D. Kulišić*

MJERE SIGURNOSTI OD TERORISTIČKIH I INIH ZLONAMJERNIH UGROZA KRITIČNE INFRASTRUKTURE (II. DIO)

UDK 331.45/.48:[323.283:338.49
PRIMLJENO: 2.2.2007.
PRIHVAĆENO: 4.3.2008.

SAŽETAK: Menadžmentima/menadžerima sigurnosti, obrane i zaštite skreće se pozornost na raspoložive pristupe u osiguranju, obrani i zaštiti sastavnica i sustava kritične infrastrukture na nacionalnoj, lokalnoj i transgraničnoj razini te ukazuje na iznimnu važnost i sve moguće koristi od sustavno, temeljito i stručno provođenih postupaka integralne raščlambe opasnosti i prosudbe (procjene) naravi i razmjera ugroza/razina rizika od bilo koje vrste ili oblika prijetnje/štetnog događaja, s posebnim težištem na one terorističke, gerilske, organizirano i individualno kriminalne ili ine zlonamjerne naravi, koje se donedavno uopće nije ni pokušavalo podrobnije sustavno razmatrati – poglavito ne kompleksnijim i sofisticiranijim temeljitim analitičkim pristupima i pouzdanijim analitičkim alatima. Polazeći, među inim, i od aktualnih zahtjeva definiranih Pravilnikom o metodologiji za izradu procjena ugroženosti i planova zaštite i spašavanja (Narodne novine, br. 20/06.), prikazan je načelan slijed i opće sastavnice tog postupka te glavni opći elementi za stručne prosudbe pogibelji od eventualnih terorističkih djelovanja s motrišta njihovih: ciljeva, počela, meta i inačica taktike napada te raspoloživih specifičnih modusa operandi, od iznimne važnosti za učinkovitu kontrolu izravno prijeteće ili nastale pogibelji te za djelotvorno i ekonomično upravljanje integralnom sigurnošću, obranom i zaštitom elemenata i cjelina objekata kritične nacionalne, lokalne i transgranične infrastrukture od svih vrsta i oblika realno mogućih opasnosti i ugroza. Tako kompleksnim pitanjima i zadaćama odgovarajuća razina društvene, specifične ustrojstvene i individualne sigurnosne kulture, uz adekvatno stimulirane odgovarajuće ljudske i potrebama primjerene materijalne resurse, čine «condicio sine qua non» realnih izgleda za uspjeh.

Ključne riječi: *kritična infrastruktura, integralna sigurnost, terorizam, visokosofisticirani kriminal, organizirani kriminal, velike nesreće, raščlamba opasnosti, prosudba ugroze/rizika, opća sigurnosno-obavještajna pitanja, razine sigurnosne i zaštitne kulture, upravljanje integralnom sigurnošću, obranom i zaštitom*

OPĆI MODELI PRISTUPA RAZVOJU I PROMICANJU KAKVOĆE SIGURNOSTI

Među prve, vrlo zapažene, sustavne i stručno podrobno argumentirane, kritičke raščlambe dotadašnje pasivne naravi i nefleksibilnog (za razvoj tehnologije i uvođenje suvremenijih – možebitno kvalitetnijih, trajnijih i jeftinijih – materijala građenja i uređenja prostora ograničavajućeg), preširoko i predetaljno preskriptivnog načina oblikovanja britanskih propisa i normi o građenju, s motrišta specifičnosti sustava sigurnosti i zaštite građevina od požara i eksplozija, dali su *Shields, T.J. i Silcock, G.W.H.* već 1987. g.

* Mr. sc. Damir Kulišić, dipl. ing. kemije, viši predavač Visoke policijske škole (u sklopu Policijske akademije MUP-a RH), Av. Gojka Šuška 1, 10000 Zagreb, dkulisic@fkz.hr, tel.: + 385 1 23 91 351, faks: + 385 1 23 91 415.

Slika 9. Zabrinjavajuće značajke suvremenog terorizma i u oružanom nasilju djelatnog dijela organiziranoga kriminala

Figure 9. Worrying aspects of modern terrorism and armed violence practised by organised crime

Malo prije, u nas je preglednim radom ovog autora[1] ukazano na prednosti i nedostatke raspoloživih suvremenih kvalitativnih i kvantitativnih pristupa, metoda i tehnika rada u raščlanjivanju opasnosti i prosuđivanju ugroza/rizika od štetnih pojava i događaja u područjima sigurnosti i zaštite od požara, eksplozija i tehnoloških havarija, zaštite na radu, zaštite okoliša, tjelesne i tehničke zaštite i zaštite od elementarnih nepogoda. Spomenuti i ini kasniji[2] kritički osvrti na tradicionalne i raspoložive suvremene modele pristupa, kako u promicanju razvoja gospodarstva i tehnologije, zatim u vrlo specifičnim i vrlo važnim segmentima područja sigurnosti i zaštite od požara, eksplozija itd. tako i u smislu mogućnosti prispodobnog sagledavanja i raščlanjivanja naravi pristupa razvoju svekolikoj suvremenoj sigurnosti, obrani i zaštiti, posebice od suvremenih vrsta i oblika ugroza kao što je suvremeni (poglavito sofisticirani i oružano djelatan) organizirani kriminal te samoumorstveni i high–tech terorizam (vidi sliku 9),[3] aktualni su i danas – na najširem planu opće i nacionalne sigurnosti, poglavito kada se u vidu ima sve vrlo osjetljive i vrlo ranjive sustave kritične nacionalne, transgranične, regionalne i šire infrastrukture.

Posebno zabrinjavajuće značajke suvremenog terorizma i u oružanom nasilju djelatnog dijela organiziranoga kriminala su: iznimno širok izbor, na crnom tržištu relativno vrlo lako dostupnog, konvencionalnog vojnog i policijskog oružja i opreme;[4] skoro neograničen izbor gotovo svih nekonvencionalnih vrsta oružja (zasad, s iznimkom samo atomskog oružja male i velike razorne moći), uglavnom improvizirane izrade; prije predočen, nezamislivo širok spektar mogućih modusa operandi (načina izvedbe) napadajnih akcija i operacija[5] i zastrašujuća sofisticiranost (tehnička inovativnost, preciznost i teško izbježiva pogibeljnost) ili brutalnosti (spektakularno masovna smrtonosnost i vrlo opsežna razornost) megabombaških te nekih izvedenih ili planiranih kemijskih, bioloških i inih vrsta nediskriminiranih atentata oružjima za masovno ubojito i za širi okoliš vrlo pogibeljno (i dugotrajno škodljivo) djelovanje (*Kulišić, 2007., 2006., 2005.*).

Deskriptivan (opisni) model pristupa

Ovaj model polazi isključivo od opisa značajki iskustava aktualne prakse i opisa značajki aktualnih rješenja retrospektivno identificiranih sigurnosnih, obrambenih i zaštitnih problema u sklopu promatranog sustava svekolike ili specifične vrste ili oblika sigurnosti, obrane i zaštite, odnosno od opisa značajki postojećih vrsta i oblika ciljeva, zadaća, ustroja, snaga, objekata,

[1] Kulišić, D., Analiziranje opasnosti i procjenjivanje ugroženosti u nekim područjima društvene samozaštite, ONO i DSZ Informator, 11 (1986) 65 -105.

[2] Vidi radove akademika Paar, V. i inih znanstvenika na temu linearnih i, posebice, nelinearnih sustava podložnih kaotičnim promjenama te radove brojnih autora koje je zbornički priredio i uredio prof. dr. sc. Juraj Božićević, 2000. i 2001. g. u sklopu naklada HATZ (Hrvatske akademije tehničkih znanosti).

[3] Značajke high–tech terorizma ili tehno-terorizma vidi, primjerice, u Kulišić, D., 1997., str. 120-123.

[4] Pa čak i posebnih vrsta oružja i opreme za posebne vojne, oružničke (žandarmerijske), policijske i ine redarstvene, diverzantske, protudiverzantske i protuterorističke postrojbe, a ponekad i posebnih vrsta oružja i opreme ukradenih ili potajice isporučenih iz posebnih radionica bojno djelatnih odjela posebne namjene vojnih i civilnih tajnih – sigurnosnih, obavještajnih i protuobavještajnih – službi.

[5] Uz izravnu i neizravnu potporu vrlo dobro prikrivene i u međusobnim odnosima i vezama vrlo zamršene, financijski, tehnički, obavještajno, nerijetko i politički, vrlo moćne međunarodne, inozemne i tuzemne logistike – tako da je nerijetko zaista iznimno teško utvrditi tko je, zapravo, stvarni naručitelj, nalogodavac ili pokrovitelj njihovih zlodjela.

procesa, tehnologija, taktika postupanja, metoda i tehnika rada, kao i od opisa značajki pojedinih sastavnica postojećih proizvodnih, transportnih, komunikacijskih, trgovinskih ili inih vrsta procesa, materijala, proizvoda ili usluga, kao osnovice za budući razvoj.

Drugim riječima, dojučerašnja, više ili manje zadovoljavajuća, opća i posebna sigurnosna, obrambena i zaštitna rješenja se rabe za sučeljavanje s nastupajućim i budućim problemima takve ili ine (možebitno tek naslućujuće ili posve nepoznate) naravi i za njihovo prevladavanje, bez dovoljno promišljenog uzimanja u obzir mogućih različitosti u strukturi i naravi novonastajućih (promjena) promatranih općih ili posebnih sustava, pa ni novonastajućih (promjena) općih i/ili posebnih uvjeta i okolnosti njihova ostvarivanja, funkcioniranja ili primjene.

Svojevrsnu *jezgru* deskriptivnog modela pristupa tvori vrlo kompleksan i, zbog toga, pokatkad visoko *entropičan* (teško uskladiv i u reakcijskom smislu prečesto konfuzan, inertan i nedovoljno djelotvoran) konglomerat relevantnih sastavnica sustava opće i posebne sigurnosti, obrane i zaštite, uobičajeno definiranih, zadanih, ponuđenih, zahtijevanih ili potaknutih odgovarajućim međunarodnim, asocijacijskim i međudržavnim aktima i odlukama te ustavnim, zakonskim, podzakonskim i inim aktima, kao i cijelim nizom relevantnih međunarodnih, asocijacijskih, državnih i internih normi (vidi sliku 10).

Čak i u većini vrlo specifičnih i već tradicionalno etabliranih područja sigurnosti, obrane i zaštite, sadržaj ove *jezgre* se, unatoč bogatom iskustvu, u načelu, relativno vrlo sporo mijenja i relativno vrlo teško prilagođava potrebama koje proizlaze iz pojava suvremenih, već prepoznatih, vrsta i oblika prijetećih pogibelji (vidi prije opisane ili spomenute eklatantne primjere i moduse operandi suvremenog terorizma te organiziranog i individualnog kriminala).

Slika 10. Shematski prikaz naravi deskriptivnog modela pristupa

Figure 10. Scheme showing the nature of the descriptive approach model

Kružnim vijencem simbolično predočeno područje aktualnih iskustava u praksi provedbe tvori vrlo fluidan, znanstveno i stručno nedovoljno ili necjelovito praćen, istraživan ili još neprovjeren, konglomerat stanovitih društvenih, skupnih i individualnih iskustava ili pouka stečenih praktičnom primjenom raspoloživih redovitih i izvanrednih mjera sigurnosti, obrane i zaštite u sučeljavanju s pojedinim tradicionalnim i suvremenim vrstama i oblicima pogibelji, uglavnom u vrlo specifičnim (iznimno rijetko ponovljivim) uvjetima i pod vrlo specifičnim (skoro neponovljivim) okolnostima. Ovo područje, premda s prevelikim kašnjenjem, ipak postupno utječe na stanovite (uglavnom nesustavne, parcijalne i kratkodometne) koncepcijske, doktrinarne, ustrojstvene i ine nužne intervencije u dotad neupitne sadržaje jezgre.

Derivativan (izveden) model pristupa

Ovaj model pristupa polazi od pomno planiranog i organiziranog te kontinuirano logistički podupiranog sustavnog, (više) timskog i usklađenog multidisciplinarnog/interdisciplinarnog, kontinuiranog znanstvenog i stručnog promatranja, raščlanjivanja i proučavanja integralne naravi i sadržaja cjeline sustava globalne, međunarodne,

regionalne, nacionalne i interne sigurnosti, obrane i zaštite te specifičnih značajki sastavnica i sadržaja svih posebnih područja koja tvore takav sustav i mogućih uzajamnih utjecaja i posljedica učinaka pojava različitih vrsta, oblika i intenziteta kontinuiranih ili diskretnih interreakcija u sklopu pojedinih područja i cjeline (razmotri sastavnice uvodno, u I. dijelu članka predočene slike 1).

