetični napad po mojem mnenju predstavlja šolski primer osnovnega kibernetičnega napada na avtomatizirane zračne bojne sisteme. Slednje je v grobem najlažje pojasniti glede na potek dejanskega kibernetičnega napada. Gre za to, da ena država upravlja svoj avtomatizirani zračni bojni sistem na ozemlju druge države. Druga država nato ob detekciji s kibernetičnim napadom vdre v avtomatizirani zračni bojni sistem, zmanipulira podatke navigacijske naprave, s čimer doseže, da avtomatizirani zračni bojni sistem pristane na njihovem ozemlju, kjer ga vzamejo pod drobnogled.

Tako je Iran leta 2011 s kibernetičnim napadom prevzel nadzor nad modelom avtomatiziranega zračnega bojnega sistema ZDA. Sam model je bil model podjetja Lockheed Martin z oznako RQ-170 Sentinel, ki se uporablja za obveščevalne dejavnosti, nadzorovanje in izvidništvo (Lockheed Martin 2016).

Avtomatizirani zračni bojni sistem Lockheed Martin RQ-170 Sentinel je bil napaden na območju meje med Iranom in Afganistanom, kjer je opravljal omenjene naloge. Sam oborožitveni sistem je kljub kibernetičnemu napadu utrpel manjšo škodo, kar je Iranu omogočilo analiziranje samega modela (Infosec resources 2016).

Kako je torej sam napad bil izveden? Po navedbah so iranski strokovnjaki za kibernetiko uporabili druge avtomatizirane zračne sisteme, s pomočjo katerih so identificirali frekvenco, preko katere je model Lockheed Martin RQ-170 Sentinel komuniciral s satelitom. S tem podatkom so nato pripravili sam napad, pri katerem so sprva blokirali povezavo s satelitom (*GPS signal jamming*), s čimer so avtomatizirani zračni bojni sistem prisilili, da je zagnal sistem avtopilota. Nato so s posredovanjem lažnih podatkov o lokaciji (*GPS spoofing*) poskrbeli, da je sam oborožitveni sistem pristal drugje (natančneje v Iranu), namesto da bi se vrnil na točko vzleta. Z manipulacijo podatkov o trenutnem položaju je avtomatizirani zračni bojni sistem deloval tako, kot da je v bližini svoje točke vzleta, zaradi česar je pričel s postopkom pristajanja (Peterson 2011).

Kar zadeva same protiukrepe ob tem napadu je bilo predhodno sicer opravljeno kodiranje povezave med samim avtomatiziranim zračnim bojnim sistemom ter drugimi akterji, s katerimi je v stiku, a je bil ukrep nezadosten, saj je kljub temu prišlo do vdora in prevzema nadzora. Prav tako je potrebno omeniti funkcijo avtopilota, ki sicer v primerih mehanskih okvar deluje kot varnostni ukrep, ob tem napadu pa se je pokazalo, da hkrati predstavlja tudi veliko varnostno tveganje. Sam način oz. funkcija avtopilota je omogočila zajetje samega avtomatiziranega zračnega bojnega sistem v zelo dobrem stanju, medtem ko bi v nasprotnem primeru prišlo do strmoglavljenja, kar bi v določeni meri onemogočilo analizo samega oborožitvenega sistema s strani sovražnika.

5.1.6 Kibernetični napad – Avstralija

Kibernetični napad v Avstraliji leta 2014 (z izjemo vaje v ZDA) predstavlja med analiziranimi kibernetičnimi napadi na avtomatizirane zračne (bojne) sisteme prvega, ki ni usmerjen proti tovrstnim sistemom, ki jih uporablja vojska. Med analiziranimi primeri gre za prvi kibernetični napad na avtomatizirani zračni sistem, ki se ga uporablja v civilne oz. v tem primeru za komercialne namene.

Kratek oris samega dogajanja incident umešča na športni dogodek (triatlon) v Avstraliji, kjer je dotični in kasneje napadeni avtomatizirani zračni sistem bil uporabljen kot snemalna naprava, in sicer ga je uporabljalo podjetje New Era Photography and Film. Po navedbah naj bi upravljalec letel na oddaljenosti desetih metrov od občinstva in tekmovalcev, ko je nenadoma izgubil nadzor nad avtomatiziranim zračnim sistemom, le-ta pa je strmoglavil in pri tem lažje poškodoval eno izmed tekmovalk (ABC 2016).

Podatki o sami metodologiji napada so sicer skopi, natančnejšega odgovora, kako je prišlo do samega strmoglavljenja ni, vendar pa se ob tem porajajo določene špekulacije, da bi lahko nekdo iz občinstva začasno vdrl v povezavo med avtomatiziranim zračnim sistemom ter

njegovim upravljavcem, kar bi rezultiralo v izgubi nadzora in strmoglavljenju sistema. Ob tem se prav tako (kar zadeva metodologijo) omenja, da bi bilo tak napad mogoče lansirati s pomočjo pametnih telefonov (BBC 2014).

Pri napadu protiukrepov ni bilo, saj se je ob izvedbi napada le-to rezultiralo v neposredni izgubi nadzora ter strmoglavljenju (prav tam). Glede na predhodno analizirane primere kibernetičnih napadov bi bil tudi pri tem napadu ustrezen protiukrep samo kodiranje povezav. Verjetnost, da je tovrstni ukrep bil uporabljen, je majhna – zlasti, ker tudi v nekaterih primerih kibernetičnih napadov na vojaške avtomatizirane zračne bojne sisteme ukrepov ni bilo, saj gre za komercialno uporabo avtomatiziranih zračnih sistemov.

5.1.7 Kibernetični napad – ZDA

V naslednjem »primeru« kibernetičnih napadov gre pravzaprav za skupek dogajanja na južni meji ZDA leta 2015, pri uporabi avtomatiziranih zračnih (bojnih) sistemov za nadzorovanje meje. Ker obstoječa struktura ne uspe pokrivati celotnega območja prehoda meje, za to uporablja avtomatizirane zračne sisteme, a so na drugi strani prekupčevalci z drogami odkrili način, kako izničiti nasprotnikovo prednost (Thompson 2015).

Tako prekupčevalci z drogami manipulirajo z navigacijsko napravo nekega avtomatiziranega zračnega sistema, pri čemer gre tako za blokiranje samega signala oz. povezave s satelitom (*GPS jamming*) kot tudi manipuliranje s samimi podatki o navigaciji (*GSP spoofing*), kar avtomatiziranemu zračnemu sistemu popači sliko o tem, kje se trenutno nahaja in ga v določenih primerih usmeri na drugo lokacijo. Posledično le-to ustvari vrzel na mejnem območju, ki v danem trenutku ni nadzorovan, kar predstavlja priložnost za vse, ki zaradi kakršnihkoli razlogov želijo nelegalno prečkati mejo (Tucker 2015).

Na tej točki je potrebno analizirati same protiukrepe, katerih pri avtomatiziranih zračnih sistemih, ki se uporabljajo za nadzorovanje meje, praktično ni. Raven zaščite je praktično

neobstoječa, saj povezave med samimi sistemi ter sateliti oz. splošno gledano vsemi preostalimi akterji niso kodirane.

Razlog? Razlaga, ki jo je moč zaslediti, je po navedbah ta, da bi za kodiranje kakršnihkoli povezav bilo potrebno namestiti poseben modul, ki pa je domnevno precej težak in bi okrnil delovanje samega avtomatiziranega zračnega sistema, zlasti kar zadeva samo vzdržljivost sistema. Prav tako je eden izmed ključnih razlogov, da tovrstni sistemi niso zaščiteni, tudi ta, da bi dodajanje komponente oz. modula za kodiranje povezav dvignilo ceno samega modela (Tucker 2015).

5.2 Primerjalna analiza študij primerov

Primerjalna analiza študij primerov bo v nadaljevanju izpostavila splošne šibke točke avtomatiziranih zračnih sistemov, podobnosti med napadi oz. skupne imenovalce ter razkrila izstopajoče karakteristike analiziranih primerov kibernetičnih napadov. V grobem lahko glede na lastnosti kibernetičnih napadov analizirane primere razdelimo v tri skupine.

Prvo skupino predstavljata kibernetični napad v Iraku leta 2008 ter kibernetični napad v Izraelu leta 2009. Kibernetični napad leta 2008 je bil izveden z namenom pridobivanja podatkov, kar velja tudi za kibernetični napad v Izraelu leta 2009, s to razliko, da je pri slednjem nekoliko več podatkov o sami izvedbi (spremljanje trenutnega dogajanja iz perspektive avtomatiziranega zračnega sistema). Kar zadeva same protiukrepe v času obeh kibernetičnih napadov se nobena od »žrtev« ni zavedala, da je prišlo do vdora. Ob tem je potrebno dodati, da so bile povezave med avtomatiziranim zračnim sistemom kodirane.

Drugo skupino predstavljata kibernetični napad na nemški avtomatizirani zračni sistem leta 2013 v Afganistanu ter kibernetični napad v Avstraliji, leta 2014. Pri obeh kibernetičnih napadih je bil cilj strmoglavljenje avtomatiziranega zračnega sistema in ne kakršenkoli odvzem podatkov. Kar zadeva same protiukrepe le-teh v času kibernetičnega napada ni bilo.

Tretjo skupino predstavljajo kibernetični napad (vaja) leta 2012 v ZDA, kibernetični napad v Iranu leta 2011 ter kibernetični napad v ZDA leta 2015. Vsem trem je skupno, da je šlo za vdor v navigacijsko komponento avtomatiziranega zračnega sistema z namenom prevzema nadzora. Vsi napadi so bili uspešni, kar zadeva same protiukrepe pa je bilo kodiranje povezav zgolj pri kibernetičnem napadu v Iranu (leta 2011), a je bilo neuspešno.

Glede na analizirane kibernetične napade šibke točke pri avtomatiziranih zračnih sistemih predstavljajo navigacijska komponenta posameznega sistema ter povezave med sistemom in bodisi satelitom bodisi kopensko nadzorno postajo. Iz analiz kibernetičnih napadov lahko sklepamo, da so bili le-ti v grobem usmerjeni na: povezavo med avtomatiziranim zračnim sistemom in kopensko nadzorno povezavo z namenom odtujitve podatkov, navigacijsko komponento z namenom prevzema nadzora ali na povezavo s satelitom in/ali povezavo s kopensko nadzorno postajo z namenom strmoglavljenja samega avtomatiziranega zračnega sistema. Ob tem je potrebno izpostaviti, da tudi v primeru protiukrepov (pri čemer kodiranje povezav predstavlja praktično *unikum*) le-ti niso zadostni.

