OBJAVLJENO :

ZBORNIK SAŽETAKA RADOVA 5. MEĐUNARODNE ZNANSTVENO-STRUČNE KONFERENCIJE

Istraživački dani Visoke policijske škole u Zagrebu.

Unaprjeđivanje sigurnosne uloge policije primjenom novih tehnologija i metoda.

Zagreb, Hrvatska, 21. - 22. travnja 2016.

5 TH INTERNATIONAL SCIENTIFIC AND PROFESSIONAL CONFERENCE

The Police College research days in Zagreb

New Technologies and Methods Used for Improvement of the Role of the Police in Security Matters

Zagreb, Croatia, 21-22 April 2016

NEISKORIŠTENE MOGUĆNOSTI PRIVATNOG SEKTORA U PODIZANJU RAZINE JAVNE SIGURNOSTI

Uvod

Današnji razvoj društva, te sve brutalniji i učestaliji događaji koji su posljedica kriminalnih radnji utječu i na osjećaj sigurnosti pojedinaca pa tako i zaposlenika kompanija. Radi zaštite svojih zaposlenika i kupaca, ali i smanjenja šteta, kompanije postavljaju sustave tehničke zaštite na svoje objekte i prostore. Obzirom da je sigurnost zaposlenika i zaštita imovine jedan od osnovnih preduvjeta uspješnog kompanijskog poslovanja kompanije nastoje na različite načine zaštititi svoje zaposlenike, imovinu, ali i druge interesne dionike. Kompanije koriste, uz već spomenute sustave tehničke zaštite, tjelesnu zaštitu (zaštitare), određene mehaničke zaštite, usluge detektivskih agencija, propisane sigurnosne procedure i dr.. Sve to značajno ovisi i kojom djelatnošću se određena kompanija bavi te koliko je velika. Čovjek i njegovo znanje i

vještina najveće su bogatstvo svake kompanije, pa je i to jedan od razloga zašto kompanije ulažu u sigurnost svojih zaposlenika.

Podatak da se danas tržište privatne sigurnosti procjenjuje na 85 milijardi američkih dolara, s godišnjom stopom rasta 6-8 posto (Abrahamsen i Williams, 2005) govori sam za sebe. Međutim taj podatak ne prati istovremeno i razvoj suradnje između privatnog i javnog sektora zaduženog za javnu sigurnost u Republici Hrvatskoj i za sada taj međuodnos ne možemo nazvati „partnerskim". Cilj rada je prikaz mogućnosti jednog dijela sustava tehničke zaštite koji koristi privatna kompanija i kako te mogućnosti staviti u funkciju podizanja javne sigurnosti.

I. Korporativna sigurnost-osnovne napomene

Poslovanje kompanije svakodnevno je izloženo različitim utjecajima, od financijskih kriza, sve većim zahtjevima tržišta, promjenama radnog zakonodavstva, poreznih pravila, štetnim (kriminalnim) događajima i dr. Značajan element uspješnog poslovanja kompanije je i „sigurnosno okruženje" u kojem kompanija posluje. Na dio tog „sigurnosnog okruženja" kompanija ne može direktno utjecati, međutim mogu se primijeniti razni alati kako bi sigurnosno okruženje u kojem posluje određena kompanija imalo što manje utjecaja i činilo što manje šteta kompaniji, a sve s ciljem uspješnijeg poslovanja. Poradi toga i drugih razloga, dio kompanija razvija i strategiju korporativne sigurnosti. Glavni cilj korporativne sigurnosti u kompaniji trebao bi biti ostvarenje sigurnosti poslovnog uspjeha kompanije, a što se odnosi na:

- smanjenje ili uklanjanje svih rizika i ugrožavanja koji mogu utjecati na poslovne aktivnosti i ostvarenje poslovnog uspjeha;
- uspješno poslovno funkcioniranje i u uvjetima kriza;
- prevladavanje kriza i nastavak normalnog poslovanja (Ivandić Vidović i sur., 2011).

Isti autori smatraju da se strategija korporativne sigurnosti u kompaniji provodi na funkcionalnoj razini i pripada jednoj od funkcijskih strategija poslovnog sustava (Ivandić Vidović i sur., 2011). Temeljem ovakvih stavova možemo se složiti da sigurnost nije tehničko već strategijsko pitanje, ugroze mogu dolaziti iz vanjske i unutarnje poslovne okoline te je taj koncept usredotočen na materijalno-tehnički i ljudski faktor. Kovachic i Halibozek (2002) navode nešto veći broj funkcija korporativne sigurnosti od kojih ćemo nabrojiti neke funkcije:

- administrativna sigurnost (engl. Administrative Security) koja se odnosi na procedure i politike;

- tjelesna i tehnička sigurnost (engl. Protetctive Security) kojoj se odnosi na zaštitu imovine kompanije;
- sigurnost vlasništva i vanjskih partnerstva (engl. Out-Source/Proprietary);
- osobna sigurnost (engl. Personnel Security) koja se odnosi na zaštitu ljudi i zaštitu na radu;
- programi izobrazbe i razvoja svijesti u odnosu na sigurnost (engl. Security Education Awareness and Training Program) kojoj je primarna funkcija edukacija zaposlenih;
- istrage (engl. Investigations) koje se odnose na program zaštite od kriminala;
- informacijska sigurnost (engl. Information Security);
- sigurnost menadžera (engl. Executive Security)
- sigurnost na raznim poslovnim događajima (engl. Event Security).