Ovaj model se može razviti, predočiti i sustavno raščlanjivati u odgovarajućem matričnom obliku, tj. putem matrice mehanizama uzajamnih djelovanja, putem: vektora ciljeva u odnosu na plan djelovanja; matrice taktike u odnosu na ciljeve; vektora taktike u odnosu na plan djelovanja; matrice sastavnica u odnosu na taktiku; matrice sastavnica u odnosu na plan djelovanja

Slika 11. Derivativni model pristupa
Figure 11. Derivative approach model

Zbog toga je takav pristup daleko temeljitiji, logistički i intelektualno znatno zahtjevniji, ali je i po ciljevima, kakvoći i dometima učinaka puno širi, odnosno daleko pouzdaniji, djelotvorniji i razvojno dugoročno isplativiji i korisniji (vidi sliku 11).

Na osnovi takvog modela pristupa moguće je razviti stanovite alternativne koncepcije i, u sklopu njih/odabranih, više alternativnih strategija, odnosno niz pogodnih alternativnih ili pojedinih optimalnih rješenja.

i matrice uzajamnih djelovanja, što konačno rezultira razvrstavanjem sastavnica prema prinosu postizanju plana djelovanja.

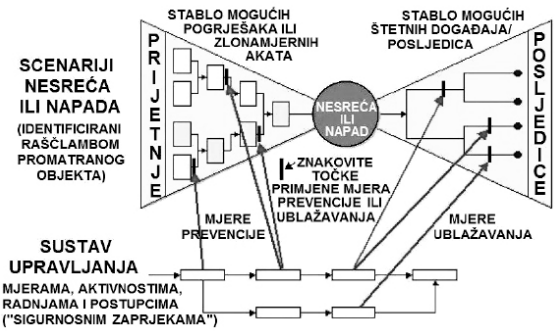
RASPOLOŽIVI ALATI ZA RAŠČLAMBU OPASNOSTI I PROSUĐIVANJE UGROZE ILI RIZIKA

Iz svega predočenog je razvidno kako je vrlo temeljito poznavanje:

- ponajprije, značajki svih realno mogućih vrsta i oblika posve slučajnih nesreća ili nezgoda,
- potom, objektivno mogućih uvjeta i okolnosti za njihovu pojavu,
- realno mogućih scenarija načina njihova iniciranja, razvoja i zbivanja te
- bitnih obilježja njihovih realno mogućih opasnih učinaka i posljedica (vidi slike 3 – 6 i 8 predočene u I. dijelu članka te slike 14 - 16), kao i
- opasnosti od mogućih izvedbenih inačica eventualnim organizirano kriminalnim, terorističkim, ekstremističkim ili inim razlozima motiviranih napada (uključujući stadije organizirano kriminalnog operativnog planiranja, pripreme, izvedbe i prikrivanja počinitelja i pomagača takvih vrsta napada), a pritom i
- stvarnih vlastitih mogućnosti i sposobnosti pravodobnog uočavanja i prepoznavanje (što većeg broja), već prvih, indicija možebitnog zbivanja onih djelovanja i aktivnosti koje možebitno upućuju na realnu mogućnost od terorističkog ili inog ekstremističkog ili zločinačkog napada,

ključ i, ujedno, *condicio sine qua non* realnih izgleda za osiguranje konačnog uspjeha u suzbijanju eventualnih pokušaja terorističkih i inih zločinačkih djelovanja, kao i za izgradnju svim realnim pogibeljima primjerenog sustava djelotvornog integriranog upravljanja sigurnošću dijelova i specifičnim cjelinama sustava iz područja kritične nacionalne i lokalne infrastrukture (vidi donji dio slike 6 u I. dijelu članka i a. dop. sliku 12 – *Pitbaldo, Smith, 2000.,* str. 11).

Osim toga, nedvojbeno je i to kako, općenito gledajući, svi korisni učinci od sveobuhvatnih stručnih raščlambi opasnosti i prosudbi ugroza/rizika, kako od nesreća tako i od terorističkih pogibelji i inih zlonamjernih djelovanja, za objekte kritične nacionalne i lokalne infrastrukture, kao i od odgovarajućeg upravljanja prepoznatim opasnostima primjerenim spektrom generativnih/inherentnih, proaktivnih i reakcijskih **AT, PT, AK i PK** mjera i aktivnosti (vidi slike 6, 11, 12 i 13), mogu doći do punog izražaja samo onda ako se ti postupci rabe u svim stadijima ili segmentima razvoja i funkcioniranja sigurnosno zanimljivog (pod)sustava, procesa ili aktivnosti – već od trenutka njihova idejnog kreiranja/nastanka, pa do konca (njihova nestanka, prestanka, gašenja ili gubitka statusa kritičnosti). Pritom se najsloženije vrste raspoloživih analitičkih (kvalitativno-) kvantitativnih metoda i tehnika raščlambe preporuča primjenjivati gdje god i kada god za to ima objektivnih potreba, mogućnosti i uvjeta.



Slika 12. Načelan prikaz počela kvalitativno–kvantitativnog definiranja realno mogućih scenarija, ***posljedica i utjecaja sigurnosnih zapreka*** *nesreća ili zločinačkih napada (vidi dalje i sliku 13)*

Figure 12. General concepts underlying the qualitative and quantitative definitions of possible ***scenarios, consequences*** *and* ***effects of safety measures*** *in accidents or criminal assault (see further on and figure 13)*

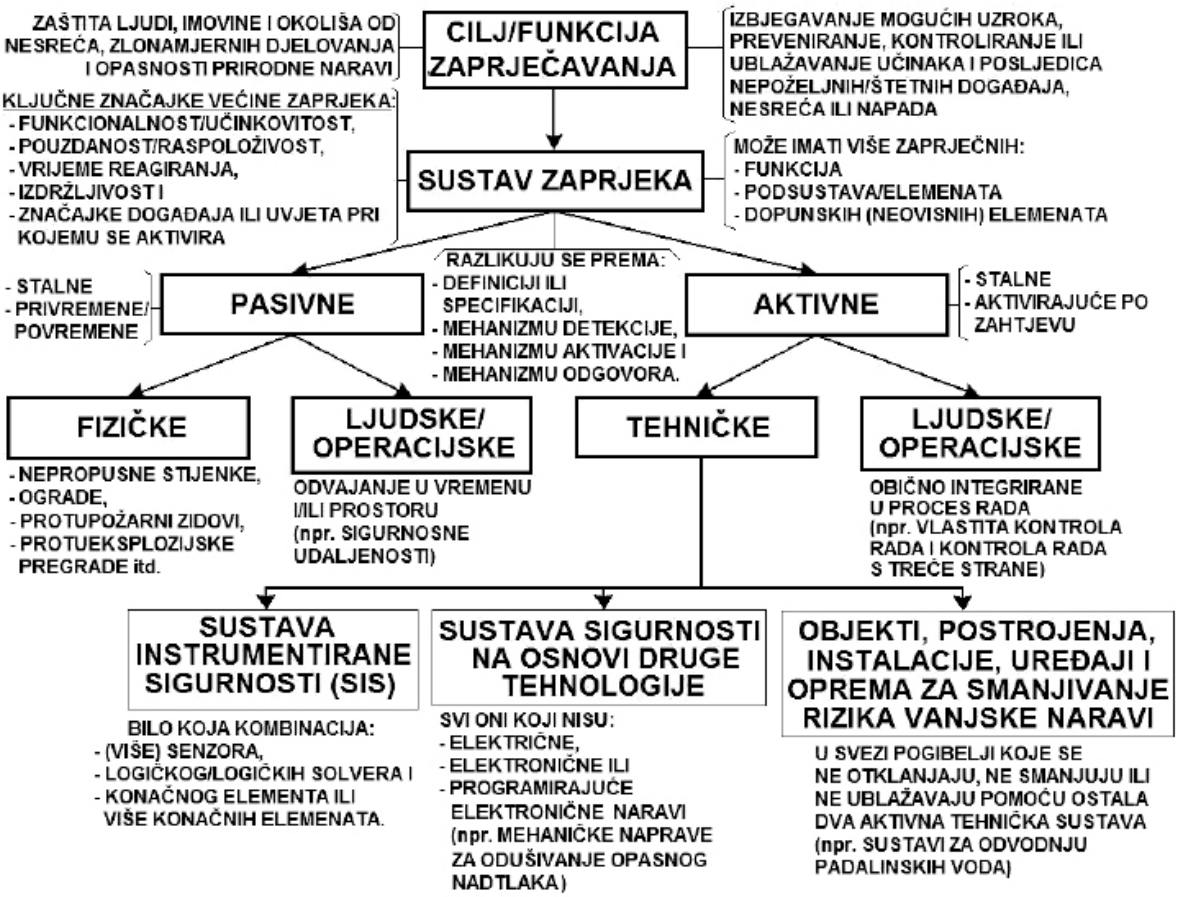
Izbor analitičkih pristupa, metoda i tehnika za raščlanjivanje opasnosti i prosuđivanje ugroženosti mora biti primjeren značajkama promatranog dijela raščlanjivanog kritičnog sustava, procesa ili aktivnosti, u svim možebitnim uvjetima i okolnostima njegova funkcioniranja/zbivanja (vidi sliku 14); (a. dop. prikaza prema *Dziubin´ski, M., Fratczak, M. i Markowski, A.S., 2006., str. 400*).

Zato se preporuča, kada god je to moguće, kombinirana primjena nekoliko pogodnih metoda i tehnika, a posebice izvedba prispodobnih provjera rezultata primjene svih onih, previše krutih ili jednoobraznih, jednom rječju univerzalnih «metodika/metodologija» koje su, navodno, pogodne za vrlo širok spektar vrsta predmeta raščlambe i prosudbe njihovih kritičnih značajki.

Kako je svakom promatranomu sustavu, procesu ili aktivnosti svojstven samo ograničen broj vrsta i oblika realnih opasnosti, one se mogu uspješno identificirati samo u onoj mjeri u kojoj ih tim službeno angažiranih analitičara poznaje i prepoznaje (vidi neke znakovite načelne primjere u slikama 15 i 16).

Što nam je više detalja o ključnim obilježjima sigurnosno zanimljivih sustava, procesa, operacija ili aktivnosti poznato, to se aktualno raspoložive suvremene metode i tehnike, kao alati za raščlanjivanje opasnosti i prosuđivanje značajki razmjera mogućih ugroza ili razina rizika, mogu djelotvornije primijeniti poradi lakšeg i pouzdanijeg lociranja svih onih kritičnih mjesta gdje se nalaze potencijalni uzroci nesreća ili inih štetnih događaja, bez obzira na mogući način njihova iniciranja, pa tako i od terorističke ili ine zlonamjerne ruke.