6 Sklep

Analiza avtomatiziranih zračnih bojnih sistemov – neglede na sam tip – dokazuje, da tovrstni oborožitveni sistemi v številnih pogledih predstavljajo prihodnost vojskovanja. Prednosti obsegajo predvsem zaščito človeškega življenja, hkrati pa zaenkrat delna avtonomnost zmanjšuje možnosti napak. Tako je sama analiza prikazala številne možnosti uporabe. Le-te obsegajo širok spekter, ki zajema od uporabe destruktivne moči, do zbiranja in analiziranja informacij ob izvajanju obveščevalnih dejavnosti, nadzorovanju, opazovanju ipd. Prav tako je analiza prikazala še en zelo pomemben spekter uporabe tovrstnih sistemov, in sicer je ena izmed posebnosti avtomatiziranega zračnega bojnega sistema tipa *fare nad ogret*, ameriškega podjetja Northrop Grumman z oznako Chukar III, tudi uporaba za namene urjenja vojaških sil (Northrop Grumman 2016č).

Opravljena analiza ter kasneje primerjava med izbranimi modeli je pokazala na številna razlikovanja med posameznimi modeli posameznih proizvajalcev. Tako je denimo primerjava med modeli pokazala, da enoznačnih kriterijev za produkcijo nekega avtomatiziranega zračnega bojnega sistema ni. Razlikovanja med posameznimi modeli, denimo znotraj ene same skupine oz. tipa tovrstnih oborožitvenih sistemov, so se pojavljala pri tipu oborožitve, zmogljivostih pogonskih agregatov, dodatnih komponentah ter seveda pri posebnostih določenega modela. Primerjava med skupinama oz. tipoma avtomatiziranih zračnih bojnih sistemov je pokazala, da specifičnih omejitev pri višini, vzdržljivosti, oborožitvi itd. za posamezno skupino ni, saj je prihajalo do križanja zmogljivosti ene in druge skupine, kar pomeni, da je zasnova nekega avtomatiziranega zračnega bojnega sistema v celoti prepuščena proizvajalcu.

Zaradi izbranih modelov, ki so vsak zase prihajali iz svoje države, je sama analiza do določene točke tudi pokazatelj stopnje razvitosti tehnologije avtomatiziranih zračnih bojnih sistemov v posamezni državi. Tako je denimo analiza samostojnih avtomatiziranih zračnih bojnih sistemov pokazala, da pri tovrstnih sistemih prednjačijo ZDA, sledi ji Kitajska in nato Rusija, pri kateri je večina tehnologije še v začetni fazi proizvajanja prototipov. Pokazatelj le-

tega je nakup modelov avtomatiziranih zračnih bojnih sistemov izraelskega izvora (Russia & India report 2015) ter močna proizvodnja bojnih letal kot kompenzacija za pomanjkanje tovrstne tehnologije. Analiza avtomatiziranih zračnih bojnih sistemov tipa *fire and forget* je na drugi strani pokazala manjšo fluktuacijo pri stopnji razvoja med Izraelom, Francijo ter ZDA, pri čemer je prihajalo do odklona pri vseh štirih parametrih primerjave, kar bolj kaže na široko paleto možnosti uporabe ter same opremljenosti kot pa na razliko v stopnji razvoja samih oborožitvenih sistemov.

Kar torej zadeva odgovor na raziskovalno vprašanje – kakšni podsistemi odlikujejo avtomatizirane zračne bojne sisteme – je potrebno obrazložiti, da je le-te moč razdeliti v najmanj štiri skupine, ki so v toku tega magistrskega dela hkrati predstavljali tudi parametre primerjave, in sicer: pogon, oborožitev, dodatne komponente ter specifične karakteristike posameznega modela. Ob tem je potrebno dodati, da je pri analizi avtomatiziranih zračnih bojnih sistemov tipa *fire and forget* sam podsistem in hkrati parameter primerjave, ki predstavlja pogon, bil sestavljen iz dveh delov, in sicer iz izstrelitvene komponente in pogonskega agregata, prav tako pa je pri modelu ameriškega proizvajalca Northrop Grumman z oznako Chukar III močno izstopal parameter dodatnih komponent.

Nazadnje je parameter specifičnih karakteristik posameznega modela pokazal, kako daleč seže iznajdljivost posameznega proizvajalca – neglede na to ali je prikazoval posebno zasnovo kril, pristajalni mehanizem, izstrelitveni mehanizem ali širok nabor uporabe določenega modela. Podsistem pogona določenim modelom na eni strani omogoča vzdržljivost do 24 ur, na drugi strani pa zgolj do 78 minut. Sam podsistem oborožitve se več ne nahaja nujno na zunanji strani oborožitvenega sistema, temveč je vanj integriran, hkrati pa se kot oborožitev tudi pri avtomatiziranih zračnih bojnih sistemih vseh tipov začenja uporabljati t. i. pametno strelivo.

Podsistem dodatnih komponent kaže na uporabnost tovrstnih oborožitvenih sistemov v vseh vremenskih pogojih, v vseh delih dneva ter njihovo vsestranskost, saj tudi tovrstni oborožitveni sistem tipa *fire and forget*, ki poseduje oborožitev, lahko do uničenja svoje tarče ter posledično samouničenja opravlja naloge izvidništva, nadzorovanja, obveščevalne

dejavnosti ipd. Dotične dodatne komponente modela Chukar III prav tako kažejo na razvoj dodatnih komponent, katerih namen je povečanje zaščite samega oborožitvenega sistema pred nasprotnikovimi zračnimi sistemi (Naval air systems command 2016e). Podsistem oz. same specifične karakteristike predstavljajo omejen uvid v razvoj tovrstnih oborožitvenih sistemov v bodoče, saj so v ta parameter primerjave spadali posebni načini pristajanja in posebna zasnova kril, ki je rezultirala v povišani zmogljivosti samega oborožitvenega sistema itd.

Kar zadeva odgovor na raziskovalno vprašanje, kako varni so avtomatizirani zračni bojni sistemi pred kibernetičnimi grožnjami, lahko na podlagi analize možnih kibernetičnih napadov ter samih sistemov zaščite oz. protiukrepov v primeru kibernetičnih napadov trdim, da je varnost tovrstnih oborožitvenih sistemov vprašljiva. Število kibernetičnih groženj narašča, sama analiza možnih kibernetičnih napadov ter na drugi strani sistemov zaščite oz. protiukrepov pa kaže na to, da tudi na poznane možne načine kibernetičnih napadov proizvajalci tovrstnih modelov niso pripravljeni.

Glede na študije primerov kibernetičnih napadov ter njihovo analizo je moč trditi, da kritične šibke točke predstavljajo navigacijska komponenta v samem avtomatiziranem zračnem (bojnem) sistemu, povezava med samim sistemom in satelitom ter povezava med samim sistemom in kopensko nadzorno postajo. Sama analiza izbranih kibernetičnih napadov na avtomatizirane zračne (bojne) sisteme je pokazala tudi na pomanjkanje zaščite in protiukrepov.

Tako je pri uporabi avtomatiziranih zračnih sistemov v komercialne namene moč opaziti, da je stopnja zaščite praktično nična, saj niso kodirane niti povezave z upravljalcem, kar se je izkazalo pri kibernetičnem napadu v Avstraliji leta 2014. Na drugi strani se samo kodiranje uporablja pri uporabi avtomatiziranih zračnih (bojnih) sistemov v vojaških namenih, vendar zgolj pri nekaterih modelih, pri čemer naj bi za to ključen razlog bili dodatni stroški (Infosec resources 2016). Ob tem je potrebno izpostaviti tudi dejstvo, da – razen samega kodiranja povezav – drugi protiukrepov oz. načinov zaščite praktično ni, kljub temu da so že bili predstavljeni različni drugi načini zaščite ter protiukrepov, kar je razvidno iz prejšnjega poglavja.

Tako se posledično zdi, da je na področju avtomatiziranih zračnih bojnih sistemov, neglede na tip, do napredka prihajalo zgolj zavoljo napredka, kar je moč prevesti v angleščino kot *progress for the sake of progress* (op. p.).

Glede na trenutno število poznanih možnih kibernetičnih napadov se zdi, da je sama varnost na področju tovrstnih oborožitvenih sistemov v zaostanku. Sodeč po analizi možnih kibernetičnih napadov ter trenutnih sistemov zaščite oz. protiukrepov je pri slednjih prevelik poudarek na teoretskih in simulacijskih sistemih (primere predstavljajo integrirano omrežje za kibernetično bojevanje CWIN, Drone DOME ter TAME Cyber defense suite), medtem ko bi bilo potrebnega več poudarka na samem preprečevanju vdora ter na bojevanju in protiukrepih znotraj samega sistema v času napada.

Omenjeni teoretski ter simulacijski sistemi se uporabljajo za predvidevanje kibernetičnih napadov, odkrivanje šibkih točk (kar jim daje določeno uporabno vrednost) ter za analizo in sledenje kibernetičnega napada po tem, ko se je zgodil. Ker vršilci kibernetičnih napadov za seboj redko puščajo sled oz. jih s precejšnjo lahkoto zlahka zakrijejo, bi moral primarni fokus biti na drugačnih protiukrepih oz. sistemih zaščite.

Pri tem najmanj dobro idejo predstavljata sistema *Supervisor* ter *Hypervisor*, katerih lastnosti oz. sposobnosti bi bilo po mojem mnenju potrebno združiti, medtem ko na drugi strani sistem trojnega podvajanja (*Triple-redundant avionics system architecture*) sicer predstavlja dobro idejo, a je sam sistem ranljiv, ker kljub obstoječim trem vzporednim sistemom, pri katerih dva služita kot alternativa, ki omogoča ponoven prevzem nadzora v primeru vdora, med temi operacijskimi sistemi obstajajo t. i. ključavnice. Ker je vsako ključavnico moč odpreti, ima sam sistem že *a priori* v zasnovi šibko točko. Ob tem je potrebno dodati tudi, da noben sistem ni stoodstotno varen, česar pa se zavedajo tudi podjetja na tem področju.

7 Literatura

ABC. 2016. Triathlete injured as drone filming race falls to ground. Dostopno prek: http://www.abc.net.au/news/2014-04-07/triathlete-injured-as-drone-filming-race-drops-to-ground/5371658 (26. maj 216).

Adamy, Dave. 2013. ES vs. SIGINT. *The journal of electronic defense*, 11. januar. Dostopno prek: http://indianstrategicknowledgeonline.com/web/Sigint%20vs%20ES.pdf (04. april 2016).

Airforce technology. 2015. Bird Eye 400 Unmanned aerial vehicle, Israel. Dostopno prek: http://www.airforce-technology.com/projects/birdeye400/birdeye4002.html (08. oktober 2015).

