

Javna bezbednost i sigurnost u konceptu pametnih gradova

Koncepti, funkcije, subjekti i resursi – uporedna analiza evropskih gradova

Serbian/English version

Ključne preporuke za efikasan pametan-bezbedan grad :

1. Bezbednost projektovati kao osnovni sloj, ne kao dodatak. Bezbednost kao nužni uslov nastanka pametnog grada od prve faze planiranja. Sastavni deo arhitekture sistema (security-by-design).
2. Upostaviti jedinstveni plan odgovora na krize. Zamena niza nepovezanih reakcija pojedinačnih službi jednim integrisanim planom. Definisati jasne protokole komandovanja, eskalacije i koordinacije između policije, vatrogasaca, hitne pomoći i civilne zaštite.
3. Integrisati tri sloja sistema kroz zajedničku platformu. Pošto se funkcionalni, bezbednosni i inteligentni sloj prepliću (ista kamera služi i funkcionalnosti i bezbednosti), izgraditi jedinstvenu operativnu platformu (integrisani bezbednosni operativni centar) koja objedinjuje podatke iz svih slojeva.
4. Prioritizovati brzinu reagovanja kao ključni metrički pokazatelj. U kriznoj situaciji vreme je razlika između života i smrti. Merenje i optimizacija vremena odgovora (response time) kao primarni KPI — od detekcije pretnje do intervencije na terenu.
5. Kombinovati inteligentna i proverena „analogna“ rešenja. Ne oslanjati se isključivo na AI i IoT. Zadržati i osnažiti proverene mere bezbednog grada: javnu rasvetu, patrole, fizičku zaštitu, planove evakuacije i civilnu zaštitu, koje ne zavise od tehnologije i funkcionišu i pri otkazu sistema.
6. Osigurati sajber-otpornost kritične infrastrukture. Pošto AI, 5G i IoT povezuju energetiku, saobraćaj i javne servise, jedan sajber-napad može paralisati grad. Ugraditi redundanciju, segmentaciju mreža i planove kontinuiteta rada pri otkazu digitalnih sistema.
7. Upostaviti upravljanje podacima i zaštitu privatnosti. Masovni video-nadzor i senzori generišu ogromne količine podataka. Definisati jasne politike prikupljanja, čuvanja, pristupa i brisanja podataka usklađene sa GDPR-om, kako bi se izbegli incidenti povezani sa zloupotrebom podataka.
8. Prevazići usko shvatanje bezbednosti svedeno na video-nadzor. Kamere su alat, ne strategija. Proširiti koncept bezbednog grada na smanjenje kriminala, urbanog nasilja, terorističkih pretnji i upravljanje velikim krizama — kroz prevenciju, a ne samo detekciju.
9. Definisati subjekte, funkcije i resurse kroz jasnu podelu odgovornosti i nadležnosti. Precizno mapiranje ko šta radi (subjekti), koje funkcije sistem obavlja i koji su resursi (ljudski, tehnički, finansijski) potrebni i koje su nadležnosti sa ovlašćenjima. Izbegnuti preklapanja nadležnosti i „sive zone“ odgovornosti.

10. Graditi otpornost (resilience), ne samo zaštitu. Cilj nije samo sprečiti incident, već osigurati da grad nastavi da funkcioniše tokom i posle krize. Ugraditi redundanciju, brz oporavak (recovery) i sposobnost adaptacije na nove i hibridne pretnje.

1. Uvod i pojmovno određenje

Pametni grad danas nije tehnološka moda, već strateški izbor. Gradovi širom sveta menjaju način svog funkcionisanja da bi bili efikasniji, zeleniji i sigurniji. Ulaganja govore jasno: dok je 2018. godine na pametne gradove globalno potrošeno oko 80 milijardi američkih dolara, vrednost ovog tržišta dostigla je preko 950 milijardi do čak 1 bilion američkih dolara u 2025. godini (u zavisnosti od obuhvaćenih tehnoloških sektora poput pametne mrežne infrastrukture, IoT rešenja i pametnog saobraćaja). Iza te cifre stoji politička odluka donosilaca odluka da digitalnu transformaciju grada tretiraju kao pitanje razvoja, konkurentnosti i, sve više, nacionalne bezbednosti. Integracija veštačke inteligencije (AI), 5G mreža i interneta stvari (IoT) u pametno upravljanje energijom, javni prevoz i bezbednost građana

Ipak, jedan sloj te transformacije sistematski zaostaje. Istraživanja pokazuju da oblast bezbednosti u razvojnim strategijama pametnih gradova dobija manje pažnje nego mobilnost, energetika ili e-uprava. To je strateška greška. Grad je složeno okruženje, sistem sistema, u kojem su pametni i bezbedni koncepti neodvojivi. Bez bezbednosti nema pametnog grada - postoji samo tehnološki opremljen grad izložen riziku. Zato bezbedan grad ovde tretiramo kao osnovni, nužni uslov nastanka pametnog grada, a dva pojma definišemo na sličan način.

Slojevita struktura sistema. Sistem se može posmatrati kroz tri sloja. Prvi je funkcionalni sloj - komponente koje obezbeđuju samu funkcionalnost sistema, bez daljeg bavljenja bezbednošću ili „pametnošću“ rešenja. Drugi je bezbednosni sloj - komponente i delovi komponenti koji primarno služe kompleksnoj zaštiti korisnika, samog sistema i njegovog okruženja. Treći je sloj inteligentnih komponenti, kojim se istraživanja pametnih gradova pretežno i bave. Ova tri sloja se prepliću. Ista kamera, isti senzor, ista mreža istovremeno mogu služiti i funkcionalnosti, i bezbednosti, i „pametnosti“ sistema. Upravo to preplitanje čini bezbednost pametnog grada tako zahtevnom za projektovanje.