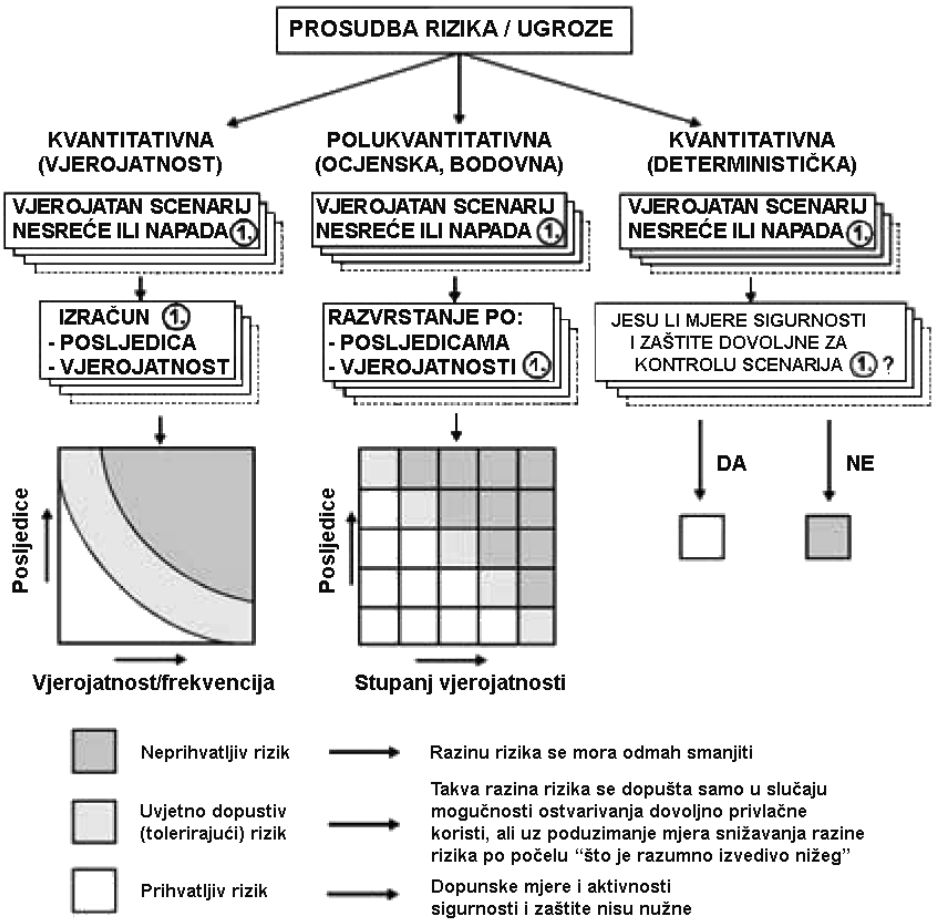
Na slici 13 prikazana su ključna obilježja i sustav raznovrsnih zapreka (barijera) razvoju pogibeljnih pojava ili štetnih događaja koji mogu rezultirati nesrećama ili težim posljedicama zlonamjernih/terorističkih djelovanja (a. kom. dopunjen prikaz prema: *Sklet, S., 2006., str. 502.*).[6]



Slika 13. Ključna obilježja i jedan od mogućih načina općeg razvrstavanja raspoloživih sustava raznovrsnih zapreka
Figure 13. Key features and one of the possible ways of classifying the available systems

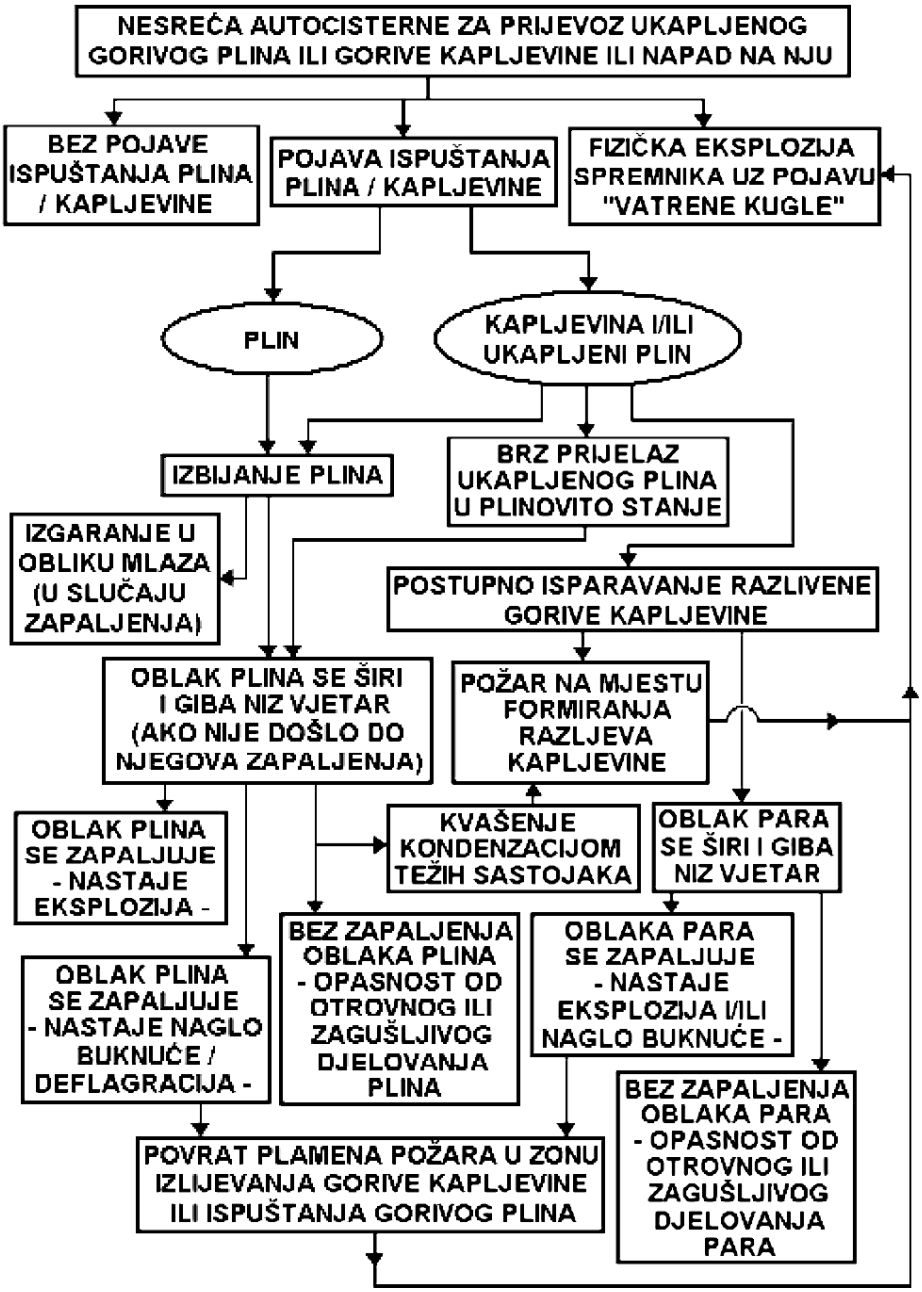
Kako kakvoća rezultata svake od kvalitativnih i kvantitativnih raščlambi opasnosti i prosud-

[6]Prema: Sklet, S., Safety barriers: Definition, classification, and performance, Journal of Loss Prevention in the Process Industries, 19 (2006) 494–506.



Slika 14. Opća podjela skupina metoda i tehnika za prosudbu mogućih razina rizika
Figure 14. General classification of methods and tools for the assessment of possible risk levels

bi rizika ovisi o ispravnosti pristupa i pravilnosti provedenih postupaka, kao i o pouzdanosti (točnosti) potrebnih podataka i širih informacija o načinima, uzrocima (odnosno modusima operandi), uvjetima i okolnostima nastajanja (odnosno zlonamjernog izazivanja) štetnih pojava i događaja, to se sve više intenzivira pitanje – praksi prevencije primjerenog – poboljšanja pouzdanosti analitičkih metoda i tehnika. Naravno, a time i uporabne vrijednosti njihovih rezultata, ponajprije poboljšanjem procedure te strukture i sadržaja obrazaca po kojima pojedina nacionalna i međunarodna tijela i organizacije u pojedinim područjima sigurnosti, obrane i zaštite (od požara i eksplozija, na radu, okoliša, od elementarnih nepogoda, tjelesne i tehničke zaštite, od terorizma, ekstremizma, organiziranoga ili individualnog kriminala itd.) organizirano prikupljaju, stručno selekcioniraju te kvalitativno i (polu)kvantitativno obrađuju i tumače, a potom pohranjuju i distribuiraju sve one podatke iz područja od interesa za takve raščlambe i prosudbe. Na slici 15 dan je primjer mogućih scenarija razvoja potencijalnih vrsta i oblika opasnosti od nesreća autocisterni (ili vagoncisterni) za prijevoz ukapljenog, stlačenog ili otopljenog gorivog plina ili lakozapaljive gorive kapljevine, ili za slučaj eventualnog zločinačkog pokušaja napada na njih, koje se mora uzeti u obzir i pozorno razmotriti prilikom raščlambi opasnosti za svaki takav elemenat kritične lokalne, nacionalne i/ili transgranične infrastrukture te za sve realno moguće prisutne visoko/dovoljno vrijedne i vrlo ranjive sadržaje u njihovu okružju – počevši od



Slika 15. Primjer realno mogućih scenarija razvoja nesreća autocisterni (ili vagoncisterni) za prijevoz ukapljenog gorivog plina ili gorive kapljevine

Figure 15. Possible accident scenarios for lorry cisterns or train cisterns carrying LPG, or leak accidents

trenutka nastanka eventualne nesreće ili izvedbe zločinačkog napada – sukladno desnom dijelu slike 12 (*a. dop. prema CCPS, 1989.*).

Zahvaljujući iznimno brzom razvoju suvremene znanosti i tehnologije, povezanom s pojavom i uočavanjem novih vrsta i oblika opasnosti i ugroza, te sve češćim i ozbiljnijim prigovorima pouzdanosti tradicionalnih modela pristupa, isključivo kvalitativnih, kvalitativno-polukvantitativnih ili kvazikvantitativnih metoda i tehnika prosudbi razina ugroženosti ili rizika od različi-

tih štetnih događaja (poglavito u području ratne i mirnodopske nuklearne tehnologije), pridonijeli su (već tijekom zadnjih tridesetak godina prošlog stoljeća) pronalaženju, usavršavanju i praktičnoj primjeni niza novih, sofisticiranijih vrsta metoda i tehnika rada **determinističkog, vjerojatnosnog** (probabilističkog) i **kombiniranog** (determinističkog i vjerojatnosnog), odnosno **kvalitativnog, kvantitativnog, polukvantitativnog i kvalitativno-(polu)kvantitativnog, pristupa.**

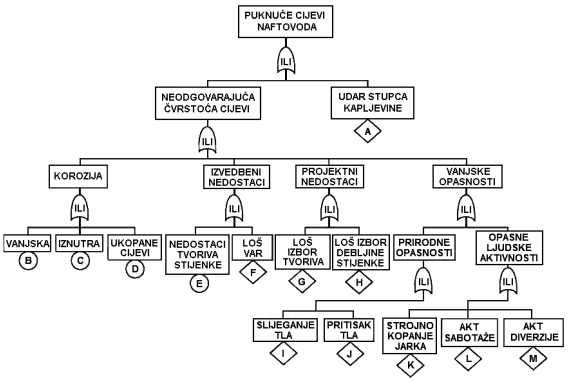
Danas postoji više od 60, zapravo, koliko je autoru ovog rada poznato (na osnovi raščlambe sadržaja dosad publiciranih ili neizravno literaturno opisanih/spominjanih), najmanje 65, metodički – po područjima i po ograničenjima primjene/valjanosti te po vrsti ulaznih i izlaznih podataka – posve različitih ili donekle/vrlo sličnih (ali bitno modificiranih), metoda i tehnika raščlambe opasnosti i prosudbe razine ugroženosti ili rizika. Od tog broja, 38 su determinističkog (25 kvalitativne i 13 kvantitativnih), 9 vjerojatnosnog (3 kvalitativne i 6 kvantitativnih) i 18 kombiniranog determinističkog i vjerojatnosnog tipa pristupa (5 kvalitativnih i 13 kvantitativnih).[7]

Sastoje se od najmanje jednog do najviše tri temeljna stadija postupka:

- **Prepoznavajućeg (identifikacijskog) stadija**, zasnovanog na opisu metodički sustavno raščlanjivanog, potencijalno opasnog i/ili ugroženog, sustava – važnom za konačan izbor i primjenu (kompleta) najprikladnijih metoda i tehnika raščlambe i prosudbe. Njime se utvrđuju sve prisutne, otprije poznate, i prepoznaju sve ostale realno moguće opasnosti koje izviru iz naravi te mogućih uvjeta i okolnosti zbivanja promatranih procesa, operacija, aktivnosti, postupaka i radnji; sve opasnosti u svezi sirovina, poluproizvoda, proizvoda, pomoćnih medija i/ili tvoriva i energenata; sve opasnosti u svezi postrojenja, tehnoloških jedinica, uređaja, instalacija te njihovih sastavnica, relevantnih podsastavnica i njihovih gradiva; sve opasnosti mogućih utjecaja i učinaka iz užeg i šireg procesnog/tehnološkog okružja i okoliša, kao i mogućih utjecaja i učinaka na njih (uključujući moguće vrste, oblike i načine zlonamjernih djelovanja) itd.
- **Prosudbenog (evaluacijskog) stadija** koji omogućuje utvrđivanje vrste, naravi i scenarija razvoja te razmjera mogućih ugroza ili mogućih razina rizika od svakog, utvrđenog kao realno mogućeg, scenarija pojave bilo kojeg od prepoznatih (znakovito specifičnih) štetnih ili škodljivih događaja, koji se mogu razviti i koji mogu, u stanovitim oblicima i razmjerima, ugroziti promatrani sustav. Ovaj stadij može biti izveden dvama načinima pristupa, tj. determinističkim i/ili vjerojatnosnim pristupom.
- **Razvrstavajućeg (hijerarhizacijskog) stadija** koji se provodi poradi što objektivnijeg rangirajućeg razvrstavanja prema rezultatima dobivenim prethodnim stadijima postupka, kako bi se prepoznale, poredale i posebno istaknule bitno prevladavajuće razine svih utvrđenih i međusobno prispodobljavanih vrsta, oblika i razmjera ugroze ili razine rizika. Zahvaljujući ovom stadiju, svi objektivno gorući problemi sigurnosti, obrane i zaštite mogu se odmah jasno prepoznati i, potom, objektivnim redoslijedom žurnosti i zahvata početi otklanjati (uklanjati, mijenjati, premještati, izolirati, izbjegavati, ugovorno prenositi na druge subjekte) ili barem do prihvatljive mjere (tj. razine rizika) ublažavati ili kontrolirati.

