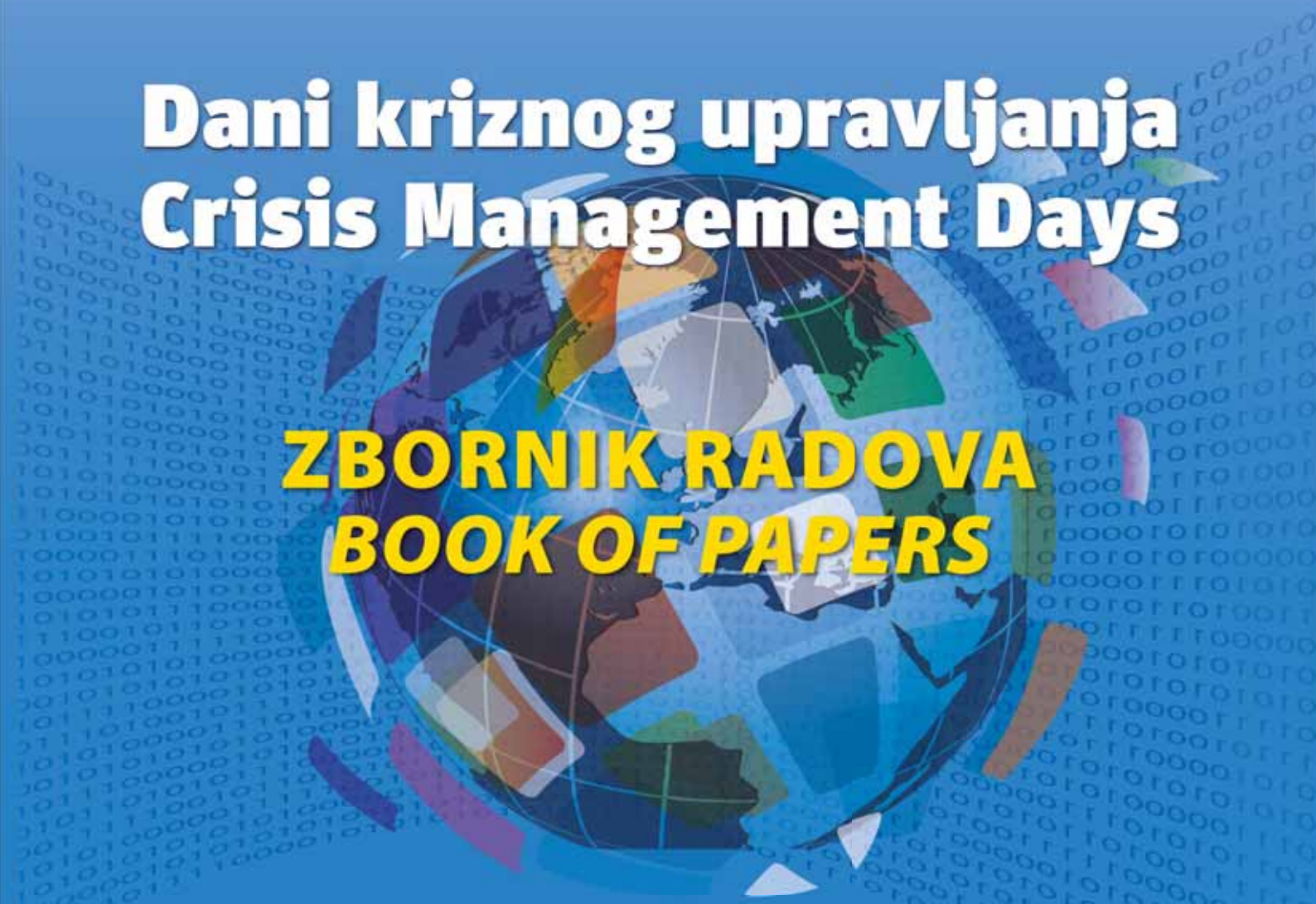
VELEUČILIŠTE VELIKA GORICA
UNIVERSITY of APPLIED SCIENCES VELIKA GORICA

DKU
Dani kriznog upravljanja
Crisis Management Days

8. MEĐUNARODNA ZNANSTVENO-STRUČNA KONFERENCIJA
8th INTERNATIONAL SCIENTIFIC CONFERENCE

Dani kriznog upravljanja
Crisis Management Days



ZBORNIK RADOVA
BOOK OF PAPERS

14. i 15. svibnja 2015.
Velika Gorica, Hrvatska

14 and 15 May 2015
Velika Gorica, Croatia

VELEUČILIŠTE VELIKA GORICA
UNIVERSITY of APPLIED SCIENCES VELIKA GORICA

8. MEĐUNARODNA ZNANSTVENO-STRUČNA KONFERENCIJA
8th INTERNATIONAL SCIENTIFIC CONFERENCE

Dani kriznog upravljanja
Crisis Management Days

ZBORNIK RADOVA
BOOK OF PAPERS

DKU
Dani kriznog upravljanja
Crisis Management Days

14. – 15. svibnja 2015.
14 – 15 May 2015
Velika Gorica,
Hrvatska - *Croatia*

ZNANSTVENI ODBOR

Predsjednik Znanstvenog odbora, **Siniša Tatalović** *(Hrvatska)*

Potpredsjednik Znanstvenog odbora, **Ivan Toth** *(Hrvatska)*

Potpredsjednik Znanstvenog odbora, **Branko Mihaljević** *(Hrvatska)*

Mo Hamza *(Velika Britanija)*, **Filip Ejdus** *(Srbija)*, **Nina Aniskina** *(Rusija)*, **Anica Hunjet** (Hrvatska), **Jadran Perinić** *(Hrvatska)*, **Ognjen Čaldarović** (Hrvatska), **Dejan Škanata** *(Hrvatska)*, **Ivo Šlaus** *(Hrvatska)*, **Ismet Alija** *(B i H)*, **Istvan Endordi** *(Mađarska)*, **Ivan Nađ** *(Hrvatska)*, **Ante Sanader** *(Hrvatska)*, **Izet Beridan** *(B i H)*, **Iztok Podbregar** *(Slovenija)*, **Sanja Kalambura** *(Hrvatska)*, **Marjan Malešić** *(Slovenija)*, **Olivera Injac** *(Crna Gora)*, **Lucrina Stefanescu** *(Rumunjska)*, **Ružica Jakešević** *(Hrvatska)*, **Marinko Ogorec** (Hrvatska), **Mohamed Morina** *(Hrvatska)*, **David Fabi** *(Italija)*, **Mirza Smajić** *(B i H)*, **Predrag Zarevski** *(Hrvatska)*, **Želimir Kešetović** *(Srbija)*, **Zoran Keković** *(Srbija)*, **Vinko Morović** *(Hrvatska)*, **Teodora Ivanuša** *(Slovenija)*, **Robert Socha** *(Poljska)*, **Robert Mikac** (Hrvatska), **Petar Veić** *(Hrvatska)*, **Vlatko Cvrtila** *(Hrvatska)*, **Nenad Kacian** *(Hrvatska)*, **Nedžad Korajlić** *(B i H)*, **Ladislav Novak** (Slovačka), **Oliver Bakreski** *(Makedonija)*.