--- 2016: Harop loitering munitions UCAV system, Israel. Dostopno prek: http://www.airforce-technology.com/projects/haroploiteringmuniti/ (18. marec 2016).

Aquino, Judith. 2011. Nine jobs that humans may lose to robots. *NBCnews*, 22. marec. Dostopno prek: http://www.nbcnews.com/id/42183592/ns/business-careers/t/nine-jobs-humans-may-lose-robots/#.VzB4X4SLTIU (09. maj 2016).

Armada international. 2013. Compendium by Armada. Dostopno prek: file:///C:/Users/umetnik/Downloads/compendium%20April-May%202013a.pdf (04. april 2016).

Army Technology. 2015a. MQ-1C Gray Eagle ER/MP Unmanned aricraft system UAS, United States of America. Dostopno prek: http://www.army-technology.com/projects/mq1c-gray-eagle-uas-us-army/ (23. april 2015).

--- 2015b. Hellfire II Missile. Dostopno prek: http://www.army-technology.com/projects/hellfire-ii-missile/ (07. oktober 2015).

--- 2016. Sperwer tactical unmanned air vehicle, France. Dostopno prek: http://www.army-technology.com/projects/sperwer-uav/ (04. april 2016).

Aviations Militaires. 2015. Guizhou WZ-2000. Dostopno prek: https://www.aviationsmilitaires.net/v2/base/view/Model/1142.html (18. januar 2016).

BAE Systems. 2016. 155 BONUS. Dostopno prek: file:///C:/Users/umetnik/Downloads/bae_pdf_bonus.pdf (04. april 2016).

BBC. 2012. Researchers use spoofing to 'hack' into a flying drone, 29. junij.

BBC. 2014. Australian triathlete injured after drone crash. Dostopno prek: http://www.bbc.com/news/technology-26921504 (26. maj 2016).

Bi, Frank. 2015a. Drones are intercepting cell phone signals in L. A. *Forbes*, 23. februar. Dostopno prek: http://www.forbes.com/sites/frankbi/2015/02/23/drones-are-already-intercepting-cell-phone-signals-in-l-a/ (13. marec 2015).

--- 2015b. Two thirds of US consumers expect drone delivery within the next five years. *Forbes*, 2. marec. Dostopno prek: http://www.forbes.com/sites/frankbi/2015/03/02/two-thirds-of-u-s-consumers-expect-drone-delivery-within-the-next-five-years/ (13. marec 2015).

Boyle, Vern. 2015a. The need for speed: how america's next military advantage relies on nimbler cybersecurity. *The christian science monitor*, 17. september. Dostopno prek: http://www.csmonitor.com/World/Passcode/2015/0917/The-need-for-speed-How-America-s-next-military-advantage-relies-on-nimbler-cybersecurity (15. april 2016).

--- 2015b. Speed wins: the next strategic technology advancement for continuous US military dominance. *Northrop Grumman whitepaper*, junij. Dostopno prek: http://www.northropgrumman.com/Capabilities/Cybersecurity/Documents/Literature/Future_Cyber_eProcs_15-1425.pdf (17. april 2016).

Boyuan, Chen. 2014. GAIC reveals story of unmanned vehicle. *China.org.cn*, 14. januar. Dostopno prek: http://www.china.org.cn/china/2014-01/14/content_31180117.htm (09. november 2015).

BP p.l.c. 2016. About MoGas. Dostopno prek: http://www.bp.com/en/global/bp-air/aviation-fuel/aviation-gasoline/about-mogas.html (13. marec 2016).

Canadian american strategic review. 2008. Unattainable aerial vehicles? Sperwer, Predator and afghanistan overview – Canadian forces CU-161 UAV in Afghanistan. Dostopno prek: http://www.casr.ca/id-afghan-uavs-1.htm (05. april 2016).

Cenciotti, David. 2013. German Heron drone hacked and crashed by Taliban in Afghanistan. *The aviationist*, 13. november. Dostopno prek: https://theaviationist.com/2013/11/13/heron-hacked-afghanistan/ (25. maj 2016).

Chhabra, Esha. 2015. Drones for good: Projects from around the world on how drones can help us. *Forbes*, 27. februar. Dostopno prek: http://www.forbes.com/sites/eshachhabra/2015/02/27/drones-for-good-projects-from-around-the-world-on-how-drones-can-help-us/ (13. marec 2015).

China national aero-technology import & export corporation. 2011. TY-90 Multi-purpose missile. Dostopno prek: http://www.catic.cn/indexPortal/home/index.do?cmd=goToChannel&cid=746&columnid=1914&cpid=1653&dataid=4298&columnType=102&likeType=view&ckw=ATAM# (20. januar 2016).

Currier, Cora in Henrik Moltke. 2016. Israeli drone feeds hacked by british and american intelligence. *The Intercept*, 29. januar. Dostopno prek: https://theintercept.com/2016/01/28/israeli-drone-feeds-hacked-by-british-and-american-intelligence/ (24. maj 2016).

Delta expo. 2006. Rotary engine: advantages and disadvantages. Dostopno prek: http://www.deltaexpo.com/content/view/117/35/ (13. marec 2016).

Dictionary. com. 2016. Loiter. Dostopno prek: dictionary.reference.com/browse/loiter (04. marec 2016).

Encyclopaedia Britannica. 2016. Rocket and missile system. Dostopno prek: www.britannica.com/technology/rocket-and-missile-system (04. marec 2016).

Federal aviation administration. 1975. Radar enhancement of small aircraft in the air traffic control system. Dostopno prek: http://www.dtic.mil/dtic/tr/fulltext/u2/a016666.pdf (06. april 2016).

Fisher, D. Richard. 2011. China seeks UAV capability. *AviationWeek*, 1. julij. Dostopno prek: http://aviationweek.com/awin/china-seeks-uav-capability (18. januar 2016).

--- 2015. UPDATE: IDEX 2015: Blue Arrow 9 further expands Chinese UAV weapon options. *IHS Jane's 360*, 25. februar. Dostopno prek: http://www.janes.com/article/49455/update-idex-2015-blue-arrow-9-further-expands-chinese-uav-weapon-options (20. januar 2016).

General Atomics. 2015a. About. Dostopno prek: http://www.ga-asi.com/about/index.php (20. april 2015).

--- 2015b. Gray eagle UAS. Dostopno prek: http://www.ga-asi.com/Websites/gaasi/images/products/aircraft_systems/pdf/Gray_Eagle021915.pdf (07. oktober 2015).

Globalsecurity.org. 2016. Intelligent munition system (IMS). Dostopno prek: www.globalsecurity.org/military/systems/ground/ims.htm (05. marec 2016).

Gorman, Siobhan, Yochi J. Dreazen in August Cole. 2009. Insurgents hack U.S. drones. *The Wall Street Journal*, 17. december. Dostopno prek: http://www.wsj.com/articles/SB126102247889095011 (13. maj 2016).

Haddick, Robert. 2015. Stopping mobile missiles: Top picks for offset strategy. *Breaking defense*, 23. januar. Dostopno prek: breakingdefense.com/2015/1/stopping-mobile-missiles-top-picks-for-offset-strategy/ (05. marec 2016).

Handwerk, Brian. 2013. 5 Surprising drone uses (Besides Amazon delivery). *National Geographic*, 2. december. Dostopno prek: http://news.nationalgeographic.com/news/2013/12/131202-drone-uav-uas-amazon-octocopter-bezos-science-aircraft-unmanned-robot/ (06. maj 2016).

Hartmann, Kim in Christoph Steup. 2013. The vulnerability of UAVs to cyber attacks – an approach to the risk assessment. Prispevek objavljen na 5th International conference on cyber conflict, 4.–7. junija, v Talinu, Estonija. (30. april 2016).

Heavy fuel international. 2015. What is heavy fuel? Dostopno prek: http://www.hfeinternational.com/heavy-fuel (30. april 2016).

Hsiao, Russel. 2010. Advances in China's UCAV program. *The Jamestown foundation*, 24. september. Dostopno prek: http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=36913#.Vp-f7_nhDIU (20. januar 2016).

Hughes, Robin. 2016. Singapore airshow 2016: IAI unveils three loitering systems. *IHS Jane's defence weekly*, 18. februar. Dostopno prek: http://www.janes.com/article/58131/singapore-airshow-2016-iai-unveils-three-loitering-systems (01. april 2016).

iHLS. 2016. Rafael unveils Drone Dome: drone detection and neutralization system. Dostopno prek: http://i-hls.com/2016/04/rafael-unveils-drone-dome-drone-detection-and-neutralization-system/ (17. april 2016).

Immortal today. 2014. New MiG UCAV – Skat, the Russian deadly drone. Dostopno prek: http://immortaltoday.com/new-mig-ucav-skat-russian-deadly-drone/ (08. oktober 2015).

Infosec resources. 2016. Hacking drones...Overview of the main threats. Dostopno prek: http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/ (26. maj 2016).

Israel Aerospace Industries. 2002a. POP family. Dostopno prek: http://www.iai.co.il/2013/18688-16661-en/SystemMissileandSpace_Tamam_Electro-Opti cal.aspx (01. april 2016).

--- 2002b. POP-200. Dostopno prek: http://www.iai.co.il/Sip_Storage//FILES/6/35596.pdf (01. april 2016).

--- 2002c. Scout. Dostopno prek: http://www.iai.co.il/2013/36718-15801-en/BusinessAreas_UnmannedAirSystems.aspx (04. maj 2016).

--- 2013a. Harpy NG. Dostopno prek: www.iai.co.il/2013/36694-16153-en/Business_Areas_Land.aspx (05. marec 2016).

--- 2013b. TAME Cyber defense suite. Dostopno prek: http://www.iai.co.il/2013/36388-45022-EN/Groups_SystemMissileandSpace_MLM_Produ cts.aspx (17. april 2016).

--- 2015a. Searcher Mk III. Dostopno prek: http://www.iai.co.il/2013/36718-15742-en/BusinessAreas_UnmannedAirSystems.aspx (04. november 2015).

--- 2015b. Bird eye 400. Dostopno prek: http://www.iai.co.il/2013/36720-34720-en/BusinessAreas_UnmannedAirSystems.aspx (04. november 2015).

Israeli Air Force. 2016. Delilah's secrets. Dostopno prek: www.iaf.org.il/5642-35312-en/IAF.aspx (04. marec 2016).

Ivchenko Progress. 2015a. AI-25 Aircraft bypass turbofan engine. Dostopno prek: http://ivchenko-progress.com/?portfolio=ai-25&lang=en (10. januar 2016).