[7]Uočljivo bitno prevladavajući broj svih donedavno razvijenih metoda **determinističkog tipa** je posljedica stalnih, već tradicionalnih interesa i težnji tvrtki u svim, glede ljudskih gubitaka i materijalnih šteta, vrlo rizičnim granama gospodarstva i u nekim inim djelatnostima, a poglavito u osiguravateljskom sektoru, kao i u sklopu nadležnih državnih tijela i njihovih službi upravnog nadzora, da ponajprije pokušaju kvantificirati lako moguć broj vjerojatnih žrtava, razmjere mogućih izravnih i neizravnih materijalnih šteta i gubitaka te inih gospodarskih/financijskih i eventualnih društvenih posljedica – za slučaj moguće nesreće, i prije nego li se uopće pokušalo istražiti i razumijeti zašto i kako se zapravo promatrane vrste i oblici nesreća uopće mogu događati i na koje sve načine se to može, dovoljno djelotvorno, (skoro) posve izbjeći.

Neke od tih metoda i tehnika (one najsuvremenije), zahvaljujući uporabi (super)računala i odgovarajućoj programskoj potpori te sve kvalitetnijim (sveobuhvatnijim, popunjenijim, selektivnijim, vjerodostojnijim) internim i eksternim bazama podataka, odnosno zahvaljujući sve savršenijim ekspertnim programima[8] i neprestance razvijajućim/usavršavajućim ekspertnim sustavima iz problematike svekolike, skupno problemske ili specifične sigurnosti, obrane i zaštite, u stanju su dati pravodoban odgovor o (istodobnom) riziku pojave jednog i više štetnih događaja, čiji nastanak je uvjetovan cijelim spletom dinamički povezanih (prostorno, vremenski, tehnološki, operacijski i inim uvjetima i okolnostima ovisnih, mogućom reakcijom ljudskog čimbenika uvjetovanih) štetnih pojava i događaja.[9]



Slika 16. Načelan primjer kvalitativne raščlambe mogućih opasnosti od nastanka oštećenja i proboja stijenki cjevovoda naftovoda

Figure 16. Example of a qualitative analysis of possible hazards arising from damage and punctures of oil pipelines

Sve to, kako bi se u opasnim situacijama poduprlo pravodobno i pravilno taktičko i/ili strategijsko odlučivanje, ili automatsko reagiranje, zbog izbjegavanja, otklanjanja ili eliminiranja pogibelji, odnosno poradi preuzimanja nadzora nad eventualno nastalom opasnom pojavom/događajem, njezinim učincima i posljedicama te kako bi se bitno reducirala razina rizika od pojave pogubno pogibeljnih ili težih štetnih i dugoročnije škodljivih posljedica.[10]

[8]Među nekima od najpoznatijih računalnih programa za raščlambe opasnosti i prosudbe rizika, posebice za potrebe industrije ili transporta, su primjerice (abecednim redoslijedom): AIDRAM-CARGO (vidi: http://www. lsa.ethz.ch); ALOHA (vidi: http://www.epa.gov/ceppo/cameo/aloha.htm); ARIPAR (vidi: http://www.jrc.cec. eu.int/mahb/bequar/sub_pages/ARIPAR.htm); AVRIM 2/SAVRIM (vidi: http://www.savrim2000.com); BIS v1.0 (vidi: www.thermdyne.com); BREEZE (postoji najmanje 5 inačica, ovisno o skupinama razmotrivih sigurnosnih, prevencijskih i zaštitnih problema – vidi: http://www.breeze-software.com/); CALPUFF View v1.5 (vidi: http://www.weblakes. com); CAMEO (vidi: http://www.epa.gov/ceppo/cameo/what.htm); CHARM v11.0 (vidi: http://ursaustin.urscorp.com/pages/services/information_technology/charm/index.htm); DISMA v3.1 (vidi: http://www.de.tuv.com/de/images/industrial_services/DISMAInfo.pdf); DOMIFFECT (DOMIno eFFECT – vidi internet); DominoXL v2.0 (vidi: http://www.fpms.ac.be); EXPSYS (vidi: internet); ExTool v2.1 (vidi: http://www.swissre.com); FLACS98 (vidi: http://www.gexcon.com/index.php?src=flacs/flacs.html); FRED v4.0/Shepherd Desktop v1.1 (vidi: http://www.shellshepherd.com); GASTAR (vidi: http://www.cerc.co.uk/ software/gastar.htm); Hazard Review Leader v4.1.17 (vidi: http://www.absconsulting.com); LEAK v3.1 (vidi: http://www.dnv.com/software/riskManagement/index.asp); MIDAS (vidi: http://www.absconsulting.com/midas/); NEPTUNE v2.0 (vidi: http://www.dnv.com/software/riskManagement/index.asp); ORBIT v2.4.18 (vidi: http://www.dnvsoftware.com); OSIRIS (vidi: http://www.ema.fr/LGEI/Version%20Francaise/equipe%20risque/ Logiciel%20OSIRIS/PresentOSIRIS.htm); RISKIT (vidi: internet); SLAB View+SLAB 3D View v2.0 (vidi: http://www.weblakes.com); SAFETI (vidi: internet); SAVE (vidi: http://www.save.nl); SEVEX (vidi: http:// www.atmpro.be/software/sevex/sevexsummary.htm); Summit v1.306 (vidi: http://www.dnv.com/software/risk Management/index.asp); THESIS v4.0 (vidi: http://www.absconsulting.com/THESIS/index.html); TORAP (vidi: internet); TOXFLAM (vidi: internet); WHAZAN (vidi: internet) itd. O koncepciji, strategiji i taktici djelovanja te načinima funkcioniranja suvremenih integriranih inteligentnih sigurnosno-obavještajnih/kriminalističko-obavještajnih i analitičkih sustava za predviđanje (preveniranje i pravodobno sprečavanje izvedbe) terorističkih i inih slično organizirano zločinačkih napada vidi više, primjerice, Scheiber, L. B., Hartka, J.E. i Murch, R.S., Defender's Edge: Utilizing Intelligent Agent Technology To Anticipate Terrorist Acts, Institute for Defense Analyses, Alexandria (VA), June 2003. (IDA Document D-2849).

[9]Uključujući posebice one vrlo teških posljedica, a vrlo niske čestine (frekvencije) pojavljivanja, kao što su to pojedine vrste (velikih i katastrofalnih) nesreća ili kao što to u politički tradicionalno stabilnim dijelovima svijeta mogu biti teroristički, opasni obavještajni i organizirano kriminalni ili eventualni ratni napadi *(Brannigan, 1998., Coster, Hankin, 2003., FEMA, 2005., 2002., Herman, 1996., HSE, 2005., Marighella, 2003., Markoff, 2007., Moore, 2006., 2004., Whiteley, 2004., Wilkinson, 1993.).*

[10]S obzirom na uobičajeno vrlo ograničen prostor u sklopu ovakvih znanstvenih i stručnih časopisa, ali i cilj te visoku razinu stručnosti čitalačke publike ovog časopisa, nije bilo moguće – a ni potrebno – upuštati se u opis, područja primjenjivosti te u prednosti, nedostatke i znakovite posebitosti svih vrsta kvalitativnih, polukvantitativnih (racionaliziranih, ocjenskih, bodovnih) i kvalitativno-kvantitativnih metoda i tehnika rada, ekspertnih programa i ekspertnih sustava, koje se danas neprestance aplikacijski interdisciplinarno istražuje, poboljšava i razvija, a potom šire ili uže (ciljano) rabi u mnogim specifičnim područjima ili specifičnim (skupnim) pitanjima sigurnosti, odnosno obrane i zaštite od najrazličitijih vrsta pogibelji i prijetnji, uključujući, naravno, i one terorističke i ine zločinačke naravi. Zato se eventualno manje upućenim čitateljima skreće pozornost na priloženi popis literature, dvije prethodne fusnote i na ine relevantne reference iz ove tematike.

No, unatoč tomu, čini se kako prije (uz sliku 10) opisan tradicionalan i nedovoljno pouzdan *deskriptivan model pristupa* problematici ugroza u sklopu goleme većine suvremenih tehničko-tehnoloških i inih složenih sustava, zanimljivih s motrišta globalne, međunarodne, regionalne, nacionalne ili interne sigurnosti, obrane i zaštite, presporo odstupa pred daleko pouzdanijim, ali i zahtjevnijim, *derivativnim modelom pristupa*. Unatoč, također, već vrlo razvidnom napretku u daljem razvoju, kakvoći i opsegu dizajnerske, inženjerske i tehnološke uporabe niza sofisticiranih kvalitativnih, kvantitativnih i kvalitativno-kvantitativnih analitičkih metoda i tehnika rada u raščlanjivanju opasnosti i prosuđivanju rizika od relevantnih vrsta i oblika slučajnih nezgoda i nesreća tehničke, tehnološke, procesne, operacijske ili postupovne naravi, pa i od onih zlonamjerno izazvanih (aktom sabotaže ili diverzije).[11]

Na slici 16. dan je načelan primjer jednog uvodnog dijela pristupa procesu kvalitativne raščlambe mogućih opasnosti od nastanka oštećenja i proboja stijenki cjevovoda naftovoda, kao eklantantnog primjera kritične nacionalne i transgranične infrastrukture, metodom «stabla pogrješaka» (*a. dop. prema Dziubin´ski, Fratczak, Markowski, 2006.*).

Međutim, pritom se svakako mora priznati kako takvom stanju, u dobroj mjeri, pridonose i stanoviti ponajprije objektivni, ali i subjektivni razlozi koje se nikako ne smije zanemariti i koji se ubrajaju u kategoriju spomenutih *potencijalno ugroženim sustavima svojstvenih i analitički/metodički svojstvenih ograničenja*. Ta ograničenja lako mogu biti, primjerice, sljedeće naravi:

- Nedostatak ili ključno/presudno važne manjkavosti (pravodobno) raspoloživih pouzdanih informacija (analitičkih ulaznih podataka), posebice kada se prelazi na razmatranje pogibelji od mogućih zlonamjernih djelovanja, izravnih i naknadnih učinaka (pogibeljnih interreakcija relevantnih čimbenika) unutar slučajnim štetnim događajem ugroženih ili napadnutih i učincima/posljedicama takvog štetnog događaja ili napada potencijalno ugroženih tehničko-tehnoloških mikro i makro sastavnica ili cjelina sustava.[12]
- Valjanost raspoloživih podataka koja je presudno važna za pouzdanost rezultata primjene metoda i tehnika rada vjerojatnosnog tipa pristupa raščlambama opasnosti i prosudbama rizika.[13]
- Stalno prikupljanje, selekcioniranje, razvrstavanje i ažuriranje svih možebitno relevantnih informacija i specifičnih podataka je, po složenosti i težini posla, pravi rudarski posao koji zahtijeva primjerenu organizaciju, tehniku i tehnologiju rada te vrsno obrazovane izvršitelje, a najčešće oduzima dragocjeno vrijeme ili koči rad tima analitičara koji nastoje svoje raščlambe opasnosti i prosudbe ugroza/rizika provesti pravodobno kako bi i potom poduzete nužne preventivne ili interventne, korektivne ili dopunske mjere i aktivnosti bile, još uvijek, pravodobne i očekivano djelotvorne.
- Što je stanovita analitička metoda ili tehnika općenitija (tj. šire primjenjivija, univerzalnija), to su izgledi za prepoznavanje svih prisutnih čimbenika eventualno znakovitih posebitosti te za sagledavanje

[11]Vidi, primjerice, *Biringer, Matalucci, O'Connor, 2007., Coster, Hankin, 2003., Crowe, 2000., Delvosalle, C. et al., 2006., Dziubin´ski, Fratczak, Markowski, 2006., Jaeger, 2003., Janeš, Čavrak, 2002., Kacian, 1994., Kulišić, 1991., 1990., Kuhn, 1997., Kumamoto, Henley, 1996., Lundin, Jönsson, 2002., Moore, 2006., 2004., Morgan, Henrion, 1990., OSCE, 2004., Pitblado, R. i Smith, 2000., Salvi, Debray, 2006.*

[12]Vidi prije opisanu kompleksnost sadržaja i procedura izvedbi raščlambi opasnosti i prosudbi ugroza/rizika od mogućih pojava i pogibelji, posebice od terorističkih i slično vrlo opasnih vrsta i oblika organizirano kriminalnih i individualnih subverzijskih akata/djelovanja, koje su – bez uspostavljene vrsne sigurnosno-obavještajne infrastrukture i njezine informacijske i analitičke potpore, kao i zakonski jasno reguliranih subjekata, vrsta, načina, oblika i eventualno nužnih ograničenja suradnje koji jamče i osiguravaju djelotvornost međusobne (kako interne tako i eksterne) suradnje svih ključnih sudionika u tom procesu – najčešće nedovoljno pravodobne, posve zakašnjele ili posve promašene.

