Procjena cyber rizika na sustav upravljanja zračnim prometom

Šinjor Cvetković, Jan

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Jan Šinjor Cvetković

PROCJENA *CYBER* RIZIKA NA SUSTAV UPRAVLJANJA ZRAČNIM PROMETOM

ZAVRŠNI RAD

Zagreb, 2017.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 24. travnja 2017.

Zavod: **Zavod za zračni promet**
Predmet: **Zaštita u zračnom prometu**

ZAVRŠNI ZADATAK br. 3959

Pristupnik: **Jan Šinjor Cvetković (0135234700)**
Studij: Promet
Smjer: Zračni promet

Zadatak: **Procjena cyber rizika na sustav upravljanja zračnim prometom**

Opis zadatka:

U uvodnim postavkama potrebno je opisati predmet istraživanja, objasniti svrhu i cilj istraživanja te dati kratak pregled strukture završnog rada. Definirati cyber prijetnje i dati prikaz regulatornog okvira zaštite zračnog prometa s posebnim osvrtom na cyber zaštitu i recentna istraživanja koje se bave navedenom problematikom. Analizirati cyber rizike koji se mogu javiti u sustavu upravljanja zračnim prometom i navesti metode zaštite. Usporediti i procijeniti američki i europski model zaštite sustava za upravljanje zračnim prometom (prema FAA i EUROCONTROL-u). Procijeniti i opisati utjecaj cyber prijetnji na budućnost zaštite sustava za upravljanje zračnim prometom. Interpretirati dobivene rezultate.

Zadatak uručen pristupniku: 28. travnja 2017.

Mentor:

Arijana Modić

Arijana Modić, mag. ing. traff.

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

PROCJENA *CYBER* RIZIKA NA SUSTAV UPRAVLJANJA ZRAČNIM PROMETOM

ASSESSMENT OF CYBER RISK ON AIR TRAFFIC MANAGEMENT SYSTEM

Mentor: Arijana Modić, mag.ing.traff.

Student: Jan Šinjor Cvetković
JMBAG: 0135234700

Zagreb, rujan 2017.

SAŽETAK

Zračni promet kao najkompleksnija grana prometa zahtjeva adekvatan sustav upravljanja koji osigurava nesmetano odvijanje operacija potrebnih za odvijanje samih procesa prijevoza i usluga kojih pruža. S obzirom na globalnu povezanost i poslovanje, jedinstveno zakonodavstvo je neophodno kako bi sustav funkcionirao. Tendencija napretka prisutna je i u zrakoplvstvu što donosi razne pozitivne, ali i negativne strane. *Cyber* prijetnje, kao jedna od negativnih strana, poslate su prisutne i trenutno predstavljaju veliki problem zaštite zrakoplovstva.Kako bi se održala željena, ali i nužna razina zaštite sustava te same kvalitete za krajnjeg korisnika, potrebno je pratiti trendove i razvijati sustav sukladno tome.

KLJUČNE RIJEČI: *cyber* prijetnje, *cyber* rizici, procjena rizika, mjere zaštite, kritična infrastruktura, pravni okvir, sustav upravljanja zračnim prometom, modernizacija

SUMMARY

Air transport is the most complex type of transport which require adequate management system to enable continuous flow of operation needed for transport and services it offers itself. Considering global connectivity and management, unique legislation is necessary for system to function. Progress tendency is present in aviation too, which brings various positive and negative sides. Cyber threats, as one of the negative sides, became present and brought big problem to aviation security. In order to maintain desired and required safety level just like quality for end user as well, it is a must to follow trends and further develop the system according to those.

KEY WORDS: cyber threats, cyber risk, risk assessment, security measures, critical infrastructure, legal framework, Air traffic management, modernisation

SADRŽAJ

1. UVOD

Zračni promet je jedna od najatraktivnijih prometnih grana. Danas popularnija više nego ikad, najviše zbog dostupnosti korištenja za već broj ljudi čemu je prodonijela modernizacija i ekonomičnije poslovanje.Prema statistici je najsigurnija grana prometa, a za to je najviše zaslužan sustav upravljanja zračnim prometom.Da bi se taj status održao, potrebno je pratiti trendove i razvijati ga sukladno njima.

Cilj završnog rada je pokušati definirati *cyber* prijetnje u sustavu upravljanja zračnim prometom te predstaviti važnost uspostave adekvatnog sustava zaštite koji mora polaziti od čvrstog i konkretno propisanog zakona te kompleksne infrastrukture koja će biti u mogućnosti obraniti se od mogućih prijetnji i napada. Završni rad je podijeljen u 8 cjelina:

1. Uvod
2. *Cyber* prijetnje
3. Pravni okvir zaštitnih mjera
4. SESAR strategija upravljanja *cyber* zaštitom
5. CSFI sigurnosni program
6. Procjena rizika i *cyber* zaštite
7. Utjecaj na budućnost sigurnosti i zaštite
8. Zaključak

Prvo poglavlje je uvod u završni rad, njegov smisao i cilj.

U drugom poglavlju pokušati će se definirati *cyber* prijetnje teopćenito prikazati njihova kratka povijest.

Treće poglavlje definira glavna zakonodavna tijela te konkretne zakone na kojima se temelje mjere zaštite.

U četvrtom poglavlju opisuje se europski model zaštite od*cyber* prijetnji, dok je u petom poglavlju prikazan američki model pod nazivom CSFI sigurnosni program.

U šestom poglavlju procijenjuju ju se mogući rizici *cyber* napada te modeli zaštite od istih.

Sedmo poglavlje osvrće se na dosad razvijene modele zaštite te se procjenjuje potreban napredak s obzirom na predvidene trendove modernizacije i pojave novih rizika i prijetnji.

2.*CYBER* PRIJETNJE

Svjedoci smo izrazito brzog napretka tehnologija i modernizacije sustava koji pridonose zračnom prometu s raznih aspekata, što podrazumijeva puno efikasniji sustav koji je u mogućnosti nositi se s velikim brojem procesa i operacija potrebnih za realizaciju samog zračnog prijevoza.Unatoč svim poboljšanjima, simultano je neophodno razvijati nove modele zaštite kako bi se održala propisana razina sigurnosti.

2.1. Općenito

Cyber napadi su globalni problem, a zrakoplovstvo je podložno napadima jer ovisi o informacijskim i komunikacijskim tehnologijama. U početcima se pokazalo da je ljudska pogreška nosila velik postotak uzroka nesreća u zrakoplovstvu općenito, a dolaskom informatizacije, taj postotak se znatno smanjio.Informatika egzizstira u virtualnom tzv.*cyber space-u*.Ako se uzme u obzir anonimnost, težina u postavljanju odgovornosti, ekonomičnost, velika brzina i ograničen broj protumjera koje se mogu poduzeti, takvi napadi mogu biti katastrofalni za zrakoplovnu industriju.[1]

2.2. Povijest

Početkom 2015. godine, zračna kompanija United Airlines je prizemljila sve svoje zrakoplove nakon što su određeni piloti prijavili čudne promjene u planovima leta. Nekoliko tjedana kasnije, poljska zračna kompanija LOT - *Polskie Linie Lotnicze* je bila žrtva napada na sustav prihvata i otpreme, što je rezultiralo nemogućnošću kreiranja planova leta i odlaznih letova iz Varšave. Nešto ranije, 2013.godine tzv. etički hakeri su predstavili opremu vrijednu 2000 američkih dolara koja radi na principu stvaranja imaginarnih zrakoplova koji se pojavljuju na ekranima kontrole zračne plovidbe te na taj način stvaraju pomutnju.[2] Isto tako, pokazano je kako ostvariti pristup kokpitu zrakoplova i kontrolirati sve komande sa zemlje, koristeći jednostavnu aplikaciju i elektroničke komponente koje manje više svi posjedujemo u svojim računalima.

Žrtva takvih napada je bio i Globalni sustav pozicioniranja (GPS - Global Positioning System) za vrijeme rata u Iranu. Nakon te nesreće pojavila su se upozorenja o mogućim *cyber* otmicama zrakoplova. Todd Humphreys je demonstirao u sklopu svoje studije kako je moguće oteti zrakoplov jednostavnom GPS podvalom. Ušavši u kontrolu zrakoplova, preusmjerio ga je u poniranje te isto abortirao samo 40-ak metara iznad zemlje kako bi spriječio nesreću. Puno ranije, 2009.godine, zračna luka Newark Liberty International Airport se suočila s neobjašnjenim prekidima sustava preciznog prilaza koji je baziran na GPS-u. Savezna uprava za civilno zrakoplovstvo (FAA – Fedaral Aviation Agency) je istragom zaključila da se radilo o

[1]Deepika, J.: Cyber Security in Civil Aviation – EALA Prize, Leiden University, 2015.
[2] Ibid

jednostavnom ometaču GPS signala koji je koristio vozač kamiona, kako bi spriječio vlastitog šefa da ga prati.[3]

2.3. Definiranje problema

Mogućih točaka napada je puno uključujući početni proces proizvodnje zrakoplova koji je moguće na taj način kompriminirati i onesposobiti određenu opremu čak bez pravovremene spoznaje. Bilo da se radi o individualcima, udruženjima ili čak državama, meta može biti elektronički sustav kompanija koje su posrednik u samom dizajniranju i proizvodnji hardvera i/ili softvera korištenog u zrakoplovima, zračnim lukama te u sustavima kontrole zračne plovidbe. Kao i kod osobnih računala, sustavi u zrakoplovstvu koriste slične ako ne i iste komponente te su stoga potencijalne mete za narušavanje sigurnosti u obliku udaljenog pristupa sučelju i nezakonitog upravljanja samim sustavom. To je pogotovo povećano kod najmodernijih zrakoplova velikog dometa kao što su Boeing 787 Dreamliner i Airbus modeli A350 i A380. Napad može biti na određenu komponentu te na čitav sustav. Bez obzira na to, moguća je i samo manipulacija sustavom koja može dovesti do fizičkog napada.[4]

Ministarstvo domovinske sigurnosti SAD-a definiralo je prijetnju kao bilo koju radnju koja podrazumijeva pristup, izvlačenje, manipulaciju te poremećaj integriteta, povjerljivosti, sigurnosti i dostupnosti podataka, aplikacija ifederalnog sustava. Prijetnja može biti namjerna ili ne namjerna, s ciljem ili bez te može doći od različitih izvora uključujući strane zemlje uključene u špijunažu i ratovanje informacijama, kriminalce, hakere, stvoritelja virusa, ali i nezadovoljnih zaposlenika i izvođača radova unutar organizacije. Nenamjerne prijetnje najčešće su uzrokovane od strane nepažljivih i needuciranih zaposlenika, općenito te prilikom nadogradnje softvera, procedura održavanja opreme i trenutaka zakazivanja opreme što poremećuje rad računala i uzrokuje oštećivanje podataka. Namjerne prijetnje uključuju napade sa i bez cilja. Ciljani napad podrazumijeva grupu ili individualca koji napadaju specifično kritičnu točku infrastrukture sustava, dok neciljani napad podrazumijeva nedefiniranu željenu točku napada, kao što je virus koji se pušta s jednim ciljem, a to je zaraziti što više korisnika bez specifikacije kojeg točno. Najzabrinjavajuća prijetnja je tzv. *insider*, odnosno osoba koja posjeduje sve ovlasti te kao takva ima legitimitet i pristup sustavu i mreži. U većini slučajeva riječ je o organiziranom zločinu ili terorističkoj grupi koja zaposli takvu osobu koja je možda nezadovoljna sa svojim radim okruženjem i sl. te je spremna za određenu novčanu naknadu raditi protiv svojeg poslodavca. Naravno, prijetnja može biti i kombinacija između *cyber* i fizičkog napada kao npr. fizički upad i nametanje u infrastrukturu i modificiranje softverskog koda koji se nalazi u toj infrastrukturi. To bi se klasfificiralo kao namjerni fizički i