Treba razlikovati dva pojma. Pametan grad počiva na inteligentnim inovacijama. Bezbedan grad je širi pojam - on koristi i starija, proverena rešenja koja još ne zavise od inteligentnih tehnologija: civilnu zaštitu, javnu rasvetu, patrole, fizičku zaštitu, planove evakuacije, sisteme osmatranja i obaveštavanja. Termin „bezbedan grad“ prisutan je u stručnoj literaturi, ali nije obrađivan ni tako često ni tako duboko kao „pametan grad“. Dok se većina autora zaustavlja na smanjenju kriminala pomoću kamera, širi uvid koji nude pojedini autori ukazuje na kompletan set funkcionalnosti koji se tiču vanrednih situacija, elementarnih nepogoda i drugih bezbednosnih izazova.

Mnogi autori odbacuju usko shvatanje bezbednog grada svedeno na video-nadzor. Njihov zaključak je da bezbedan grad ima tri neodvojiva cilja. Prvo, on mora uspostaviti jedinstveni plan odgovora na velike krize, a ne niz nepovezanih reakcija pojedinačnih službi. Drugo, on

treba da unapredi bezbednost i kvalitet života smanjenjem kriminala, urbanog nasilja i terorističkih pretnji, reč je o podizanju osećaja sigurnosti, koji posledično dovodi do povećanja ekonomske aktivnosti. Treće, i po njima presudno, on mora ubrzati reagovanje na krizne pojave - jer u kriznoj situaciji vreme nije statistika, već razlika između života i smrti. Zaključak iz analize literature: kamera koja samo snima, a ne skraćuje vreme reakcije, nije bezbednosno rešenje nego arhiva. Ovu tezu uzimamo kao polaznu tačku analize odgovora na savremene pretnje.

2. Bezbednosna funkcija u uslovima izazova velikih gradova

Veliki grad je koncentracija svega - ljudi, kapitala, infrastrukture, ali i rizika. Gustina koja grad čini produktivnim istovremeno ga čini ranjivim. Zato bezbednosna funkcija pametnog grada mora odgovoriti na nekoliko izazova koji su specifični upravo za velike urbane sredine.

2.1. Opšta i ljudska bezbednost

Bezbednost grada odavno nije samo suzbijanje kriminala. Uporedo sa konvencionalnim rizicima rastu i nevojni rizici: hibridne pretnje, sajber napadi, prekidi u lancima snabdevanja, ranjivost transportnih koridora, požari, poplave, zemljotresi i narušavanje kritične infrastrukture. Bezbedan grad zato mora da štiti opštu bezbednost - otpornost sistema kao celine - ali i ljudsku bezbednost, odnosno konkretnog čoveka u konkretnoj ulici. Reč je o zaštiti od poplava, požara, saobraćajnih nesreća, zdravstvenih kriza i nasilja. Grad koji obara stopu kriminala, a ne ume da zaštiti građanina od poplave ili da ga brzo evakuise, nije bezbedan grad.

2.2. Osećaj sigurnosti

Bezbednost je kriterijum, dok je sigurnost subjektivan osećaj pojedinca. Postoji razlika između bezbednosti i osećaja sigurnosti, i ta razlika je politička ili sociološka. Statistika može pokazivati pad kriminala, a građani se i dalje osećati nesigurno. Osećaj sigurnosti je resurs - on određuje da li će ljudi koristiti javni prostor, da li će investitori dolaziti, da li će grad noću živeti. Vidljiva rasveta, prisustvo patrola, funkcionalne kamere i brz odgovor službi grade poverenje. Nevidljiv, netransparentan ili prekomeran nadzor to poverenje troši. Zadatak bezbednog pametnog grada nije da građanina posmatra, već da ga zaštiti - i da on to zna.

2.3. Brzina reakcije i uloga veštačke inteligencije

Ovde se odlučuje sve. Grad ima previše kamera i previše podataka za ljudsko posmatranje. Ogroman broj kamera stvara više snimaka nego što ijedan tim operatera može delotvorno da prati, pa deo incidenata prođe nezapaženo dok se ne dogode. Tu nastupa veštačka inteligencija. Video-analitika ne zamenjuje operatera - ona mu vraća pažnju. Sistem sam prepoznaje sumnjivo ponašanje, formiranje gužve, pad čoveka, napušten predmet ili opasan objekat, i tek tada podiže upozorenje. Operater dobija filtriran signal umesto zid od ekrana i gomile kadrova koje treba analizirati.

Efekat je merljiv u sekundama. Kada algoritam detektuje incident i automatski prosledi upozorenje kontrolnom centru, službeniku ili vozilu najbližem mestu događaja, lanac odluke se skraćuje. Upravo to je ono što je Fedorov(bivši ministar odbrane Ukrajine) tražio, kada je preuzeo modernizaciju borbenih sistema na osnovu AI analitike, ubrzanje reagovanja na krizne

pojave i situacije. Veštačka inteligencija je, u tom smislu, tehnološko ispunjenje jednog starog bezbednosnog zahteva. Ali brzina bez pouzdanosti je opasna: lažna uzbuna troši resurse, a pristrasan algoritam kreira neadekvatan odgovor. Zato AI u bezbednom gradu mora biti brza, ali i tačna, proverljiva i pod ljudskom kontrolom.

2.4. Pouzdanost infrastrukture

Nijedna od nabrojanih funkcija ne vredi ako je infrastruktura na kojoj počiva nepouzdana. A pouzdanost nije samo tehničko pitanje otpornosti mreže na kvar — ona je i pitanje toga ko je proizveo opremu i ko joj, u krajnjoj liniji, može pristupiti. Bezbednosni sistem grada obrađuje najosetljivije podatke: lokacije, kretanja, lica (po posebnom odobrenju), obrasce ponašanja miliona ljudi bez ličnog nadzora pojedinaca. Ako ta oprema sadrži ranjivosti ili skrivene pristupne tačke, grad nije izgradio štit - izgradio je vrata za ulaz zlonamernih aktera.