[13]Nerijetko predstavlja ozbiljan problem pri raščlambama opasnosti i prosudbama rizika, čak i od onih štetnih događaja posve slučajne (akcidentalne) naravi, s kojima se dosad imalo podosta iskustava (temeljito/forenzično ispitanih, uredno dokumentiranih te analitički podrobno raščlanjivanih).

njihovih, možebitno vrlo relevantnih (poglavito onih ključno ili presudno važnih), utjecaja na analitički promatrani slučaj sastavnice ili cjeline sustava, obično – bitno slabiji.

- Ako je stanovita analitička metoda ili tehnika, usuprot prije navedenom, previše specifična, neće se moći pravilno/pouzdano primijeniti u nekom (već samo malo) drugačijem analitički razmatranom primjeru.
- Za zadaće raščlanjivanja opasnosti i prosuđivanja specifičnih vrsta i oblika ugroza i njihovih rizika neodgovarajuća znanja (kompetentne stručnosti, specijalnosti) i vještine, izostanak ili nedovoljan stupanj uključenosti pojedinih vrsta struka/specijalnosti te izostala motiviranost i uvježbanosti za takve složene analitičke poslove i zadaće, u dijela osoba stručnog tima angažiranog za taj posao.
- Nedovoljna objašnjenja, nejasni ili nepotpuni naputci za praktičnu primjenu pojedinih analitičkih metoda ili tehnika mogu bitno otežati njihovu primjenu ili uzrokovati njihovo posve pogrešno razumijevanje, kako glede njihovih specifičnih ograničenja posebice dopustivih/primjerenih područja dovoljno pouzdane primjene) tako i glede stanovitih dijelova postupaka i pojedinih koraka u njihovoj primjeni.[14]
- Složenost pojedinih analitičkih metoda i tehnika može biti tolika da zahtijeva posebno doobrazovanje i iskusnim znalcima vođeno specijalističko uvježbavanje za njihovu pravilnu i optimalnu primjenu.
- Razvoj i kakvoća metoda i tehnike rada za raščlanjivanje opasnosti i prosuđivanje ugroza/rizika od relevantnih vrsta i oblika potencijalno opasnog djelovanja *ljudskog čimbenika*, a poglavito onog zlonamjernog (uključujući sve objektivno moguće motive njegove/njihove zlonamjernosti), su još uvijek *u povojima*[15] i po aktualnoj zastupljenosti u golemom nerazmjeru u odnosu na sve one koje uopće ne obuhvaćaju i ne razmatraju utjecaj tog iznimno osjetljivog i posebno teško predvidivog ključnog (a u daleko najvećem broju slučajeva – presudno važnog) čimbenika sigurnosti, obrane i zaštite.

Jedan tipičan primjer aktualno rabljenog i, razvidno – kako to iskustva suvremene prakse prečesto pokazuju, još uvijek nedovoljno pouzdanog (tradicionalnim deskriptivnim modelom pristupa preopterećenog) načina određivanja ključnih značajki *prijetnje napadom, ranjivosti na napadaj i mogućih utjecaja izvedenih napadaja, kao ključnih sastavnica rizika od napada, te načina rangiranja rezultata* takvih raščlambi (na primjeru *razine prijetnje napadom*), u sklopu poprilično pojednostavljenog (*racionaliziranog*) postupka kvalitativno-(kvazi)kvantitativne ocjenske metode OPSEC[16] za brzo preliminarno određivanje relativne razine rizika od terorističkih, gerilskih ili inih vrsta napada, vidi sliku 17 (*Hawley, Noll, Hildebrand 2001., sl. 3-8*). Na slici 17. dan je primjer vrlo pojednostavljenog (racionalizirano kvantificiranog) pristupa za relativno brzo, ali samo preliminarno i, s motrišta pouzdanosti/valjanosti rezultata raščlambi i prosudbi, poprilično upitno određivanje relativne razine prijetnje, u sklopu prosudbe relativnog «rizika» (zapravo samo relativne razine ugroze) od ratnih, terorističkih, organizirano kriminalnih i/ili inih mogućih vrsta zločinačkih napada.[17]

---

[14]Zbog toga se, pri njihovu stručno-znanstvenom recenziranju te eventualnom službenom prihvaćanju, propisivanju i normiranju, sve češće inzistira na prilaganju dovoljno podrobno objašnjenih i jasnih popratnih naputaka za njihovu stručnu primjenu.

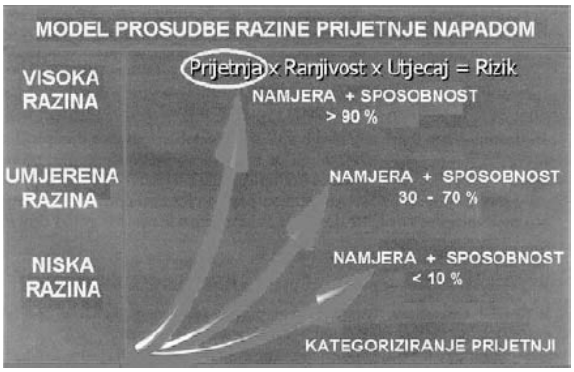
[15]U prilog tomu, možda najbolje, govore i sljedeći stavovi/preporuke OSCE, 2004., str. 15.:

... Još se uvijek ne zna mnogo o metodama i tehnikama kvalitativne raščlambe i kvantitativne prosudbe te o svim mogućim mjerama prevencije, njihovoj važnosti, ograničenjima i djelotvornosti...

... U slučajevima zapošljavanja, odabira i promicanja upravnog osoblja te osoblja koje provodi politiku prevencije kriminaliteta, veću bi važnost trebalo dati poznavanju stručne literature i metodama analize te njihovoj primjeni u praksi prevencije kriminaliteta…

[16]OPSEC je akronim izveden iz prvih slogova anglosaksonske složenice Operations Security (operativna sigurnost).

[17]Namjera potencijalnih opasnih napadača na sastavnice ili cjeline sustava kritične infrastrukture se obično grubo prosuđuje na osnovi: motivacije za napad, dosadašnjih iskustava s napadima, obilježja ponašanja potencijalnih napadača, njihovih trenutnih aktivnosti itd. Sposobnost za napad se grubo prosuđuje na osnovi: potencijalnim napadačima raspoložive tehnologije, strukture snaga potencijalnih napadača, njihove pokretljivosti, mjesnih značajki pristupa potencijalnim metama napada i vremena s kojim može raspolagati potencijalni napadač.



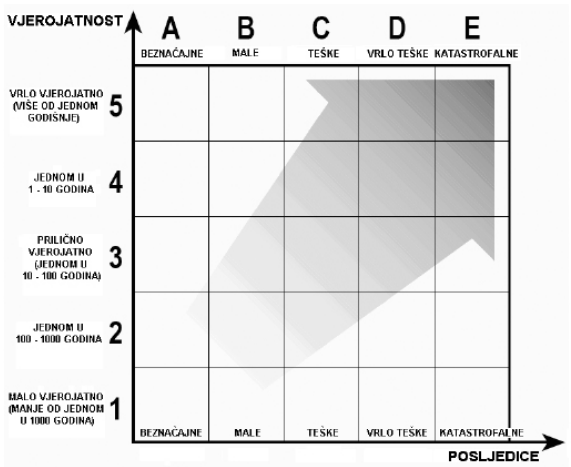
Slika 17. Model prosudbe razine prijetnje napadom

Figure 17. Model for assessing the level of threat of assault

Naime, takve (vrlo grube) raščlambe i na osnovi njih izvedene grube prosudbe (grubo kvantificirane razine) ugroze/rizika pogodne su samo za što brže približno identificiranje i sagledavanje obilježja onih predmeta i sadržaja od stanovite razine sigurnosnog interesa koji – ovisno o prosuđenoj razini relativnog rizika – moraju dobiti **prioritet** u pronalaženju i funkcionalnom ugrađivanju (implementiranju) optimalnih mjera i aktivnosti prevencije, obrane i zaštite, među možebitnim mnoštvom lako mogućih potencijalnih meta terorističkih, organizirano kriminalnih i inih napadaja. Na slici 18 prikazan je jedan, šire poznati, primjer načina grube preliminarne prosudbe relativne razine rizika od svakog promatranog industrijskog kompleksa/objekta koji je (na bilo koji način) potencijalno opasan za živote i zdravlje ljude, okoliš i ina materijalna dobra prema **matrici rizika** (prema UNEP IE-ovom programu APELL, str. III: 52).[18]

Takve mjere i aktivnosti prevencije moraju proizaći iz rezultata daljih nužnih (bitno detaljnijih, preciznijih i kvantitativnim pokazateljima potkrijepljenih) ekspertnih timskih kvalitativno-kvantitativnih raščlambi pogibelji.

Slične je naravi i namjene, pa otuda i od sličnih manjkavosti može patiti (poglavito ako se u odlučivanju o konkretnim mjerama i aktivnosti-



Slika 18. Primjer načina grube preliminarne ocjenske prosudbe relativne razine rizika

Figure 18. Example of a rough preliminary assessment of the relative risk level

ma prevencije ostane na rezultatima samo njezine primjene), i primjer, u SAD-u (od njihova *General Accounting Office*) službeno preporučane, vojno normirane metode Ministarstva obrane (DOD) *Military Standard 882C* (*MIL-STD-882C*). Nju su, već u drugoj polovici 80-ih godina, prihvatile službe sigurnosti, obrane i zaštite dijela multinacionalnih naftnih i (petro)kemijskih tvrtki, samo kao *preliminarnu ocjensku metodu*[19] za prosudbe razina mogućih prijetnji i ugroza, poradi što djelotvornijeg upravljanja rizicima, tj. zbog što lakšeg prepoznavanja i rangiranja prioriteta nužnih promjena i prilagodbi sigurnosne naravi. Otuda i logičnih prioriteta u odlučivanju o ulaganjima raspoloživih financijskih sredstava u zaštitu svojih postrojenja, instalacija, procesa, operacija, opreme, tvoriva i proizvoda od terorističkih i inih vrsta ugroza. Slično dotadašnjem pristupu u širokoj kampanji aktivnosti na promicanju kakvoće zaštite kritične nacionalne infrastrukture (bankarstva i financija, telekomunikacija, elektroenergetskog sustava itd.) od fizičkih i na zloporabi računala zasnovanih ugroza (Tablica 1). Ovom matricom se kombinira **relativna mogućnost pojave i relativna razina težine posljedica** promatrane vrste/oblika štetnog do-

[18]Značenje akronima: UNEP IE (United Nations Environment Programme - Industry and Environment, tj. UN-ov Program za okoliš – Industrija i okoliš); APELL (Awareness and Preparedness for Emergencies at Local Level, tj. Svjesnost i pripravnost za žurno djelovanje na lokalnoj razini).