--- 2015b. History. Dostopno prek: http://ivchenko-progress.com/?page_id=22&lang=en (10. januar 2016).

--- 2015c. AI-25TL, AI-25TLK turbofan. Dostopno prek: http://ivchenko-progress.com/?portfolio=ai-25-tl&lang=en (13. januar 2016).

Jennings, Gareth. 2016. IAI performs flight test of Harop loitering munition for unspecified customer. *IHS Jane's defence weekly*, 7. junij. Dostopno prek: http://www.janes.com/article/52074/iai-performs-flight-tests-of-harop-loitering-munition-for-unspecified-customer (18. marec 2016).

Kim, Alan, Brandon Wampler, James Goppert in Inseok Hwang. 2012. Cyber attack vulnerabilities analysis for unmanned aerial vehicles. Prispevek objavljen na Infotech Aerospace 2012, 19.–22. junija, v Kaliforniji, Združene države Amerike. (30. april 2016).

Le Pera, E. Maurice. 2005. The reality of the single fuel concept. Dostopno prek: http://www.alu.army.mil/alog/issues/MarApr05/reality.html (30. april 2015).

Lockheed Martin. 2016. UCLASS. Dostopno prek: http://www.lockheedmartin.com/us/products/uclass.html (26. maj 2016).

Lugansk news today. 2015. Ukraine shot down 2 million worth Russian drone »Zastava« aka Israel Bird Eye 400 UAV. Dostopno prek: http://lugansk-news.com/ukraine-shot-down-2-million-worth-russian-drone-zastava-aka-israel-bird-eye-400-uav/ (08. oktober 2015).

Lynx Software Technologies Inc. 2016. Lynxsecure Separation Kernel Supervisor. Dostopno prek: http://www.lynx.com/products/secure-virtualization/lynxsecure-separation-kernel-hypervisor/ (18. april 2016).

Merrill, Jamie in Oliver Troen. 2014. Drones are filling Britain's skies: Look up now to see what is looking back down at you. *Independent*, 21. september. Dostopno prek: http://www.independent.co.uk/news/uk/home-news/drones-are-filling-the-skies-look-up-now-to-see-what-is-looking-back-down-at-you-9746459.html (09. maj 2016).

MI technologies. 2014. RF target and decoy simulator. Dostopno prek: http://www.mitechnologies.com/papers/11/RF%20Target%20and%20Decoy%20Simulator.pdf (06. april 2016).

MilitaryFactory. 2015. Guizhou WZ-2000 (WuZhen-2000 / WZ-9) Unmanned Combat Air Vehicle (UCAV). Dostopno prek: http://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=1029 (09. november 2015).

Ministrstvo za obrambo Velike Britanije– *Ministry of defence of Great Britain*. 2010. *Unmanned aircraft systems: terminology, definitions and classification*. Dostopno prek: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33713/JDN310Amendedweb1June10.pdf (27. marec 2015).

Mount, Mike in Elaine Quijano. 2009. Iraqi insurgents hacked Predator drone feeds, U.S. official indicates. *CNN*, 18. december. Dostopno prek: http://edition.cnn.com/2009/US/12/17/drone.video.hacked/ (13. maj 2016).

Moxnes, F. John, Prytz K. Anne, Froyland, Oyvind, Klokkehaug, Siri, Skriudalen, Stian, Friis, Eva, Teland A. Jan, Dorum, Cato in Gard, Odegardstuen. 2014. Experimental and numerical study of the fragmentation of expanding warhead casings by using different numerical codes and soluton techniques. *Defence technology* (10): 161–176. Dostopno prek: http://www.sciencedirect.com/science/article/pii/S2214914714000415 (18. marec 2016).

MULTIROTOR GmbH. 2016a. Agriculture. Dostopno prek: https://www.service-drone.com/en/applications/agriculture (06. maj 2016).

--- 2016b. Logistics and transport. Dostopno prek: https://www.service-drone.com/en/applications/logistics-and-transport (06. maj 2016).

--- 2016c. Technical maintenance. Dostopno prek: https://www.service-drone.com/en/applications/technical-maintenance (06. maj 2016).

NASA technical reports server. 1994. ISTAR: Intelligent system for telemtry analysis in real-time. Dostopno prek: http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19940030564.pdf (04. april 2016).

National security agency. 2009. SIGINT. Dostopno prek: https://www.nsa.gov/sigint/faqs.shtml (04. november 2015).

Naval air systems command. 2016a. BQM-74E Chukar. Dostopno prek: http://www.navair.navy.mil/index.cfm?fuseaction=home.displayPlatform&key=2EDB872D-9CF2-436C-B1AA-2B47117E2266 (05. april 2016).

--- 2016b. Thermic pot. Dostopno prek: http://www.navair.navy.mil/pma208/?fuseaction=controller.target_view&target_id=21&type=taas (06. april 2016).

--- 2016c. Mini towed decoy. Dostopno prek: http://www.navair.navy.mil/pma208/?fuseaction=controller.target_view&target_id=23&type=taas (06. april 2016).

--- 2016d. AN/DSQ-50 miss distance sensor set. Dostopno prek: http://www.navair.navy.mil/pma208/?fuseaction=controller.target_view&target_id=7&type=taas (06. april 2016).

--- 2016e. AN/ALE 44 countermeasures dispensing set. Dostopno prek: http://www.navair.navy.mil/pma208/?fuseaction=controller.target_view&target_id=25&type=taas (06. april 2016).

Northrop Grumman. 2015. AN/ZPY-1 STARLite Small Tactical Radar – Lightweight. Dostopno prek: http://www.northropgrumman.com/capabilities/starlite/Pages/default.aspx (07. oktober 2015).

--- 2016a. Global Hawk. Dostopno prek: http://www.northropgrumman.com/Capabilities/GlobalHawk/Pages/default.aspx (22. januar 2016).

--- 2016b. Battlefield airborne communications node. Dostopno prek: http://www.northropgrumman.com/Capabilities/BACN/Pages/default.aspx (01. marec 2016).

--- 2016c. Multi-platform radar technology insertion program. Dostopno prek: http://www.northropgrumman.com/Capabilities/MPRTIP/Pages/default.aspx (01. marec 2016).

--- 2016č. Chukar III aerial target. Dostopno prek: http://www.northropgrumman.com/Capabilities/ChukarIIIAerialTarget/Pages/default.aspx (05. april 2016).

--- 2016d. Targets brochure. Dostopno prek: http://www.northropgrumman.com/Capabilities/ChukarIIIAerialTarget/Documents/Targets-05.pdf (05. april 2016).

--- 2016e. Targets fact sheet. Dostopno prek: http://www.northropgrumman.com/Capabilities/ChukarIIIAerialTarget/Documents/TGTS-Fact-Sheet.pdf (05. april 2016).

--- 2016f. Cyber warfare integration network. Dostopno prek: http://www.northropgrumman.com/Capabilities/CWIN/Pages/default.aspx (15. april 2016).

Orbital ATK Inc. 2015a. Defense systems. Dostopno prek: https://www.orbitalatk.com/defense-systems/missile-products/hellfire/ (06. oktober 2015).

--- 2015b. Hellfire rocket motor. Dostopno prek: http://www.orbitalatk.com/defense-systems/missile-products/hellfire/docs/HELLFIRE%20 RM%20Fact%20Sheet%20-%20Rebranded%20032015.pdf (06. oktober 2015).

Passary, Anu. 2014. Drone invading your privacy? Now, there's a warning system for that. *Tech times*, 20. junij. Dostopno prek: http://www.techtimes.com/articles/8816/20140620/drone-invading-your-privacy-now-theres-a-warning-system-for-that.htm (09. maj 2016).

Pavlin, Barbara. 2014. Ime dneva: Marko Mesarič, Modri planet. *Delo*, 27. december. Dostopno prek: http://www.delo.si/gospodarstvo/podjetja/marko-mesaric-modri-planet.html (04. maj 2016).

Peterson, Scott. 2011. Exclusive: Iran hijacked US drone, says Iranian engineer. *The christian science monitor*, 15. december. Dostopno prek: http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video (26. maj 2016).

Phelps, Mark. 2013. Continental Motors acquires Thieler Aircraft engines. *Flyingmag*, 23. julij. Dostopno prek: http://www.flyingmag.com/news/continental-motors-acquires-thielert-aircraft-engines (30. april 2015).

Rafael advanced defense systems ltd. 2010. SPIKE ER. Dostopno prek: http://www.rafael.co.il/Marketing/332-893-en/Marketing.aspx (04. april 2016).

Raytheon. 2013. MTS. Dostopno prek: http://www.raytheon.com/media/sas/mts/ (07. oktober 2015).

Resch, Stefan, Steininger Andreas in Christoph Scherrer. 2013. Software Composability and Mixed Criticality for Triple Modular Redundant Architectures. Matthieu ROY. SAFECOMP 2013 - Workshop SASSUR (Next Generation of System Assurance Approaches for Safety-Critical Systems) of the 32nd International Conference on Computer Safety, Reliability and Security, Sep 2013, Toulouse, France.

Robinson, A. Clarence Jr. 2006. Smack'em flattens targets. *Signal*, 23. februar. Dostopno prek: www.afcea.org/content/?q=smack-em-flattens-targets (05. marec 2016).

Robonic. 2016a. Launching tactical UAS. Dostopno prek: http://www.robonic.fi/launching-tactical-uas/ (04. april 2016).

--- 2016b. Robonic kontio (MC2555LLR) pneumatic UAV launcher. Dostopno prek: http://www.robonic.fi/wp-content/uploads/2013/11/MC2555LLR_KONTIO_A4_vers 3_WEB.pdf (04. april 2016).

Rogers, Simon. 2012. Drones by country: who has all the UAVs. *The Guardian*, 3. avgust. Dostopno prek: http://www.theguardian.com/news/datablog/2012/aug/03/drone-stocks-by-country (10. marec 2015).

Russia & India report. 2015. Future belongs to air combat drones – MiG creator. Dostopno prek: http://in.rbth.com/economics/2015/04/06/future_belongs_to_air_combat_drones_-_mig_creator_42431 (07. oktober 2015).

SAGEM. 2016a. Company. Dostopno prek: http://www.sagem.com/company (03. april 2016).

--- 2016b. Sperwer system. Dostopno prek: http://www.sagem.com/land-defense/tactical-uav-systems/sperwer-system (04. april 2016).

--- 2016c. Sperwer Mk. II Tactical UAV system. Dostopno prek: http://www.sagem.com/sites/sagem/files/d1446e-sperwer_mkii.pdf (04. april 2016).

--- 2016d. Euroflir 350. Dostopno prek: http://www.sagem.com/search/global/Euroflir%2520350 (04. april 2016).