Ovo više nije teorijska bojazan. Nezavisni istraživači godinama dokumentuju „backdoor“ pristupe, ugrađene fabričke lozinke i nezakrpljene ranjivosti u opremi pojedinih kineskih proizvođača, pre svih Hikvision-a i Dahua-e. Zbog toga se niz država kreće ka njihovom isključivanju iz osetljivih sistema. Sjedinjene Države su ove kompanije, zajedno sa Huawei-em, ZTE-om, stavile na „Covered List“, a Savezna komisija za komunikacije (FCC) je 2025. i 2026. godine proširila zabranu i na starije, ranije odobrene modele kada se koriste za javnu bezbednost, zaštitu državnih objekata i fizičko obezbeđenje kritične infrastrukture. Ujedinjeno Kraljevstvo je naložilo uklanjanje kineske nadzorne opreme sa osetljivih državnih lokacija, sa rokom koji je vodio ka potpunoj zameni. Kanada je zabranila nabavku ove opreme na saveznom nivou, dok pojedine članice EU — Litvanija je uklonila Hikvision iz državnih zgrada, a nemačke bezbednosne službe upozoravaju na kinesku opremu u kritičnoj infrastrukturi jer deluju samostalno.

Poruka je nedvosmislena. Kineski invazivni alati nadzora predstavljaju direktnu opasnost po nacionalnu, društvenu i korporativnu bezbednost, i njihova cena nikada nije samo cena uređaja - to je cena zavisnosti. Nekritička nabavka „jeftine“ opreme danas znači skupu i tešku zamenu sutra, uz rizik da su podaci već kompromitovani. Pouzdan bezbedan grad zato ne bira dobavljača po ceni, već po tome čijoj jurisdikciji taj dobavljač odgovara. Bezbednost lanca snabdevanja opremom postala je sastavni deo bezbednosti samog grada.

3. Funkcije, subjekti i resursi bezbednog pametnog grada

3.1. Funkcije

Operacionalizovan, bezbedan grad obavlja pet funkcija:

- Prevencija (odvraćanje) - vidljive kamere, rasveta i patrole smanjuju priliku i motiv za krivično delo ili prekršaj.
- Detekcija i rano upozoravanje - prepoznavanje incidenata, sumnjivog ponašanja, gužvi ili opasnih objekata u realnom vremenu, sve češće uz pomoć VI.
- Reagovanje - usmeravanje patrola, vozila hitnih službi i resursa ka mestu incidenta, uz koordinaciju više službi.

- Istraga i dokazivanje - snimci i podaci služe identifikaciji, gonjenju i procesuiranju učinilaca, čime raste stopa rešenih predmeta.
- Upravljanje krizama - jedinstveni plan odgovora na velike krize (poplave, požari, teroristički napadi, masovni događaji, akcidenti) i obaveštavanje stanovništva.

3.2. Subjekti

Bezbednost pametnog grada nije zadatak isključivo policije. Policija preduzima zakonite radnje iz svoje nadležnosti, koordinira i pomaže, ali uz nju deluje širok krug subjekata:

- Gradske i lokalne uprave sa službama za komunalnu bezbednost i javni red (buka, divlje odlaganje otpada, vandalizam...).
- Civilni operateri video-nadzora -obučeni operateri u urbanim nadzornim centrima koji kamere prate 24 časa dnevno, 7 dana u nedelji, i prosleđuju informacije policiji.
- Hitne službe - vatrogasci, hitna pomoć i civilna zaštita, povezani preko zajedničke platforme za dojavu i dispečing.
- Privatni sektor - tehnološke i bezbednosne kompanije, telekom operateri, integratori sistema i pružaoci privatnog obezbeđenja.
- Operateri kritične infrastrukture i javnog prevoza, koji upravljaju sopstvenim, ali umreženim kamerama.
- Građani i zajednica - putem aplikacija za dojavu, privatnih kamera i saradnje sa vlastima.

3.3. Resursi

Resursi obuhvataju tehničku infrastrukturu (optičke mreže, 5G, senzore, IP kamere, video-analitikum i platforme za hipernadzor), ljudske resurse (operatere, analitičare, patrole), organizacione resurse (urbane nadzorne centre i zajedničke operativne centre) i finansijske resurse, sve češće spojene javnim i privatnim ulaganjima. Ključno pitanje jeste ko te resurse obezbeđuje i kontroliše - a naročito ko nadgleda gradske kamere. Na to odgovaraju studije slučaja. Važna napomena se odnosi na to da privatni sektor deluje u sopstvenom kapacitetu ali u okviru sistema nad kojim nadzor, sertifikaciju, standardizaciju, licence i obuke vrši državni organ – Ministarstvo unutrašnjih poslova ili Ministarstvo Odbrane. Istovremeno delokrug rada privatnog sektora je strogo uređen zakonima i podložen je kontroli u svakom trenutku. Dakle, država se ni u jednom svetskom primeru nije odrekla svoje ključne uloge kada je reč o oblasti bezbednosti, već racionalizuje kapacitete. Privatna tehnološka kompanija u oblasti bezbednosti na osnovu svoje poslovne odluke i tržišta razvija određene proizvode koji mogu biti uspešni, a mogu se pokazati kao propala investicija, dok država bira najbolji proizvod, umesto da sama ulaže novac u istraživanje i razvoj.

4. Studije slučaja evropskih gradova

4.1. London - najnadziraniji zapadni grad i model javno-privatne saradnje

London se s razlogom naziva prestonicom video-nadzora zapadnog sveta. Procene ukupnog broja kamera dostižu i preko 940.000 uređaja u javnom i privatnom prostoru. Odnos je poučan: privatni akteri -preduzeća, stambene zgrade, domaćinstva /- poseduju otprilike sedamdeset puta više kamera od javnih vlasti. Metropolitanska policija upravlja sa oko 3.000 javnih kamera i koristi dodatnih oko 24.000 kamera koje policajci nose na telu, dok Transport for London u metrou održava preko 15.000 kamera. Prosečan Londonac biva snimljen do sedamdeset puta dnevno.