[3]Deepika, J.: Cyber Security in Civil Aviation – EALA Prize, Leiden University, 2015.
[4]Ibid

cyber napad. Isto tako, u slučaju da autorizirano osoblje ne slijedi procedure provjere infrastrukture dok ta infrastruktura generira i prenosi varljive podatke.[5]

2.4. Klasifikacija

Motivacija za napad se može pojaviti s raznih strana kao što je već navedeno, strane države, terorizam, kriminal te organizacije koje se bave društvenim pitanjima. Izvoditelji prijetnji mogu biti neautorizirani entiteti ili pojedinci, tzv. *insider*, s ciljem stvaranja potencijalne opasnosti i gubitka u preformansama sustava, konkretno upravljanja zračnim prometnom, koji je danas baziran na mreži podataka. Širok je raspon mogućnosti, resursa i motiva koji su im na raspolaganju. Na kraju piramide napdača možemo svrstati tradicionalne hakere koji usavršavaju svoje vještine i žele dobiti pažnju napadajući lake mete. Naravno, njihovi resursi nisu veliki, ali niti potrebni jer je njihov cilj napad na bilo koji ranjiv sustav spojen na internet kako bi napravili štetu neciljanoj meti. Rezultat takvog napada može biti zanemariv, dok s druge strane može prouzročiti veliki efekt na cjeloukupni sustav i donijeti štetu uvelike veću nego što je napadač imao u planu. Metode obrane na toj razini fokusiraju se na uspostavljanje perimetra oko infrastrukture informacijskog sustava organizacije te obrane tog perimetra upotrebom tzv. *firewalls* vatrenih zidova i sličnih komercijalnih alata za virtualnu zaštitu.[6]

U sljedeću razinu spadaju *cyber* lopovi koji pokušavaju doći do određenih informacija koje nazivamo kritičnima, sve od kreditnih kartica pa do poslovnih planova. Obrana u tom smislu podrazumijeva zaštitu informacija i sustava ne samo unutar perimetra, već kompletnu zaštitu takvih kritičnih informacija koje egzistiraju unutar sustava koristeći vrlo jednostavne tehnike enkripcije tvrdih diskova na kojima su ti podaci pohranjeni.[7]

Treća razina je *cyber* nadzor u kojoj se nastoje pratiti mogući napadači koji traže mjesto za ulazak u sustav kako bi izvršili napade visoke razine po vlastitom rasporedu. Napadači te razine posjeduju veću razinu stručnosti te su u mogućnosti pokrenuti višestruke napade ciljajući na određe organizacije ili dijelove organizacije. Posljedice za sustav upravljanja zračnim prometom (ATM – Air Traffic Management) mogu biti vrlo ozbiljne u ovoj razini napada. Sve od gubitka vlastitih informacija pa sve do potpunog kraha čitavog sustava bez obzira je li napad bio namjeran ili nenamjeran. Obrana podrazumijeva konstantno interno nadziranje i očvršćivanje sustava.[8]

Četvrta razina podrazumijeva špijunažu i postrojbe, sofisticirane protivnike koji su u mogućnosti izvestivišestruke koordinirane napade s ciljem uspostavljanja rupe u

[5]CANSO: Cyber Security and Assesment Guide, Civil Air Navigation Services Organisation, Amsterdam, 2014.
[6]Ibid
[7]Ibid
[8]Ibid

infrastrukturi sustava, koju mogu iskoristiti za filtraciju osjetiljivih informacija ili osiguranje mogućnosti za onesposobljavanje ili ometanje sustava. Obrana zahtijeva arhitekturu sustava koja je u mogućnosti ometati radnje napadača i osigurati kontinuitet kritičnih operacija koje ne smiju biti prekidane.[9]

Zadnja, peta razina je *cyber* rat.Napadači su vrlo sofisticirani i posjeduju resurse za kontinuirane i koordinirane napade.Obrana zahtijeva hitrost, adaptaciju i fleksibilnost za dinamično preoblikovanje operacija kako bi se održao kontinuitet sustava čak i za vrijeme neprekidnih napada.[10]

Globalno gledajući, postoji porast hakera i krađe podataka, ali ne nužno vezano za zračni promet već u svim informatiziranim sustavima. Situacija u svijetu je takva da privlači hakere aktiviste koji namjerno ometaju sustav i podatke na internetu kako bi privukli pažnju radi želje za promjenom, bilo da se radi o političkom ili ideološkom razlogu. Prevelik je raspon mogućnosti za takve prijetnje tako da ne postoji jedna solucija za rješenje tog problema u kratkom razdoblju. Naivno je vjerovati da će bilo kakve promjene kroz zakonodavstvo i propise osigurati zaštitu. Kao što napadači razvijaju svoje alate, taktiku i strategije, potrebno je nastaviti razvijati i metode zaštite te pokušati provoditi mjere koje će omogućiti da sustav upravljanja zračnim prometom uvijek bude korak ispred napadača i na taj način spreman obraniti se od bilo koje prijetnje.[11]

[9]CANSO: Cyber Security and Assesment Guide, Civil Air Navigation Services Organisation, Amsterdam, 2014.
[10]Ibid
[11]Ibid

Slika 1.*Cyber* prijetnje i spremnost na njih

Izvor: [2]

3.PRAVNI OKVIR ZAŠTITNIH MJERA

Unutar konteksta Organizacije međunarodnog civilnog zrakoplovstva(ICAO – International Civil Aviation Organization), dokumenta 7300, Čikaške konvencije, propisani su zahtjevi za osiguranje informacija.Na samom vrhu piramide*cyber* zaštite u sustavu upravljanja zračnim prometom, nalazi se integritet podataka i osiguranje informacija.Potrebno je shvatiti zahtjeve za očuvanje razine zaštite te važnost potrebnih mjera i strategija radi osiguranja istog.[12]

Uvjerljivost da informacije u zrakoplovstvu nisu otkrivene neovlaštenim osobama, procesima i uređajima spada pod povjerljivost podataka.To uključuje protekciju operativnih zrakoplovnih informacija i osiguranje informacija o lozinkama i konfiguracijskim datotekama.[13]

Integritet osigurava da te iste informacije nisu modificirane od strane neautoriziranih entiteta ili kroz neautorizirane procese. Isto tako, jamči da informacijama neće biti slučajno ili zlonamjerno rukovano, da neće biti mijenjane ili oštećene. Detekcija se pojavljuje bez ikakvih ili minimalnih lažnih alarma kada se podaci promijene. Naravno, izvor promjene podataka mora biti prepoznat.[14]

Dostupnost osigurava pravovremeni, pouzdan i kontinuirani pristup zrakoplovnim podacima i sustavima informacija od strane autoriziranih korisnika. Kontrolira se zaštita od poricanja servisnih uvjeta.[15]

Ovjera podrazumijeva uvjerenje o identitetu pošiljatelja i primatelja poruke.Podržava zahtjeve za potvrđivanje poruka i informacija sustava.Autorizacija podrazumijeva da dokaziv identitet obje strane koje rukuju s bilo kojom imovinom bude provjeren kao i da li posjeduju zadovoljavajuće dozvole.[16]

Neosporavanje se odnosi na osiguranje da pošiljatelj podataka bude obaviješćen s dokazom o pristizanju podataka te da je primatelju pružen dokaz identiteta pošiljatelja, naravno ako obje strane sudjeluju u obradi tih podataka.[17]

Da bi se osigurala sljedljivost podataka, sve radnje izvršene na bilo kojoj imovini se moraju prijaviti i zabilježiti, a vremenski prozor u kojem se te radnje mogu obavljati mora biti takav da zadovolji regulatorne zahtjeve i potrebe korisnika.[18]

Moguće je pronaći benefite korištenjem sustava zaštite i sigurnosti oblakovnog računaltsva prilikom razmjene informacija na zemlji. Bežična sigurnost na bilo kojoj

[12]ICAO: Assembly Resolution A33-1, International Civil Aviation Organization, 2001.
[13] Deepika, J.: Cyber Security in Civil Aviation – EALA Prize, Leiden University, 2015.
[14]Ibid
[15]Ibid
[16]Ibid
[17]Ibid
[18]Ibid

razini, uključujući fizičku razinu zaštite bežične mreže, može osigurati zaštićeni sustav upravljanja zračnim prometom.[19]

3.1. Osnovni dokumenti o zaštiti

Kao što je već spomenuto, ICAO kao bazična organizacija zadužena za regulative, propisala je još davnih 70-ih godina Priručnik zaštite kako bi usmjerila svoje države članice u mjerama prevencije od djela nezakonitog ometanja, umanjila njihov efekt te s vremenom postavila i standarde koji se nalaze u Dodatku 17. Konvenciji o međunarodnom ciivlnom zrakoplovstvu(Čikaškoj konvenciji).Danas su ti standardi dio kulture zaštite i sigurnosti. Jedini problem je nastao pojavom *cyber* prijetnji jer, prijetnje kao te, nikad prije viđene nisu bile pokrivene unutar barem jedne mjere. Nedugo nakon terorističkog napada 2001.godine na američke blizance, ICAO provodi reviziju sigurnosnih nedostataka sustava koji uključuju informacijsko - komunikacijske tehnologije (ICT – Information and Communications Technology).[20]Time se potaknuo prvi korak pri identifikaciji potencijalnih *cyber* rizika u zračnom prometu općenito.Ogranizacija međunarodnog civilnog zrakoplovstva godinama razvija i ojačava postojeće standarde i preporučene prakse (SARPs – Standards and Recommended Practices), ali i razvija nove preporuke konkretno za sustav upravljanja zračnim prometom s obzirom na novonastalu situaciju i pojavu raznih mogućih prijetnji koje svrstavamo u *cyber* prijetnje.