Samuel, Henry. 2014. France's La Poste develops drone to deliver parcels. *The Telegraph*, 25. december. Dostopno prek: http://www.telegraph.co.uk/news/worldnews/europe/france/11313044/Frances-La-Poste develops-drone-to-deliver-parcels.html (10. marec 2014).

Save the Royal navy. 2015. Unmanned platforms & the Royal navy – part 1 aerial systems. Dostopno prek: http://www.savetheroyalnavy.org/unmanned-platforms-the-royal-navy-part-1-aerial-systems/ (11. marec 2016).

SIPRI. 2007. Briefing paper: UAVs and UCAVs: Developments in the European union. Dostopno prek: http://www.sipri.org/research/armaments/transfers/publications/other_sipri_publ/20071000 (27. marec 2015).

Textron systems. 2015a. Spider. Dostopno prek: www.textronsystems.com/products/weapon-sensor/spider (05. marec 2016).

--- 2015b. Scorpion. Dostopno prek: www.textronsystems.com/products/weapon-sensor/scorpion (05. marec 2016).

--- 2015c. BLU-108. Dostopno prek: www.textronsystems.com/capabilities/smart-weapons/blu108 (05. marec 2016).

--- 2015d. Common smart submunition. Dostopno prek: www.textronsystems.com/products/weapon-sensor/common-smart-submunition (05. marec 2016).

The office of Operational test and evaluaton director. 2012. *Future combat systems: non line of sight launch system*. Dostopno prek: http://www.dote.osd.mil/pub/reports/FY2008/pdf/army/2008fcsnlosls.pdf (11. marec 2016).

The Times of Israel. 2016. US, UK didn't crack Israeli drone encryption officials say, 17. februar.

Thompson, Cadie. 2015. Drug traffickers are hacking US surveillance drones to get past border partol. *Tech insider*, 29. december. Dostopno prek: http://www.techinsider.io/drug-traffickers-are-hacking-us-border-drones-2015-12 (26. maj 2016).

Topham, Gwyn. 2016. Drones in four near-misses at major UK airports, air investigators reveal. *The Guardian*, 29. januar. Dostopno prek: https://www.theguardian.com/technology/2016/jan/29/drones-near-misses-major-uk-airports-heathrow-stansted#img-1 (09. maj 2016).

Tucker, Patrick. 2015. DHS: Drug traffickers are spoofing border drones. *Defense one*, 17. december. Dostopno prek: http://www.defenseone.com/technology/2015/12/DHS-Drug-Traffickers-Spoofing-Border-Drones/124613/ (26. maj 2016).

UAV Engines ltd. 2016a. Home. Dostopno prek: http://www.uavengines ltd.co.uk/ (13. 03. 2016).

UAV Engines ltd. 2016b. Products. Dostopno prek: http://www.uavengines ltd.co.uk/products/ar731-38-bhp/ (13. marec 2016).

Unmanned. 2015. Searcher Mk II – Unmanned vehicle (UAV) Specifications & Data Sheet. Dostopno prek: http://www.unmanned.co.uk/autonomous-unmanned-vehicles/uav-data.-.specifications-fact-sheets/searcher-mk-ii-unmanned-vehicle-uav-specifications-data-sheet/ (08. oktober 2015).

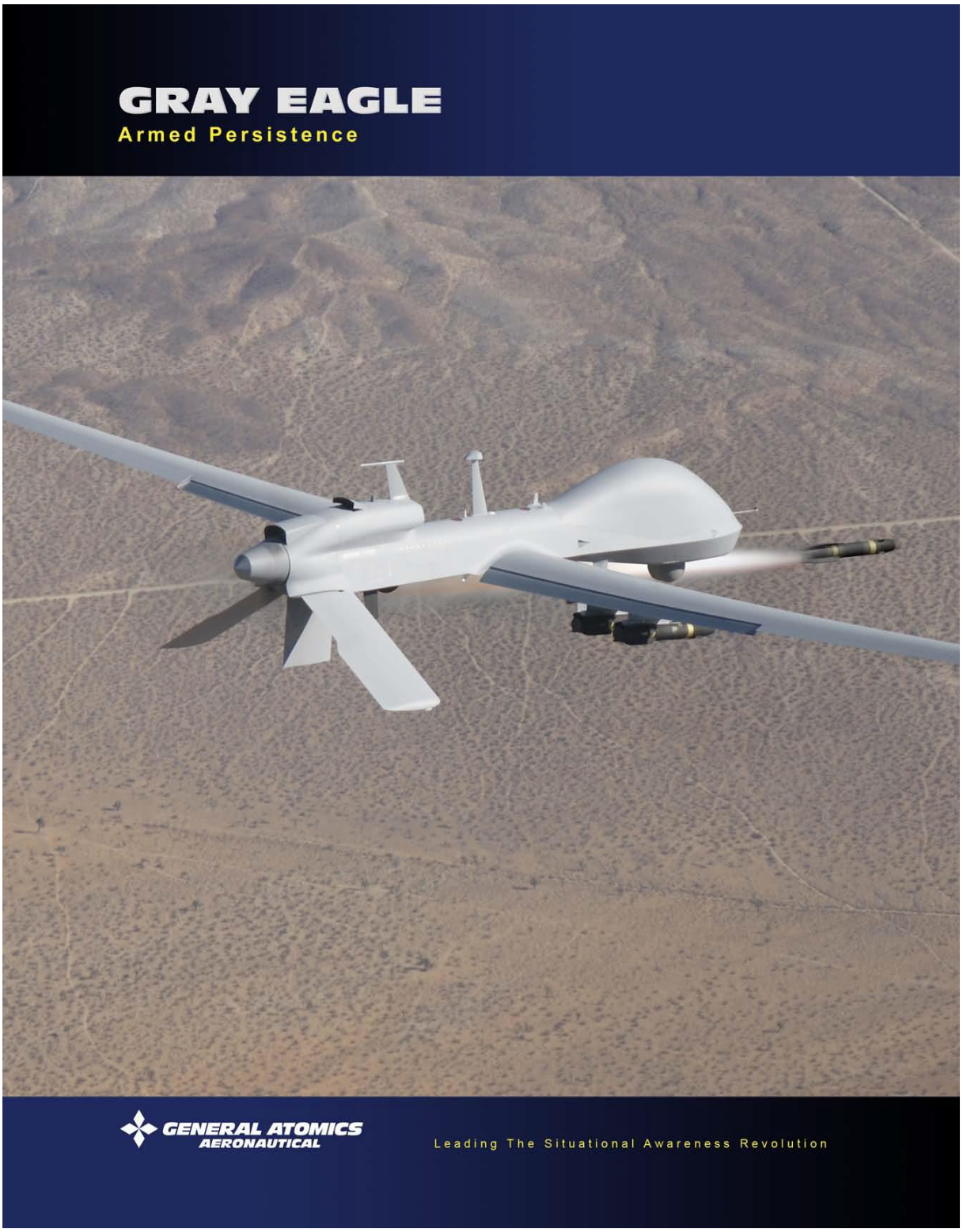
Vičič, Denis. 2015. Brezpilotni letalniki nad jedrskimi elektrarnami. *Mladina*, 21. januar. Dostopno prek: http://www.mladina.si/163630/brezpilotni-letalniki-nad-jedrskimi-elektrarnami/ (13. marec 2015).

Wallace, Anthony. 2015. UAV and the law: data collection v invasion of privacy. *Spatial source*, 17. november. Dostopno prek: http://www.spatialsource.com.au/uav-and-the-law-data-collection-v-invasion-of-privacy/ (09. maj 2016).

Zitun, Yoav. 2016. The missile that looks like a UAV. Ynet news, 17. februar. Dostopno prek: www.ynetnews.com/articles/0,7340,L-4767278,00.html (18. marec 2016).

Priloge

PRILOGA A: General Atomics MQ-1C Gray Eagle



GRAY EAGLE®

Extended Range/Multi-Purpose (ER/MP) Aircraft for U.S. Army Operations

OBJECTIVE

Provide a long-endurance, persistent Intelligence, Surveillance, Reconnaissance (ISR) and tactical strike capability.

CHARACTERISTICS

Wing Span:	56 ft (17m)
Length:	28 ft (9m)
Powerplant:	Thielert 165 HP heavy-fuel engine
Max Gross Takeoff Weight:	3,600 lb (1633 kg)
Fuel Capacity:	575 lb (261 kg)
Payload Capacity:	575 lb int. (261 kg) 500 lb ext. (227 kg)
Weapons:	4 Hellfire missiles
Payloads:	EO/IR SAR/GMTI Communications relay
Power:	9 kW (redundant)