Javno-privatna i međuopštinska saradnja. Londonski model počiva na partnerstvu više nivoa. Kroz program Connected London i ulaganje gradske uprave od oko 30 miliona funti u optičku pokrivenost, instalirano je i unapređeno preko 300 kamera, uz senzore za kvalitet vazduha i praćenje saobraćaja; jasnija slika postala je dostupna policiji radi identifikacije i gonjenja učinilaca. Na opštinskom nivou, Hammersmith & Fulham ulaganjem od oko 5,4 miliona funti mrežu je proširio na blizu 2.000 kamera, a sporazumom sa Vestminsterom njegovi operateri nadgledaju 100 novih kamera u vestminsterskim stambenim zonama — finansiranih od Vestminstera, bez troška za poreske obveznike Hammersmith & Fulham-a.

Ko nadgleda kamere. Snimke ne prati policija, već posebno obučeni civilni operateri video-nadzora, 24 časa dnevno, usredsređeni na antisocijalno ponašanje, buku i žarišta nezakonitog odlaganja otpada, dok policajci rade rame uz rame u zajedničkom partnerstvu. Britansko iskustvo pokazuje i granicu modela: ogroman broj kamera stvara previše podataka za delotvorno ljudsko posmatranje. Odatle zaokret ka pametnom nadzoru - policija je od privatnog sektora tražila „dokaz koncepta“ za VI nadzor sposoban da otkrije predmete poput noževa. London istovremeno ilustruje i pitanje pouzdanosti opreme: upravo je Ujedinjeno Kraljevstvo među prvima naložilo uklanjanje kineske nadzorne opreme sa osetljivih državnih lokacija.

4.2. Nica - „safe city“ laboratorija Francuske

Nica je najvideonadzirani grad Francuske. Broj kamera porastao je sa 220 (2008) na oko 5.000 (2024). Srce sistema je *Centre de Supervision Urbain (CSU)* - prvi kompleks video-zaštite stvoren u Francuskoj. Operateri, raspoređeni u tri sale, u realnom vremenu prate oko 90 ekrana: prva prostorija utvrđuje prekršaje „na delu“, druga prati kameru ispred svake škole i preko 1.000 kamera u mreži tramvaja i autobusa. CSU raspolaže pametnim kamerama sa 360° vizurom, nomadskim kamerama za privremene potrebe, kamerom za detekciju šumskih požara na dometu do 10 km i zvučnicima za emitovanje preventivnih i uzbunjivačkih poruka.

Javno-privatno partnerstvo, AI i krize. Nica je „Safe City“ projekat razvila sa privatnim gigantima (Thales, ranije Engie Ineo), uz operativno-istraživačko finansiranje od oko 10,9 miliona evra u vidu bespovratnih sredstava javne investicione banke BPI France, pod okriljem državnih tela. Cilj je bio prevazići puko prikupljanje podataka i razviti algoritme koji koreliraju izvore - uključujući društvene mreže, dojave građana i saobraćajni video - radi boljeg razumevanja situacija i predviđanja. Sistem centralizovanog upravljanja objedinjuje lokaciju incidenata, broj raspoloživih patrola i pristup kamerama u jedinstveni komandni centar. U vanrednim situacijama prate se morski udari i izlivanja reka radi zatvaranja priobalnih saobraćajnica, a snimke koriste spasilačke službe za procenu razmera nesreće.

Nica pokazuje i granicu. Grad je 2019. tokom karnevala sproveo prvi test prepoznavanja lica na javnim ulicama u Francuskoj, čime je otvorio raspravu o individualnim slobodama. Kritičari ukazuju na netransparentnost partnerstva grada i privatnih kompanija. Prema podacima grada, kriminal je opao a stopa rešenih slučajeva porasla, ali nezavisna procena je otežana upravo zbog te netransparentnosti - a netransparentnost, videli smo, troši osećaj sigurnosti.

4.3. Barselona - multi-agencijska platforma i 5G reagovanje

Barselona je svetski lider u primeni tehnologija pametnog grada. Grad je 2016. implementirao multi-agencijsku platformu za upravljanje vanrednim situacijama zasnovanu na sistemu računarski potpomognutog dispečinga, koja povezuje policiju, vatrogasce i hitnu pomoć u jedinstven odgovor - tačno onako kako je Fedorov zamislio jedinstveni plan reagovanja. Ekosistem je plod javno-privatnog konzorcijuma: Gradsko veće Barselone sarađivalo je sa Tehničkim univerzitetom Katalonije, superračunarskim centrom i kompanijama poput Cisca i Schneider Electrica na više od 3.000 uličnih ormarića i pet upotrebnih scenarija.

5G i brzina reakcije. U pilot-projektu 2022–2023. učestvovala je Guardia Urbana, gradska policija Barselone. Pet kamera povezanih na 5G omogućilo je brojanje vozila, analizu saobraćajnih tokova i automatske dojave o zagušenju, a automatizovana video-analitika osposobila je kamere da same detektuju vanredne situacije i generišu upozorenja koja se šalju kontrolnom centru, službenicima ili vozilima najbližim incidentu. Projekat je vodio konzorcijum od osam kompanija uz podršku fondacije Mobile World Capital Barcelona - još jedan primer da se bezbedan grad danas gradi kroz javno-privatna partnerstva. Barselona podseća i na organizacioni izazov: pametan grad nije samo tehnologija, već i saradnja stanovnika, lokalnih vlasti i profitno orijentisanih tehnoloških firmi u procesu urbanog planiranja.

5. Uporedna zapazanja

Javno-privatna partnerstva. Sve tri studije potvrđuju da se savremeni bezbedni gradovi grade kroz partnerstva. London kombinuje gradski program optičke infrastrukture, opštinska ulaganja i međuopštinske sporazume; Nica se oslanja na privatne integratore uz državno sufinansiranje; Barselona formira konzorcijume kompanija i akademskih institucija. Model se širi i van Evrope - inicijativa „Safe City Surat“ u Indiji prvi je projekat video-nadzora zasnovan na javno-privatnom modelu, sa 5.000 kamera. Ali partnerstvo nosi rizik. Izveštaji civilnog društva upozoravaju da pojedini dobavljači nude sisteme „bez početnih troškova“, čime lokalne vlasti ostaju zaključane u skupom i teško promenljivom ekosistemu, uz eroziju odgovornosti koja postoji kada nadzor sprovede javno odgovorni organi. Partnerstvo sa pogrešnim dobavljačem nije ušteda, već ranjivost.