Iako ICAO pridonosi veliku važnost u regulativi svojih članica, većina dokumeta su preporuke i prakse dok svaka država posjeduje svoje nacionalne zakone koji mogu u određenom postotku odstupati od ICAO-a ili ga mogu potpuno prihvatiti. Nekoliko informatičkih organizacija, u suradnji s FAA i Europska organizacija za sigurnost zračne plovidbe (EUROCONTROL – European Organisation for the Safety of Air Navigation) su na skupu 2008. godine s ICAO-om zaključili da se zrakoplovna mreža, pa čak i na globalnoj razini, mora odvojiti od javno dostupne internetske mreže. Procijenjeno je da će u sljedećem desetljeću biti više do 30 000 zrakoplova koji će letjeti nebom, a svaki od njih korisititi vlastite internet baze koje će biti u nadležnosti države koje posjeduju i/ili kontroliraju njihove mrežne operacije. Prema procjenama, taj se model čini bolji od korištenja idealne jedinstvene mreže. U svijetu gdje se promet, podaci, audio i video prenose putem internet protokola,neophodno je sagraditi zatvorenu i izoliranu mrežnu infrastrukturu koja će omogućiti lakše upravljanje mrežnim operacijama,ali i izolaciju zrakoplovstva od globalnog interneta.[21]

3.2. Utjecaj države na sustav zračnog prometa

Zrakoplovstvo je jedinstveni dio nacionalne infrastrukture koji zahtjeva visoke mjere sigurnosti kako bi se osigurala potpuna zaštita od *cyber* i bilo kojih drugih

[19]Deepika, J.: Cyber Security in Civil Aviation – EALA Prize, Leiden University, 2015.
[20]http://www.icao.int/Meetings/FAL12/Documents/Biernacki.pdf 30.07.2017.
[21] Deepika, J.: Cyber Security in Civil Aviation – EALA Prize, Leiden University, 2015.

mogućih napada. Naravno, dio zaštite koji se odnosi na općenitu sigurnost, može biti samo dio lektroničke infrastrutkure, ako je konkretno riječ o zaštiti od *cyber*prijetnji. S obzirom da je to relativno nova grana zaštite, potrebno je vrijeme kako bi zakoni i regulative sazrijele i dosegle adekvatan nivo. To ne znači da je riječ o potpunom kaosu, već da rad i trud koji je započet, evoluira na internacionalnoj, regionalnoj i nacionalnoj razini s ciljem uspostavljanja kompletnog pravnog okvira koji će pokriti sve vrste prijetnji zajedno.[22]

Organizacija međunarodnog civilnog zrakoplovstva klasificira telekomunikacije kao nacionalni subjekt, što znači da svaka država samostalno određuje što prolazi kroz njen teritorij, a time ima na teret i potpunu odgovornost za bilo kakvu nepravilnost u zaštiti istog.Na panelu zrakoplovne sigurnosti (AVSEC – Report of the Aviation Security) 2009. godine, donešene su određene preporuke koje bi trebale biti dio SARPs-a, a glase: "Svaka država članica mora razviti mjere kako bi osigurala informacijsko – komunikacijski sustav, korišten za civilno zrakoplovstvo, od interferencija koje mogu ugroziti sigurnost civilnog zrakoplovstva.". Iako je ova preporuka napisana u imperativu, ICAO se nada da države članice shvaćaju važnost novonastalih rizika te da će usmjeriti sigurnost u dobrom pravcu.[23]

Na konvenciji o *cyber* kriminalu održanoj 2001.godine zaključeno je da su države nužne uspostaviti alate presretanja i izmjene u nacionalnom zakonu koji se odnose na krivična djela. Sukladno tome, razne strategije, kooperativni sporazumi i sl. razvijeni su i prisvojeni od strane Europske unije, ASEAN, Azijsko – Pacifičke ekonomske kooperacije, Internacionalne Telekomunikacijske Unije te Ekonomske Unije zapadnoafričkih država. Na konvenciji je isto tako predložena ideja o uspostavljanju kaznenog suda, odnosno tribunala isključivo za *cyber* prostor i *cyber* krivična djela. Naravno, takav dio regulative ne može služiti kao dio infrastrukture preventivnih mjera, ali može dovesti u red već nastala djela te služiti kao garancija i upozorenje potencijalnim budućim počiniteljima. Stručnjaci nalažu da iako većina država prihvaća preporuke organizacija, kazne i rukovođenje osuđenih počinitelja i dalje su preblagi i ne učinkoviti koliko bi mogli biti. Naprimjer, zakon u Brazilu spominje manipulaciju podataka od strane autoriziranog osoblja i nigdje nema riječi o trećim osobama, koje se ako nisu ovlaštene, smatraju počiniteljima. S druge strane, u Indiji, termin hakiranje je definirano kao takvo, ali kazna je maksimalna od 3 godine zatvora i/ili novčana kazna do 1000 eura. Kina je nešto stroža po godinama zatvora od Indije, dok je Koreja država s najstrožim zakonima kada je riječ od *cyber* zločinu. Kazne se kreću od oko 10 godina zatvora uključujući i novčanu kaznu od 100 miliona korejskih vona (KRW – South Korean Won) što je od prilike 75 000 eura. Slične uredbe se nalaze i u zakonima Sjedinjenih Američkih Država i Ujedinjenog Kraljevstva.[24]

[22]Deepika, J.: Cyber Security in Civil Aviation – EALA Prize, Leiden University, 2015.
[23]AVSEC: Report of the Aviation Security, Aviation Security Service, London, 2009.
[24]Ibid

Prema stručnjacima *cyber* zaštite, Pekinška konvencija iz 2010.godine, smatra se kao prvi korak naprijed u osiguranju zrakoplovne industrije. Ugovori usvojeni u Pekingu kriminaliziraju djelo korištenja civilnog zrakoplova kao oružje te korištenje opasnih materijala za napad zrakoplova ili drugih objekata na zemlji.[25] Prema zaključku konvencije, problem *cyber* prijetnji je implicitno adresiran, što znači da je prekršaj počinjen kada osoba uništi ili ošteti postrojenje zrakoplovne navigacije ili interferira s njenim operacijama, odnosno ako bilo koji takav akt ugrozi sigurnost zrakoplova u letu. Zaključak konvencije je taj da najveća prepreka u samom razvitku zaštitinih mjera i standarda, odnosno osiguranju zaštite od*cyber* napda i prijetnji je ta što uvijek u potpunosti nije moguće procijeniti i klasificirati sve prijetnje te na temelju toga donositi zaključke i potrebne alate zaštite.[26]

Nadalje, doprinos raznih internacionalnih i regionalnih organizacija, čiji se elementi mogu aplicirati i u zrakoplovstvu, trebao bi biti korišten ili barem razmotren prilikom razvoja zakona i regulative za adresiranje problema *cyber* zaštite u zrakoplovstvu. Konkretno, neke od organizacija koje unutar svojih priručnika i rezolucija o *cyber* kriminalu posjeduju mehanizme obrane od problema koje nose nove tehnologije su: Ujedinjeni Narodi, Europski Parlament, Interpol, Organizacija američkih država (OAS – Organisation of American States), Konferencija europskog civilnog zrakoplovstva (ECAC – European Civil Aviation Conference) te Organizacija za ekonomiju i kooperaciju te razvoj (OECD – Organization for Economics Co-operation and Development).[27]

Problem ne samo da je klasifikacija prijetnji i rizika te razvitak mjera i instrumenata zaštite na temelju toga, već i sama razina zaštite od države do države. To je čak i jedan od glavnih razloga zašto ICAO većinu toga publicira kao preporuku. Naravno da nije svaka država u mogućnosti usvojiti sve preporuke u cijelosti i na preporučenoj razini. Iz tog razloga su nacionalni zakoni uvelike važni. Poneke države su čak usvojile razne preporuke, bilo da se radi o konvencijama ili ICAO službenim publikacijama. Bitna stvar je ta da je njihova provedba upitna, što znači da je učinkovitost tih zakona nikakva. Diskutabilna je tema da li su države niže razine zaštite uopće ranjive i potencijalne žrtve takvih napada. Svakako je teško procijeniti i klasificirati nekoga po važnosti i prioritetima te odrediti čiji je život više vrijedan.[28]

Neizbježno je postrožiti kazneni zakon kako bi se povećala sigurnost i smanjio rizik.Isto tako, iako razne organizacije kao što su EUROCONTROL, Međunarodno udruženje zračnih prijevoznika (IATA – Internacional Air Transport Association), ECAC itd.objavljuju smjernice i preporučene prakse, neophodno je da države članice počnu s implementacijom istih u svoje nacionalne zakone koji su na neki način zastarjeli i jednostavno ne pokrivaju *cyber* prijetnje. Na razini regija, ako gledamo

[25]Abeyrante. R.: The Beijing Convention of 2010 On The Suppression of Unlawful Acts Relating To International Civil Aviation, Journal of Transportation Security, Beijing, 2011.
[26]Deepika, J.: Cyber Security in Civil Aviation – EALA Prize, Leiden University, 2015.
[27]Ibid
[28]Ibid

svijet kao cjelinu, EUROCONTROL u sklopu istraživanja Jedinstvenog europskog neba (SES – Signle European Sky) isto tako daje nekolicinu primjera koje se odnose i na*cyber* prijetnje, a članice Europske unije bi ih svakako trebale razmotriti i pridonijeti u uspostavljanju SES-a. Slična stvar se pojavljuje i u Ujedinjenom Kraljevstvu, od strane Centra za zaštitu nacionalne infrastrukture te nekolicine organizacija koje pokušavaju privući pozornost problema i zatražiti koordinirani odgovor. Savezna uprava za civilno zrakoplvstvo je organizacija koja najviše istražuje zaštitu od*cyber* kriminala. U veljači 2015.godine, donijeli su nekoliko promjena u zakonu zrakoplovstva te proveli procjenu *cyber* prijetnji i rizika u suradnji s domovinskom sigurnošću SAD-a, o čemu će više biti riječ u 5. poglavlju.[29]

Potrebno je uspostaviti hibridni sustav koji će obuhvatiti zrakoplovstvo i informacijski – komunikacijski sektor kako bi se osiguralo okruženje u kojem će se moći provoditi sigurne zrakoplovne operacije. Za početak je najvažnije, razmotriti, shvatiti te definirati i klasificirati *cyber* prijetnje i rizike. Tek tada je moguće sastaviti adekvatne zakone, uz preduvjet da su zakonodavci država članica svjesni važnosti problema, čije bi rješenje trebalo biti na globalnoj razini.[30]

[29]Deepika, J.: Cyber Security in Civil Aviation – EALA Prize, Leiden University, 2015.
[30]Ibid

4. SESAR STRATEGIJA UPRAVLJANJA *CYBER* ZAŠTITOM

Europska unija smatra da je prisutan rapidan porast srednje klase društva koji posjeduje dovoljnu platežnu sposobnost te je u mogućnosti koristiti zračni promet sve više. Zračni promet godišnje Europi donosi 110 milijardi eura te omogućuje zaposlenost preko 1.4 milijuna ljudi. S obzirom na to, neophodno je modernizirati sustav upravljanja zračnim prometom kako bi Jedinstveno europsko nebo bilo održivo. Istraživanje te jedan od najambicioznih tehnoloških projekata pokrenut od strane Europske unije je Istraživanje sustava upravljanja zračnim prometom jedinstvenog europskog neba (SESAR – Single European Sky ATM Research), a cilj projekta je definirati, razviti te implementirati poboljšanja, odnosno solucije potrebne za povećanje sposobnosti ATM-a kako bi sustav uspješno odgovorio na predviđeni trend. Strategija se temelji na ATM master planu.[31]

4.1. Definiranje problema

O *cyber* napadima se često govori u vijestima te na internetu, bilo da se radi o prijetnjama političara ili o organiziranim aktivističkim napadima na specifične mete, kao i o hakerima individualcima koji pronalaze nedostatke sustava kako bi mu naštetili. Svaki uspješan napad podrazumijeva narušavanje privatnosti kritične infrastrukture i dovodi do velikih troškova popravka sustava i ojačavanja mjera zaštite. Europska unija smatra da je ATM, zračni promet te zrakoplovstvo općenito, vrlo atraktivna meta za takve napade, s čim se rijetko tko ne bi složio.[32]