ORGANIZACIJSKI ODBOR

Predsjednica Organizacijskog odbora, **Martina Mihalinčić**

Potpredsjednik Organizacijskog odbora, **Ivan Nađ**

Alen Stranjik, Hrvoje Janeš, Igor Milić, Ivan Markotić, Jasna Jursik, Tamara Čendo Metzinger, Marina Črnko, Ana Mirenić, Marina Manucci, Nives Jovičić, Marko Toth, Vedrana Čemerin, Dorotea Bačurin, Ivana Rubić, Vladimir Bralić, Luka Jurković, Siniša Stein, Ivan Turković, Lada Crnobori, Matea Penić Sirak, Ivica Turčić.

POKROVITELJ

PATRON

Predsjednica Republike Hrvatske Kolinda Grabar-Kitarović

***Kolinda Grabar-Kitarović**, President of the Republic of Croatia*

Organizator konferencije
Conference Organizer

VELEUČILIŠTE VELIKA GORICA
UNIVERSITY of APPLIED SCIENCES VELIKA GORICA

VELEUČILIŠTE VELIKA GORICA
UNIVERSITY of APPLIED SCIENCES VELIKA GORICA
Dani Kriznog Upravljanja
Crisis Management Days
8. Međunarodna znanstveno-stručna konferencija 14.-15. svibnja 2015. Hotel Aristos, Zagreb, Hrvatska

Pregledni rad
UDK 338.49:005.931.11

ZAŠTITA KRITIČNE INFRASTRUKTURE – ULOGA I ODGOVORNOST

Marjan Marjanović, spec. krim.
Security Guard, Republika Crna Gora

Sažetak

Događaji koji odlikuju savremene međunarodne odnose su uticali i doveli do povećanja broja izazova i pretnji bezbjednosti sa visokim stepenom neizvjesnosti, nepredvidivosti i diskontinuiteta. Većina država danas zavisi od kritične infrastrukture (CI) koja je kičma nacionalne ekonomije, bezbjednosti i napretka, i nastoje pružiti efikasan i efektivan odgovor na savremene prijetnje, kao što su terorizam, organizovani kriminal, sukobi, prirodne katastrofe i nesreće, ili kompjuterski kriminal, posebno u kontekstu vanrednih situacija. Svaka država, region, ili pojedinačni objekat CI, odgovorni su za identifikovanje pretnje/i od kojih pokušavaju da se zaštite. Direktivom Savjeta 2008/114 / EC od 8. decembra 2008 za identifikaciju i određivanje evropske kritične infrastrukture i procjene o potrebi poboljšanja njihove zaštite, članom 5, je predviđena obaveza postojanja Plana bezbjednosti operatera (OSP). Ovaj rad se bavi odnosom i ulogama države i operatera/vlasnika u izradi, implementaciji i ažuriranju tih planova i mjera predviđenih tim planovima. Cilj je da se motivišu svi subjekti da jačaju svoje potencijale u njenoj zaštiti.

Ključne riječi: kritična infrastruktura, prijetnje bezbjednosti, procjena prijetnji, vanredne situacije, plan bezbjednosti operatera, zaštita, odgovornost, država, vlasnik/operater

1. Uvod

Evropski program za zaštitu kritične infrastrukture (EPCIP)

"... Uspostavlja postupak za identifikaciju i označavanje Europske kritične infrastrukture ('ECIs'), i zajednički pristup u procjeni potrebe za poboljšanjem zaštite takvih infrastruktura kako bi se doprinijelo zaštiti ljudi. "[206].

Moderna društva danas u potpunosti zavise od naučno-tehnološkog razvoja i primjene tehničko-tehnoloških inovacija u svim segmentima društva. Ta činjenica čini ih ranjivijim iz bezbjednosne perspektive, umnožava rizike i prijetnje nesmetanom i efikasnom funkcioniranju CI, povećavajući finansijske troškove pružanja adekvatne zaštite CI. Trenutna ekonomska kriza, klimatske promjene, urbanizacija, demografski rast i njegove socio-ekonomske posledice, povećavaju potencijalne prijetnje koje počinju predstavljati stvarne bezbjednosne rizike za CI.[207] Realne su procjene da će se učestalost i ozbiljnost incidenata na CI povećavati u budućnosti.[208] Svaka država, region, ili pojedinačni objekat CI, odgovorni su za identifikovanje prijetnje/i od kojih pokušavaju da se zaštite. Ovo je važno prilikom definisanja i razvoja sistema za zaštitu i neutralisanje prijetnje. Osnovni princip zaštite CI treba da se zasniva na trenutnoj procjeni da li je država u opasnosti, odnosno na procjeni prijetnji.[209]Procjena prijetnje/i[210]

206 *EC, 2008, str.77*
207 Cornelis, B., *Federal Risk Inventory, Survey and Knowledge Building*, SPIRAL, Liège, 2004.
208 Maliszewski P. J., *Modeling Critical Vaccine Supply Location: Protecting Critical Infrastructure and Population in Central Florida*, Florida State University College of Social Sciences, 2008.
209 The Physical Protection Objectives and Fundamental Principles (GOV/2001/41/Attachment), IAEA, Vienna, 2001.
210 Procena pretnji podrazumeva evaluaciju postojećih pretnji i obično uključuje i obaveštajne projcene koje opisuju motivaciju, namjere i mogućnosti da se počini zlonamerna radnja.