Ivandić Vidović i sur. (2011) u normativni okvir korporativne sigurnosti uključuju uz spomenuto i privatnu zaštitu, zaštitu intelektualnog vlasništva, zaštitu podataka, privatnu istražnu djelatnost, „business intelligence“, sprečavanje pranja novca i financiranja terorizma, obrambene pripreme i poslove koji se odnose na zaštitu na radu i protupožarnu zaštitu (Ivandić Vidović i sur., 2011).

II. Temeljni zakonski i drugi akti koji reguliraju poslove privatne zaštite

Temeljni zakon koji regulira područje privatne zaštite je Zakon o privatnoj zaštiti (NN 68/03, 31/10, 139/10.). Ovaj zakon regulira način obavljanja zaštite osoba i imovine koju ne osigurava država. U njemu se određuju ovlasti i opseg obavljanja tjelesne i tehničke zaštite. Obzirom na sadržaj rada nešto detaljnije ćemo prikazati regulativu koja se odnosi na „tehničku zaštitu“. Tehnička zaštita je definirana u Pravilniku o uvjetima i načinu provedbe tehničke zaštite (NN 198/03). Pravilnik već u članku 1. definira tehničku zaštitu kao „…skup radnji kojima se neposredno ili posredno zaštićuju ljudi i njihova imovina, a provodi se tehničkim sredstvima i napravama te sustavima tehničke zaštite kojima je osnovna namjena sprečavanje protupravnih radnji usmjerenih prema štićenim osobama ili imovini kao što su: protuprovalno djelovanje, protuprepadno djelovanje i protusabotažno djelovanje. Mišljenja smo da ovakav koncept daje vrlo široku osnovu za projektiranje sigurnosnih mjera i otvara mogućnosti primjene suvremene tehnologije koja se u današnje vrijeme na području sigurnosti razvija impresivnom brzinom. Takve mogućnosti se dodatno povećavaju međusobnim „povezivanjem dvaju ili više sredstava, naprava i uređaja koji zajedno čine funkcionalnu cjelinu“ (članak 2. Pravilnika). Pri tome se misli na integriranje protuprovalnih i protuprepadnih sustava s javljačima raznih izvedbi

(aktivnim i pasivnim); sustava kojima se obavlja stalni nadzor nad štićenim objektom s jednog mjesta (video nadzorni sustavi); sustava centralnog prijama i signalizacije alarma; Centralni dojavni sustav i Centralni tehnički nadzor; integralnih sustava zaštite s najmanje jednim nadzornim mjestom unutar štićenog objekta . Iz navedenog je vidljivo da zakonske odredbe predviđaju mogućnost povezivanja svih sustava na jedno mjesto, što olakšava pristup i nadzor svih situacija i alarma, ali otvara i neslućene mogućnosti pristupa svim tim podacima iz „udaljenih lokacija“ pa i osobama/institucijama koje nisu dio kompanije. Donošenjem i stupanjem na snagu Zakona o zaštiti novčarskih institucija (NN 56/15) još su detaljnije uređene odredbe o karakteristikama (kvaliteti) opreme koja se ugrađuje u takvim institucijama. Tako kamere koje imaju funkciju identifikacije moraju imati horizontalnu rezoluciju od minimalno 330 piksela po metru a brzina snimanja video zapisa mora biti minimalno 2 fps po kameri s minimalnom rezolucijom za „identifikacijske“ kamere najmanje 4 CIF-a. (Čl. 8., točka 1 i 6 Zakona). Ovakve odredbe primorale su kompanije da ugrađuju opremu (kada govorimo o sustavima video nadzora) čija kvaliteta snimke omogućuje identifikaciju osoba ali i bolje praćenje bilo kakvih događaja u tom prostoru. U nastavku je primjer snimke lica različitih funkcionalnosti kamera.

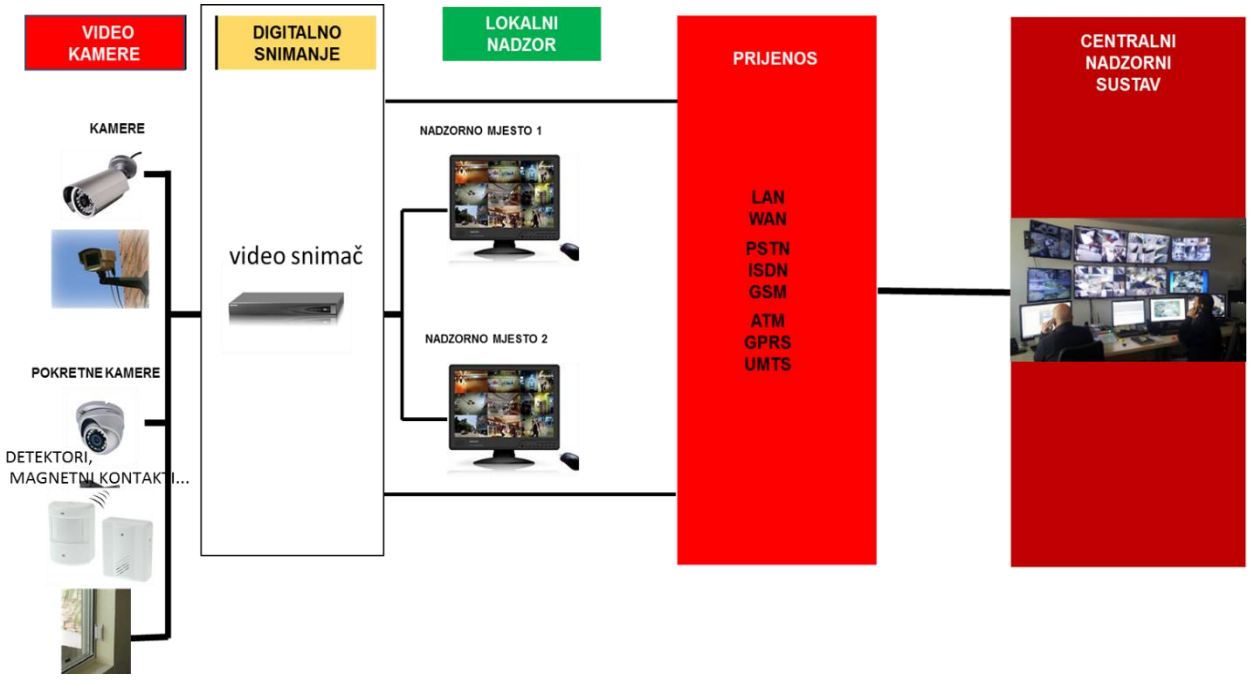
Funkcija kamere		
nadzor/detekcija	prepoznavanje	identifikacija
66 piks/m	135 piks/m	330 piks/m