Tradicionalno, ATM je bio baziran na mreži usklađenih sustava povezanih s nizom raznih sučelja koji su koristili nacionalne i/ili vlasničke standarde. Posljednih godina, s obzirom na porast modernizacije, automatizacije i razine interoperabilnosti unutar sustava, javne internet mreže se koriste za prijenos podataka za razliku od nekad, kad je povezivanje bilo isključivo od točke do točke (PPP – Point-to-Point Protocol). Inicijativa modernizacije, uključujući ICAO Globalni plan zrakoplovne navigacije i SESAR program se fokusiraju na izuzetno povezan sustav koji omogućuje poboljšanja u interakciji između tradicionalnih strana kao što su pružatelji navigacijskih usluga (ANSP – Air Navigation Service Provider), zrakoplovne kompanije, zračne luke itd. Korištenje javnih mreža i interneta donosi mnoga poboljšanja u preformansama.Isto tako, smanjuju se troškovi infrastrukture jer se koriste isti materijali i dijelovi koji su javno dostupni što opet predstavlja nove mogućnosti za napad. Svaki novi sustav nije savršen jer je teško uvijek predvidjeti sve moguće probleme. Unutar Europe, ne postoji baš puno vjere u nove sustave i

[31] Paul R., Matt S.: Strategy and Management Framework Study for Information Cyber-Security - Application to System Wide Information Management Research and Development, SESAR, Hampshire, 2015.
[32]Ibid

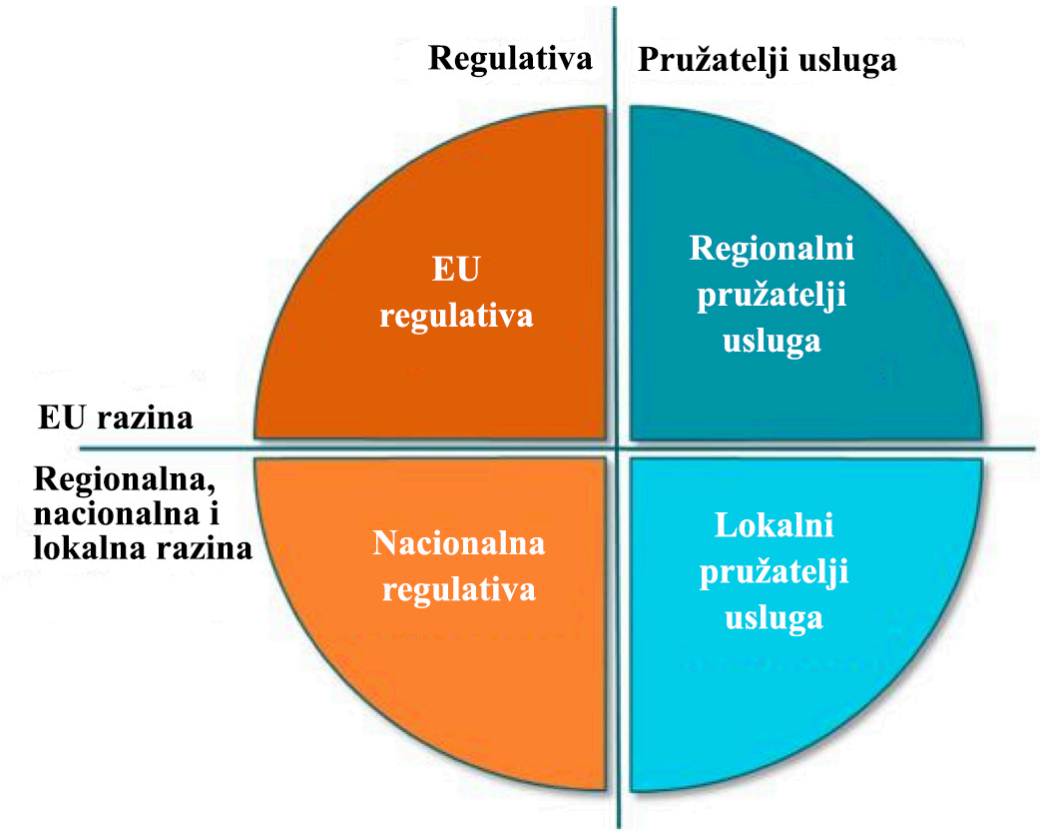
koncepte, pa čak niti u SES inicijativu, barem za vrijeme tranzicije.U sustavu u kojem je sve povezano kao negativna posljedica napada se može pojaviti tzv.domino efekt kroz čitav sustav te prouzročiti potpuni prekid zračnog prometa na neodređeno razdoblje.[33]

Neophodno je da se *cyber* zaštita razvija paralelno s razvitkom tehničkih uvjeta te da mjere budu uvedene progresivno kroz razvoj.Ekonomski gledano, isplativije je razmišljati unaprijed i implementirati zaštitu sustava prilikom izgradnje samog sustava nego ga naknadno opremati prilikom pojave određenog problema. Sigurnost se nikad ne može osigurati isključivo sa samom tehnologijom, već uz suradnju i pomoć politike i zakonodavstva. Zbog prirode *cyber* prijetnji, jedinstveno rješenje za sve probleme ne postoji.S vremenom, prijetnje postaju sve sofisticiranije, pa tako je potrebno kontinuirano razvijati i metode zaštite. Efektivna zaštita je ona koja evoluira te se lako adaptira promjenama, minimalizira ranjivost sustava i moguće prijetnje.[34]

4.2. Razvoj europskog odgovora

Sustav upravljanja zračnim prometomje podvrgnut mnoštvom regulativa i europskim, regionalnim i nacionalnim zakonima. Slika 2. prikazuje organizaciju ATM-a u Europi te separaciju između regulative i pružatelja usluga, ali i distinkciju između funkcije koja se provodi na europskoj razini i one koja se provodi na razini zemlja funkcionalnog bloka (FAB – Functional Airspace Block), nacionalnoj te razini kao što su zračne luke i sl. Europska komisija u suradnji sa Europskom agencijom za sigurnost zračnog prometa (EASA – European Aviation Safety Agency) brine za uspostavljanje regulative. Potrebno je formulirati europsku politiku i uspostaviti pravni okvir za sve države članice te osigurati da je sve regularno i implementirano na nacionalnoj razini. Nadležnost u provođenju kontrola i inspekcija predali su državama članicama, odnosno nacionalnim nadzornim tijelima (CAA- Civil Aviation Authorities), što je naravno isto propisano zakonom kako i na koji način ih provoditi.[35]

[33]Paul R., Matt S.: Strategy and Management Framework Study for Information Cyber-Security - Application to System Wide Information Management Research and Development, SESAR, Hampshire, 2015.
[34]Ibid
[35]Ibid

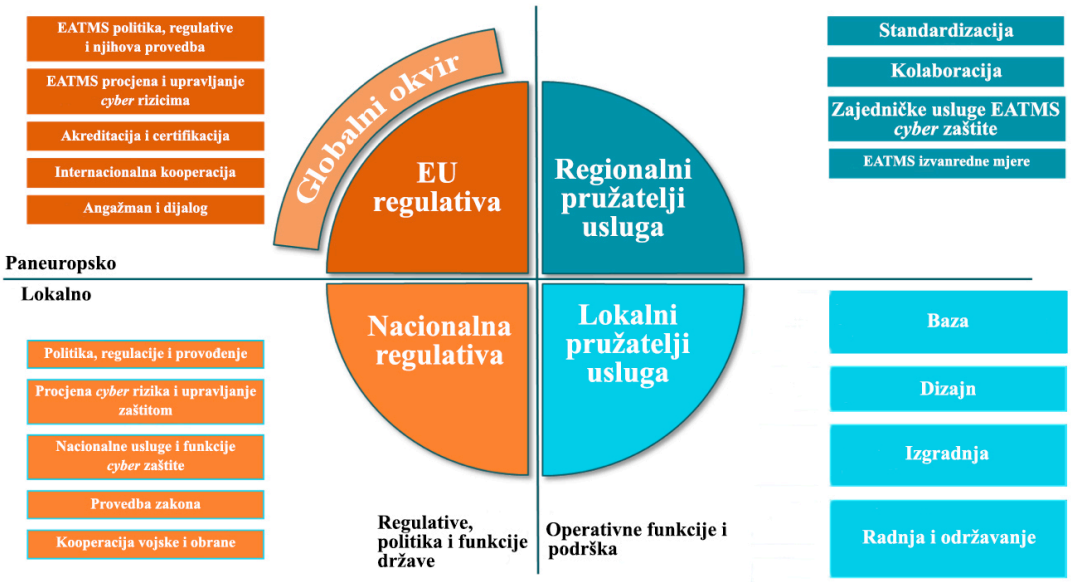


Slika 2. Organizacija ATM-a u Europi

Izvor: [6]

Da bi sustav bio siguran, zaštićen i elastičan u odnosu na prijetnje kojim je izložen, četiri kvadranta iz slike 2. moraju međusobno funkcionirati. Svaki kvadrant ovisi jedan o drugom, kao npr. zakonodavci uspostavljaju zakone i važno je da podržavaju konkretne probleme iz praktičnog sektora, a regije bi trebale biti podrška lokalnim razinama. Odnos između europskih i nacionalnih zakona varira ovisno o kompetenciji Europske unije od regije do regije, dok s druge strane Europska unija ima jaku kompetenciju u ATM sustavu. Zbog prirode problema *cyber* prijetnji, pokazalo se najefikasnije da države članice imaju određenu fleksibilnost te da prilagode zakone i mjere zaštite ovisno o vlastitim resursima i mogućnosti infrastrukture. Okvir *cyber* zaštite ATM sustava je najbolje prikazan na slici 3, a zapravo je nadogradnja već implementiranog sustava zaštite od ranije.[36]

[36]Paul R., Matt S.: Strategy and Management Framework Study for Information Cyber-Security - Application to System Wide Information Management Research and Development, SESAR, Hampshire, 2015.



Slika3. Europski okvir osiguranja *cyber* zaštite ATM-a

Izvor: [6]

4.3. Regulatorni odgovor

Neophodno je postojanje koherentne politike koja će ujediniti doprinos svih tijela, kao što su: Europska Komisija, EASA, EUROCONTROL itd. U tablici 1 prikazane su funkcije potrebne od strane zakonodavnih tijela EU. Cilj je osiguranje regulatornog okvira koji podržava krajnji cilj bez predstavljanja prepreke za sve uključene strane.Naglašava se izgradnja povjerenja među svim uključenim stranama.S druge strane, u tablici 2.prikazana je poveznica između EU i država članica, odnosno zahtjevi usmjereni prema članicama od strane EU. Može se reći da su ti zahtjevi fleksibilniji jer se radi o praktičnom problemu gdje se svakoj državi članici ulazi u susret i problem se rješava na najbolji mogući problem ovisno o njenoj konkrentoj situaciji i mogućnostima. Prioritet se ne postavlja niti na jednu stranu jer jedno polazi od drugog, a suradnja i napredak je obavezan ukoliko se želi osigurati razina ATM sustava koja postoji danas.[37]

[37]Paul R., Matt S.: Strategy and Management Framework Study for Information Cyber-Security - Application to System Wide Information Management Research and Development, SESAR, Hampshire, 2015.