PERFORMANCE

Max Altitude:	29,000 ft
Max Endurance:	25 hr
Max Air Speed:	167 KTAS

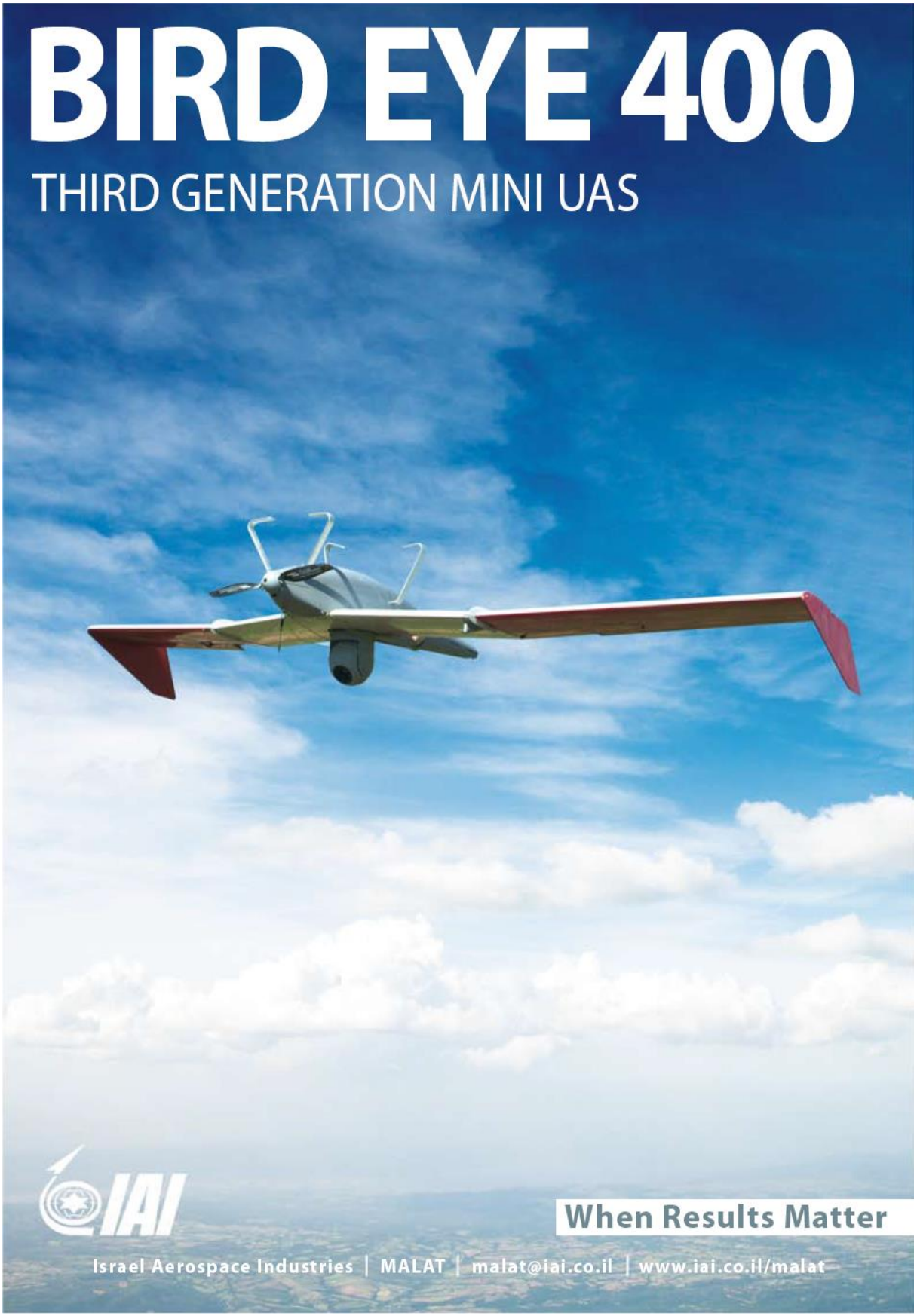
SYSTEM FEATURES

- Controllable from U.S. Army One System Ground Station or GA-ASI GCS
- Triple-redundant flight control system
- Redundant flight control surfaces
- Redundant automatic takeoff and landing
- De-ice wings and tails
- TCDL line-of-sight satellite communications
- Over-the-horizon Ku-Band SATCOM
- TCDL air data relay communications
- Over 90% system operational availability
- C-130 transportable
- Automatic takeoff and landing system

General Atomics Aeronautical Systems, Inc. • 14200 Kirkham Way, Poway, CA 92064 • (858) 312-2810 • www.ga-asi.com

R0310712

PRILOGA B: Israel Aerospace Industries Bird Eye 400



BIRD EYE 400

THIRD GENERATION MINI UAV

General

THE BIRD EYE 400 is an advanced, affordable Mini UAV System providing real-time day/night imagery data for urban operation and "over the hill" intelligence. The Bird-Eye 400 offers a high-level of operational flexibility with latest generation autonomous flight and mission capabilities.

Typical Missions

- Surveillance
- Reconnaissance
- Damage assessment
- Urban operation

Main Features

- Safe, reliable and easy operation
- Man-portable system with fast field deployment by 2 crewmen
- 'Under belly' camera for optimal coverage, stabilized picture with high-resolution imagery
- Bungee launch and optimized recovery concept
- Fully automated flight including Takeoff and Landing
- Electrical propulsion for minimal audio signature
- Low lifecycle cost

Technical data

Max. takeoff weight	5.8 kg / 12.76 lb	Operational alt	500-1500 ft AGL
Payload	Color TV/IR	Endurance	up to 90 min
Max. payload weight	1.2 kg / 2.64 lb	Mission radius	20 km / 6.25 mi
Engine	Electrical Propulsion	Max. speed	60 ktas
Wingspan	2.2 m / 7.21 ft		

Israel Aerospace Industries
MALAT Division
www.iai.co.il/malat
malat@iai.co.il

05/2014

PRILOGA C: Israel Aerospace Industries Searcher Mk. III

SEARCHER Mk III

THE MULTI MISSION TACTICAL UAS

Main Features and Capabilities

- Multiple operational configurations:
  - EO/IR Configuration
  - SAR/GMTI Configuration
  - SIGINT Configuration
- Safe, reliable and easy operation
- Aerial Data Relay (ADR) capability for Beyond Line of Sight (BLOS) operations
- proven dual Automatic Takeoff and Landing (ATOL) systems for maximal safety
- Operational in extreme weather
- Fully redundant, state-of-the-art avionics
- Integrated 4-stroke reliable engine for a minimal acoustic signature

Performance

Mission Radius	250 km
Endurance	18 hrs
Ceiling	23,000 ft
Loiter Speed	60 - 80 ktas
Max. Speed	110 ktas

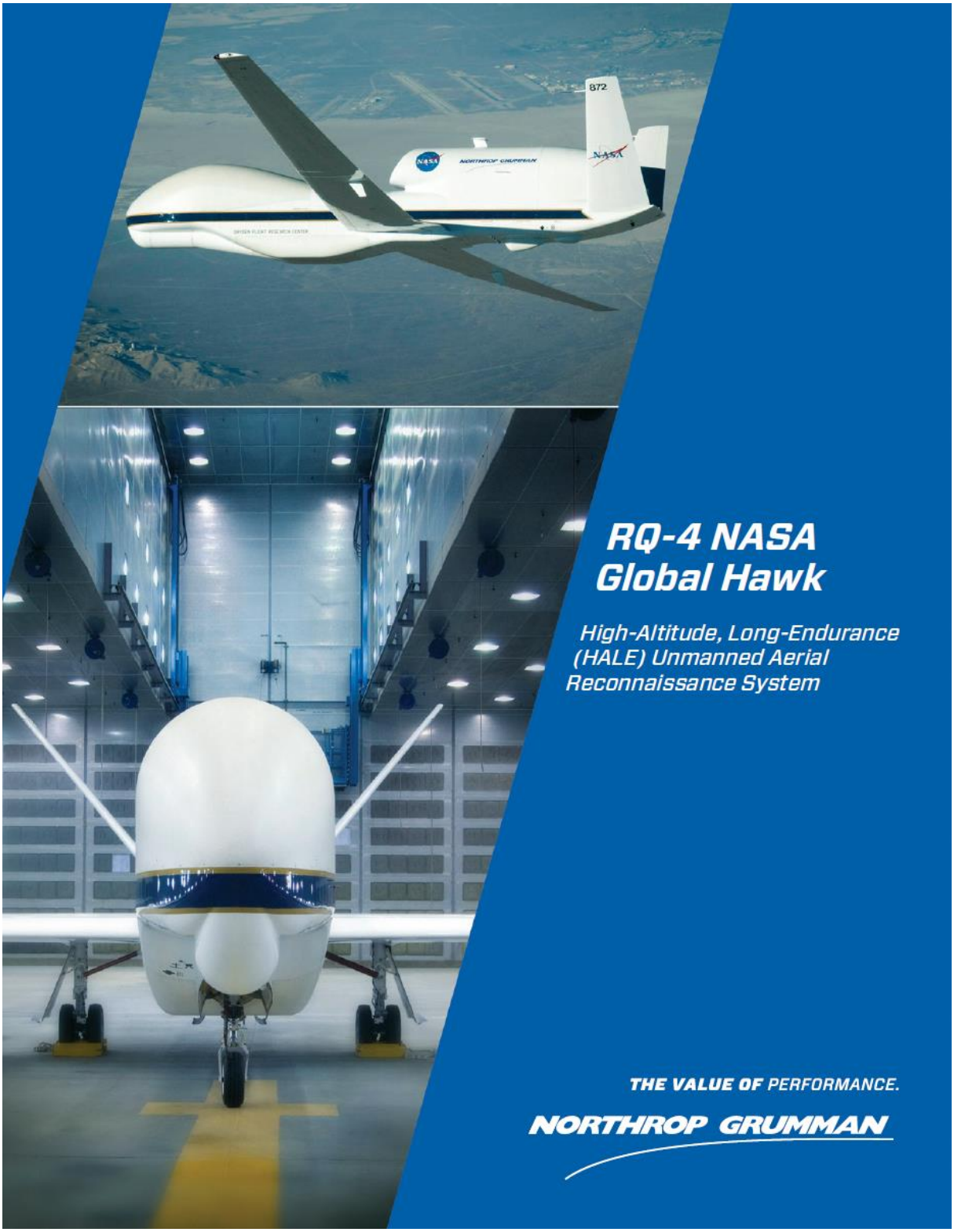
Technical Data

Max. Takeoff Weight - MTOW	450 kg
Max. Payload Weight	120 kg
Wingspan	8.55 m

IAI
Israel Aerospace Industries
MALAT Division
www.iai.co.il/malat
malat@iai.co.il

06/2014

PRILOGA D: Northrop Grumman Global Hawk



RQ-4 NASA Global Hawk

The NASA Global Hawk Project Office at the Dryden Flight Research Center (DFRC) is managing Advanced Concept Technology Demonstration (ACTD) RQ-4 Global Hawk air vehicles in partnership with Northrop Grumman Corporation. These preproduction Global Hawk air vehicles were acquired by NASA from the U.S. Air Force to be used to support NASA science customers and other customers who need access to a high-altitude, long-endurance (HALE) system. DFRC and Northrop Grumman have entered into a five-year Space Act Agreement that includes the stand-up and operation of the NASA Global Hawk system. Northrop Grumman is providing technical, engineering, maintenance, and operations support and will share access to the air vehicles with NASA.

Environmental Science Capability

In April 2010, NASA Global Hawk completed the first UAS flights for science research. These flights over the Pacific and Arctic Oceans were part of the Global Hawk Pacific (GloPac) mission, a joint project between NASA and the National Oceanic and Atmospheric Administration (NOAA), with Northrop Grumman support. In August 2010, NASA Global Hawk examined hurricanes, their formation process, and the possibility of improving hurricane forecasts.

In the Spring of 2011, NASA flew winter storm (WISPAR) missions over the Pacific and Arctic, observing among other weather phenomena, an "atmospheric river" which sometimes causes flooding on the West Coast. They also flight tested payloads for Hurricane and Severe Storm Sentinel flights planned for 2012.

In Fall 2011, Airborne Tropical Tropopause Experiment (ATTREX) flights over the Pacific studied the composition of the tropopause by climbing and descending between 65,000 feet and 45,000 feet.

The Global Hawk air vehicle provides a unique combination of high altitude and long endurance performance capabilities that can meet many demanding payload and mission requirements. The air vehicle provides the customer with an unprecedented long endurance flight capability through the troposphere into the lower regions of the stratosphere. Thus, the NASA Global Hawk is an excellent platform for hosting research instruments and sensors, and for conducting HALE airborne research.