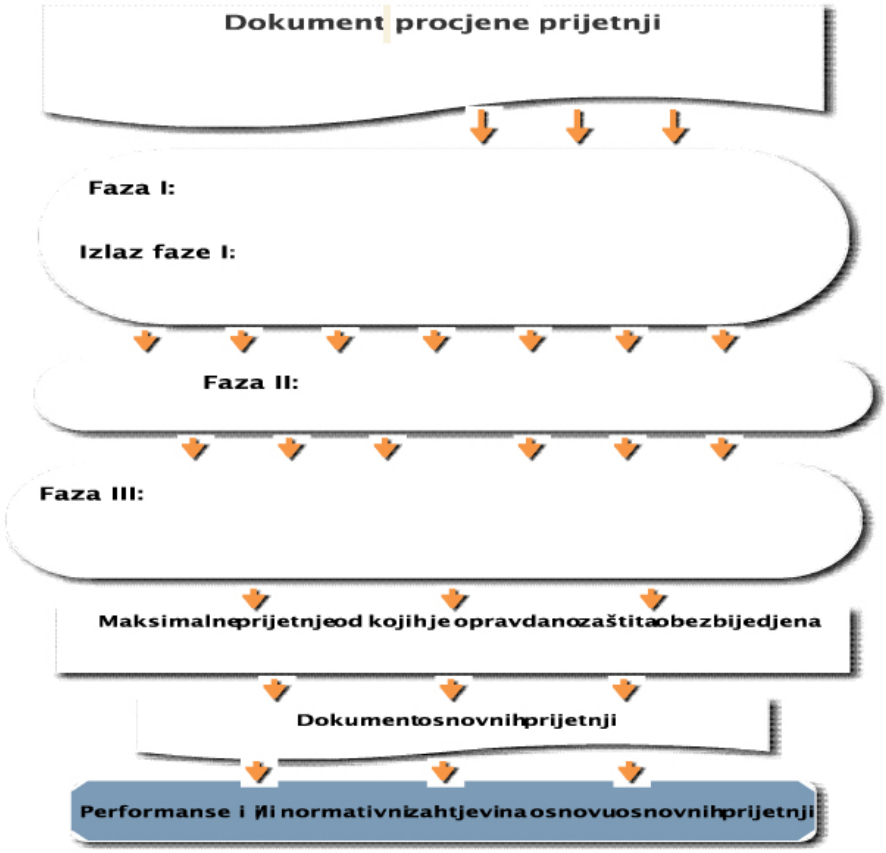
od strane države dovodi nas do ***skeleta osnovnih prijetnji*** za datu klasu objekata (***design basis threat - DBT***)[211], koji je podskup procjene prijetnji za objekat CI koji se štiti. DBT određuje potrebne performanse sistema bezbednosti za određeni objekat CI, i pruža osnovu za procjenu promjena u nivou prijetnji. Dakle, DBT je izvedena iz procjene prijetnji državi, i njome se olakšava razvoj fizičke zaštite od prijetnji.

DBT je opis atributa i karakteristika potencijalnih protivnika (insajdera i autsajdera) koji bi mogli pokušati zlonamjerni akt, protiv kojih je sistem zaštite CI namijenjen i ocjenjivan.[212]

DBT se definiše na državnom nivou i moraju se uzeti u obzir tehnički, politički i ekonomski faktori.Kao alat za pomoć u uspostavljanju performansi za projektovanje i procjenu sistema zaštite CI, DBT pomaže operaterima i državnim organima da utvrde kriterijume za otkrivanje, zadržavanje i odgovor pri projektovanju i procjeni efikasnog sistema zaštite CI.

Država može da ima više od jednog DBT za različite vrste kritične infrastrukture, da bi odrazila različite potrebe za zaštitom.

Slika 1: Proces procjene osnovnih prijetnji



Skelet osnovnih prijetnji:

- daje detaljnu i preciznu tehničku osnovu za projektovanje i plan bezbjednosti,
- daje kriterijume za evaluaciju zaštite CI, pa stoga pruža veću garanciju da je nivo zaštite dovoljan i vodi ka efikasnoj raspodjeli resursa za zaštitu, kroz smanjenje proizvoljnosti, koja bi inače postojala u uspostavljanju sistema zaštite,
- omogućava fleksibilan pristup regulisanju ovog problema,
- dopušta prilagođavanje projekta sistema zaštite CI za rešavanje jedinstvenih karakteristika sistema, odnosno objekata,
- pruža i jasnu osnovu za definisanje odgovornosti operatera za zaštitu CI.

211 ***Development, Use and Maintance of the Design Basic Threat***, IAEA Nuclear Security Series No. 10, IAEA, Austria, 2009
212 ***The Physical Protection of Nuclear Material and Nuclear Facilities***, INFCIRC/ 225/Rev. 4 (corrected), IAEA, Vienna, 1999.