Slika 1.: Prikaz kvalitete snimke kod različitih funkcija kamera

III. Centralni nadzorni sustav kompanije-funkcionalnosti i mogućnosti

Kompanije koje korite različite sustave tehničke zaštite, naročito one koje imaju veći broj takvih sustava uglavnom imaju jedno centralno mjesto (bilo u kompaniji bilo da su spojene na neku zaštitarsku kompaniju koja pruža takve usluge) gdje centralno zaprimaju alarme i imaju pristup svim video nadzornim kamerama.

Sukladno čl. 3 Pravilnika o uvjetima i načinu provedbe tehničke zaštite , (NN 198/03), CDS – Centralni Dojavni Sustav je sustav zaštite koji omogućava dojavu alarmnog signala s javljača štićenih objekata na centralni dojavni prijemnik dojavnog centra radi pružanja intervencije tjelesne zaštite. To je mjesto u koje putem sustava komunikacijskih kanala dolaze dojave sa svih sustava tehničke zaštite štićenih objekata i/ili prostora. Takav dojavni centar ili centar za nadzor ili centralni nadzorni sustav kako se naziva u nekim kompanijama obrađuje sve alarme odnosno alarmne situacije na jednom mjestu. Po zaprimanju alarmnog signala (bilo zaprimljenog alarma npr. za provalu ili razbojništvo ili alarmne situacije s video nadzornog sustava) signal se „obrađuje“ te se upućuje interventna ekipa ovlaštene zaštitarske kuće i izvješćuje se policija, a ovisno o situaciji i druge nadležne službe. Integracija različitih sustava tehničke zaštite omogućena je softverima razvijenima za tu namjenu. Cijeli sustav je izgrađen da alarmni uređaj, preko alarmne centrale šalje informaciju o incidentu trenutno, što znači da operater u nadzornom centru raspolaže odmah s informacijom o potencijalnom štetnom događaju na mjestu odakle je došao signal. Osim što su svi alarmi vidljivi trenutno, moguće je vršiti i pregled ranije zaprimljenih i obrađenih alarma. Uz popis alarma u sustavu moguće je vidjeti i detalje o svakom pojedinačnom događaju-alarmu, jer zaštitar mora upisati što je poduzeo i utvrdio (npr. upućena interventna ekipa, obaviještena policija, utvrđeno da se radi o provali, razbojništvu...). Pojednostavljeni shematski prikaz jednog ovakvog sustava tehničke zaštite prikazujemo u nastavku