Autonomous Aerial Refueling

Northrop Grumman is leveraging its synergistic partnership with NASA Dryden to execute the DARPA KQ-X program, which has demonstrated technologies that should enable autonomous high altitude fuel transfer between two Global Hawks, extending flight endurance. The engineering and development effort resulted in the first HALE formation flight, a dual-ship close formation with one UAV flying 30 feet from the extended refueling drogue of the other UAV. Northrop Grumman is responsible for all engineering and design/modification of both aircraft.

System Development

During the stand-up of the program, the air vehicles were modified with new command, control, and communications for worldwide access and to allow rapid configuration changes for new payloads.

Global Hawk Operations Center (GHOC) is configured to support air vehicle and payload operations independently.

www.northropgrumman.com/globalhawk

Printed in the USA
MARCOM San Diego
12-1653 • AS • 08/13 • 1020-AS-5926

Airborne science research and autonomous aerial refueling.

The Flight Operations Room, contained within the GHOC, consists of the workstations occupied by the personnel controlling various payloads. NASA has completed a portable ground control station, which can be used in support of upcoming Earth Science deployments.

Environmental Science Mission Categories

- Calibrate satellite sensors and develop or validate data algorithms
- Collect in situ measurements for Earth science process studies
- Develop and test new instruments and future satellite mission concepts

Specifications

Wingspan	116.2 ft (35.4 m)
Length	44.4 ft (13.5 m)
Height	14.6 ft (4.2 m)
Gross Take-off Weight	26,700 lbs (12,110.9 kg)
Internal Payload Capacity	1,500 lbs (680.4 kg)
Pod Payload Capacity	700 lbs per side (317.5 kg)
Ferry Range	11,000 nm (20,372 km)
Maximum Altitude	≤ 65,000 ft (19.8 km)
Loiter Velocity	343 knots True Air Speed (TAS)
Maximum Endurance	31 hrs

For more information, please contact:

Northrop Grumman Aerospace Systems
Unmanned Systems
Jessica Burtness
858-618-6931 • jessica.burtness@ngc.com

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

PRILOGA E: Israel Aerospace Industries Harop

HAROP

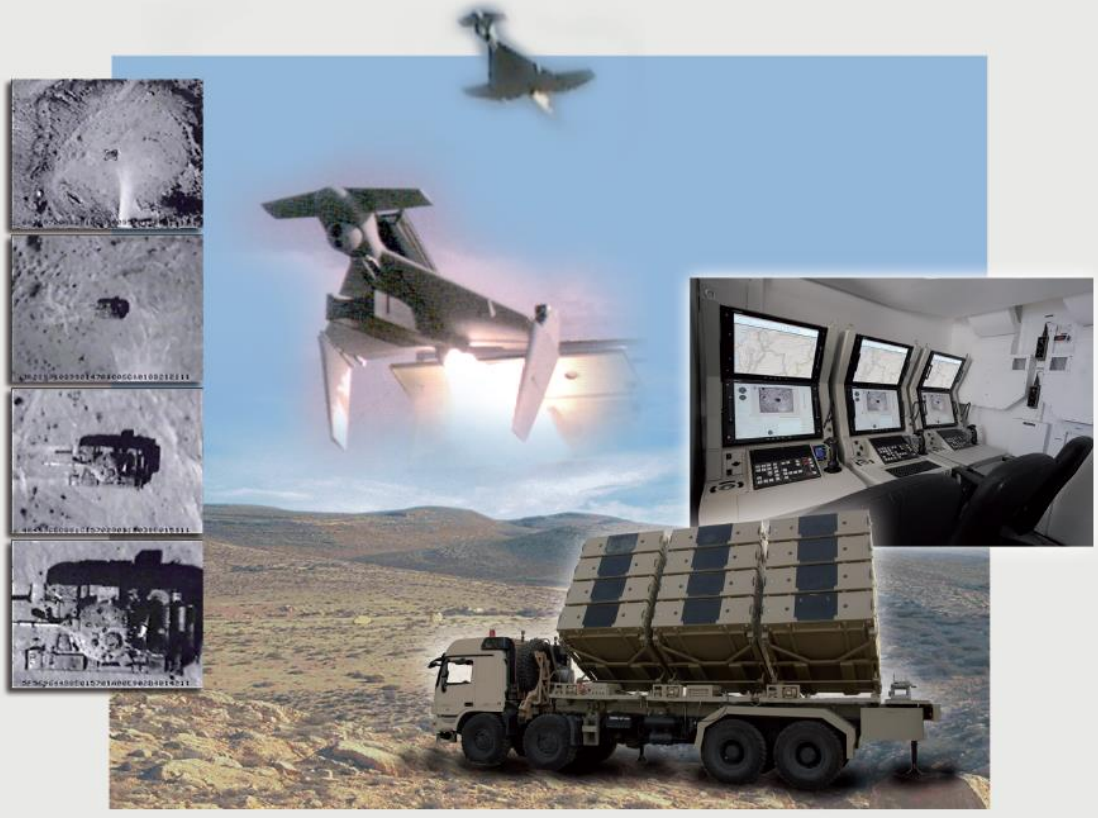
LOITERING SYSTEM WEAPON

When Results Matter

25 years of In-service Experience of Loitering Weapon Systems

Combining capabilities of a UAV and a lethal missile, HAROP searches, finds, identifies, attacks and destroys targets, and performs battle damage assessment. Independent of real-time intelligence, HAROP is uniquely capable against time-critical, high-value, relocatable targets.

- Extended loitering at long ranges
- Autonomous platform operation
- Man-in-the-loop attack, avoiding collateral damage
- EO seeker: FLIR / color CCD, hemispherical coverage
- Full hemispherical attack angle
- Attack abort capability
- Continuous, suppresson of air defense systems



IAI
Israel Aerospace Industries
Missiles Division
www.iai.co.il/mbt
mbt@iai.co.il

01/2016

PRILOGA F: Israel Aerospace Industries Harpy NG

HARPY NG

ANTI RADIATION LOITERING WEAPON SYSTEM

When Results Matter

25 years of Field Operational Experience

Combining capabilities of an UAV and a missile, HARPY NG searches, identifies, acquires, attacks and destroys enemy radar targets.
Not dependent on real-time intelligence, HARPY NG is highly effective against a wide spectrum of modern air defense systems.

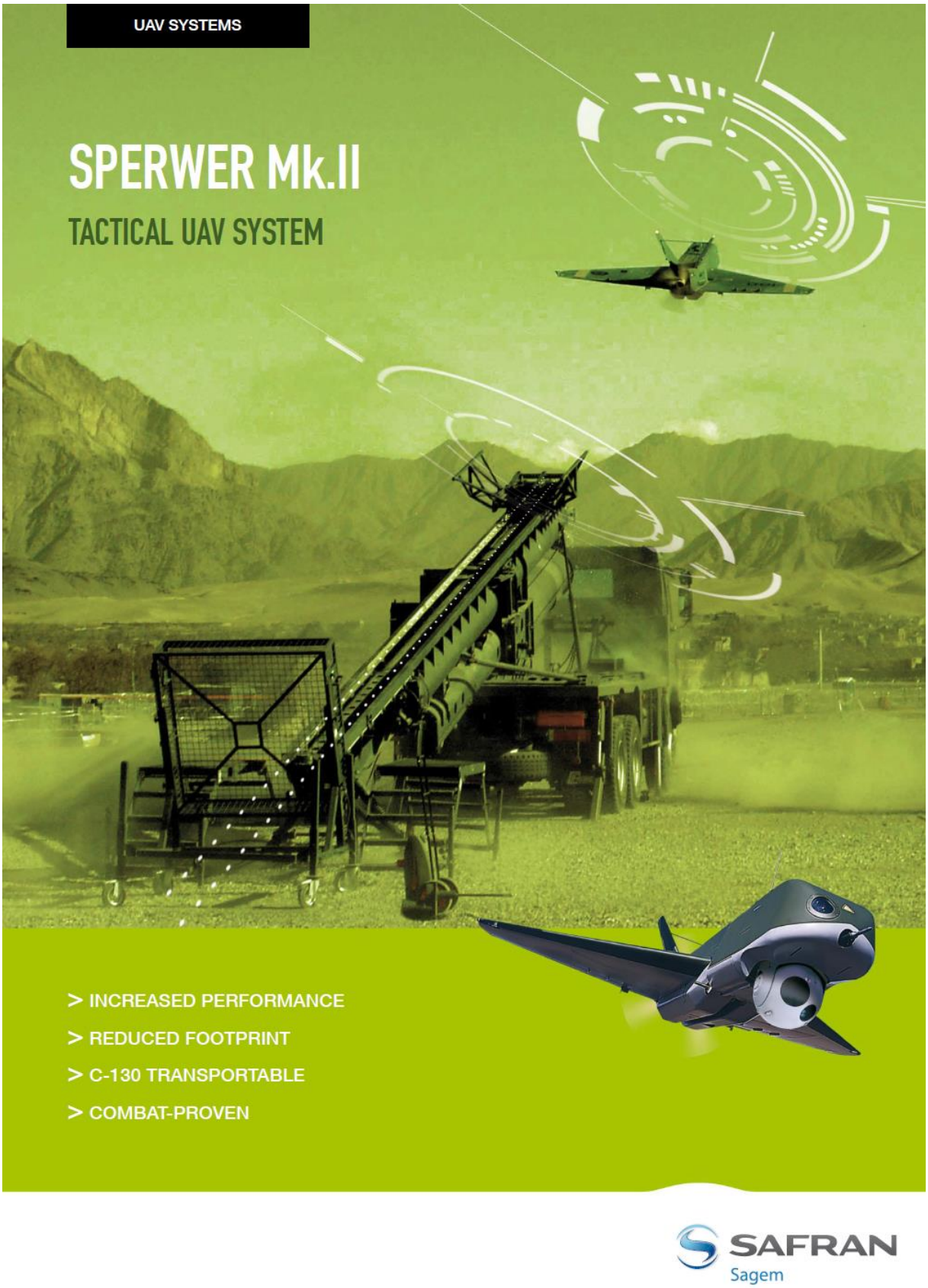
- **S**uppression / **D**estruction **E**nemy **A**ir **D**efense Missions
- Autonomous operation
- State of the art Anti-Radiation seeker with wide RF coverage
- Vertical attack capability maximizing weapon lethality
- Abort attack in case of target shut down
- Longer range and extended loitering capability
- Continuous, persistent, lethal threat to enemy air defense systems

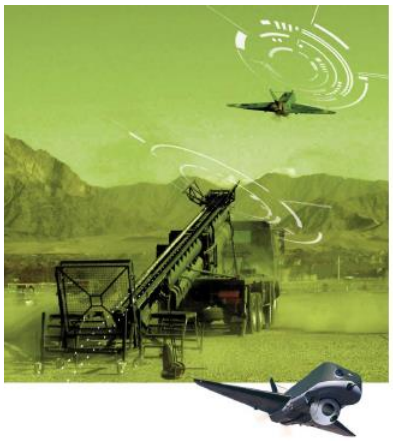
IAI

Israel Aerospace Industries
MBT Missiles Division
www.iai.co.il/mbt
mbt@iai.co.il

03/2015

PRILOGA G: SAFRAN Sagem Sperwer MK. II





SPERWER Mk.II

Tactical UAV system

Best-selling tactical UAV system in Europe, Sperwer has become a NATO reference. Drawing on Sagem's state-of-the-art technologies and on users' operational feedback, Sperwer Mk.II is a modernized version of the Sperwer system combining extended autonomy, high-performance image chain and reduced footprint. Combat-proven, it is being used daily on missions in international theaters.