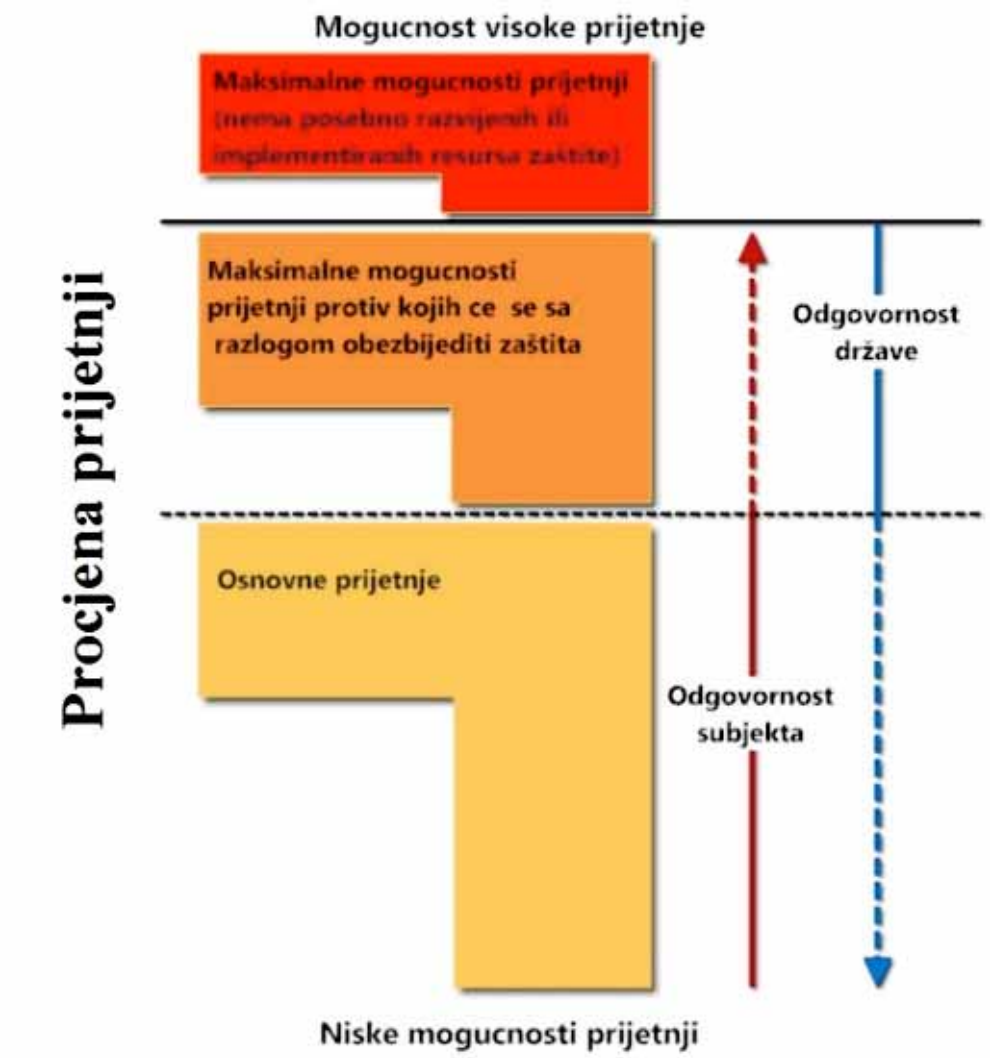
- treba da budu uključen u regulatorni okvir i koristi za:
  - uspostavljanje ciljeva performansi i zahteva za sisteme zaštite CI;
  - određivanje kriterijuma projektovanja za sisteme zaštite CI;
  - uspostavljanje kriterijuma za ocenjivanje sistema zaštite CI; i
  - podjelu odgovornosti između države i operatera[213].

2. Odnos odgovornosti između države i operatera za sprovođenje efikasne zaštite

Prilikom procjene prijetnji dajemo opseg od niskih mogućnosti prijetnji do visokih mogućnosti prijetnji. Ovaj opseg predstavlja poznate stvarne i preovlađujuće prijetnje koje se ocjenjuju u procjeni prijetnji. Procesom prečišćavanja će biti određene maksimalne mogućnosti prijetnji:

- u odnosu na koje će biti obezbijeđena zaštita i
- u odnosu na koje nema posebno razvijenih ili implementiranih resursa zaštite , nego mjere ublažavanja

Slika 2: Zaštita prema opsegu prijetnji[214]



Na osnovu opsega prijetnji:

- Država će obezbijediti resurse zaštite koji će se primijeniti na sve prijetnje obuhvaćene maksimalnim mogućnostima prijetnji, u odnosu na koje će biti zaštita opravdano obezbijeđena.
- Država i operater će dijeliti odgovornost za ovu zaštitu, gdje operater ima primarnu odgovornost za mogućnosti prijetnje u okviru DBT, a država ima odgovornost za borbu protiv prijetnji između DBT i maksimalnog potencijala prijetnji kojima će zaštita biti opravdano obezbijeđena.

213 Operater je svaka organizacija ili lice sa odobrenjem ili ovlašćenjem za obavljanje delatnosti iz domena CI.
214Development, Use and Maintance of the Design Basic Threat, op. cit., p. 6.

- Resursi zaštite neće biti ni razvijani ni dodijeljeni za zaštitu od mogućnosti prijetnji koje prevazilaze prag od maksimalnih mogućnosti prijetnje u odnosu koje će zaštita biti opravdano obezbijeđena. Međutim, postoje mjere za ublažavanje za koje se očekuje da pruže neku svojstvenu zaštitu protiv mogućnosti ovih prijetnji

Odgovornost za razvoj i kontrolu zaštite CI može imati samo organ države. U svakom slučaju, sledeće odgovornosti treba da budu jasno dodijeljene:

- koordiniranje procesa kroz koji treba da se utvrdi da li odgovarajući mehanizam obezbjeđuje adekvatan nivo zaštite[215];
- koordiniranje procesa za razvoj DBT i donošenje odluka;
- obezbjeđivanje da su DBT zaključci u skladu sa zakonskim ili regulatornim zahtjevima;
- distribucija DBT onima koji su odgovorni za zaštitu CI, kao i onima koji su uključeni u razvoj Sistema za zaštitu CI;(Osjetljive informacije u vezi zaštite CI i ECI mogu da tretiraju samo lica koja imaju odgovarajući nivo bezbjednosne provjere)
- odlučivanje kako će se DBT koristiti i koje regulatorne zahtjeve treba primijeniti;

ZaštitaodprijetnjikojenijesuuključeneuDBTidefinisaneuprocjeniprijetnjićeostatiunadležnostidržave,ipak,operateridaljeimaodlučujućuulonguupružanjupomoćidržavi,iliuzaštitiodprijetnjiiliublažavanjunjihovihposledica.Ovo jebilovrlovažnodefinisatizboganalizeglavnihscenarijaprijetnji,rizikairanjivostisvakogdijelakritičneinfrastrukture;i identifikacije, selekcije i davanje prioriteta kontra-mjerama i postupcima za stalne mjere bezbjednosti i stepenovane mjere bezbjednosti.

Efikasna identifikacija rizika, prijetnji i sposobnosti odbrane u određenim sektorima zahtijeva obostranu komunikaciju između vlasnika / operatera CI i države, a u slučaju da je ona proglašena za ECI onda i između država članica i Komisije[216]. Primarna i krajnja odgovornost za zaštitu CI i ECI pada na države članice i vlasnike / operatere tih infrastruktura.[217]

Operater/vlasnik ima glavnu odgovornost za direkno sprovođenje mjera zaštite CI, kao i specifičnih mjera koje je podržavaju, koje su razvijene od strane operatera i potvrđene od strane regulatornog tijela, ili direktno definisane od regulatornog tijela.