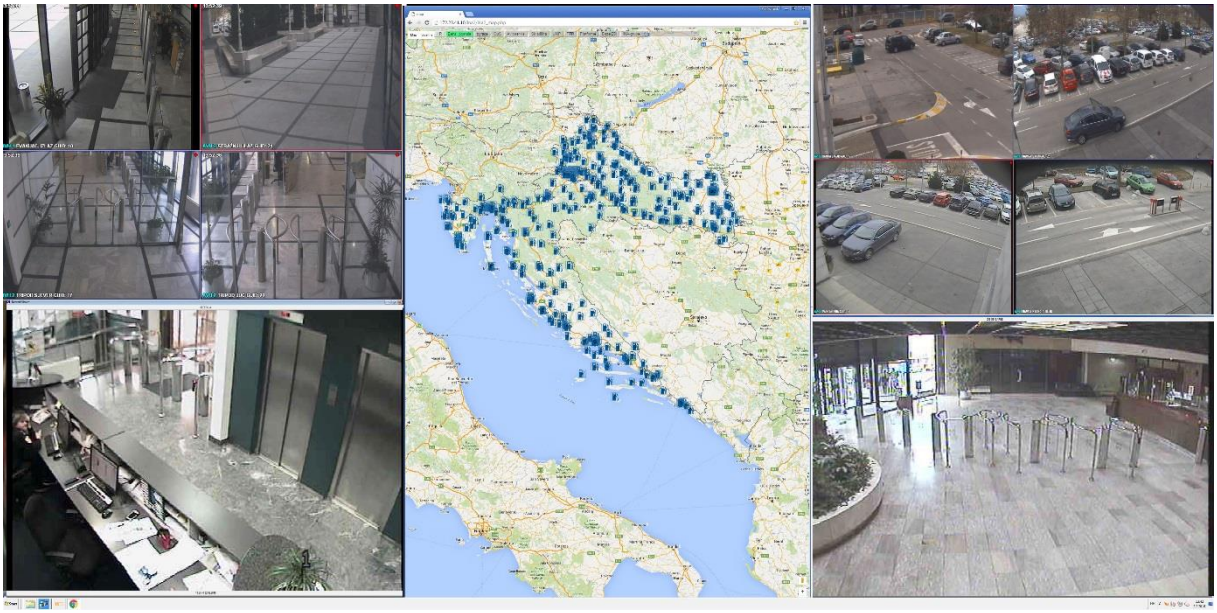


Shema 1: Pojednostavljeni prikaz sustava tehničke zaštite

Nemoguće je definirati sve incidente koje aktiviraju alarme, međutim važno je da svaki takav alarm bude trenutan kako bi reakcija i utvrđivanje zašto je do alarmne situacije došlo bila što brža. Razvoj tehnologije omogućio je da se temeljem alarma odmah povezuju kamere (ili neki drugi sustavi, npr. kontrola prolaza osoba i vozila) tako da operater odmah može vidjeti i sliku s mjesta aktiviranog alarma. Na taj način se pažnja operatera usmjerava na kritičnu situaciju na koju je potrebno reagirati odmah. Ukoliko se radi o pokretnim kamerama i operater ima mogućnost udaljenog upravljanja kamerama, operater može dodatno fokusirati kameru na određeni događaj.

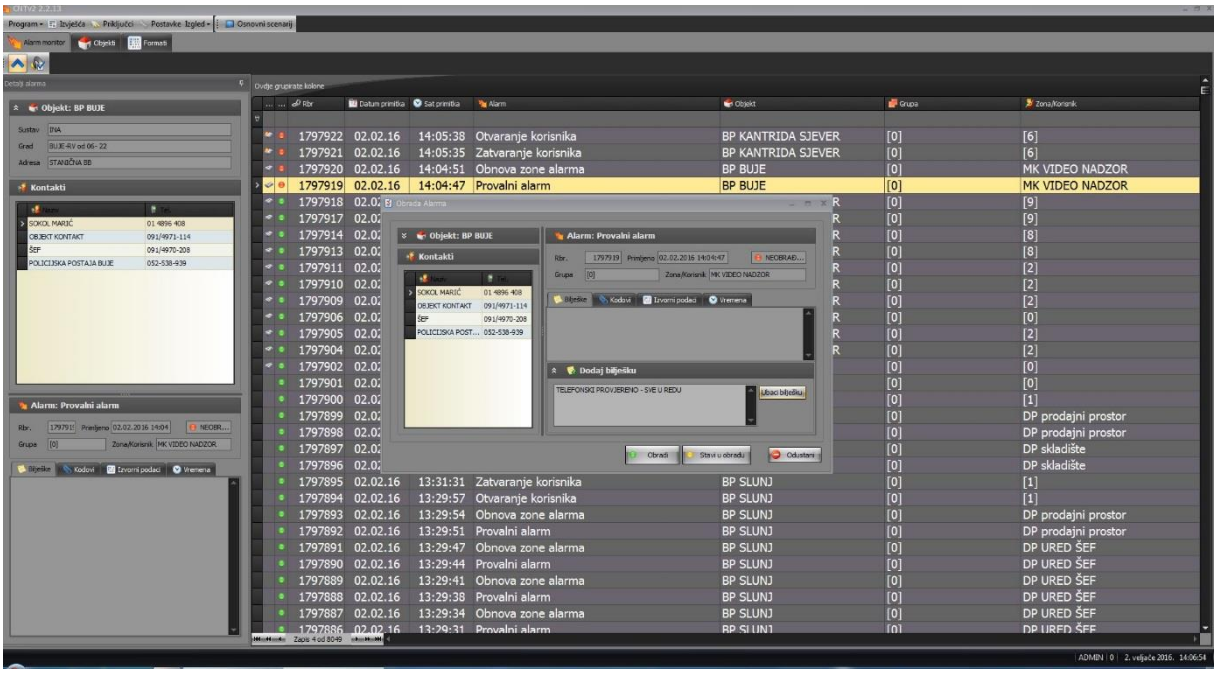
Prije prikaza i obrade cijelog postupka jedne alarmne situacije važno je naglasiti najznačajnije karakteristike jednog takvog sustava: *trenutan prijem alarma, mogućnost udaljenog pristupa sustavu i integracija više sustava*. Upravo ove karakteristike važne su u definiranju mogućnosti korištenja ovakvih sustava tehničke zaštite privatnih kompanija za potrebe javne sigurnosti.

Kako bi mogli prikazati sve mogućnosti korištenja jednog ovakvog sustava opisati ćemo ukratko postupak i funkcionalnosti koje se prikazuju kod zaprimanja alarma (npr. protuprovale). Slika 2. prikazuje početni zaslon na video zidu nadzornog centra.