Ko, pored policije, pomaže i ko nadgleda kamere. Pored policije deluju gradske službe komunalne bezbednosti, hitne službe, operateri javnog prevoza, privatne kompanije i sami građani. Video-nadzor po pravilu ne prate policajci, već obučeni civilni operateri u urbanim nadzornim centrima - u Londonu operateri Hammersmith & Fulham-a, u Nici operateri CSU-a, u Barseloni dispečeri - koji filtriraju i prosleđuju relevantne informacije nadležnim službama.

Da li je nadzor sprečio kriminal. Dokazi su mešoviti. Nica navodi pad kriminala i rast stope rešenih slučajeva; londonske opštine ističu brže vreme reakcije i suzbijanje prekograničnog, međuopštinskog kriminala. Ipak, delotvornost masovnog nadzora ostaje sporna, pre svega jer previše kamera stvara više podataka nego što ih operateri mogu efikasno da prate. Zato se težište pomera ka video-analatici i veštačkoj inteligenciji - ali AI vredi samo koliko je pouzdana oprema na kojoj radi.

Reagovanje na krize. Najzrelija je upravo krizna dimenzija. Multi-agencijska platforma i 5G dojava Barselone, CSU u Nici sa praćenjem poplava, morskih udara i požara i sa zvučnicima za uzbuđivanje, kao i povezivanje kontrolnih soba u Londonu - sve to potvrđuje zaključak Fedorova da bezbedan grad znači jedinstveni plan odgovora na velike krize i ubrzano reagovanje, a ne puko suzbijanje kriminala kamerama.

6. Zaključak

Bezbednost je najzapostavljeniji, a najvažniji sloj pametnog grada. Bez nje digitalna transformacija ostaje ranjiva. Bezbedan grad objedinjuje funkcionalni, bezbednosni i inteligentni sloj i spaja staro sa novim - rasvetu i patrolu sa video-analitikom, 5G mrežama i veštačkom inteligencijom. Primeri Londona, Nice i Barselone potvrđuju četiri zajedničke crte: oslonac na javno-privatna partnerstva; širok krug subjekata izvan policije; civilne operatere kao stvarne nadziratelje gradskih kamera; i sve dublju integraciju sistema radi bržeg odgovora na krize.

Ali iskustvo istih gradova povlači i tri crvene linije. Prvo, masovan nadzor sam po sebi ne obara kriminal - brzinu i tačnost donosi tek veštačka inteligencija koja operateru vraća pažnju i budnost. Drugo, osećaj sigurnosti gradi se transparentnošću i zaštitom prava, a troši prekomernim i nevidljivim nadzorom; građanin mora biti zaštićen subjekt, a ne posmatran objekat. Treće, i strateški presudno, pouzdanost sistema počinje kod dobavljača. Oprema kineskih proizvođača sa dokumentovanim ranjivostima nije jeftino rešenje nego skupa zavisnost, i sve veći broj država je zato uklanja iz osetljivih sistema. Bezbedan pametan grad bira infrastrukturu po pouzdanosti i jurisdikciji, a ne po ceni.

Zaključak je jednostavan. Bezbednost treba ugraditi kao integralni sloj od prvog dana planiranja - sa jasnim pravnim okvirom, transparentnim partnerstvima, pouzdanom infrastrukturuom i građaninom kao ravnopravnim subjektom. Upravo ta ravnoteža između efikasnosti, otpornosti na krize i zaštite prava bila je u središtu i 4. izdanja konferencije „Safe & Smart City“, vodećeg evropsko-izraelskog skupa koji okuplja preduzetnike, inovatore, globalne kompanije, startapove i donosiocima odluka u raspravi o budućnosti modernih gradova. Grad budućnosti biće pametan samo ako je, pre svega, bezbedan.

Public Safety and Security in the Concept of Smart Cities

Concepts, functions, subjects, and resources – a comparative analysis of European cities

Key recommendations for an effective safe-smart city:

1. **Design security as a foundational layer, not an add-on.** Security is a necessary condition for the creation of a smart city from the very first planning phase. It must be an integral part of the system architecture (security-by-design).
2. **Establish a unified crisis response plan.** Replace a series of disconnected reactions by individual services with a single integrated plan. Define clear protocols for command, escalation, and coordination between the police, fire departments, emergency medical services, and civil protection.
3. **Integrate the three system layers through a common platform.** Since the functional, security, and intelligent layers intertwine (the same camera serves both functionality and security), build a single operational platform (an integrated security operations center) that unifies data from all layers.
4. **Prioritize response speed as a key metric.** In a crisis situation, time is the difference between life and death. Measure and optimize response time as the primary KPI — from threat detection to field intervention.
5. **Combine intelligent and proven "analog" solutions.** Do not rely exclusively on AI and IoT. Retain and strengthen proven safe city measures: public lighting, patrols, physical protection, evacuation plans, and civil protection, which do not depend on technology and will function even during system failures.
6. **Ensure the cyber-resilience of critical infrastructure.** Because AI, 5G, and IoT connect energy, transport, and public services, a single cyber-attack can paralyze the city. Incorporate redundancy, network segmentation, and business continuity plans for when digital systems fail.
7. **Establish data management and privacy protection.** Mass video surveillance and sensors generate massive amounts of data. Define clear policies for data collection, storage, access, and deletion in compliance with GDPR, in order to avoid incidents related to data misuse.
8. **Overcome the narrow understanding of security reduced to video surveillance.** Cameras are a tool, not a strategy. Expand the safe city concept to include the reduction of crime, urban violence, terrorist threats, and major crisis management — through prevention, not just detection.
9. **Define subjects, functions, and resources through a clear division of responsibilities and competencies.** Precisely map who does what (subjects), which functions the system performs, what resources (human, technical, financial) are needed, and what the competencies and authorities are. Avoid overlapping jurisdictions and "gray zones" of responsibility.