S obzirom na potencijalno teške posledice nekih zlonamjernih akata i visoke troškove pružanja zaštite, neadekvatan nivo potrebne zaštite vjerovatno neće biti prihvatljiv nadležnim organima države.

Metodologija za izradu Plana bezbjednosti operatera (OSP)

- Plan bezbjednosti operatera (OSP) će identifikovati imovinu kritične infrastrukture i bezbjednosna rešenja koja postoje ili se sprovode za njihovu zaštitu(postojeće stanje zaštite). Metodologija za izradu OSP minimalno morada pokriva[218]:1. identifikaciju kritičnih sredstava;2. analizu glavnih scenarija prijetnji, rizika i ranjivosti svakog dijela kritične infrastrukture; i3. identifikaciju, selekciju i davanje prioriteta kontra-mjerama i postupcima za:
- **Stalne mjere bezbjednosti**Mjere kojima se identifikuju neophodna bezbjednosna ulaganja i sredstva koje su od značaja za zaštitu i prevenciju i neophodna su svo vrijeme:

  tehničke mjere (uključujući instalaciju detekcije upada, kontrolu pristupa);
- organizacione mjere (mjere sprečavanja, postupci za upozorenje i upravljanje krizama);
  - mjere kontrole i verifikacije;
  - komunikacija;
  - podizanje svijesti i obuka; i

215Ukoliko se nivo zaštite ne smatra prikladniom, nadležni organ treba da identifikuje alternativni pristup da obezbedi adekvatnu sigurnost i odgovarajuću zaštitu baziranu na pretnjama.

216 DIREKTIVA VIJEĆA 2008/114/EC od 8. decembar 2008

217 Ibid

218 DIREKTIVA VIJEĆA 2008/114/EC od 8. decembar 2008 DODATAK II

- bezbednost informacionih sistema.

- **Stepenovane mjere bezbjednosti** Mjere koje su određene u skladu sa nivoom rizika i prijetnje i koje se aktivirajusamo u skladu sa tim nivoom rizika i prijetnje (u zavisnosti od države i odgovora na prijetnje, može biti 3,4 ili 5 nivoa označenih različitim bojama ili brojevima).

Nivo prihvatljivog rizika utvrđuje regulator, odnosno nadležni organ države.

Na nivou operateratreba da se razvija metoda za ocenjivanje mjera zadržavanja i odgovora na zlonamjerna akta, za rešavanje atributa i karakteristika protivnika opisanih u DBTCI, i vanrednim situacijama.

4. Izrada OSP

Prilikom izrade Bezbjednosnog plana operatera (OSP) će se odrediti imovina CI i ECI, i koja bezbjednosna rešenja postoje ili se sprovode za njihovu zaštitu.Minimalni sadržaj ECI OSP je dat u Aneksu II.

Odgovornost za identifikaciju CI leži na državi. CI se identifikuje korišćenjem metoda za identifikovanje nacionalnih kritičnih infrastruktura ili međusektorskih kriterijuma, na odgovarajućem nacionalnom nivou. Način na koji će se to uraditi zavisi od države, razvojne politike, zakonodavstva i druge pravne regulative.

U slučaju da CI zadovoljava kriterijume za ECI država će obavijestiti Komisiju o tome.

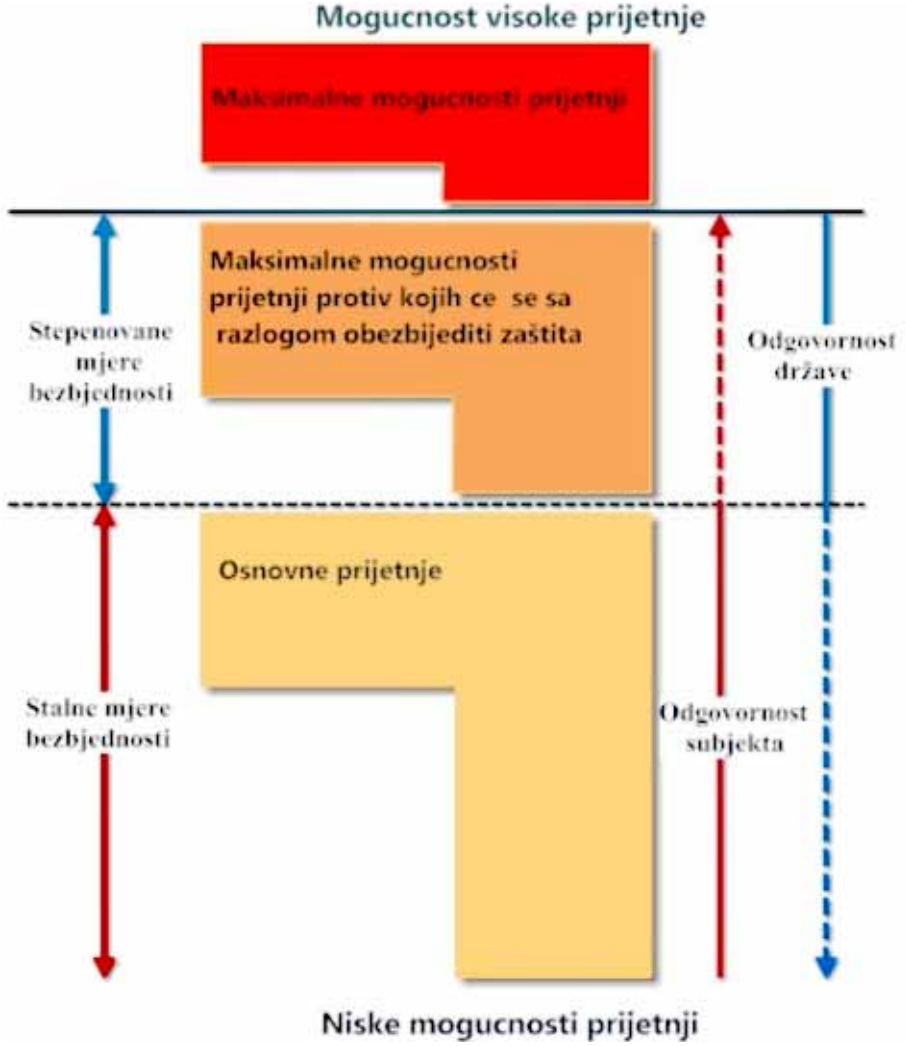
U konkretnom slučaju, potrebna je bliska saradnja između organa države i vlasnika / operatera tih infrastruktura da se identifikuju kritični objekti/resursi i da se obezbijedi da se uzmu u obzir : ozbiljnost uticaja, dostupne alternative i trajanje poremećaja / oporavka.