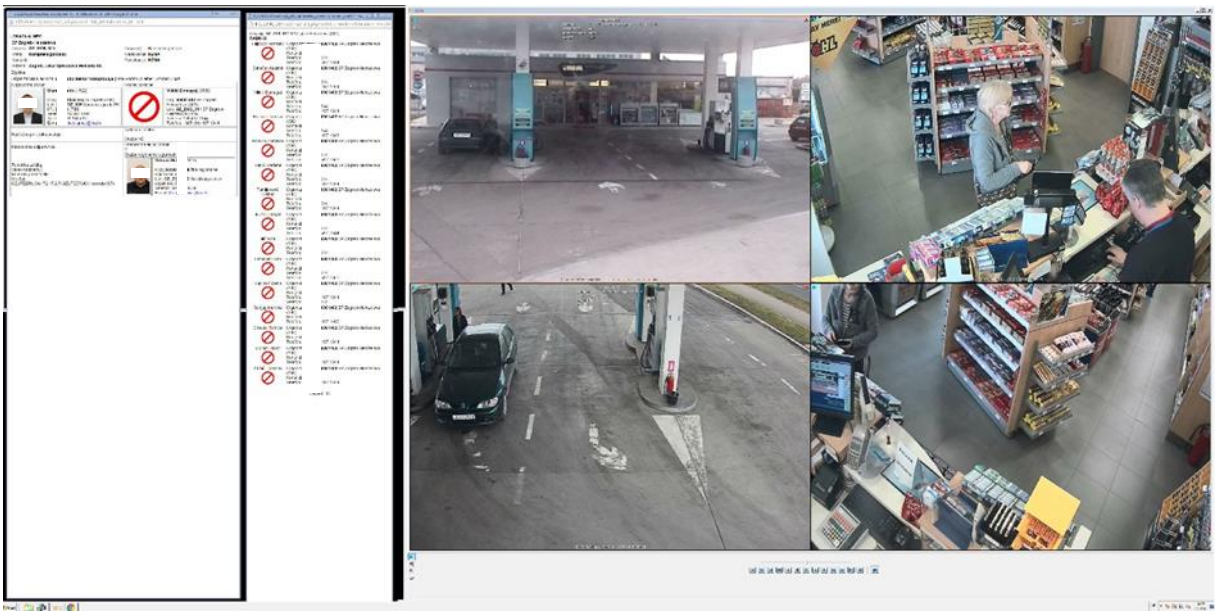
Slika 2.: Početni zaslon na video zidu nadzornog centra

Nakon što se u nadzornom centru zaprimi alarm s neke od lokacija (alarm je vidljiv na monitoru i daje zvučni signal), od strane operatera izvješćuje se telefonom interventna ekipa i policijska postaja.



Slika 3.: Prikaz monitora centralnog dojavnog sustava u trenutku dolaska alarma

Istovremeno se na centralnom monitoru (video zidu) prikazuju sve kamere s trenutnom slikom lokacije s koje je zaprimljen alarm (slika 4.) Operater osim kamera na monitoru vidi i druge podatke, točnu adresu lokacije, podatke i kontakte odgovornih osoba za tu lokaciju, tlocrt i dr.



Slika 4.: Prikaz video zida nakon prijema alarma

Prilikom pozivanja policije operater javlja točne podatke o adresi s koje je zaprimljen alarm, točnom vremenu zaprimanja alarma te svemu što je vidljivo na video nadzoru. Ukratko, nakon zaprimanja alarma, operater mora nazvati interventnu ekipu, nakon toga *nadležnu policijsku*

postaju (biranjem broja 192 s fiksnog telefona dobije se operativno dežurstvo najbliže policijske uprave/stanice, a signal alarma dolazi s područja neke druge policijske uprave pa ponekad treba „prespajanje“). Uz sve to operater gleda kamere i pokušava opisati trenutnu situaciju na lokaciji, opisati osobe, odjeću, vozila, kretanje... . Već kod uspostave poziva s policijom gubi se dosta vremena u javljanju točne adrese lokacije s koje je došao alarm, a dosadašnja iskustva ukazuju da primjerice događaji provale u benzinske postaje koje imaju sustave tehničke zaštite traju manje od 2-3 minute s počinjenom štetom više desetaka tisuća kuna, što jasno govori koliko je važno točnu informaciju prenijeti što prije. Posebno je rizično prenošenje opisa stanja temeljem video nadzora koji promatra operater i koji sve prenosi policijskom službeniku. Uz moguću subjektivnost u bilo kojem detalju opisivanja trenutne situacije s video nadzora, postavlja se pitanje dali operater (uz vremenski pritisak!) može odrediti koji su detalji važni u toj situaciji za policijskog službenika. Iako se za svaki događaj pohranjuje videoverifikacija koja omogućuje naknadni pregled događaja identičan onome koji operater ima u realnom vremenu, s mogućnošću vraćanja u vremenu kako bi se mogao pregledati točno određeni trenutak, i u takvom naknadnom pregledu snimke od strane operatera (bez vremenskog pritiska) velika je mogućnost prenošenja nepotpune informacije.

Za potrebe ovog rada prikazan je samo osnovni prikaz funkcionalnosti i mogućnosti jednog ovakvog nadzornog centra privatne kompanije (konkretan primjer iz INA d.d.) i dio procedura koje su uobičajene u alarmnim situacijama. U spomenuti nadzorni centar spojeno je preko 1700 kamera s oko dvjestotinjak lokacija te alarmi s preko 230 različitih lokacija. Iako u konkretnom primjeru dio kamera ne pokriva samo „javni prostor“ (benzinske postaje, poslovne objekte...) već i prostore (unutar štićenih prostora) gdje se odvijaju poslovni procesi, svakako da ovoliki broj kamera i alarma (a radi se samo o jednoj kompaniji) otvara velike mogućnosti korištenja za podizanje javne sigurnosti.

IV. Kompanijski resursi-javna sigurnost

Pojam javne sigurnosti možemo promatrati kao skup mjera i aktivnosti koje neka državna tijela (rjeđe i pojedinci, ne vladine organizacije ili privatne kompanije) poduzimaju kako bi se zaštitio život, zdravlje i imovina građana nekog područja, prvenstveno od kriminala, ali i od drugih događaja kao što su prometne nezgode, požari ili prirodne katastrofe. Ovdje ćemo javnu sigurnost promatrati sa stajališta aktivnosti i radnji kojima se prvenstveno bavi policija u cilju smanjivanja kriminaliteta na javnim prostorima i objektima, a gdje se nalaze sustavi video nadzora privatnih kompanija.