Tablica1. Funkcije potrebne od strane zakonodavnih tijela Europske unije

Funkcija	Cilj
Politika, regulative i izvršenje	Ambiciozna politika *cyber* zaštite na temelju detaljne procjene, nadzora te mehanizami za osiguranje poštivanja zakona.
Procjena i upravljanje rizicima	Redovno preispitivanje rizika u bilo kojem kontekstu. Egzistencija politike te financiranje aktivnosti.
Akreditiranje i certifikacija	Zahtjevi za harmonizirani sustav koji se temelji na akreditacijama i/ili certificiranim procesima.
Internacionalna kooperacija	Europski pristup uspostavljanja konzistentnog sustava zaštite ATM-a na globalnoj razini.
Angažman i dijalog	Mehanizmi za angažman svih uključenih strana te zajednično izlaganje problema i donošenje zaključaka i rješenja.

Izvor: [6]

Regionalna suradnja je potrebna da podržavau svrhu podržavanja lokalne lokalnih pružatelje pružatelja usluga. Iako su na kraju lanca, svaki entitet je jednako bitan kako bi se osigurao harmonizirani sustav i međusobna podrška. U tablici 3.su prikazane potrebne funckije funkcije na regionalnoj razini.[38]

Tablica2. Funkcije potrebne od strane država članica

Funkcija	Cilj
Politika, regulative i izvršenje	Nacionalna politika *cyber* zaštite postoji za ATM. U pratnji je s nadzorom, auditima i izvršnim mehanizmima.
Procjena i upravljanje rizicima	Redovno preispitivanje rizika u bilo kojem kontekstu. Nacionalne procjene definiraju nacionalne probleme te informiraju nacionalnu politiku.
Usluge i funkcije nacionalne	Raspon usluga je dostupan na nacionalnoj razini

[38]Paul R., Matt S.: Strategy and Management Framework Study for Information Cyber-Security - Application to System Wide Information Management Research and Development, SESAR, Hampshire, 2015.

cyber zaštite	kroz nacionalnu vlast nadležnu za *cyber* zaštitu koja je podrška pri implementiranju internacionalne, europske i nacionalne regulative ATM-a.
Izvršenje zakona	Uspješno istraživanje, ispitivanje i analiziranje *cyber* napada.
Obrana i vojna kooperacija	Kooperacija i koordinacija vojske u zaštiti.

Izvor: [6]

Unatoč zahtjevima od svih mogućih strana, fokus se na kraju bazira na četiri glavna termina od čega sve i polazi kako bi se ostvario primarni cilj. Osnova je postaviti temelj za postizanje željenih rezultata, što će se započeti drugim korakom, odnosno dizajniranjem. Na temelju kompleksne analize i procjene, izrađuju se planovi i nacrti za izgradnju sustava, što je sljedeći korak do ostvarenja cilja. Nakon što je sustav izgrađen prema planu, potrebno ga je održavati i nadograđivati kako bi se ostvarila operabilnost i osigurala predviđena kvaliteta zaštite. [39]

Tablica3. Funkcije potrebne na regionalnoj razini

Funkcija	Cilj
Standardizacija	Standardi služe kao potpora zaštiti, uključujući temeljne standarde i uključenje mjera zaštite u ATM tehničke standarde i protokole.
Kolaboracija	Istraživanje izazova zaštite te njihov utjecaj na ATM te kako modernizirati i poboljšati sustav.
Zajedničke usluge	Usluge i aktivnosti koje su najbolje pružene na paneuropskoj razini.
Mjere za nepredviđene situacije	Paneuropske mjere pomažu odgovoriti i oporaviti se od *cyber* napada. Države članice su dio cjeloukupne strategije za povećanje elastičnosti SES-a.

Izvor: [6]

Studija je pomogla identificirati mnoge potrebne parametre za izgradnju sustava i adekvatnog odgovora na prijetnje te se smatra da će predviđeni planovi biti ostvareni i kao takvi pomoći u izgradnji kvalitetnog sustava zaštite.

[39]Paul R., Matt S.: Strategy and Management Framework Study for Information Cyber-Security - Application to System Wide Information Management Research and Development, SESAR, Hampshire, 2015.

5. CYBER SECURITY FOORUM INITIATIVE PROGRAM ZAŠTITE

Autori smatraju da je program Inicijative foruma *cyber* zaštite (CSFI – Cyber Security Forum Initiative) preliminarni temeljni izvještaj koji problem sagledavaiz persepektive *cyber* ratovanja.Cilj programa je identifikacija ranjivosti ATM sustava koji je trenutno u nadogradnji te pružanje protumjera za obranu i minimiziranje rizika od mogućih*cyber* napada. Isto tako, razviti scenarij u kojem će se testirati ranjivost sustava u koordiniranom napadu na američki aerodrom. Tim profesionalaca informatičke sigurnosti, analitičara obavještajnih podataka i inženjera su se udružili kako bi minimizirali špekulacije i logičko razmišljanje. Smatraju da je situacija komplicirana iz razloga što se na međunarodnoj razini događaju promjene i javljaju prijetnje. Stoga se smatra da je potrebno podignuti svijest na globalnoj razini, odnosno upozoriti sve sudionike zračnog prometa diljem svijeta o ugroženosti zračnog prometa *cyber* prijetnjama i napadima.[40]

5.1. Pozadinske informacije

Sadašnji sustav je dizajniran i implementiran kasnih 50-ih godina kroz sredinu 60-ih.Minimalne nadogradnje su naravno bile napravljene tijekom godina. Doppler-ov vremenski radar i zasloni u boji su bili najveći korak naprijed koji je sustav napravio od samog početka.S ciljem kreiranja sigurnijeg letačkog iskustva, FAA je u suradnji s ostalim međunarodnim agencijama pokrenula proces nadogradnje sustava.Kada je ideja bila predstavljena prije nepunih 20 godina, *cyber*prijetnje nisu uopće bile briga. Međutim, od početka instalacije novih sustava, *cyber* prijetnje su postale veliki problem.[41]

5.2. Ranjivost sustva

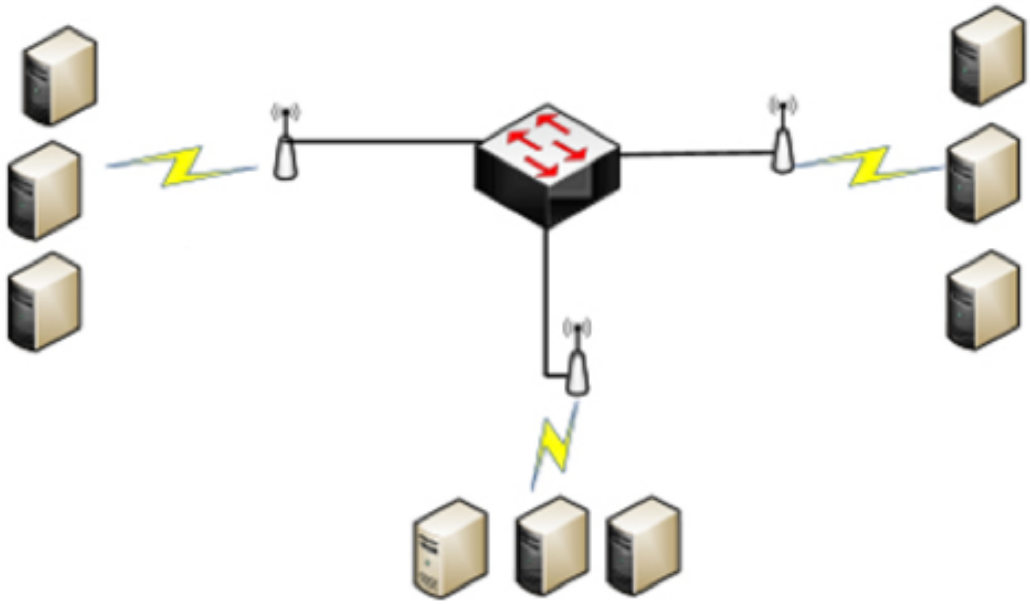
Američki sustav kontrole zračne plovidbe (ATC – Air Traffic Control) je već moderniziran kroz NextGen program.Iako se prilikom dizajniranja i same implementacije sustava razmotrio problem i važnost *cyber* prijetnji, međusobna komunikacija entiteta unutar sustava je i dalje neautorizirana i nekodirana.Razlog tome je potreba za modifikacijom svakog zrakoplova koji bi želio ostvariti zaštićenu komunikaciju s ATC sustavom. Rješenje tog problema leži u načinu komuniciranja putem komercijalnih frekvencija, odnosno TCP/IP i IPv6 protokolima koji sami po sebi uključuju enkripciju. Postoje i kompleksniji načini enkripcije čija je implementacija neekonomična te se s toga izbjegava.[42]

Poboljšanja i promjene većinom imaju dobru i lošu stranu. Npr. način komunikacije između kontrolnog tornja i zrakoplova u prilazu se vrši na vrlo visokim

[40]CSFI: Cyber Security Project, Cyber Security Forum Initiative, Manassas, Virginia, 2015.
[41]Ibid
[42]Ibid

frekvencijama (VHF – Very High Frequency), ultra visokim frekvencijama (UHF – Ultra High Frequency) te na visokim frekvencijama (HF – High Frequency). Takav sustav je bio i više nego dovoljan u vremenima kada promet nije bio tako gust, ali danas kada imamo sve više operacija slijetanja i polijetanja, jednostavno ne postoji dovoljan broj kanala unutar tih frekvencija pa se komunikacija više strana isprepliće unutar jedne frekvencije. Da bi se riješio taj problem, komunikacija se prebacuje naprijenos zvučne komunikacije putem internet protokola (VoIP – Voice over Internet Protocol), čime sustav postaje ranjiv. Kao kratkoročna rješenja se predlaže korištenje kompleksnijeg IPv6 protokola te frekvencija koje nisu dostupne otvorenim izvorima. S druge strane, američki proizvođač zrakopova Boeing u partnerstvu s American Airlines razvijaju bežični sustav za pohranu podataka koji može uvelike olakšati život pilotima, mehaničarima, letačkom osoblju i drugim uključenim osobama. U tom slučaju napadači mogu probiti u mrežu podataka te saznati i identificirati potencijalne problem sa zrakoplova te čak i izbrisati zabilješke što će prouzročiti da zrakoplov ne bude podvrgnut potrebnom popravku i kao takav postane opasan zrakoplov bez ičije spoznaje. Konkrentno koncept tzv.fly – by – wireless smanjuje broj vodova i žičanih sustava u zrakoplovu što utječe na smanjenje same težine zrakoplova pa se time povečava i njegova efikasnost, s obzirom na manju potrošnju goriva što opet omogućuje veću zaradu po putniku ili komadu prtljage.Na slici 5.je prikazana shema tog sustava s tzv. hibridnim grozdom koji minimizira potencijalnu opasnost jer se ne može izbijeći da napadač probije u sustav, ali na taj način osigurava da štetu koju može napraviti bude samo minimalna, odnosno da ne može doći do krajnjih dijelova sustava.[43]

[43] Khanh, D., Katja, G.: Fly-By-Wireless for Next Generation Aircraft: Challenges and Potential Solutions, NextGen, Dublin, 2012.