[19]Vidi primjerice Kulišić, D. (1991. i 1995.), Kacian, N. et al. (1994.), Janeš, V. i Čavrak, B. (2002.) i ine reference o značajkama i postupcima uporabe takvih vrsta metoda.

gađaja (terorističkog napadaja na cjelinu promatranog štićenog sustava ili na svaku njegovu, zasebno promatranu, važnu sastavnicu – prilagođeno za potrebe civilnog sektora prema U.S. MIL-STD-882C).[20]

ZAKLJUČAK

Nema dvojbi kako je stupanj razvijenosti znanosti i tehnologije danas na takvoj razini da je u stanju (ako se to zatraži i osiguraju potreb-

Tablica 1. Primjer matrice za preliminarnu (grubu) ocjensku prosudbu relativne razine rizika

Table 1. Matrix proposed for the preliminary assessment of the relative risk level

Mogućnost pojave promatrane vrste ili oblika štetnog događaja[21]	**Razina težine posljedica promatrane vrste/oblika štetnog događaja[22]**			
	I. («katastrofalne»)	**II.** («kritično opasne»)	**III.** («marginalne»)	**IV.** («neznatne»)
A («često»)	I. A	II. A	III. A	IV. A
B («vjerojatno»)	I. B	II. B	III. B	IV. B
C («povremeno»)	I. C	II. C	III. C	IV. C
D («neznatna»)	I. D	II. D	III. D	IV. D
E («malo vjerojatno»)	I. E	II. E	III. E	IV. E

Kategorije relativnog rizika	**Razina rizika**	**Tretman razine relativnog rizika**
I.A, I.B, I.C, II.A, II.B i III.A	**1.**	**Neprihvatljivo visoka razina rizika** (nužno reduciranje protuterorističkim i inim mjerama prevencije)
I.D, II.C, II.D, III.B i III.C	**2.**	**Nepoželjna (teško izdrživa) razina rizika** (nužne stanovite odluke menadžmenta)
I.E, II.E, III.D, III.E, IV.A i IV.B	**3.**	**Prihvatljiva razina rizika** (tek uz prezentaciju i pozoran uvid menadžmenta)
IV.C, IV.D i IV.E	**4.**	**Prihvatljiva razina rizika** (bez potrebe posebnog prezentiranja menadžmentu)

[20]Vidi GAO/NSIAD (1998.). Ostale šire poznate normirane preliminarne metode prosudbe rizika tog tipa su, primjerice, novija inačica: **MIL-STD-882D te SEMI S10, EN 1050, EN 292, Draft ISO 17776** itd. U noviju inačicu **MIL-STD-882D**, kao *mogućnost pojave promatrane vrste ili oblika štetnog događaja*, uveden je i stupanj **F** («nije moguće»), bez kojeg ne bi bilo moguće raščlanjivati ***preostali*** (rezidualni) ***rizik*** u slučajevima nastanka opasnosti ili kreiranja ugroza izvan promatranog sustava. Pod složenicom ***preostali rizik*** razumijeva se aktualna razina rizika – pod uvjetom/uz pretpostavku posvemašnje usklađenosti izvedbe cjeline i svih sastavnica i/ili funkcija analitički raščlanjivanog ugroženog/rizičnog sustava kritične infrastrukture s aktualno raspoloživim relevantnim zakonskim, podzakonskim, obvezatnim normativnim i inim obvezatnim stručnim propisima.

[21]Nositeljima (zapravo ekspertnim timovima izvršitelja) procesa i specifičnih postupaka raščlambe opasnosti i prosudbe razine ugroze/rizika prepušteno je definiranje kvantificiranih razina **«mogućnosti pojave promatrane vrste/oblika štetnog događaja»**. Tako se, primjerice, tim može dogovoriti kako pojam **«često»** znači kako se *pojave promatrane vrste/oblika štetnog događaja ili terorističke prijetnje njime* može dogoditi «najmanje dva puta godišnje», ili kako su «izgledi za takvo što čak u 9 od 10 možebitnih incidenata u godini rada». Premda menadžmenti tvrtki najčešće tvrde kako baš i nije razumno programe mjera i aktivnosti protuterorističke i ine sigurnosti, obrane i zaštite zasnivati na scenariju **«najgoreg mogućeg slučaja»**, pa uglavnom preporučaju usredotočivanje na one scenarije štetnih pojava i događaja koji imaju **«veće izglede»**, neka resorna ministarstva SAD-a (npr. iz područja energetike/U.S. DOE) preporučaju da se mjere prevencije glede scenarija «najgoreg mogućeg slučaja» ipak razmatraju, unatoč činjenici kako aktualno raspoloživa ograničena sredstva mogu biti privremeno nedostatna za ostvarivanje programa posvemašnje sigurnosti, obrane i zaštite od «najgoreg mogućeg slučaja». Zato traže da i takve inačice scenarija budu predmetom rada svakog programa sigurnosti, obrane i zaštite.

Pod pojmom **«vjerojatno»** normom se razumijeva kako se pojava promatrane vrste oblika štetnog događaja «može dogoditi nekoliko puta». Pod pojmom **«povremeno»** razumijeva se kako se pojava promatrane vrste/oblika štetnog događaja «može dogoditi ponekad». Pod pojmom **«neznatna»** razumijeva se kako je takav štetni događaj «malo vjerojatan, ali se ipak može dogoditi». Pod pojmom **«malo vjerojatno»** razumijeva se kako je takav štetni događaj «tako malo vjerojatan da se može pretpostaviti kako se ne može dogoditi».

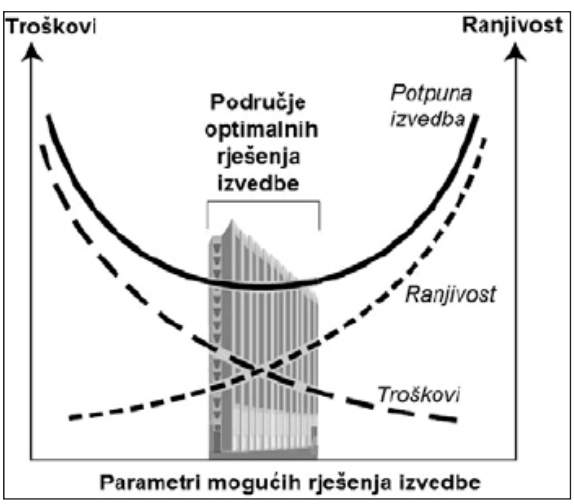
[22]Pod pojmom **«katastrofalne»** razine težine posljedica, navedenom normom se razumijevaju (mnogobrojne) pogibije (i ozljede), posvemašnji gubitak (raspad, pad) promatranog ugroženog sustava ili vrlo teške posljedice za okoliš zbog ispuštanja golemih količina opasnih tvari. Pod pojmom **«kritično opasne»** razine težine posljedica, tom normom se razumijevaju teške tjelesne ozljede, pojava teških obolijevanja u zaposlenika, velike štete na promatranom ugroženom sustavu ili teške posljedice za okoliš. Pod pojmom **«marginalne»** razine težine posljedica, normom se razumijevaju lakše tjelesne ozljede, pojava lakših obolijevanja u zaposlenika ili manje štete na promatranom ugroženom sustavu ili manje posljedice za okoliš. Pod pojmom **«neznatne»** razine težine posljedica, razumijevaju se sve one vrste koje su manje od lakših tjelesnih ozljeda, lakših obolijevanja u zaposlenika ili koje mogu uzrokovati neznatne štete na promatranom ugroženom sustavu ili neznatne posljedice za okoliš.

na financijska i nužna tehnička sredstva) razviti i, po potrebi, usavršiti funkcionalno (privremeno) skoro idealne sustave sigurnosti, obrane i zaštite po mnogim pitanjima i u mnogim područjima sigurnosti, obrane i zaštite (posebice glede sigurnosti, obrane i/ili zaštite: od požara i eksplozija; pri radu; od najrazličitijih vrsta i oblika ugroza posebno štićenih osoba, procesa i objekata; okoliša; od tehnoloških havarija; pri prometu – u najširem smislu tog pojma, pa i od mnogih vrsta elementarnih nepogoda). Ali, isto tako, nesporno je i to kako bi takvi sustavi u mnogim slučajevima, s motrišta gospodarstvenih ili društvenih *cost benefit* raščlambi bili preskupi, odnosno za državni proračun neizdrživi (neprihvatljivi), za zaštitu onih vrijednosti koje bi se njima štitile (taj ograničavajući element, posebno je znakovit za sva liberalno tržišna gospodarstva; vidi utjecaj tih kriterija u sklopu slike 6, 19 i 20).

Problem nastaje čim se zatraže (proračunska ili interna investicijska) sredstva za poduzimanje možebitno nužnih preliminarnih ili konačnih sustavnih ili parcijalnih mjera i aktivnosti otklanjanja ili ublažavanja mogućih učinaka ili za otklanjanje eventualno teško izbježivih posljedica, već prepoznatih ili razvidno prijetećih nedostataka iz bilo koje opće ili specifične problematike sigurnosti, obrane i zaštite, posebice ako one još nisu precizirane ili definirane (zahtijevane) već važećim zakonskim i podzakonskim propisima ili internim aktima (pravilnicima) državnih tijela ili pravnih osoba. Zato je nužno i za utemeljeno odlučivanje korisno, prije donošenja konačne odluke o odobravanju i svrsishodnom angažiranju tih sredstava, raščlambom odrediti sve izvore opasnosti (ugrožavanja), moguće scenarije i putove razvoja štetnih pojava i događaja, vjerojatnosti njihovog sukcesivnog pojavljivanja i zbivanja u konkretnim uvjetima i okolnostima, moguće opsege pogibeljnih domino učinaka te njihove moguće primarne i sekundarne posljedice i ine reperkusije na promatrani mikro i makro sustav sigurnosti.

Svaka takva raščlamba i njome rezultirajuća prosudba je očito nepotpuna bez razmatranja svih relevantnih značajki mogućih pogibelji, ujedno i sa stajališta eventualnih pokušaja terorističkih, gerilskih, organizirano i individualno kriminalnih napada ili inih zlonamjernih djelovanja, jednako sustavnim i temeljitim sofisticiranim analitičkim pristupima i primjerenim, dovoljno pouzdanim, aktualno raspoloživim analitičkim alatima.

Predočeni načelan slijed i opće sastavnice tog postupka te ključni opći elementi za stručne prosudbe pogibelji i od eventualnih terorističkih i inih zlonamjernih djelovanja – s motrišta njihovih mogućih: ciljeva, počela, meta i inačica taktike napada te raspoloživih specifičnih modusa operandi – od iznimne su važnosti za razinu uspješnosti u postizanju učinkovite kontrole za slučaj izravno prijetećih ili nastalih pogibelji i takvog uzroka te za djelotvorno i ekonomično upravljanje integralnom sigurnošću, obranom i zaštitom elemenata i cjelina objekata kritične nacionalne, lokalne i transgranične ili šire regionalne infrastrukture, od svih vrsta i oblika realno mogućih opasnosti i ugroza. Slika 19 prikazuje utjecaj mogućih razina ranjivosti i razina troškova na izbor parametara mogućih/optimalnih rješenja oblikovanja i izvedbe bilo koje vrste objekta kritične infrastrukture odgovarajućeg oblika i funkcije s motrišta zahtjeva za «razumno izvedivom» razinom njegove integralne sigurnosti, obrane i zaštite od najrazličitih vrsta prirodnih i tehničkih opasnosti, kao i od pogibeljnih akata napada suvremenoga terorizma – posebice onoga «high-tech» tipa *(WACE, 2006.)*.



Slika 19. Simbolički prikaz utjecaja mogućih razina ranjivosti i razina troškova

Figure 19. A symbolic presentation of the impact of the possible vulnerability levels and cost levels

Naime, na osnovi zaključaka kvalitetno izvedenih raščlambi će neminovno proizaći i odgovarajući **prioriteti za rješavanje**, potom, eventualne **opcije rješenja problema**, kao i odgovarajuće *cost benefit* i *cost effectiveness* raščlambe pojedinih rješenja. One bi na koncu morale rezultirati relativno prihvatljivim rješenjima, otklanjanja ili ublažavanja **naravi** i **razmjera ugroza** ili **prihvatljivim** (dovoljno niskim) **razinama apsolutnog** ili **relativnog rizika** od štetnog događaja (vidi sliku 20). Osnovni pristup općeg načina reagiranja po prosuđenoj razini svake pojedine vrste/naravi rizika u bilo kojem području od interesa za sigurnost, obranu i/ili zaštitu zastupa i «Seveso II direktiva» Savjeta EU-a.[23]

Teoretski, što je vjerojatnost nastanka i ugroženost od nekog štetnog događaja manja (vidi slike 17 i 18, te Tablicu 1), to su preventivne mjere i aktivnosti koje je potrebno poduzeti poradi sprečavanja njegove pojave i/ili ublažavanja mogućih učinaka i posljedica njegova djelovanja, jednostavnije i ne zahtijevaju angažiranje većih financijskih sredstava i kadrovskih potencijala. U obrnutom slučaju, potrebe za ulaganjem financijskih sredstava može se reći da gotovo eksponencijalno rastu s porastom vjerojatnosti nastanaka takvog događaja (vidi sliku 19).[24] U slučaju vrlo velike vjerojatnosti nastanka štetnog – za život ljudi te materijalnog dobra opasnog – događaja i iznimno visokih troškova vezanih za sustav sigurnosti, obrane, zaštite i spašavanja, takav proces rada ili aktivnosti se u takvim uvjetima i okolnostima obično obustavlja ili koncipira na nekoj drugoj, mnogo sigurnijoj, tehnološkoj, procesnoj ili prostornoj osnovi.