Uz već poznate i djelomično korištene sustave video nadzora na javnim površinama i prostorima koje je postavila i koje djelomično koristi i policija (npr. Gradska uprava Zagreba i Zagrebački holding danas u svom vlasništvu imaju oko 4.000 kamera, (Ostojić, 2015)) policija u svojim aktivnostima i dalje nedovoljno koristi kapacitete ovakvih sustava privatnih kompanija. Ostojić smatra da ne postojanje registra kamera u gradu Zagrebu kojima bi direktan pristup imala i policija pokazuje nedovoljnu inicijativu policije i gradskih vlasti, posebno iz razloga što u većim gradovima u drugim zemljama uz registre gradskih i javnih kamera postoje i registri korporativnih kamera. (Ostojić, 2015).

Potrebu takve suradnje jasno je naglasio i Pavliček (2010) u svojem izlaganju na IV Konferenciji hrvatskih menadžera sigurnosti iz 2010. godine gdje navodi da za uspostavu partnerstva javne i privatne sigurnosti treba težiti podizanju razine profesionalizma i stručne osposobljenosti svih učesnika u tom procesu. Naglasak stavlja i na svakodnevnoj komunikaciji i suradnji na operativnoj razini jer se jedino na takav način može postići temeljni cilj partnerstva, bolja sigurnost građana i njihove imovine. Iako se u svojem izlaganju uglavnom bavi mogućnošću suradnje policije i privatnog sektora s naglaskom na tjelesnu zaštitu (zaštitari), Pavliček spominje i „tehničku zaštitu“ gdje navodi „da sustavi video nadzora postavljeni na javnim površinama mogu značajno utjecati na sigurnost na pojedinim kriminalnim žarištima“ (Pavliček, 2010). Svoj doprinos obradi ove teme u Republici Hrvatskoj dali su i Podhraški, Tršinski i Kancir (2007) koji navode da bi uvođenje videonadzora javnih prostora bio veliki napredak u metodologiji rada policije jer bi, s obzirom na sve prisutniji problem nedovoljnog broja policijskih službenika u odnosu na postojeći ustroj i problematiku, omogućio da jedan policijski službenik istodobno nadzire više javnih površina. Iz ovoga se može zaključiti da autori pretpostavljaju da bi policijski službenici vršili nadzor nad kamerama na „javnom prostoru“ što je idealno, ali porast broja takvih kamera bi u budućnosti mogao znatno otežati nadzor svih tih kamera od strane policijskih službenika. Iako se autori uglavnom bave suradnjom s lokalnom zajednicom i novčarskim institucijama (Zakon o zaštiti novčarskih institucija (NN 56/15)) i zakonskim mogućnostima takve suradnje i korištenja snimaka u kasnijim sudskim postupcima, u svojem radu spominju i mogućnost korištenja (i način korištenja) kamera koje su postavljenje (ili poradi zakonskih obaveza ili poradi vlastite zaštite) od strane privatnih kompanija. Autori smatraju da bi cijeli taj sustav već postojećih videonadzora bio potpuno funkcionalan (sa stajališta policije) samo ako se međusobno povežu i stave pod jedinstveni nadzor u koji bi uvid imala i policija. Na taj način bi se prema istim autorima povećala efikasnost policijskih službenika ali i mogućnosti kasnijeg dokazivanja

određenih protupravnih ponašanja. Da postoji znatan napredak upravo u smjeru direktnog udaljenog pristupa kamerama od strane policije govori i činjenica da policija pristupa direktno prema 354 kamere instalirane na 118 lokacija u gradu Zagrebu, a koje je instalirao Grad Zagreb. (Kraljević, Direktno.hr, 10.2.16.) Korisnost ovakvog pristupa potvrđuje i činjenica da je policija do sada izuzela tri tisuće slika ili detalja s ovih kamera.

Kako bi mogli prikazati sve stvarne prednosti jednog takvog sustava tehničke zaštite koje bi policija imala kada bi bila spojena na njega, koristiti ćemo funkcionalnost već ranije opisanog nadzornog centra. Dakle, pretpostavimo da policija ima direktnu vezu na ovakav sigurnosni centar u koji su spojeni svi alarmi i kamere neke kompanije, s mogućnošću uvida u bilo koju kameru od strane policije.

Nakon što bi do nadzornog centra došao alarm protuprepada (pretpostavimo da se radi o razbojništvu), isti takav signal zaprimila bi i policija u svojem nadzornom centru ili operativnom dežurstvu. Obzirom da su jasno propisane zakonske odredbe tko treba i što poduzeti po zaprimanju alarma, policija nebi bila dužna reagirati sve do trenutka dok nebi dobila obavijest zaštitara da se radi o razbojništvu. Takva procedura je i sada, samo bi u pretpostavljenoj situaciji policija imala alarm nekoliko minuta prije. Istovremeno, ukoliko se radi o razbojništvu (prethodno smo opisali da se u nadzornom centru s dolaskom alarmnog signala na centralnom video zidu prikazuju kamere s lokacije) policija bi u svojem nadzornom centru mogla vidjeti sve kamere koje se nalaze na tom objektu a time i osobe (počinitelje?) koje su na tom objektu, karakteristike i boju odjeće, obuće, maskiranost, vozila, reg oznake, sredstva s kojim se vrši razbojništvo ako se koriste, smjer kojim odlazi počinitelj ako je razbojništvo već počinjeno, jesu li žrtve ozlijeđene i niz drugih podataka.