Projektant zaštite CI treba da razumije uslove pod kojima se mora vršiti zaštita i nivo prihvatljivog rizika koji utvrđuje regulator, odnosno nadležni organ države. Jasan opis prijetnji definiše ove uslove, i zbog toga je definisanje i opis prijetnji bitan preduslov za razumno uvjeravanje i efikasnu zaštitu CI. U idealnom slučaju, obavještajni i drugi izvori informacija će obezbijediti dovoljno informacija za specifikaciju uslova za projektovanje i izvođenje sistema zaštite CI, jer u nedostatku dovoljno detaljnih i specifičnih opisa pretnji, teško je precizno odrediti nivo zaštite koji će biti odgovarajući i efikasan za dati objekat ili aktivnost.

Da bi vlasnik /operater mogao da ima sopstveni OSP, država mora da razvije sveobuhvatan nacionalni plan za obezbjeđivanje ključnih resursa i kritične infrastrukture,kao i fizičkih i tehnoloških sredstva koja podržavaju takve sisteme ipreporuči mjere za zaštitu u koordinaciji sa drugim lokalnim vlastima, privatnim sektorom, i drugim subjektima.[219]

219 Homeland Security Act of 2002

Slika 3: Mjere zaštite prema opsegu prijetnji



Organi operatera zaduženi za zaštitu moraju da poznaju finansijske, operativne i bezbjednosne uticaje određenih mjera koje mogu da utiču na zaštitu, a samim tim i na podjelu odgovornosti za mjere bezbjednosti između operatera i drugih subjekata. Zbog toga, ulazne informacije od operatera, formalne ili neformalne, od velikog su značaja. Operater treba da obezbijedi povratne informacije nadležnom organu u vezi sa finansijskim, operativnim i bezbjednosnim uticajima potencijalnih odluka u vezi sa zaštitom CI, sa mogućim nedoumicama oko insajderskih prijetnji i incidenata koji možda imaju negativno porijeklo. On razvija i sprovodi neophodne mjere zaštite od SOPKI[220], uključujući i kontrolu, pripravnost i zakonitost.Na osnovu toga nacionalnog plana i preporučenih mjera se radi OSP sa svim specifičnostima i prijetnjama koje su karakteristične za konkretnu CI.

U zavisnosti od DBT, specifičnosti i prijetnji koje su karakteristične za konkretnu CI projektujusestalne mjere bezbjednosti.

Stepenovane mjere bezbjednostisu određene u skladu sa nivoom rizika i prijetnjikoje prevazilaze mogućnosti stalnih mjera zaštite predviđenih za osnovni nivo prijetnji. Svakim nivoom je određeno ko je odgovoran za proglašenje mjera i pokretanje odgovora na prijetnje.Postupak odgovora mora se odvijati u skladu sa OSP i u skladu sa situacijom na terenu.

Značenje "odgovor" ili "snage za odgovor" varira od zemlje do zemlje, a često čak i od objekta do objekta u datoj zemlji. U snage odgovora u zavisnosti od nivoom prijetnje mogu biti uključene, osim policije i vojske, i posebno visoko obučeni timovi agencija za obezbeđenje u mjeri u kojoj to zakoni i propisi dozvoljavaju.

U OSP moraju postojati posebne procedure ili zadatci za snage odgovora, jer moraju da djeluju na jasnim osnovama i pravilima angažovanja. U tom odgvoru na prijetnje zajedničke obaveze države i samih operatera/vlasnika su:

220Procjena prijetnji od teškog i organizovanog kriminala(obaveza države)

- cijelo osoblje uključeno u zaštitu i snage za odgovor mora proći provjeru pouzdanosti (bezbjednosnu provjeru);
- integrisani plan odgovora mora biti razvijen tako da definiše odgovornost za sprovođenje i komunikaciju tokom odgovora;
- stalne vježbe za potvrdu spremnosti za odgovor na vanredne situacije, koje obuhvataju: definisane kriterijume uspešnosti i izvršenja, simulacije, i višestruko sprovođenje vežbi.
- Osoblje uključeno u zaštitu i snage za odgovor treba da ima redovnu obuku koja se zasniva na programu obuke zasnovanom na prijetnjama koje su definisane u OSP.
- Neophodna je zajednička obuka snaga za odgovor iz svih agencija u slučaju vanrednih situacija.
- Snage za odgovor moraju biti obučene i kvalifikovane do tačke da mogu da kompenzuju neke nedostatke u drugim karakteristikama zaštite CI.
- Oprema osoblja uključenog u zaštitu i snage za odgovor mora da bude u stanju da ublaži prijetnju identifikovanu u OSP.

Dio odgovora jei "ublažavanje posledica". To ublažavanje je važno u smanjenju uticaja na ukupni uspjeh prijetnje, ali je primarna odgovornost države i operatera da se spriječi uspjeh prijetnje. Ako su operativne procedure na objektu odgovarajuće i osoblje za odgovor i ublažavanje pouzdano i kvalifikovano, posledice uspješnog napada protivnika mogu biti znatno smanjene.

Za ublažavanja posledica nastalih kao rezultat prirodnih katastrofa država i objekti CI treba da izrade planove za reagovanje na vanredne situacije. Ovi planovi treba da se redovno testiraju i ocjenjuju.

5. Implementacija i ažuriranje OSP planova i mjera predviđenih tim planovima

Svaka država članica će osigurati da je OSP ili ekvivalent napravljen i redovno pregledan u roku od jedne godine od označavanja infrastrukture kao kritične. Ovaj period može biti produžen u izuzetnim okolnostima, po dogovoru sa nadležnim organom države.

Poštovanje mjera uključuje i mjere zajednice koje se u određenom sektoru zahtijevaju (spisak tih mjera), ili se odnose na one koji moraju da imaju plan slični ili ekvivalentan OSP i nadzor od strane nadležnog organa takvog plana.