Slika 4. Shema strukture Fly – by – wireless sustava

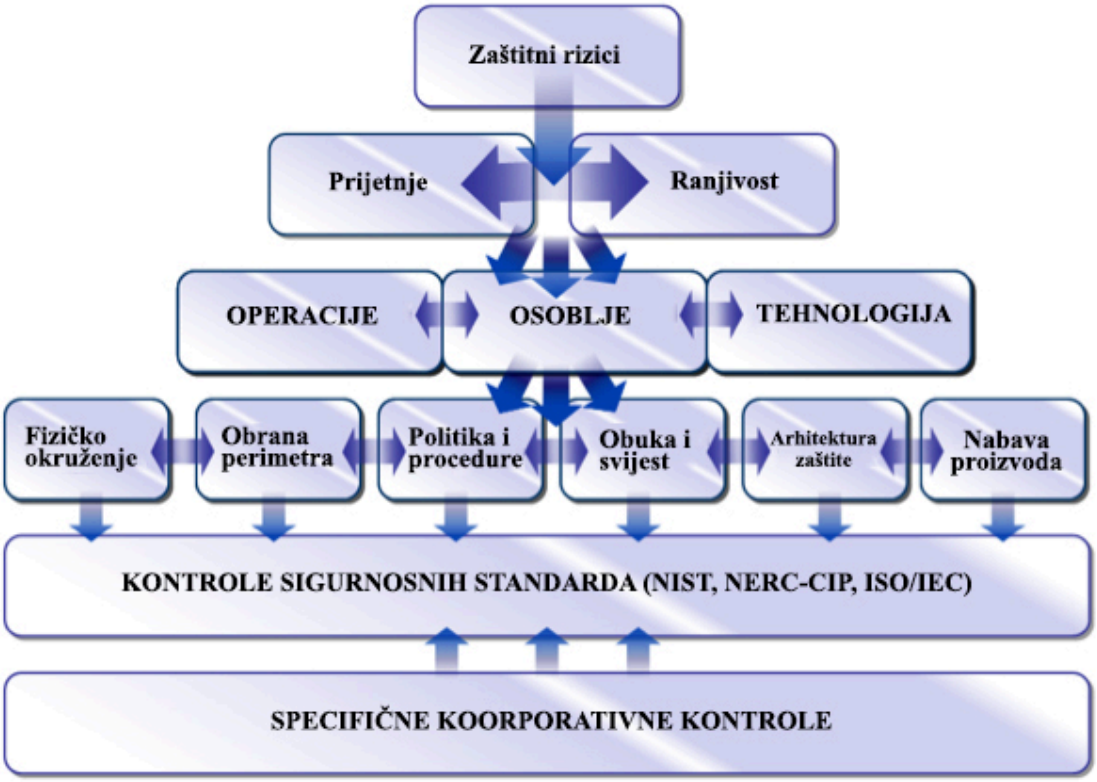
Izvor: [7]

Smatra se da je vjerojatnost napada na taj sustav jako mala, ali postoji mogućnost direktnog napada putem ATC signala. Iako je možda to sljedeća tehnologija vrhunske klase, s bezbroj benefita za pouzdanost zrakoplova, održavanje i ekonomiju, rizik je jednostavno prevelik, barem tako smatraju autori CSFI programa. Stručnjaci preporučaju da se provede kompletna procjena sustava zaštite te da se obavezno implementiraju šifriranje i kodiranje, autentikacija između klijenta i tzv. oblaka s dva čimbenika. Isto tako, da se propiše plan upravljanja mogućim rizicima.[44]

5.3. Plan sustava zaštite

Najbolji početak implementacije bilo koje napredne solucije je okrenuti se na najbolju praksu i vodstvo koje je trenutno u industriji. Zajedničke strategije se mogu koristiti kako bi se ojačala elastičnost organizacija protiv destruktivnih zlonamjernih softvera – *malware*. Željena razina zaštite zahtjeva adekvatnu segmentaciju mreže na principu komunikacije server – poslužitelj i server – server putem minimalnih priključaka i protokola. Smjer podataka bi trebao biti točno definiran, dokumentiran i autoriziran.Kada je riječ o kontroli pristupa neophodna je već navedena autentikacija s minimalno dva faktora.Nadalje, potrebno je osigurati adekvatan nadzor putem audita i recenzija sigurnosnih zapisnika. Autori programa naglašavaju kako je važno uspostaviti plan oporavka i rekonstrukcije ukoliko slučajno dođe do napada.[45]

[44]CSFI: Cyber Security Project, Cyber Security Forum Initiative, Manassas, Virginia, 2015.
[45]Ibid



Slika 5. Plan sustava zaštite

Izvor: [7]

Jasno je vidljivo da je čitav sustav potrebno sagledati iz perspektive *cyber* zaštite, FAA treba istražiti sposobnost odgovora na incidente te identificirati kritične točke sustava te razviti plan odgovora kako bi sustav ostao operativan za vrijeme i nakon potencijalnog napada. Taj odgovor mora biti koordinacija između zračnih kompanija, proizvođača zrakoplova i nadležnih zakonodavnih tijela države.Potpunu odgovornost ne snosi FAA, već služi kako bi usmjeravala ostale strane.Sljedeća kritična točka je korištenje adekvatnog softvera i nadzor elektroničke infrastrukture.Na slici 6.je prikazan plan sustava zaštite. Program navodi niz kokretnih primjera nedostataka u infrastrukturi koje je potrebno promijeniti, ali jasno je vidljiva sličnost europske strategije iz 4. poglavlja. Nakon jasnog definiranja problema i klasificiranja *cyber*prijetnji potrebno je uspostaviti pravni okvir zaštitnih mjera u kojem će sudjelovati već navedeni subjekti koji zajedno čine sustav zračnog prometa. Nakon njene uspostave potrebno je te mjere i provesti u praksi te osigurati konstatan nadzor sustava kako bi se održala željena razina zaštite.[46]

[46]CSFI: Cyber Security Project, Cyber Security Forum Initiative, Manassas, Virginia, 2015.

6. PROCJENA RIZIKA I *CYBER* ZAŠTITE

Vodič procjene rizika i *cyber* zaštite je dokument pružan od strane organizacije za usluge civilne zrakoplovne navigacije (CANSO – Civil Air Navigation Services Organization) koji služi kao za upoznavanje ATM-a s*cyber* prijetnjama i motivima koje počiinelji mogu imati. Isto tako, pokušava objasniti važnost definiranja i klasifikacije *cyber* prijetnji kao prvi korak u stvaranju sustava zaštite, kao što je već ranije i navedeno.[47]

6.1. Međunarodni standardi

Standardi Međunarodne organizacije za standardizaciju (ISO – International Standardization Organization) serije 27000 propisani su još 2005.godine i tada su pružali specifikacije o sustavu upravljanja zaštitom informacija (ISMS – Information Security Management System). Općenito, standardi pružaju zahtjeve za uspostavu, implementaciju, održavanje i kontinuirano poboljšanje ISMS sustava. Naravno, radi bliskosti problema, predlaže se da svaka organizacija ili sustav primijene navedene smjernice prilikom uspostave vlastite strategije zaštite. Konkretno, ISO 27002 standard sadrži kod praktične zaštite informacija, dok ISO 27001 preporuča kontrolne mehanizme. Oba standarda su zamišljena da se koriste zajedno, nadopunjujući jedan drugog.[48]

ISO 27005 standard odnosi se na smjernice upravljanja rizikom informacijske zaštite (ISRM – Information Security Risk Management) unutar organizacije, podržavajući zahtjeve zaštite informacija definirane unutar ISO 27001. Taj novi standard prvi puta uključuje procjenu, tretman, prihvaćanje, nadzor i reviziju rizika. U tablici 4.prikazana je SESAR metoda procjene rizika u zaštiti ATM-a predstavljen 2012. godine kao dodatak prethodnim standardima, ali se opet konkretno odnosi na specifičan problem.[49]

Tablica 4.SESAR metoda procjene rizika zaštite ATM sustava

Gubitak osnovnih usluga	Kvar klimatizacijskog uređaja
	Gubitak napajanja
	Kvar telekomunikacijske opreme
Poremećaj zbog radiacije	Elektromagnetsko zračenje

[47]CANSO: Cyber Security and Assesment Guide, Civil Air Navigation Services Organisation, Amsterdam, 2014.
[48]ICAO: Doc 9985 ATM Security Manual, International Civil Aviation Organization, Montreal, 2010.
[49]CANSO: Cyber Security and Assesment Guide, Civil Air Navigation Services Organisation, Amsterdam, 2014.

	Toplinsko zračenje
	Elektromagnetski impulsi
Kompromitiranje informacija	Presretanje signala interferencije
	Špijunaža na daljinu
	Prisluškivanje
	Krađa medija ili dokumenata
	Krađa opreme
	Vađenje recikliranih ili odbačenih medija
	Otkriće izvora smetnji
	Podaci od nepouzdanih izvora
	Tempiranje hardvera i softvera
	Otkrivanje pozicije
Tehnički neuspjeh	Zasićenje informacijskog sustava
	Onemogućavanje sposobnosti opskrbe
Neautorizirane akcije	Neautorizirano korištenje opreme
	Kopiranje softvera
	Korištenje lažnog ili kopiranog softvera
	Korupcija podataka
	Ilegalno procesuiranje podataka
Kompromitiranje funkcija	Zlouporaba prava
	Falsifikacija prava
	Uskraćivanje djelovanja
	Onemogućavanje dostupnosti osoblja

Izvor: [2]

6.2 Okvir Nacionalnog instituta standarda i tehnologija *cyber* zaštite

Okvir poboljšanja kritične infrastrukture *cyber* zaštite je izrađen od strane američkog Nacionalnog instutita standarda i tehnologija (NIST – National Instutute of Standards and Technology) u veljači 2014. godine. Sam po sebi ne predstavlja niti jedan novi standard ili koncept već utječe na postojeće prakse zaštite. Sami okvir se sastoji od smjernica temeljenih na procjeni rizika, a opet služi za identifikaciju, implementaciju i poboljšanje *cyber* zaštite. Procjena omogućuje organizaciji da ustanovi trenutne sposobnosti sustava *cyber* zaštite te da odredi plan za poboljšanje i

održavanje sposobnosti sustava. U tablici 5.prikazane su funkcije koje je moguće konstantno ponavljati kroz kružni proces kako bi se održao učinkovit sustav.[50]

Tablica 5. Funkcije NITS okvira *cyber* zaštite

Funkcija	Opis	Kategorija
Identifikacija	Razumijevanje upravljanja rizicima	Upravljanje imovinom
		Poslovno okruženje
		Pravilna identifikacija
		Procjena rizika
		Strategija upravljanja rizicima
Zaštita	Kontrolne i zaštite mjere potrebne za zaštitu ili sprečavanje od *cyber* prijetnji	Kontrola pristupa
		Svjest i obuka
		Zaštita podataka
		Procesi i protokoli zaštite informacija
		Održavanje
Detekcija	Kontrolne i zaštite mjere potrebne za zaštitu ili sprečavanje od *cyber* prijetnji	Anomalije i događaji
		Konstantan nadzor zaštite
		Procesi detekcije
Odgovor	Aktivnosti odgovora na incident	Planiranje odgovora
		Komunikacija
		Analiza
		Ublažavanje
		Poboljšanja
Oporavak	Plan održavanja otpora i oporavka nakon *cyber* prodora	Planiranje oporavka
		Poboljšanja
		Komunikacija

Izvor: [2]

Jasno je da razne organizacije i industrije imaju različite poslovne potrebe, operativne modele, ali i dostupne resurse za stvaranje robusnog programa zaštite. Stoga, NITS okvir omogućuje organizaciji da uskladi i poboljša vlastitu cyber zaštitu

[50]CANSO: Cyber Security and Assesment Guide, Civil Air Navigation Services Organisation, Amsterdam, 2014.