Raspolaganje s ovakvim podacima skoro u realnom vremenu neprocjenjivo doprinosi ne samo brzini policijskog postupanja, nego i načinu na koji će policijski službenici postupati u konkretnom slučaju. Na ovaj način bitno se skraćuje vrijeme zaprimanja obavijesti od strane zaštitara, ali i smanjuje mogućnost greške kod dostavljanja podataka temeljem kojih policijski službenik donosi odluku o načinu postupanja. Upućivanje policijskih službenika na mjesto razbojništva gdje ih se može odmah obavijestiti o detaljima počinitelja kao što su da ima ili nema vatreno oružje, opis odjeće koju nosi, vozilo s kojim se je udaljio ili im se čak može dostaviti fotografija događaja, u potpunosti mijenja metodiku postupanja policijskih službenika kod dolaska do mjesta razbojništva. Sve ove mogućnosti dostupne su i kada se radi o provali u takve objekte. Direktnim pristupima kamera iz nadzornog centra policije „uživo“ bi se mogla

promatrati provala i istovremeno davati upute policijskim službenicima na terenu. Važno je naglasiti da bi takvim tehničkim rješenjem bilo moguće ne samo gledanje snimke koja bi se pojavljivala u trenutku alarma, odnosno trenutne situacije, već i pregled prijašnjih događaja, pa onda i „skidanje“ video zapisa, i sve to bez potrebe angažiranja korporativne sigurnosti kompanije. Danas ukoliko policija treba neku snimku video zapisa sa sustava video nadzora neke kompanije, dostavlja službeni zahtjev kompaniji (ponekad prethodno odlazi na lokaciju kako bi pregledala snimku i utvrdila točno vrijeme koje treba snimiti) i tada zaposlenici kompanije ili ovlašteni serviseri odlaze na lokaciju ili u nadzornom centru kompanije vrše snimanje. U situacijama kada treba sačuvati tajnost zahtjeva policije za snimkom, ovakvom trenutnom procedurom to predstavlja veliki rizik. Nedvojbeno je da bi ovakvim pretpostavljenim rješenjima policija imala mogućnost brže reakcije kod ovakvih događaja kao i neograničen pristup pregledu i snimanju video zapisa, ipak treba naglasiti da postoje i određene tehničke pretpostavke koje bi trebalo zadovoljiti kao i financijski troškovi. Jedan od preduvjeta je propusnost (engl. bandwidth) infrastrukture kroz koju prolazi video signal, kako od lokacije gdje se nalaze kamere, do nadzornog centra kompanije, tako i od nadzornog centra policije do nadzornog centra kompanije. Većina te infratrukture u vlasništvu je privatnih kompanija koje naplaćuju korištenje iste pa dolazimo i do financijskih troškova ovakvih rješenja i pitanja tko će platiti te troškove-policija ili privatna kompanija. Obzirom na brz razvoj tehnologija za pretpostaviti je da će ti troškovi svakim danom biti sve manji a mogućnosti sve veće. U ovom radu nećemo se baviti različitim tehničkim rješenjima koja su moguća već je namjera autora samo da upozori na moguće tehničke i financijske pretpostavke.

Osim spomenutih tehničkih i financijskih pretpostavki puno je važnije zakonsko uređenje ovog područja koje bi trebalo jasno definirati prava i obaveze svih koji bi bili dio ovog procesa, od državnih tijela, prvenstveno policije, do vlasnika ovakvih sustava, privatnih kompanija. Trenutno ovo područje uređuju već spomenuti Zakon o privatnoj zaštiti (NN 68/03, 31/10, 139/10.), Pravilnik o uvjetima i načinu provedbe tehničke zaštite (NN 198/03) i Zakon o zaštiti novčarskih institucija (NN 56/15). Kako je normativno uređeno upravo spajanje policije na sustave tehničke zaštite obveznika ovih zakona pokazuje i slijedeći primjer. U Članku 20. Pravilnika o uvjetima i načinu provedbe tehničke zaštite (NN 198/03) stoji: „Sustavi tehničke zaštite *ne smiju* se programirati tako da se signal nastao aktiviranjem sustava tehničke zaštite prenosi direktno na sustav veza Ministarstva unutarnjih poslova.“ Međutim, Zakon o zaštiti novčarskih institucija (NN 56/15) u Članku 13. stavak (3) navodi: „Ako postoje tehničke mogućnosti, sustavi video-nadzora iz članka 8. i protuprovalni i protuprepadni sustavi iz članka

12. ovoga Zakona mogu biti spojeni i na tehničke sustave Ministarstva unutarnjih poslova.“. Moguće obrazloženje ovih odredbi je i to da Zakon o zaštiti novčarskih institucija točno definira na koje se institucije odnosi ova odredba, dok Pravilnik općenito definira uvjete i način provedbe tehničke zaštite, međutim ovakve odredbe su i dalje zbunjujuće. Uz analizu ovih Zakonskih odredbi i Pravilnika bilo bi potrebno izvršiti i analizu zakonskih odredbi koje u sebi definiraju ovlasti policije na ovom području, od snimanja na javnim prostorima, izuzimanja snimaka i fotografija za određene potrebe, sve do direktnog spajanja s mogućnošću pregledavanja i snimanja video zapisa koji se nalazi u privatnim kompanijama i prostorima istih. Ovdje treba naglasiti i Zakon o zaštiti osobnih podataka (NN 103/03.,118/06., 41/08., 130/11., 106/12) koji također uređuje ovo područje. Protrka (2012) u svojem radu obrađuje upravo tu normativnu uređenost u Republici Hrvatskoj s naglaskom na Ministarstvo unutarnjih poslova kao voditelja najveće zbirke osobnih podataka u Republici Hrvatskoj i kao državno tijelo koje se svakodnevno susreće izazovima ustrojavanja novih evidencija. Obzirom na složenost ove problematike mišljenja smo da treba provesti dodatna istraživanja u budućim radovima kako i na području zakonodavstva koje uređuje direktan pristup službenika policije ovakvim sustavima tako i na području zaštite osobnih podataka.