Obaveza države je :

- određivanje koliko i kada treba da se kontroliše i pravilno održava sistem zaštite CI;
- kada je potrebno da se pokrene formalno ažuriranje sistema zaštite CI;
- donošenje, primjena i provjera odgovarajućih mjera bezbjednosti i pravila za zaštitu tajnosti informacija i planova sistema zaštite CI i DBT;
- pružiti pristup najboljim praksama i metodologijama u vezi sa zaštitom kritične infrastrukture ,
- podržavaja aktivnosti u vezi obuke i razmjene novih tehničkih informacija

Vlasnici/operateri treba da redovno izvještavaju rizicima, prijetnjama i ranjivostima sa kojima se suočavaja CI, a za ECIdržava je dužne da to prijavi Komisiji svake dvije godine. Potreba za dodatnim mjerama zajednice za zaštitu ECI će se procijeniti na osnovu tih izveštaja i pružitipodrška vlasnicima / operaterima CIS.

6. Zaključak

Globalna bezbjednost se promijenila. Nove složene opasnosti su prisilile mnoge države da ponovo razmotre svoje nacionalne strategije bezbjednosti. Ove promjene zahtijevaju od država ne samo da se koncentrišu na odbranu od neposrednih opasnosti ili kriminalnog djelovanja, već da se usredsrijede na preventivne mjere bezbjednosti kao neophodnost za zaštitu kritične infrastrukture.

Sa porastom pružanja javnih usluga od strane privatnih subjekata, granica između javnih institucija i privatnih subjekata/ korporacija, postaju zamagljene u određenim oblastima javnih usluga. Najočitije se to vidi u oblasti CI. Da bi društvo na vrijeme spriječilo ovakve pojave i tendencije, ono mora insistirati na egzaktnoj, empirijski identifikovanoj procjeni mjera, koje su neophodne za njegovu zaštitu. Odatle proizilazi da je društvo pozvano, kada je riječ

o društveno opasnim ponašanjima i radnjama, da i dalje razvija kaznenopravne instrumente u okviru svoje politike, instrumente koji opravdano služe i ciljevima zaštite.[221] Svaki od sistema CI je složen i izazovan sam po sebi, ali razne međuzavisnosti između njih komplikuju stvari još više. Međuzavisnosti mogu izazvati teško predvidive-kaskadne efekte koji mogu povećati uticaj neuspjeha i njegove posledice na društvo. Zbog toga, su potrebne odgovarajuće metodologije da pomognu da se odrede prioriteti i investiraju oskudni resursi i sprovedu racionalne strategije za zaštitu CI, na osnovu objektivnog i dinamičkog modeliranja, simulacije i analize.

Da bi vlasnik /operater mogao da ima sopstveni OSP, država mora da razvije sveobuhvatan nacionalni plan za obezbjeđivanje ključnih resursa i kritične infrastrukture,kao i fizičkih i tehnoloških sredstva koja podržavaju takve sisteme ipreporuči mjere za zaštitu ukoordinacija sa drugim lokalnim vlastima, privatnim sektorom, i drugim subjektima

Organi operatera zaduženi za zaštitu moraju da poznaju finansijske, operativne i bezbjednosne uticaje određenih mjera koje mogu da utiču na zaštitu, a samim tim i na podjelu odgovornosti za mjere bezbjednosti između operatera i drugih subjekata.

Na osnovu toga nacionalnog plana i preporučenih mjera se radi OSP sa svim specifičnostima i prijetnjama koje su karakteristične za konkretnu CI.U zavisnosti od DBT, specifičnosti i prijetnji koje su karakteristične za konkretnu CI projektujusestalne mjere bezbjednosti.

Stepenovane mjere bezbjednostisu određene u skladu sa nivoom rizika i prijetnji koje prevazilaze mogućnosti stalnih mjera zaštite predviđenih za osnovni nivo prijetnji. Svakim nivoom je određeno ko je odgovoran za proglašenje mjera i pokretanje odgovora na prijetnjePostupak odgovora mora se odvijati u skladu sa OSP i u skladu sa situacijom na terenu.

U OSP moraju postojati posebne procedure ili zadatci za snage odgovora, jer moraju da djeluju na jasnim osnovama i pravilima angažovanja. U tom odgvoru na prijetnje zajedničke su obaveze države i samih operatera/vlasnika. Za ublažavanja posledica nastalih kao rezultat prirodnih katastrofa država i objekti CI treba da izrade planove za reagovanje na vanredne situacije. Ovi planovi treba da se redovno testiraju i ocjenjuju.

Svaka država članica će osigurati da je OSP ili ekvivalent napravljen i redovno pregledan u roku od jedne godine. Poštovanje mjera uključuje i mjere zajednice koje se u određenom sektoru zahtijevaju (spisak tih mjera), ili se odnose na one koji moraju da imaju plan i nadzor od strane nadležnog organa takvog plana.

Obaveza države je određivanje koliko i kada treba da se kontroliše i pravilno održava sistem zaštite CI;kada je potrebno da se pokrene formalno ažuriranje sistema zaštite CI; donošenje, primjena i provjera odgovarajućih mjera bezbjednosti i pravila za zaštitu tajnosti informacija i planova sistema zaštite CI i DBT;pružianje pristupa najboljim praksama i metodologijama u vezi sa zaštitom kritične infrastrukture; podržavanje aktivnosti u vezi obuke i razmjene novih tehničkih informacija.

Vlasnici/operateri treba da redovno izvještavaju o rizicima, prijetnjama i ranjivostima sa kojima se suočavaja CI, a za ECI država je dužne da to prijavi Komisiji svake dve godine. Potreba za dodatnim mjerama zajednice za zaštitu ECI će se procijeniti na osnovu tih izveštaja i pružiti podrška vlasnicima / operaterima CIS.

Prilikom pravljenja OSPza CI treba: implementirati međunarodne norme, koristiti što je moguće više iskustva drugih sličnih sistema CI, odrediti najgore scenarije, obučiti/kvalifikovano osoblje za utvrđivanje rizika, simulirati scenarija koja uključuju sve elemente (fizičku zaštitu, snage za odgovor, i upravljačku strukturu), napraviti nivo rizika na osnovu informacija o vjerovatnoći napada ili dešavanja.

Za procjenu efektivnosti sistema zaštite CI neophodno je koristiti pristup koji se zasniva na punom DBT, koršćenju masimalne snage i najbolje strategije i scenarija po sistem zaštite, sa podacima o performansama tog sistema.