Slika 20. Suvremeni osnovni pristup općeg načina reagiranja po prosuđenoj razini svake pojedine vrste/naravi rizika

Figure 20. General modern approach to reacting to assessed levels of various types of risk

Naravno, najbolje od svega je ako postoji mogućnost da se već tijekom stadija preliminarnog planiranja pojedinih potencijalno opasnih i za moguće terorističke ili ine kriminalne napadaje možebitno zanimljivih te na njih osjetljivih i ranjivih sustava, procesa, operacija, radova ili aktivnosti, polazeći od *derivativnog modela pristupa* raščlambi, pravodobno predvide i identificiraju te na kvalitativno-kvantitativnoj osnovi definiraju svi objektivno mogući izvori ugroza, vrste i oblici opasnosti, vjerojatnosti njihova pojavljivanja i razvoja te predvide njihovi mogući učinci i posljedice.

Zbog toga se potrebi, kakvoći rada i stalnom promicanju pouzdanosti pristupa i provedbe procesa raščlanjivanja opasnosti i prosuđivanja ugroženosti, odnosno rizika, u skladu s postojećim propisima, normama, preporukama, pravilima prakse i drugim kriterijima, koji se u tom području već primjenjuju u EU, u nas i u nekim gospodarski najrazvijenijim zemljama, danas, pridaje sve veća pozornost i važnost.

Kvalitetan menadžment sigurnosti, obrane i zaštite se prepoznaje po:

[23]ALARP i ALARA su akronimi angloameričkih složenica as low as reasonably practicable (ili possible)/achievable (težnja postizanju «što je, razumno izvedivo, moguće manjeg» rizika, tj. reduciranje razine rizika od pojave pogubno pogibeljnih ili težih štetnih i dugoročnije škodljivih posljedica na razumno/društveno prihvatljivu razinu – vidi ponovo i shemu 6 u I. dijelu rada). Tako se, primjerice, poradi izbora najpovoljnije mikrolokacije i načina izvedbe građevina, u kojima se planira nazočnost zaposlenika u sklopu stanovitog kemijskog industrijskog kompleksa, naputkom britanske Chemical Industries Association (CIA): Guidance for the location and design of occupied buildings on chemical manufacturing sites, iz veljače 1998. g. (ISBN 1 85897 077 6), raspon područja ALARP – unutar kojeg se mora (uz dokazivanje i cost-benefit raščlambama) nastojati rizike od svih mogućih vrsta vrlo pogibeljnih nesreća sniziti na «što je, razumno izvedivo/postiživo, moguće manju mjeru» (tj. na neku razinu ALARA) – definira čestinama (frekvencijama) moguće pojave pogibeljno opasnih i štetnih vrsta događaja, između najmanje $1x10^{-6}$ g-1 i najviše $1x10^{-4}$ g-1, polazeći pritom od njihovih kriterija (HSE Tolerability of Risk criteria), iz naputka The Tolerability of Risk from Nuclear Power Stations (ISBN 0 11 886368 1).

[24]Područje optimalnih rješenja izvedbe dobiva se vještim uravnoteživanjem visine troškova s pitanjima oblikovanja (dizajna) i funkcionalnosti promatranog objekta te njegove ranjivosti – izborom one točke iznad koje bi eventualno povećani izdaci iz fonda raspoloživih investicijskih sredstava ili žrtvovanje dijela važnih značajki njegove radne/operativne prikladnosti i procesne funkcionalnosti rezultirali smanjivanjem potencijala sigurnosti i zaštite.

- redovitim (prema potrebama kontinuiranim ili povremenim te za izvanredne okolnosti i situacije *proaktivnim* i *reakcijski* pravodobnim) djelotvornim i učinkovitim raščlambama opasnosti i prosudbama ugroza/rizika, kao i, na osnovi toga,
- pravodobno odabranim, donositeljima odluke pravodobno i adekvatno stručno obrazloženim i predloženim te
- pravodobno ugrađenim, u što većoj mjeri *inherentnim* i *optimalnim* – tj. posve svrsishodnim, djelotvornim i gospodarski ili proračunski prihvatljivim/troškovno podnošljivim – mjerama i aktivnostima sigurnosti, obrane i zaštite.

Uz dobru suradnju s državnim sigurnosno-obavještajnim, policijskim i inspekcijskim službama svih relevantnih državnih tijela i službi, po svim ključnim pitanjima sigurnosti, obrane, zaštite i spašavanja, te kontinuiran i uporan rad na podizanju i održavanju visoke razine stanja sigurnosne svijesti i kulture – znalačka i vješta uporaba aktualno dostupne najsuvremenije metodičke, hardverske i softverske analitičke potpore stručno utemeljenom izboru i odlučivanju čini *condicio sine qua non* realnih izgleda za njihovu uspješnost u tim zadaćama.

Zato stručno prepoznati i adekvatnom procedurom probrani, potrebama kvalitetno obrazovani, primjereno specijalizirani i uvježbani, izvrsno informirani, koordinirani i vođeni te primjereno sigurnosno i (samo)zaštitno svjesni, motivirani i poticani **ljudski resursi**, uz osigurane – potrebama primjerene – **materijalne resurse**, u svakom segmentu prije opisanih kompleksnih sigurnosnih, obrambenih i zaštitnih zadaća, čine temelj uspjeha. Naravno, kako u prevencijskom suzbijanju pojava terorizma, ekstremizma, prijetećih vrsta kriminala i inih vrsta pogibelji tako i djelotvornog i ekonomičnog upravljanja integralnom sigurnošću i kontrolom bilo koje od prisutnih ili povremeno pojavljujućih pogibelji po dijelove i cjeline kritične nacionalne i lokalne ili transgranične infrastrukture.

LITERATURA

Coster, M. N. i Hankin, R. K.S.: Risk assessment of antagonistic hazards, *Journal of Loss Prevention in the Process Industries*, 16, 2003., 545-550.

Crowe, T. D.: *Crime Prevention through Environmental Design: Applications of Architectural Design and Space Management Concepts, 2nd Ed.,* Butterworth-Heinemann, Stoneham, 2000.

Delvosalle, C. et al.: ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries, *Journal of Hazardous Materials*, 130, 2006., 200-219.

Dukovski, D.: *Usud Europe; Pandorina kutija europska,* C.A.S.H., Pula, 1999.

Dziubin´ski, M., Fratczak, M. i Markowski, A.S.: Aspects of risk analysis associated with major failures of fuel pipelines, *Journal of Loss Prevention in the Process Industries,* 19, 2006., 399-408.

EC: *A Secure Europe in a Better World: European Security Strategy*, Brussels, 12 December 2003.

EC doc. 10585/04: *Declaration on combating terrorism,* General Secretariat of the Council of the European Union, Press Office, Brussels, 25 March 2004.

EC doc. 14330/1/04: *Action Plan on the Fight Against Terrorism,* General Secretariat of the Council of the European Union, Press Office, Brussels, June 2004.

EC doc. COM (2004) 702: *Critical infrastructure protection in the fight against terrorism,* General Secretariat of the Council of the European Union, Press Office, Brussels, 20 October 2004.

EC doc. 96/82/EC: Council Directive on the control of major-accident hazards involving dangerous substances, *Official Journal of the European Communities,* Luxembourg, 9 December 1996.

FEMA 386-7: *Integrating Human-Caused Hazards Into Mitigation,* Risk Management Series, Federal Emergency Management Agency (FEMA) & Department of Veterans Affairs, September 2002.

FEMA 452: *Risk Assessment, A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings, Providing Protection to People and Buildungs,* Risk Management Series, Federal Emergency Management Agency (FEMA) & Department of Veterans Affairs, January 2005.

Fischhoff, B. et al.: *Acceptable Risk,* Cambridge University Press, New York, 1981.

Freemantle, B.: *The Octopus: Europe in the Grip of Organised Crime,* Orion Books Ltd., London 1995.

GAO/NSIAD: *Combating Terrorism: Threat and Risk Assessment Can Help Prioritize and Target Program Investments,* US General Accounting Office/National Security and International Affairs Division, Washington, April 1998.

Hawley, C., Noll, G.G., Hildebrand, S.: Operations Security for Public Safety Agencies, In: *Special Operations for Terrorism and HazMat Crimes,* Red Hat Publishing, June 2001.

Herman, M.: *Intelligence Power in Peace and War,* Cambridge University Press, Cambridge, 1996.

Hrvatska u 21. stoljeću (strategija razvitka u 19 područja društvenog razvitka), svibnja 2001., dostupno na: http://www.hrvatska 21. hr, Accessed: 2006-01-30.

HSE, *Inspectors Toolkit: Human factors in the management of major accident hazards - Introduction to human factors (Draft),* Health and Safety Executive, October 2005.

IP (The Institute of Petroleum), Safety culture, *Human factors, Briefing Note No 9*, 2003., 2.

Jaeger, C. D.: Chemical facility vulnerability assessment project, *Journal of Hazardous Materials*, 104, 2003., 207-213.

Janeš, V. i Čavrak, B.: *Procjena opasnosti za opasne tvari,* Zavod za istraživanje i razvoj sigurnosti, Zagreb, 2002.

Joint Pub 3-07.2: *Joint Tactics, Techniques, and Procedures for Antiterrorism,* 2nd Ed., Joint Chiefs of Staff, Shelton, H. H. (Ed.), Washington, 17 March 1998, str. I-1 – I-2.

Kacian, N. et al.: Numeričke metode za procjenu ugroženosti od požara i tehnoloških eksplozija, *Zbornik radova*, Iproz, Zagreb, 1994.

Kazneni zakon RH, N.N., br. 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06.

Kulišić, D.: O općem postupku i ključnim elementima raščlambe opasnosti i prosudbe ugroze/rizika od terorističkih pogibelji po *kritičnu nacionalnu infrastrukturu, Zbornik znanstveno-stručnog skupa «Ljudski resursi u suzbijanju terorizma»,* Antoliš, K. (Ed), Zagreb, 7.-8. rujna 2006., Policijska Akademija – Visoka policijska škola MUP-a RH, Zagreb, (2007), str. 115-156.

Kulišić, D.: O aktualnim općim pristupima i elementima za raščlambe opasnosti od zlonamjernih ugroza sigurnosti prometnih tokova, Referat na *Međunarodnoj konferenciji «Nacionalna sigurnost i perspektive prometa u Republici Hrvatskoj»,* u Zagrebu, 27. – 28. veljače 2006., u organizaciji Odbora za unutarnju politiku i nacionalnu sigurnost Hrvatskog sabora, u tisku časopisa Policija i sigurnost, 16 (2007) 1-6.

Kulišić, D.: O aktualnim općim pristupima i elementima za raščlambe opasnosti od zlonamjernih ugroza sigurnosti prometnih tokova, Nepublicirana *PowerPoint* prezentacija referata na *Međunarodnoj konferencije «Nacionalna sigurnost i perspektive prometa u Republici Hrvatskoj»,* Grgić, Z. (Ed), Zagreb, 27. – 28. veljače 2006., Odbor za unutarnju politiku i nacionalnu sigurnost Hrvatskog sabora, Zagreb, (2006), sl. 32.

Kulišić, D.: Normizacija pod pritiskom sigurnosnih izazova suvremenog kriminala i terorizma, *Zbornik 3. savjetovanja «Hrvatska normiza-*

cija i srodne djelatnosti – Tehničko usklađivanje na putu prema Europskoj uniji», Radić, J. (Ed), str. 171-178, Plitvice, listopada 2005., HIS i DZM, Zagreb, (2005).

Kulišić, D.: *Metodika istraživanja požara i eksplozija* (skripta), Visoka policijska škola u Zagrebu, Zagreb, 2003.