Desetine tisuća kamera „pokrivaju“ razne prostore i objekte, od kamera postavljenih na bankomatima, u trgovačkim centrima, benzinskim postajama, bankama, mjenjačnicama, stotinama drugih objekata. Pretpostavka da policija ima neograničen udaljen pristup svim tim kamerama koje su u vlasništvu privatnih kompanija otvara nove neslućene mogućnosti u postupanju policije a time i podizanju razine javne sigurnosti. Iako ovakva iskustva postoje u drugim zemljama u ovom radu nismo spominjali takva iskustva niti predlagali takva rješenja. Rješenja iz drugih država mogla bi se koristiti u ostvarivanju preduvjeta u Republici Hrvatskoj koji bi omogućili da policija (ili neka druga državna tijela?) imaju udaljeni pristup svim sustavima tehničke zaštite privatnih kompanija. Bez namjere definiranja baš svih preduvjeta smatramo najvažnijima donošenje novih ili jasnije uređenje postojećih zakonskih ili podzakonskih akata koji uređuju ovo područje. Pitanje zaštite osobnih podataka odnosno općenito zaštite privatnosti i ljudskih prava predstavljati će poseban izazov. Mogući troškovi i tko će ih snositi također će se pojaviti kao jedno od pitanja. Sama operacionalizacija ovakvog modela iziskivati će i odgovore na niz „operativnih“ pitanja od toga koji policijski službenici će raditi na tim poslovima, gdje se i koliko dugo čuvaju snimke ukoliko se vrši snimanje video zapisa, tko odlučuje o uništavanju zapisa, procedure postupanja, to toga gdje se nalaze ti centri i tko sve ima pristup u njih. Privatne kompanije su i prije početka rada ovakvih nadzornih

centara trebale ispuniti sve zakonske obaveze, propisati sve interne procedure tj. dati odgovor na ova i slična pitanja. Njihovo iskustvo svakako bi se moglo iskoristiti kod mogućih budućih aktivnosti na ovom području.

Zaključak

Većina autora navedenih u ovome radu nedvosmisleno predlažu i obrazlažu potrebu suradnje privatnog sektora i policije te lokalne zajednice i policije. Isto tako opisuju se zakonske mogućnosti takve suradnje, sve prednosti takve suradnje ne samo za policiju već i za privatni sektor, sve građane, javnu sigurnost općenito, međutim, prema podacima dostupnim autoru ovog članka ta suradnja nije u potpunosti ostvarena.

Sve navedeno ukazuje da bi u slučaju da policija ima mogućnost direktnog, udaljenog pristupa svim sustavima tehničke zaštite, prvenstveno video nadzoru koje imaju privatne kompanije, može značajno utjecati na povećanje razine javne sigurnosti. Mišljenja smo da bi ovakva situacija utjecala djelomično i na dosadašnju metodologiju postupanja policije u pojedinim slučajevima.

Možda će nekima zastrašujuće djelovati mogućnost da policija ima neograničen udaljeni pristup svim kamerama koje koriste privatne kompanije i lokalna zajednica, ali će u većem ili manjem opsegu u vrlo bliskoj budućnosti to će biti svakodnevnica, a dio toga događa se već i danas. Cilj ovog rada je temeljem opisanog primjera rada nadzornog centra u privatnoj kompaniji potaknuti stručnu i znanstvenu raspravu i istraživanja o različitim mogućnostima korištenja ovakvih sustava u podizanju javne sigurnosti. Rasprava bi trebala obuhvatiti zakonska, tehnička, financijska i sva druga područja važna za ovu temu.

Literatura

Abrahamsen, R., Williams, M. C., (2005). The Globalization of Private Security, London, Royal Institute for International Affairs. The World Today, 2005, 5-7.

Ivandić Vidović D., Karlović L., Ostojić A., (2011). Korporativna sigurnost. Zagreb, AKD.

Kovacich, L. G., Halibozek, P. E. (2002). The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program. Burlington, Butterworth-Heinemann.

Kraljević, M., Direktno.hr. http://direktno.hr/en/2014/domovina/38595/Zagreb-nove-nadzorne-kamere-na-jo%C5%A1-23-lokacije-ukupno-118.htm, 10. veljača 2016.

Pavliček, J., (2010). Partnerstvo javne i privatne sigurnosti. Konferenciji hrvatskih menadžera sigurnosti, Zagreb, 25. i 26. studenog 2010.

Pothraški, F. Tršinski, S., Kancir, K.: Prijedlog unapređenja rada policije uvođenjem videonadzora javnih prostora. Policija i sigurnost, godina 17. (2008), broj 3-4, str. 243-253, Zagreb.

Protrka, N. Normativna uređenost zaštite osobnih podataka u Republici Hrvatskoj. Policija i sigurnost, godina 22. (2013), broj 4., str. 509_521, Zagreb.

Zagreb između kamera, punjenja proračuna, sigurnosti i privatnosti građana. http://www.svijetsigurnosti.com/blogs/5847-zagreb-izmedu-kamera-punjenja-proracuna-sigurnosti-i-privatnosti-gradana Ostojić, A., 5. veljače 2016.

Zakon o zaštiti novčarskih institucija. "Narodne novine", br. 56/15

Zakon o zaštiti osobnih podataka. "Narodne novine", br. 103/03.,118/06., 41/08., 130/11., 106/12. Zagreb.