10. **Build resilience, not just protection.** The goal is not only to prevent an incident but to ensure that the city continues to function during and after a crisis. Incorporate redundancy, rapid recovery, and the ability to adapt to new and hybrid threats.

1. Introduction and Conceptual Definition

A smart city today is not a technological trend, but a strategic choice. Cities around the world are changing the way they function to be more efficient, greener, and safer. Investments speak clearly: while around 80 billion US dollars were spent globally on smart cities in 2018, the value of this market has reached over 950 billion and is projected to hit up to 1 trillion US dollars in 2025 (depending on the included technological sectors like smart grid infrastructure, IoT solutions, and smart traffic). Behind this figure lies the political decision of policymakers to treat the digital transformation of a city as a matter of development, competitiveness, and, increasingly, national security. The integration of artificial intelligence (AI), 5G networks, and the Internet of Things (IoT) into smart energy management, public transport, and citizen security is paramount.

However, one layer of this transformation systematically lags behind. Research shows that the security domain in smart city development strategies receives less attention than mobility, energy, or e-government. This is a strategic mistake. A city is a complex environment, a system of systems, where smart and safe concepts are inseparable. Without security, there is no smart city - there is only a technologically equipped city exposed to risk. Therefore, we treat the *safe city* here as a basic, necessary condition for the emergence of a smart city, and we define the two concepts similarly.

Layered system structure. The system can be viewed through three layers. The first is the *functional layer* - components that provide the actual functionality of the system, without further addressing the security or "smartness" of the solution. The second is the *security layer* - components and parts of components that primarily serve the complex protection of the users, the system itself, and its environment. The third is the *intelligent components layer*, which smart city research predominantly focuses on. These three layers intertwine. The same camera, the same sensor, and the same network can simultaneously serve the functionality, the security, and the "smartness" of the system. It is exactly this intertwining that makes designing smart city security so demanding.

Two concepts should be distinguished. A smart city rests on intelligent innovations. A safe city is a broader concept - it also uses older, proven solutions that do not yet depend on intelligent technologies: civil protection, public lighting, patrols, physical security, evacuation plans, and observation and notification systems. The term "safe city" is present in professional literature, but it has not been explored as frequently or as deeply as "smart city". While most authors stop at crime reduction using cameras, the broader insight offered by certain authors points to a complete set of functionalities concerning emergencies, natural disasters, and other security challenges.

Many authors reject the narrow understanding of a safe city reduced to video surveillance. Their conclusion is that a safe city has three inseparable goals. First, it must establish a unified crisis response plan for major emergencies, rather than a series of disconnected reactions by

individual services. Second, it should improve security and quality of life by reducing crime, urban violence, and terrorist threats; this is about elevating the *feeling of safety*, which consequently leads to an increase in economic activity. Third, and crucially according to them, it must accelerate the response to crisis events - because in a crisis situation, time is not a statistic, but the difference between life and death. The conclusion from the literature analysis: a camera that only records, but does not shorten the reaction time, is not a security solution but an archive. We take this thesis as the starting point for analyzing responses to modern threats.

2. The Security Function Under the Challenges of Large Cities

A large city is a concentration of everything - people, capital, infrastructure, but also risk. The density that makes a city productive simultaneously makes it vulnerable. Therefore, the security function of a smart city must address several challenges that are highly specific to large urban environments.

2.1. General and Human Security

City security has long moved past mere crime suppression. Alongside conventional risks, non-military risks are growing: hybrid threats, cyber-attacks, supply chain disruptions, transport corridor vulnerabilities, fires, floods, earthquakes, and disruptions to critical infrastructure. A safe city must therefore protect general security - the resilience of the system as a whole - but also human security, i.e., the specific person on a specific street. This involves protection from floods, fires, traffic accidents, health crises, and violence. A city that lowers its crime rate but cannot protect a citizen from a flood or evacuate them quickly is not a safe city.

2.2. The Feeling of Safety

Security is an objective criterion, while safety is a subjective feeling of the individual. There is a difference between objective security and the feeling of safety, and that difference is political or sociological. Statistics can show a drop in crime, yet citizens may still feel unsafe. The feeling of safety is a resource - it determines whether people will use public spaces, whether investors will come, and whether the city will thrive at night. Visible lighting, the presence of patrols, functional cameras, and rapid response from services build trust. Invisible, untransparent, or excessive surveillance depletes that trust. The task of a safe smart city is not to observe the citizen, but to protect them - and to ensure they know it.

2.3. Response Speed and the Role of Artificial Intelligence

Everything is decided here. A city has too many cameras and too much data for human observation alone. A massive number of cameras creates more footage than any team of operators can effectively monitor, meaning some incidents go unnoticed until after they happen. This is where artificial intelligence steps in. Video analytics does not replace the operator - it redirects their attention. The system itself recognizes suspicious behavior, crowd formation, a person falling, an abandoned item, or a dangerous object, and only then raises an alert. The operator receives a filtered signal instead of a wall of screens and a pile of frames to analyze.

The effect is measurable in seconds. When an algorithm detects an incident and automatically forwards a warning to the control center, an officer, or the vehicle closest to the scene, the

decision chain is shortened. This is exactly what Fedorov (the former Minister of Defense of Ukraine) sought when he took over the modernization of combat systems based on AI analytics: accelerating the response to crisis phenomena and situations. Artificial intelligence is, in this sense, the technological fulfillment of an old security requirement. But speed without reliability is dangerous: a false alarm wastes resources, and a biased algorithm creates an inadequate response. That is why AI in a safe city must be fast, but also accurate, verifiable, and under human control.