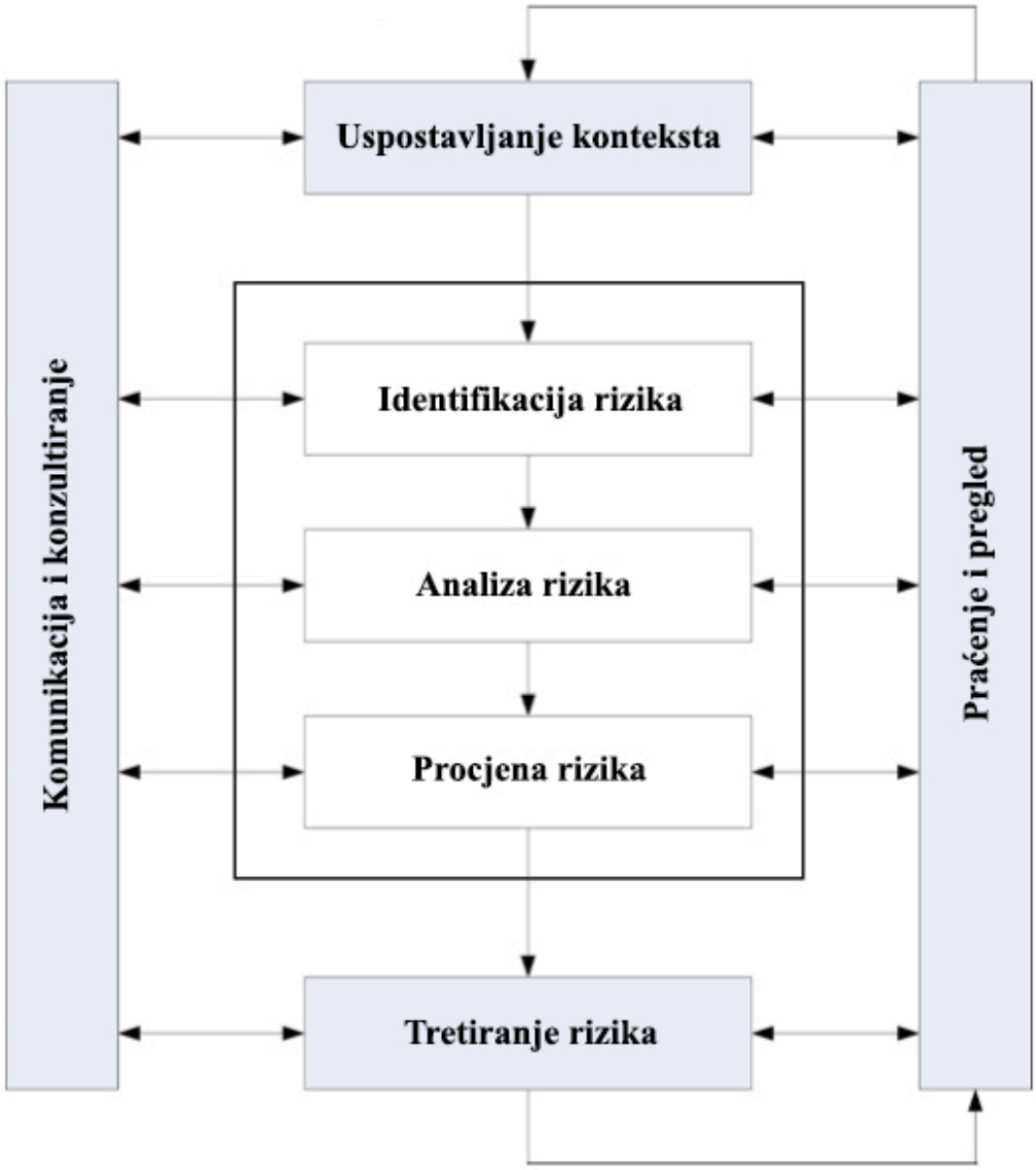
s obzirom na okolnosti.Preporuča se definiranje trenutnog i željenog profila kako bi se mogla napraviti usporedba i identificirati nedostaci s ciljem poboljšanja sustava zaštite.[51]

6.3 Metodologija procjene rizika

Metodologija procjene rizika na neki način formira standardni proces procjene rizika, koji omogućuje organizaciji da na učinkovit način identificira, procijeni i smanji taj rizik. Termin rizik se odnosi na mogućnost bivanja mene od bilo kojeg napada. Stoga se procjena rizika provodi kako bi se odredili potencijalno najvažniji nedostaci zaštite te usporedile posljedice i novčani utjecaj te uopće mogućnost da se to i dogodi. Analiziranje rizika je temeljni dio uspostave uspješne politike pa i krajnjeg sustava zaštite.[52]

Za početak najvažnije je ustanoviti kontekst procjene, odnosno definirati koji je to dio sustava ili organizacije potencijalno pod rizikom. Na slici 7.prikazan je proces upravljanja rizikom.Kao što je i već ranije navedeno, u SESAR i CSFI programu, potrebno je definirati prijetnju. Prijetnja je izvor i značenje konkretnog napada, a procjena prijetnji se provodi kako bi se definirao najbolji pristup sustavu zaštite. Procjena rizika se fokusira na analiziranje potencijala i tendencije narušavanja resursa žrtve napada, dok je procjena prijetnji fokusirana na analiziranje resursa napadača s ciljem razvitka specifične politike sustava zaštite. Potencijalne prijetnje i ranjivosti unutar ATM sustava uključuju slabosti kao što su kritične poslovne aplikacije, operativno i poslovno sučelje, nepodržani i neodržavani softver, loša kontrola pristupa, loše upravljanje promjenama, slaba kontrola mreže, loša implementacija i upravljanje virtualnim uređajima i oblacima. Isto tako, loše upravljanje imovinom, zastarjelost hardvera i infrastrukture, slaba kontrola i ažuriranje softvera, nedostatak učinkovitog nadzora izapisnika, nedostatak kompatibilnosti odgovora, nedostatak alternativa, kao što su sigurnosne kopije tenedostatak obuke i dizanja svijesti o *cyber* zaštiti. Obavezne su i sigurnosne kontrole u dobavljačkim odnosima. Sustavi nisu sinkronizirani na jedinstveni sat, a moguć je i gubitak informacijsko povezane imovine. Slabosti se još javljaju kroz odlaganje opremetetehnologije bazirane na radiju, grijanje, ventilacija i klimatizacija (HVAC – Heating, ventilation and air conditioning).[53]

[51]CANSO: Cyber Security and Assesment Guide, Civil Air Navigation Services Organisation, Amsterdam, 2014.
[52]Ibid
[53]Ibid



Slika 6. Proces u pravljanja rizikom

Izvor: [2]

Procjena rizika analizira i potencijalno vrijeme i doba javljanja rizika.U tablici 6. prikazana je procjena razine i tolerancije na rizik. Odnosi se na omjer vremena pojave prijetnje te razine utjecaja i posljedica uzrokovanih rizikom. Na primjer, rizik visoke razine, koji se pojavljuje između 5 i 50 godina ima ocjenu B, što bi bila neka srednja vrijednost.[54]

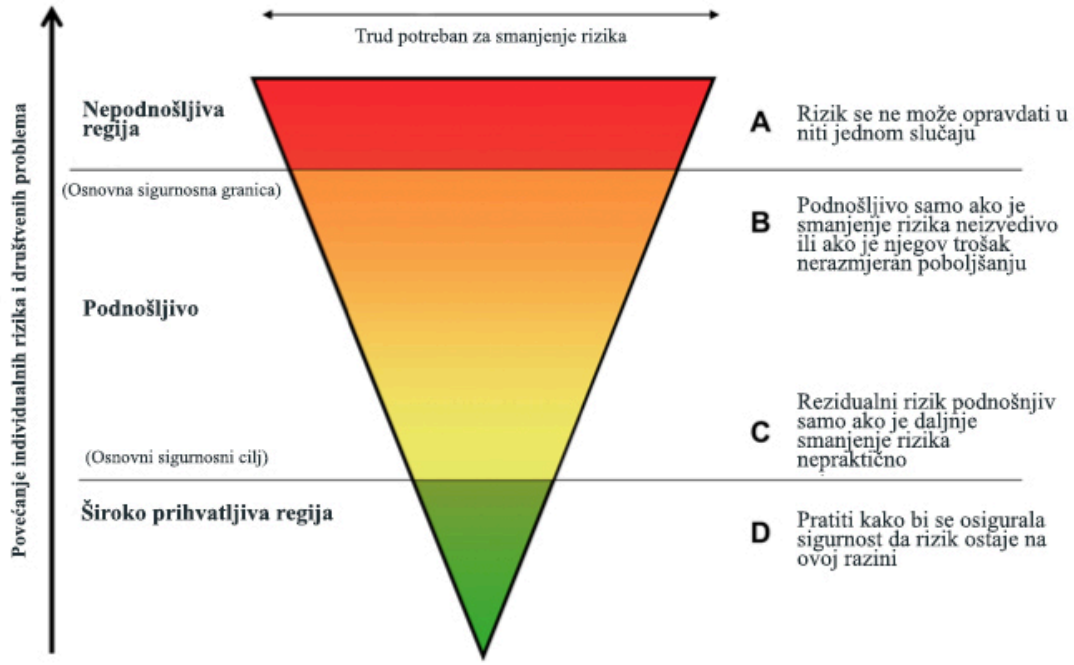
[54]CANSO: Cyber Security and Assesment Guide, Civil Air Navigation Services Organisation, Amsterdam, 2014.

Tablica 6. Procjena razine i tolerancije na rizik

Vjerojatnost		Posljedice				
Vrijeme događaja		Katastrofalne 1	Velike 2	Umjerene 3	Manje 4	Neznatne 5
1	Unutar sata	A	A	A	A	C
2	Svaki sat ili dnevno	A	A	A	B	D
3	Dnevno ili godišnje	A	A	B	C	D
4	1 do 5 godina	A	B	C	C	D
5	5 do 50 godina	A	B	C	D	D
6	Ni svakih 50 godina	B	C	D	D	D

Izvor: [2]

Taj omjer pruža smjernice za određivanje prioriteta rizika iz vremenske perspektive, dok su na slici 8. prikazane i objašnjene ocjene rizika.