Operational from unprepared areas, close to military units, Sperwer Mk.II provides highly accurate observation, threat detection and target designation to land forces as well as fire coordination for artillery.

Air transportable in C-130 type freight aircraft and mobile on light trucks, the entire modular system includes:

- a Ground Control Station (GCS) for flight control and mission analysis (including 3D mission planning, C4I connection, Geographical Information System, etc.),
- a Ground Data Terminal (GDT) housing the digital radio-link terminal,
- a catapult, allowing a quick launch near combat zones,
- air vehicles.

Sperwer Mk.II offers a high level of responsiveness and tactical situation awareness in support to ground troops. Thanks to its latest-generation Euroflir 350 optronic payload, it transmits real-time images and associated geolocation data to the GCSs or directly to dismounted soldiers on their Remote Video Terminal (Sagem RVT).

The state-of-the-art tactical UAV

Safe and airworthy design

- Fail-safe design and certified (based on JAR-VLA)
- Fully automated takeoff and landing: no runaway required
- Advanced digital avionics suite
- Digital J Band (15 GHz) data link
- Redundant back-up link in UHF
- Transponder/IFF mode 3C and VHF relay to ATC

Tactical capacity

- Reduced footprint: system integrated on light all-terrain vehicles
- C-130 transportability
- Catapult launch and parachute recovery with airbags
- Real time, day/night operations
- C4I connection and interoperability

- **> 6 hours endurance**
- **Multi-missions**
- **Multi UAV capability**
- **Real time, day & night ISTAR operations**
- **NATO interoperability**

Multi-mission capacity

- Real time ISTAR
- Targeting (1st round strike artillery accuracy)
- 2 UAVs in flight
- Handover capability between several GCSs

Multi-payload capacity

- EO/IR
- SAR
- Transmission relay
- EW (ELINT, COMINT)

RVT

- Data Link Range: - Video: 30km
  - AV telemetry: 50km
- Autonomy: 4 hours
- Transportable in a rucksack
- Cartographic display
- Image & video recording

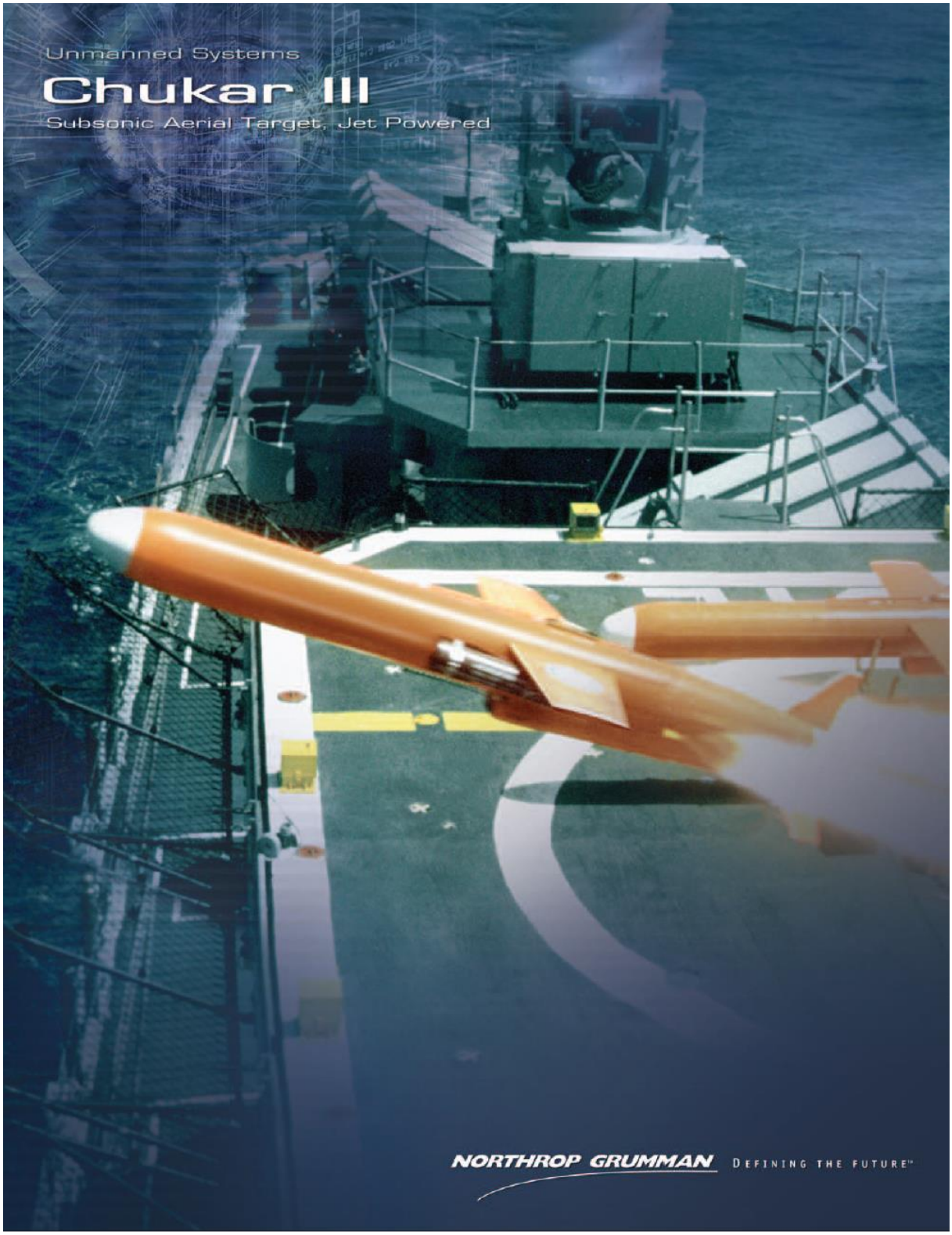
Technical specifications

- Endurance: >6 hours
- Overall length: 3.5m
- Wing span: 4.2m
- Ceiling: 15,000ft
- Speed: 90kts
- Data link range: 200km
- Payload capacity: 50kg

SAGEM
Le Ponant de Paris - 27, rue Leblanc - F-75512 PARIS CEDEX 15 - FRANCE
Phone: + 33 1 58 11 64 25 - Fax: + 33 1 58 11 68 68 - www.sagem-ds.com

SAFRAN
Sagem

PRILOGA H: Northrop Grumman Chukar III



NORTHROP GRUMMAN

DEFINING THE FUTURE™

Chukar III

Fighter Aircraft and Cruise Missile Emulation for Weapon Systems Testing, Evaluation and Training

The Chukar III is a turbojet-powered aerial target with high performance capabilities. Used by multiple customers for realistic aerial defense exercises, the target and its ground support system are highly portable. This enables the Chukar III to be operated from remote land sites or deployed for shipboard operations where maximum flexibility and rapid turnaround are required.

The primary mission of the Chukar III aerial target is to emulate enemy tactical cruise missiles or fighter/strike aircraft. It can be fitted with a variety of augmentation devices to enhance its use as a threat simulator for weapons training. Systems employed against the Chukar III include anti-aircraft guns, surface-to-air missiles, and air-to-air missiles employing active or semi-active radar homing, IR seekers, and visual guidance systems. Flying as low as fifteen feet (five meters) and at speeds up to 525 knots, the Chukar III can execute six-g maneuvers, pop-up profiles, and high-g escape, either autonomously or manually.

The Chukar III target system includes all of the elements necessary to provide a total training solution. The command and control system enables simultaneous multiple target engagements using waypoint navigation with Global Positioning System (GPS) accuracy. Target payloads include passive and active augmentation, infrared (IR) flares and plumers, chaff, scoring, and dual deployable tow bodies. Tow body payloads include active augmentation, IR flares, and scoring.

Fielded in eleven countries around the world, the Chukar III is based on the U.S. Navy's BQM-74 which has been used for over 80% of the Navy's target missions since 1978. With a high degree of operational availability and demonstrated reliability, the Chukar III provides a cost effective system solution unrivalled by other products.

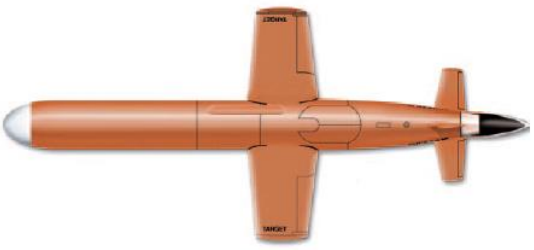
Specifications

Length	12.95 ft (4.0 m)
Wingspan	5.78 ft (1.8 m)
Range	>350 nm (648.6 km)
Altitude	
Low	15 ft (4.6 m)
High	40,000 ft (12.2 km)
Speed	>525 Knots at Sea Level
Weight	455 lbs (206.4 kg)
Endurance	78 Minutes
Navigation	GPS Way Point
Fuel	Jet Fuel (JP-4, JP-5, or JP-8)

Skeet for the Fleet
Chukar III provides the ultimate test of weapon systems and personnel performance, emulating a broad range of threats. Take your best shot.

Payloads

- Passive or Active Radar Augmentation
- Seeker Simulators
- Infrared Augmentation
- Tow Systems
- Scoring Systems
- Decoy and Chaff Dispensers



Northrop Grumman · Integrated Systems · Unmanned Systems
P.O. Box 509066 · San Diego · California 92150-9066 · www.is.northropgrumman.com
Contact: Cynthia Curiel · 858.618.4355 · E-Mail: cynthia.curiel@ngc.com
VM00-AS-4874_06.05 · Approved for Public Release · Distribution Unlimited
USN 207/04, 01/05/05 · TDEA 05504