2.4. Infrastructure Reliability

None of the listed functions matter if the underlying infrastructure is unreliable. And reliability is not just a technical issue of network resilience against failure — it is also a question of who manufactured the equipment and who, ultimately, can access it. The city's security system processes the most sensitive data: locations, movements, faces (under special authorization), and behavioral patterns of millions of people without the personal surveillance of individuals. If this equipment contains vulnerabilities or hidden access points, the city hasn't built a shield - it has built a door for malicious actors to enter.

This is no longer a theoretical fear. Independent researchers have spent years documenting "backdoor" accesses, built-in factory passwords, and unpatched vulnerabilities in the equipment of certain Chinese manufacturers, primarily Hikvision and Dahua. Because of this, a series of countries are moving toward excluding them from sensitive systems. The United States placed these companies, along with Huawei and ZTE, on the "Covered List," and the Federal Communications Commission (FCC) expanded the ban in 2025 and 2026 to include older, previously approved models when used for public safety, government facility protection, and physical security of critical infrastructure. The United Kingdom has ordered the removal of Chinese surveillance equipment from sensitive government sites, with a deadline leading toward complete replacement. Canada banned the procurement of this equipment at the federal level, while certain EU members — Lithuania has removed Hikvision from government buildings, and German security services warn against Chinese equipment in critical infrastructure because it operates autonomously.

The message is unambiguous. Invasive Chinese surveillance tools pose a direct threat to national, social, and corporate security, and their cost is never just the price of the device - it is the cost of dependency. Uncritical procurement of "cheap" equipment today means an expensive and difficult replacement tomorrow, with the risk that data is already compromised. A reliable safe city, therefore, does not choose a supplier by price, but by the jurisdiction that the supplier answers to. Supply chain security for equipment has become an integral part of the city's own security.

3. Functions, Subjects, and Resources of a Safe Smart City

3.1. Functions

Operationalized, a safe city performs five functions:

- **Prevention (deterrence)** - visible cameras, lighting, and patrols reduce the opportunity and motive for a crime or offense.

- **Detection and early warning** - recognizing incidents, suspicious behavior, crowds, or dangerous objects in real time, increasingly with the help of AI.
- **Response** - directing patrols, emergency service vehicles, and resources to the scene of an incident, alongside multi-agency coordination.
- **Investigation and proof** - footage and data serve to identify, pursue, and prosecute perpetrators, thereby increasing the case clearance rate.
- **Crisis management** - a unified response plan for major crises (floods, fires, terrorist attacks, mass events, accidents) and public notification.

3.2. Subjects

The security of a smart city is not exclusively the task of the police. The police take lawful actions within their jurisdiction, coordinate, and assist, but a wide circle of subjects operates alongside them:

- **City and local administrations** with services for communal security and public order (noise, illegal waste dumping, vandalism...).
- **Civilian video surveillance operators** - trained operators in urban monitoring centers who monitor cameras 24/7 and forward information to the police.
- **Emergency services** - firefighters, emergency medical services, and civil protection, connected via a shared platform for reporting and dispatching.
- **Private sector** - technology and security companies, telecom operators, system integrators, and private security providers.
- **Operators of critical infrastructure and public transport**, who manage their own but networked cameras.
- **Citizens and the community** - through reporting applications, private cameras, and cooperation with authorities.

3.3. Resources

Resources encompass technical infrastructure (fiber-optic networks, 5G, sensors, IP cameras, video analytics, and hyper-surveillance platforms), human resources (operators, analysts, patrols), organizational resources (urban monitoring centers and joint operations centers), and financial resources, increasingly merged through public and private investments. The key question is who provides and controls these resources - and particularly who monitors the city cameras. Case studies provide the answer. An important note refers to the fact that the private sector acts in its own capacity but within a system overseen, certified, standardized, licensed, and trained by a state body – the Ministry of Interior or the Ministry of Defense. At the same time, the private sector's scope of work is strictly regulated by laws and subject to control at any moment. Thus, in no global example has the state relinquished its key role regarding the security sector; rather, it rationalizes its capacities. Based on business decisions and market conditions, a private technology security company develops certain products that may be successful or turn out to be failed investments, while the state selects the best product instead of investing its own money into research and development.

4. Case Studies of European Cities

4.1. London - the most surveilled Western city and a model of public-private partnership

London is rightfully called the video surveillance capital of the Western world. Estimates of the total number of cameras reach over 940,000 devices in public and private spaces. The ratio is instructive: private actors — businesses, residential buildings, households — own approximately seventy times more cameras than public authorities. The Metropolitan Police manage around 3,000 public cameras and use an additional roughly 24,000 body-worn cameras, while Transport for London maintains over 15,000 cameras in the Underground. The average Londoner is recorded up to seventy times a day.

Public-private and inter-municipal cooperation. The London model rests on multi-level partnerships. Through the Connected London program and a city administration investment of around £30 million in fiber-optic coverage, over 300 cameras have been installed and upgraded, alongside air quality and traffic monitoring sensors; a clearer picture became available to the police for identifying and prosecuting perpetrators. At the borough level, Hammersmith & Fulham expanded its network to nearly 2,000 cameras with an investment of about £5.4 million, and through an agreement with Westminster, its operators monitor 100 new cameras in Westminster residential zones — funded by Westminster, at no cost to Hammersmith & Fulham taxpayers.

Who monitors the cameras. Footage is not monitored by the police, but by specially trained civilian video surveillance operators, 24 hours a day, focusing on anti-social behavior, noise, and illegal dumping hotspots, while police officers work side-by-side in a joint partnership. The British experience also shows the model's limit: a massive number of cameras creates too much data for effective human monitoring. Hence the shift toward smart surveillance - the police asked the private sector for a "proof of concept" for AI surveillance capable of detecting objects like knives. London simultaneously illustrates the issue of equipment reliability: it was the United Kingdom that was among the first to order the removal of Chinese surveillance equipment from sensitive government sites.