Slika 7. Piramida rizika

Izvor: [2]

7. UTJECAJ NA BUDUĆNOST SIGURNOSTI I ZAŠTITE

Znatan trud se ulaže u modernizaciju ATM sustava što će rezultirati povezivanjem različitih sustava, stvarajući tzv.sustav sustava – *System of systems*, koji zahtjeva visoku razinu pouzanosti. Stoga, zaštita istog mora biti implementirana od početka, kao što je već i spomenuto unutar SESAR programa, ali i CSFI programa, odnosno američke inačice.[55]

Europa je trenutno u procesu redefiniranja europskog ATM master plana, koji je prvobitno definiran 2008. godine unutar SESAR programa. S potprogramom 2016. – 2020. cilj je napraviti veliki napredak u smislu implementacije nove ATM infrastrukture. Stoga, u nadolazećim godinama, ATM će evoluirati kroz niz koraka koji korespondiraju poboljšanjima sustava.S druge strane ICAO, kao temeljno zakonodavno tijelo civilnog zrakoplvostva je 2011.godine publiciralo najveću nadopunu pravilnika pod nazivom Zaštita. Unutar Dodatka 17.koji se odnosi na zaštitu protiv djela nezakonitog ometanja, ICAO sada ubraja i *cyber* zaštitu kao jednu od bitnih stavki. Vizija je stvoriti interoperabilni globalni ATM sustav koji će korisnicima tijekom svih faza leta osigurati adekvatnu razinu sigurnosti, ekonomičnost operacija te će biti ekološki održivo i zadovoljitinacionalne sigurnosne zahtjeve.[56]Usprkos tome, trenutno ne postoji globalno prihvaćena definicija sustava zaštite ATM-a. Organizacija međunarodnog civilnog zrakoplovstva radi na razvitku priručnika koji se bazira na iskustvima EUROCONTROLA i FAA.

Sustav zaštite podrazumijeva suradnju i podršku više strana. Velik broj država već je implementirao Sustav upravljanja zaštitom (SecMS – Security Managemet System), koji povezuje više strana s jednim ciljem, kao npr. povezivanje procjene rizika, identifikacija mjera zaštite, razvoj programa te usklađivanje s regulativama i standardima.Konkretno u europskom kontekstu, zajednički zahtjevi su specificirani unutar regulative Europske Komisije EC Regulation 1035/2011.[57]

S obzirom da su ATM sustavi diljem svijeta u fazi modernizacije i implementacije novih zakona i regulative, prisutan je rizik nedovoljnih sigurnosnih zahtjeva, što u konačnici može povećati trošak cijelog procesa.Novac igra veliku ulogu u svemu, pa se takav scenarij pokušava izbjeći, što postavlja zaštitu u prvi plan fokusa čak i prije određenih operativnih problema.[58]

---

[55]Rainer, K., Martin, H.: SESAR Security 2020: How to embed and secure security in system - of systems engineering, EUROCONTROL, Brussels, Belgium, 2012.
[56]ICAO: Doc 9854 Global Air Traffic Management Operational Concept, International Civil Aviation Organization, Montreal, 2005.

[57] Regulation 1035/2011, Common Requirements for the Provision of Air Navigation Services,European Commission, Brusseles, Belgium, 2011.
[58]Rainer, K., Martin, H.: SESAR Security 2020: How to embed and secure security in system - of systems engineering, EUROCONTROL, Brussels, Belgium, 2012.

8. ZAKLJUČAK

Jasno je vidljivo da trendovi modernizacije u svijetu doprinose nizu pozitivnih strana olakšavanjem raznih procesa, smanjenjem troškova,ali i poboljšanjima kvalitete. Nažalost isto tako, jačaju i sposobnosti potencijalnih počinitelja kojima se otvaraju nove mogućnosti za napad. S obzirom da konkretno i sam sustav upravljanja zračnim prometom, ali i zrakoplovstvo općenito, u svojoj infrastrukturi koriste uređaje koji su dostupni u svakom kućanstvu, jasno je da su i potencijalnom počinitelju alati danas dostupni više nego ikad.

Kompleksnost problema zahtjeva i kompleksno rješenje koje se ne može riješiti preko noći. Najveći strah i prepreku u rješavanju problema predstavlja to što je zasad jako teško definirati i klasificirati *cyber* prijetnje. Razlog tome je to što su takve prijetnje relativno nove i nitko nije u potpunosti siguran kakve sve one mogu biti, osim onih koje su se već dogodile. Stoga je vrlo veliki zadatak ispred stručnjaka za zaštitu koji uvijek moraju biti korak ispred potencijalnih počinitelja kako bi eliminirali moguću prijetnju i kako sustav ne bi patio od potencijalnog napada.

Radi se o okruženju u kojem nema vremena ni mjesta za pokušaje i pogreške, tako da treba biti maksimalno na oprezu. Vrlo je bitno ukazati svijetu na važnosti novonastalih prijetnji i rizika kako bi uistinu bili spremni protiv njih se boriti. To je globalni problem i jedinstvenog rješenja nema, ali je bitno težiti uspostavi globalnih, regionalnih i lokalnih ciljeva, koji opet moraju biti realni i u skladu s mogućnostima pojedinca, odnosno u ovom slučaju država, koje su kao takve nadležne i dužne osigurati integritet nacionalnog zrakoplovstva i vlastitog zračnog prostora. Organizacija međunarodnog civilnog zrakoplovstva kao nadležno tijelo za civilno zrakoplovstvo na globalnoj razini, konstantno pokušava poboljšati regulative i standarde, a pogotovo one koji se odnose na *cyber* zaštitu. Na regionalnoj razini organizacije kao što su EUROCONTROL i FAA, razmatraju preporuke i namete od strane ICAO-a te ih pokušavaju implementirati u vlastitu politiku i buduće planove. Na lokalnoj razini, svaka država koja je članica bilo koje organizacije, odnosno svaka sudionica globalnog civilnog zrakoplovstva, dužna je sudjelovati u stvaranju zaštićenog sustava zračnog prometa. Naravno, mogućnosti se razlikuju od države do države, pa je stoga zadatak svake od njih, procijeniti i krenuti u najboljem smjeru za sebe, imajući na umu da su svi dio jedne zajednice i da sigurnost jednog znači i sigurnost drugog.

Moderan sustav zaštite, osim što mora polaziti od čvrsto propisanog zakona, mora biti sačinjen od infrastrukture koja povezuje razne tehnologije koje su sposobne nositi se s narednim prijetnjama. Kao i u svakom sustavu zaštite, nakon što je dizajnirana, propisana te naposljetku i izgrađena infrastruktura, potrebno je konstantno provoditi kontrole i provjeravati trenutno stanje kako bi se održala željena i prvobitno zamišljena razina zaštite. Takva zaštita je neophodna za sustav upravljanja zračnim

prometom kako bi se zrakoplovstvo uspjelo nositi s trendovima porasta prometa i sve većeg broja operacija.

LITERATURA

1. Deepika, J.: Cyber Security in Civil Aviation – EALA Prize, Leiden University, 2015.
2. CANSO: Cyber Security and Assesment Guide, Civil Air Navigation Services Organisation, Amsterdam, 2014.
3. ICAO: Assembly Resolution A33-1, International Civil Aviation Organization, Montreal, 2001.
4. AVSEC: Report of the Aviation Security, Aviation Security Service, London, 2009.
5. Abeyrante, R.: The Beijing Convention of 2010 On The Suppression of Unlawful Acts Relating To International Civil Aviation, Journal of Transportation Security, Beijing, 2011.
6. Paul, R., Matt, S.: Strategy and Management Framework Study for Information Cyber-Security - Application to System Wide Information Management Research and Development, SESAR, Hampshire, 2015.
7. CSFI: Cyber Security Project, Cyber Security Forum Initiative, Manassas, Virginia, 2015.
8. Khanh, D., Katja, G.: Fly-By-Wireless for Next Generation Aircraft: Challenges and Potential Solutions, NextGen, Dublin, 2012.
9. ICAO: Doc 9985 ATM Security Manual, International Civil Aviation Organization, Montreal, 2010.
10. Rainer, K., Martin, H.: SESAR Security 2020: How to embed and secure security in system - of systems engineering, EUROCONTROL, Brussels, Belgium, 2012.
11. ICAO: Doc 9854 Global Air Traffic Management Operational Concept, International Civil Aviation Organization, Montreal, 2005.
12. Regulation 1035/2011, Common Requirements for the Provision of Air Navigation Services, European Commission, Brusseles, Belgium, 2011
13. URL:http://www.icao.int/Meetings/FAL12/Documents/Biernacki.pdf(30.07.2017.)

POPIS KRATICA

ANSP	(Air Navigation Service Provider) Pružatelj usluga u zračnoj plovidbi
ATC	(Air Traffic Control) Kontrola zračne plovidbe
ATM	(Air Traffic Management) Sustav upravljanja zračnim prometom
AVSEC	(Report of the Aviation Security) Panel zrakoplovne sigurnosti
CAA	(Civil Aviation Authorities) Nacionalna nadzorna tijela
CANSO	(Civil Air Navigation Services Organization) Organizacija za usluge civilne zrakoplovne navigacije
EASA	(European Aviation Safety Agency) Europska agencija za sigurnost zračnog prometa
ECAC	(European Civil Aviation Conference) Konferencija europskog civilnog zrakoplovstva
EUROCONTROL	(European Organisation for the Safety of Air Navigation) Europska organizacija za sigurnost zračne plovidbe
FAA	(Federal Aviation Agency) Savezna uprava za civilno zrakoplovstvo
FAB	(Functional Airspace Block) Funkcionalni blok zračnog prostora
GPS	(Global Positioning System) Globalni sustav pozicioniranja
HF	(High Frequency) Visoke frekvencije
HVAC	(Heating, ventilation and air conditioning) Grijanje, ventilacija i klimatizacija
IATA	(International Air Transport Association) Međunarodna udruga za zračni prijevoz
ICAO	(International Civial Aviation Organisation) Međunarodna organizacija za civilno zrakoplovstvo
ICT	(Information and Communications Technology) Informacijsko – komunikacijska tehnologija
ISMS	(Information Security Management System) Sustav upravljanja zaštitom informacija

ISRM	(Information Security Risk Management) Upravljanje rizikom informacijske zaštite
KRW	(South Korean Won) Južnokorejski won
NIST	(National Institute of Standards and Technology) Nacionalni institut standarda i tehnologija
OAS	(Organisation of American States) Organizacija američkih država
OECD	(Organisation for Economics Co-operation and Development) Organizacija za ekonomiju i kooperaciju te razvoj
PPP	(Point-to-point Protocol) Protokol od točke to dočke
SARPs	(Standard and Recommended Practices) Stanradi i preporučene praise
SecMS	(Security Management System) Sustav upravljanja zaštitom
SES	(Single European Sky) Jedinstveno europsko nebo
SESAR	(Single European Sky ATM Research) Istraživanje sustava upravljanja zračnim prometom jedinstvenog europskog neba
UHF	(Ultra High Frequency) Ultra visoke frekvencije
VHF	(Very High Frequency) Vrlo visoke frekvencije
VoIP	(Voice over Internet Protocol) Prijenos zvučne komunikacije putem internet protokola

POPIS SLIKA

POPIS TABLICA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

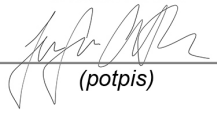
Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **PROCJENA *CYBER* RIZIKA NA SUSTAV UPRAVLJANJA ZRAČNIM PROMETOM** na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 29/08/17

Student/ica:



(potpis)