Kulišić, D.: Istraživanje uzroka šumskih i inih požara - Suvremeni temeljni koncepti, pristupi i počela, *Zbornik radova stručno - znanstvenog skupa «Zaštita šuma od požara»*, Iproz d.o.o., Zagreb, 2003., str. 4-34.

Kulišić, D.: O mogućnostima sučeljavanja pojavama akata terorizma i inog nasilja, *Seminar: «Zaštita od terorizma i drugih oblika nasilja»*, Javorović, B. (Ed), str. 13-45, Zagreb, (2002).

Kulišić, D.: Sabotaže i diverzije: Opasni klasični, glavni suvremeni i, nažalost, još važniji i pogibeljniji budući modusi operandi vojnih, civilnih i kriminalnih ustrojbi, udruga i ekstremnih pojedinaca, *Policija i sigurnost,* 6, 1997., 1-2., str. 57-131.

Kulišić, D.: Pregled elemenata za sigurnosnu raščlambu opasnosti i prosudbu ugroženosti/rizika u cestovnom prijevozu zapaljivih i/ili eksplozivnih tvari i tvoriva, *Zbornik znanstveno-stručnog skupa «Cestovna prometna delinkvencija»,* Jurina, M. (Ed), str. 35-41, Zagreb, studenoga 1995., Policijska akademija MUP-a RH - Visoka policijska škola, Zagreb, veljače 1996.

Kulišić, D.: *Elementi za raščlambu i prosudbu ugroze od terorizma i njegovih «modusa operandi»*, Interni obrazovni tekst, Visoka policijska škola MUP-a RH, Zagreb, travnja 2003.

Kulišić, D., Diskretne indicijalno-dokazne značajke paleži i podmetnutih eksplozija, *Zbornik znanstvenostručnog savjetovanja «Sigurnost u okolišu i graditeljstvu»,* u Solarisu, 09.-11. svibnja 2002., SUN ARH d.o.o., Zagreb, 2002., str. 265-280.

Kulišić, D.: Procjenjivanje ugroženosti od požara i eksplozija i odlučivanje o prevenciji na bazi metoda indeksa opasnosti, *Požar-eksplozija-preventiva,* 12, 1991., 1., str. 41-60.

Kulišić, D.: Prednosti i nedostaci suvremenih metoda i tehnika za analiziranje opasnosti i procjenjivanje ugroženosti u prometu/transportu opasnih tvari, *Priručnik za obrazovanje radnika MUP-a RH*, 28, 1990., 4., str. 283-298.

Khan, F.I. i Abbasi, S.A.: Major accidents in process industries and an analysis of causes and consequences, *Journal of Loss Prevention in the Process Industries,* 12, 1999.,, str. 361-378.

Kuhn, H.W.: *Classics in Game Theory,* Princeton University, Princeton, 1997.

Kumamoto, H. i Henley, E.J.: *Probabilistic Risk Assessment and Management for Engineers and Scientists,* 2nd Ed., IEEE Press, Piscataway, 1996.

Landan, L.: *The Book of Risks,* John Wiley and Sons, Inc., New York, 1994.

Laqueur, W.: *The Age of Terrorism,* Little, Brown and Co., Boston, 1987.

Lundin, J. & Jönsson, R.: Master of science in risk management and safety engineering, at Lund University, Sweden, *Journal of Loss Prevention in the Process Industries,* 15, 2002., 111-117.

Marighella, C.: *Mini priručnik urbane gerile,* Fokus komunikacije, Zagreb, 2003.

Markoff, J.: Attack of the Zombie Computers Is Growing Threat, *The New York Times,* 7. siječnja 2007.

Metodologija za procjenu štete od elementarnih nepogoda, N.N., br. 96/98.

Moore, D.A.: Application of the API/NPRA SVA methodology to transportation security issues, *Journal of Hazardous Materials,* 130, 2006., 107-121.

Moore, D.A.: The new risk paradigm for chemical process security and safety, *Journal of Hazardous Materials,* 115, 2004., 175-180.

Morgan, M.G. i Henrion, M.: *Uncertainty, A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*, University Press, Cambridge, 1990.

OSCE: *Prevencija kriminaliteta u Europskoj uniji,* COM, 2004., str. 15.

Pitblado, R. i Smith, E.: Safety Cases Lessons: Safety Cases for Aviation – Lessons from Other Industries, *Proceedings of International Symposium on Precision Approach and Automatic Landing,* Munich, Germany 18-20 July 2000.

Pomorski zakonik, N.N., br. 181/04.

Pravilnik o izradi procjene opasnosti, N.N., br. 48/97., 114/02. i 126/03.

Pravilnik o izradi procjene ugroženosti od požara i tehnološke eksplozije, N.N., br. 35/94. i 110/05.

Pravilnik o kontroli projekata, N.N., br. 89/00.

Pravilnik o metodologiji za izradu procjena ugroženosti i planova zaštite i spašavanja, N.N., br. 20/06.

Pravilnik o procjeni utjecaja na okoliš, N.N., br. 59/00., 136/04. i 85/06.

Pravilnik o razvrstavanju građevina, građevinskih dijelova i prostora u kategorije ugroženosti od požara, N.N., br. 62/94 i 35/97.

Pravilnik o rukovanju opasnim tvarima, uvjetima i načinu obavljanja prijevoza u pomorskom prometu, ukrcavanja i iskrcavanja opasnih tvari, rasutog i ostalog tereta u lukama, te načinu sprječavanja širenja isteklih ulja u lukama, N.N., br. 51/05.

Pravilnik o sadržaju plana zaštite od požara i tehnoloških eksplozija, N.N., br. 35/94 i 55/94.

Pravilnik o tehničkim uvjetima i normativima za siguran transport tekućih i plinovitih ugljikovodika magistralnim naftovodima i plinovodima te naftovodima i plinovodima za međunarodni transport, N.N., br. 26/85 (preuzet Zakonom o preuzimanju saveznih zakona N.N., br. 53/91).

Pravilnik o temeljnim zahtjevima za zaštitu od požara elektroenergetskih postrojenja i uređaja, N.N., br. 146/05.

Pravilnik o zahtjevima za eksplozivne tvari, N.N., br. 146/05.

Pravilnik o zapaljivim tekućinama, N.N, br. 54/99.

Pravilnik o zaštiti šuma od požara, N.N., br. 26/03.

Program i strategija prostornog uređenja RH, N.N., br. 50/99.

Salvi, O. i Debray, B.: A global view on ARAMIS, a risk assessment methodology for industries in the framework of the SEVESO II directive, *Journal of Hazardous Materials,* 130, 2006., 187-199.

Santos-Reyes, J. i Beard, A. N.: Assessing safety management systems, *Journal of Loss Prevention in the Process Industries,* 15, 2002., 77-95.

Shields, T.J., Silcock, G.W.H.: *Buildings and Fire,* Longman Scientific and Technical, Harlow, 1987.

Security Service (MI 5): Protecting Against Terrorism, *dostupno na*: http://www.mi5.gov.uk, *Accessed:* 2006-09-28.

Security Service (MI 5): Secure in the Knowledge, *dostupno na:* http://www.mi5.gov.uk, *Accessed:* 2006-09-28.

Security Service (MI 5): Expecting the Unexpected, *dostupno na:* http://www.mi5.gov.uk, *Accessed:* 2006-09-28.

Seveso II Directive [96/82/EC]: Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances, Council of the European Union, *dostupno na:* http://www.mahbsrv.jrc.it, *Accessed:* 2006-07-12.

Smithson, A.E. & Levy L.-A.: Ataxia: The Chemical and Biological Terrorism Threat and the US Response, Report No. 35, Henry L. Stimson Centre, *Chemical and Biological Weapons Non-proliferation Project,* Washington, October 2000.

Suchman, E.A.: A conceptual analysis of the accident problem, *Social Problems,* 8, 1961., 3, str. 241-246.

Stamatelatos, M. et al., *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners,* Office of Safety and Mission Assurance, NASA Headquarters, Washington, August 2002.

Tenet, G.J. (DCI): *Global Trends 2015: A Dialogue about the Future with Nongovernmental Experts,* National Intelligence Council, Washington, December 2000.

Trut, D.: Zaštita kritične infrastrukture, *Zaštita,* 2, 2006., 2, str. 23-25.

UNEP IE: Management of Industrial Accident Prevention and Preparedness (A Training Resource Package), 1st Ed., Paris, June 1996, *dostupno na:* http://www.unepie.org/home, *Accessed:* 2006-03-16.

WACE: Designing Structures to Resist Explosions, Weidlinger Associates Consulting Engineers, *dostupno na:* http://www.wai.com *Accessed:* 2006-04-28.

Whiteley, J. R. R. i Mannan, M. S.: Initial perspectives on process threat management, *Journal of Hazardous Materials,* 115, 2004., 163-167.

Wilkinson, P.: *Technology and Terrorism,* Frank Cass, London, 1993.

Wolski, A.: The Importance of Risk Perceptions in Building and Fire Safety Codes, *Fire Protection Engineering,* 10, 2001., 30-33.

Uredba o određivanju građevina od važnosti za Republiku Hrvatsku, N.N., br. 06/00. i 68/03.

Zakon o eksplozivnim tvarima, N.N., br. 178/04.

Zakon o energiji, N.N., br. 68/01. i 177/04.

Zakonu o gradnji, N.N., br. 175/03. i 100/04.

Zakon o kemikalijama, N.N., br. 150/05.

Zakon o osnovama sigurnosti transporta naftovodima i plinovodima, N.N, br. 64/73. (preuzet Zakonom o preuzimanju saveznih zakona, N.N., br. 53/91.).

Zakon o otpadu, N.N., br. 178/04.

Zakon o prijevozu opasnih tvari, N.N., br. 97/93., 34/95. i 151/03.

Zakon o prostornom uređenju, N.N., br. 30/94., 68/98., 35/99., 61/00., 32/02., 100/04.

Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske, N.N, br. 79/06.

Zakon o šumama, N.N., br. 140/05. i 82/06.

Zakon o vatrogastvu, N.N., br. 106/99.

Zakon o vodama, N.N., br. 107/95. i 150/05.

Zakon o zapaljivim tekućinama i plinovima, N.N., br. 108/95.

Zakon o zaštiti i spašavanju, N.N., br. 174/04.

Zakon o zaštiti na radu, N.N., br. 59/96., 94/96. i 114/03.

Zakon o zaštiti od elementarnih nepogoda, N.N., br. 73/97.

Zakon o zaštiti od požara, N.N, br. 58/93. i 33/05.

Zakon o zaštiti okoliša, N.N, br. 82/94. i 128/99.

Zakon o zaštiti prirode, N.N., br. 70/05.

Zakon o zaštiti zraka, N.N., br. 178/04.

Zakon o zdravstvenoj zaštiti, N.N., br. 121/03. i 85/06.

MEASURES OF PREVENTION FROM TERRORIST AND OTHER MALICIOUS ACTIVITIES OF CRITICAL INFRASTRUCTURE (PART II)

SUMMARY: Security and protection managements/managers are increasingly made aware of the available approaches to security and protection of components and systems of critical infrastructure at the national, local and transborder level and of the enormous importance and possible benefits from the systematic, thoroughly and professionally conducted procedures of integral hazard analysis and assessment of the nature and proportions of threats/risk levels from every kind of threat/hazardous events with special emphasis on those of terrorist, guerrilla, organized and individually criminal or other malicious nature, which have not been systematically studied – especially not with complex and sophisticated and thorough analytical approaches and reliable analytical tools. Starting, among other, from the current demands defined in the „Rules on methodology for risk assessment and plans for the protection and rescue" («Narodne novine», No. 20/06), the general sequence and main components of this procedure and main general elements are shown for the professional judgment of hazards from possible terrorist activities from the point of their aims, acting principles, targets of assault tactics and available specific "modus operandi", of enormous importance for the efficient control of directly threatening or actual threats as well as for efficient and economic management of integral safety, defence and protection of elements and whole facilities of critical national, local and transborder infrastructure from all kinds of possible hazards and threats. In such complex issues and tasks, adequate level of social, specific organizational and individual safety culture, together with adequately stimulated appropriate human and material resources (adequate to the needs) constitute a "condicio sine qua non" for any real chances of success.

Key words: *critical infrastructure, integral security, terrorism, highly sophisticated crime, organized crime, major accidents, hazard analysis, threats/risks assessment, general security issues, general intelligence issues, levels of security and safety culture, management of integral security, defence and safety*

Original scientific paper
Received: 2007-02-02
Accepted: 2008-03-04