4.2. Nice - France's "safe city" laboratory

Nice is the most heavily video-surveilled city in France. The number of cameras grew from 220 (in 2008) to around 5,000 (in 2024). The heart of the system is the Centre de Supervision Urbain (CSU) - the first video protection complex created in France. Operators, distributed across three rooms, monitor about 90 screens in real time: the first room identifies offenses "in the act," the second monitors the camera in front of every school and over 1,000 cameras across the tram and bus network. The CSU is equipped with smart 360° cameras, nomadic cameras for temporary needs, a camera for detecting forest fires with a range of up to 10 km, and loudspeakers for broadcasting preventive and alert messages.

Public-private partnership, AI, and crises. Nice developed its "Safe City" project with private giants (Thales, formerly Engie Ineo), supported by operational-research funding of about 10.9 million euros in grants from the public investment bank BPI France, under the auspices of state bodies. The goal was to move beyond mere data collection and develop algorithms that correlate sources - including social networks, citizen reports, and traffic video

- for better situational awareness and forecasting. The centralized management system unifies incident locations, the number of available patrols, and camera access into a single command center. During emergencies, sea swells and river overflows are monitored to close coastal roads, and rescue services use the footage to assess the scale of an accident.

Nice also shows the limits. During the 2019 carnival, the city conducted the first test of facial recognition on public streets in France, sparking a debate on individual liberties. Critics point to the lack of transparency in the partnership between the city and private companies. According to city data, crime has dropped and the clearance rate has risen, but an independent assessment is hindered precisely because of this lack of transparency - and as we have seen, a lack of transparency depletes the feeling of safety.

4.3. Barcelona - multi-agency platform and 5G response

Barcelona is a global leader in applying smart city technologies. In 2016, the city implemented a multi-agency emergency management platform based on a computer-aided dispatch system, which links the police, firefighters, and emergency medical services into a unified response - exactly as Fedorov envisioned a unified reaction plan. The ecosystem is the fruit of a public-private consortium: the Barcelona City Council collaborated with the Polytechnic University of Catalonia, a supercomputing center, and companies like Cisco and Schneider Electric on more than 3,000 street cabinets and five use cases.

5G and response speed. The 2022–2023 pilot project involved the Guardia Urbana, Barcelona's municipal police. Five cameras connected to 5G enabled vehicle counting, traffic flow analysis, and automatic congestion alerts, while automated video analytics empowered the cameras to independently detect emergency situations and generate warnings sent to the control center, officers, or vehicles closest to the incident. The project was led by a consortium of eight companies with support from the Mobile World Capital Barcelona foundation - another example that a safe city today is built through public-private partnerships. Barcelona also highlights the organizational challenge: a smart city is not just technology, but the collaboration of residents, local authorities, and profit-oriented tech firms in the urban planning process.

5. Comparative Observations

Public-private partnerships. All three case studies confirm that modern safe cities are built through partnerships. London combines a city fiber-optic infrastructure program, borough investments, and inter-municipal agreements; Nice relies on private integrators with state co-financing; Barcelona forms consortia of companies and academic institutions. The model is expanding outside Europe as well - the "Safe City Surat" initiative in India is the first video surveillance project based on a public-private model, featuring 5,000 cameras. But partnership carries risk. Civil society reports warn that some vendors offer systems with "no upfront costs," trapping local authorities in an expensive, hard-to-change ecosystem, coupled with an erosion of the accountability that exists when surveillance is conducted by publicly accountable bodies. Partnering with the wrong vendor is not a saving, but a vulnerability.

Who, besides the police, helps and who monitors the cameras. Alongside the police operate city communal security services, emergency services, public transport operators, private companies, and citizens themselves. As a rule, video surveillance is not monitored by police

officers, but by trained civilian operators in urban monitoring centers - the Hammersmith & Fulham operators in London, the CSU operators in Nice, the dispatchers in Barcelona - who filter and forward relevant information to competent services.

Has surveillance prevented crime? The evidence is mixed. Nice reports a drop in crime and a rise in cleared cases; London boroughs highlight faster response times and the suppression of cross-border, inter-municipal crime. However, the effectiveness of mass surveillance remains contested, primarily because too many cameras generate more data than operators can efficiently track. Hence, the focus is shifting toward video analytics and artificial intelligence - but AI is only as valuable as the reliability of the equipment it runs on.

Crisis response. The crisis dimension is precisely the most mature one. Barcelona's multi-agency platform and 5G alerts, Nice's CSU tracking floods, sea swells, and fires along with warning loudspeakers, and the networking of control rooms in London - all this confirms Fedorov's conclusion that a safe city means a unified crisis response plan and accelerated reaction, rather than mere crime suppression via cameras.

6. Conclusion

Security is the most neglected, yet most important layer of a smart city. Without it, digital transformation remains vulnerable. A safe city unifies the functional, security, and intelligent layers, blending the old with the new - lighting and patrols with video analytics, 5G networks, and artificial intelligence. The examples of London, Nice, and Barcelona confirm four common traits: reliance on public-private partnerships; a wide circle of subjects beyond the police; civilian operators as the actual monitors of city cameras; and ever-deeper system integration for a faster response to crises.

But the experience of these same cities also draws three red lines. First, mass surveillance in itself does not reduce crime - speed and accuracy are delivered only by artificial intelligence that restores the operator's attention and vigilance. Second, the feeling of safety is built on transparency and rights protection, and it is depleted by excessive and invisible surveillance; the citizen must be a protected subject, not an observed object. Third, and strategically crucial, system reliability starts with the vendor. Equipment from Chinese manufacturers with documented vulnerabilities is not a cheap solution but an expensive dependency, which is why a growing number of countries are removing it from sensitive systems. A safe smart city chooses infrastructure based on reliability and jurisdiction, not price.

The conclusion is simple. Security must be built in as an integral layer from day one of planning - with a clear legal framework, transparent partnerships, reliable infrastructure, and the citizen as an equal subject. It is precisely this balance between efficiency, crisis resilience, and rights protection that was at the center of the 4th edition of the "Safe & Smart City" conference, the leading European-Israeli gathering that brings together entrepreneurs, innovators, global companies, startups, and decision-makers to discuss the future of modern cities. The city of the future will be smart only if, first and foremost, it is safe.