Efikasan sistem zaštite CI mora da sadrži element "odgovora". U tom odgvoru na prijetnje zajedničke obaveze države i samih operatera/vlasnika su:

- provjeru pouzdanosti osoblja uključenog u zaštitu i snage za odgovora (bezbjednosnu provjeru);
- integrisani plan odgovora(definiše odgovornost za sprovođenje i komunikaciju tokom odgovora);

221 Radoslav Gaćinović, ***Terorizam u političkoj i pravnoj teoriji***, Evro-Giunti, Beograd, 2010.

- stalne vježbe za potvrdu spremnosti za odgovor na vanredne situacije(definisane kriterijume uspješnosti i izvršenja, simulacije, i višestruko sprovođenje vežbi).
- redovna obukasa programom obuke zasnovanom na prijetnjama koje su definisane u OSP.

Snage za odgovor moraju da mogu da kompenzuju neke nedostatke u drugim karakteristikama zaštite CI.

Za ublažavanja posledica nastalih kao rezultat prirodnih katastrofa država i objekti CI treba da izrade planove za reagovanje na vanredne situacije. Ovi planovi treba da se redovno testiraju i ocjenjuju.

U zaštiti kritične infrastrukture, odgovornost za postavljanje ciljeva zaštiteje prvenstveno na državi, ali sprovođenje koraka za smanjenje ugroženosti privatnog vlasništva i korporativnih sredstava zavisi prije svega od znanje i aktivnosti privatnog sektora. Današnji sistem zaštite kritične infrastrukture sastoji se od bezbroj entiteta.[222] Iako privatne firme razumiju svoje poslovanje i opasnosti koje idu uz to poslovanje, jasno je da oni trenutno nemaju adekvatan

podsticaj za finansiranje smanjenja ugroženosti. Za mnoge, troškovi smanjenja ranjivosti idu u korist smanjenja rizika od prirodnihi drugih nesreća.[223]

Država treba obezbijediti pravne, ekonomske, poreske i druge olakšice u oblasti zaštite CI. Te podsticaje treba pratiti i strog zakonski okvir koji se odnosi i na državu i na strukovna udruženja. Cilj je da se motivišu svi subjekti (vlasnici i korisnici) CI da nastave jačati svoje potencijale u njenoj zaštiti. Efikasna zaštita za kritične infrastrukture zasniva se na holističkoj i strateškoj procjeni rizika i prijetnji na svim nivoima kao osnov sveobuhvatne zaštite. Zato se partnerstvo javnog i privatnog sektora čini od suštinske važnosti.

Literatura

Brunner, E. M., Suter, M., ***International Critical Information Infrastructure Protection Handbook***, Center for Security Studies, ETH Zurich, 2009

Cornelis, B., ***Federal Risk Inventory***, ***Survey and Knowledge Building***, SPIRAL, Liège, 2004.

Crisis and Risk Network, ***Critical Infrastructure Protection***, Center for Security Studies (CSS), ETH Zürich, 2009

Development, Use and Maintance of the Design Basic Threat, IAEA Nuclear Security Series No. 10, IAEA, Austria, 2009.

DIREKTIVA VIJEĆA 2008/114/EC od 8. decembar 2008

Homeland Security Act of 2002

Kenneth C. Watson, PRIVATE-SECTOR PREPAREDNESS IN CRITICAL INFRASTRUCTURE PROTECTION, Ad Hoc Committee on State, Local and Private Sector Preparedness and Integration, Washington, D .C. July 12,2007

Maliszewski P.J., ***Modeling Critical Vaccine Supply Location: Protecting Critical Infrastructure and Population in Central Florida***, Florida State University College of Social Sciences, 2008.

Philip AUERSWALD, Lewis M. BRANSCOMB, Todd M. LA PORTE, Erwann MICHEL-KERJAN. The Challenge of Protecting Critical Infrastructure, Center for Risk Management and Decision Processes, Working Paper # 05-11, October 2005

Radoslav Gaćinović, ***Terorizam u političkoj i pravnoj teoriji***, Evro-Giunti, Beograd, 2010.

The Physical Protection Objectives and Fundamental Principles (GOV/2001/41/ Attachment), IAEA, Vienna, 2001.

The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/ 225/Rev. 4 (corrected), IAEA, Vienna, 1999.

The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/ 225/Rev. 4 (corrected), IAEA, Vienna, 1999.

US Department of Homeland Security, What Is Critical Infrastructure?, http:// www.dhs.gov/critical-infrastructure; U.S. Office of Homeland Security, The National Strategy for Homeland Security. July 16, 2002.

222 Kenneth C. Watson, PRIVATE-SECTOR PREPAREDNESS IN CRITICAL INFRASTRUCTURE PROTECTION, Ad Hoc Committee on State, Local and Private Sector Preparedness and Integration, Washington, D .C. July 12,2007

223 Philip AUERSWALD, Lewis M. BRANSCOMB, Todd M. LA PORTE, Erwann MICHEL-KERJAN. The Challenge of Protecting Critical Infrastructure, Center for Risk Management and Decision Processes, Working Paper # 05-11, October 2005

CRITICAL INFRASTRUCTURE PROTECTION – ROLE & RESPONSIBILITIES

Abstract Events that characterize contemporary international relations have influenced and led to an increase in the number of challenges and security threats with a high degree of uncertainty, unpredictability and discontinuity. Most states today depend on critical infrastructure (CI), which is the backbone of the national economy, security and progress, and strive to provide an efficient and effective response to modern threats such as terrorism, organized crime, conflict, natural disasters and accidents, or computer crime, especially in the context of emergency situations. Each state, region, or individual CI facility are responsible for identifying threats from which they are trying to protect themselves. The Council Directive 2008/114 / EC of 8 December 2008 for the identification and determination of the European Critical Infrastructure, and the assessment of the need to improve their protection, Article 5, predicts the obligation of existance of the Operator Security Plan (OSP). This paper deals with the relationship and roles of the state and the operator/owner in the design, implementation and updating of these plans and measures envisaged in the plans. The aim is to motivate all subjects to strengthen their potential in their protection.

Key words: critical infrastructure, threats to security, threat assessment, emergency situations, operators security plan, protection, responsibility, state, owner/operator