Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*

PRED VRATI SO NOVI RAZISKOVALNO-TEHNOLOŠKI PROJEKTI V OKVIRU PERSPEKTIVE HORIZON 2020

Nova tehnološka, organizacijska in procesna spoznanja so ključna za nadaljnji razvoj ustreznih pristopov na področju obvladovanja kompleksnih varnostnih tveganj za neprekinjeno delovanje kritične infrastrukture. V okviru že zaključene raziskovalne perspektive EU HORIZON 2020 so bili izbrani trije izredno pomembni razvojni projekti, v katerih imajo ključno vlogo tudi slovenski partnerji, ki so člani Slovenskega združenja za korporativno varnost.

Kompleksnost groženj in negativnih vplivov s strani okolja, ki obdaja naše organizacije, se iz leta v leto stopnjuje. Grožnje se med seboj korelirajo in s tem dobivajo dodatne dimenzije negativnih vplivov, ki niso več omejeni samo na eno organizacijo, lokalno skupnost ali določeno regijsko območje, temveč so vedno bolj meddržavno pogojene in prinašajo medsektorske in čezmejne posledice. Zaradi navedenega je potrebno neprestano iskati nove poti, kako v operativno delovanje naših zahtevnih sistemov, še posebno tistih, ki upravljajo s kritično infrastrukturo, vnašati najnovejše prakse in nove tehnološke rešitve, ki nam omogočajo boljše situacijsko zaznavanje in pristope za obvladovanje tveganj ter groženj. Poleg negativnih vplivov naravnih in tehnoloških nesreč, vedno večjo težo dobivata dva pomembna področja groženj, in sicer grožnje, ki izhajajo iz informacijskega in ožje kibernetskega prostora ter grožnje, ki jih povzroča človek, kot eden najpomembnejših agregatov in dejavnikov v sistemih zagotavljanja integralne korporativne varnosti naših organizacij. Zaradi navedenega, nas posebej veseli, da imajo organizacije iz Republike Slovenije, pomembno vlogo pri izvajanju razvojno-raziskovalnih projektov na področju EU in so kot take prepoznane, kot pomembni partnerji teh projektov. Še posebej pa smo ponosni na to, da je večina teh organizacij tudi v članstvu Slovenskega združenja za korporativno varnost. V mesecu septembru in oktobru začenjajo s svojim delovanjem trije izredno pomembni EU projekti s področja zaščite kritične infrastrukture, zagotavljanja varnosti na javnih površinah, predvsem pred terorističnimi grožnjami in seveda s področja kibernetske varnosti. Ti trije mednarodni projekti so: (1) APPRAISE – Facilitating Public & Private security operators to mitigate terrorism scenarios against soft targets (2) PRECINCT - Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection in (3) CyberSEAS - Cyber securing energy data services. V nadaljevanju bomo kratko predstavili osnovna težišča teh treh pomembnih projektov.

APPRAISE

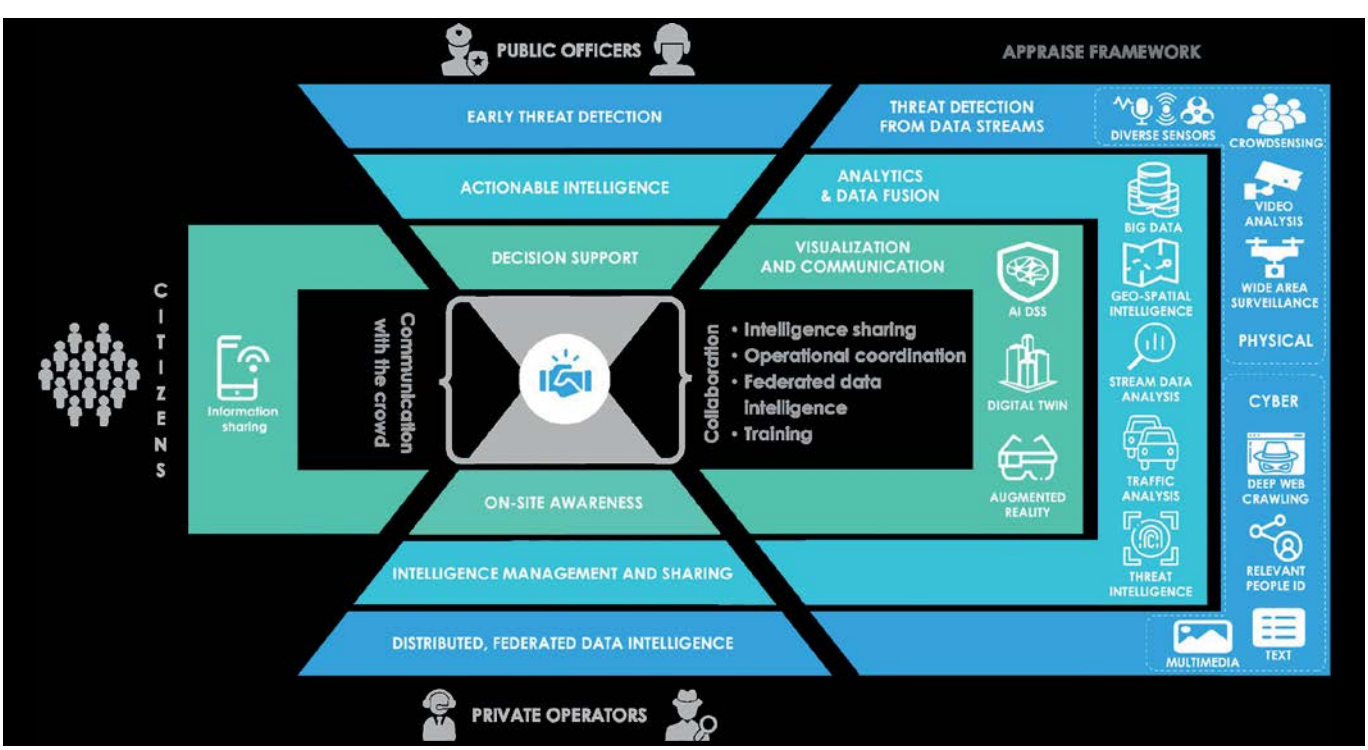
APPRAISE želi doseči učinkovitejše in proaktivno zagotavljanje varnosti v EU na javnih površinah s posebnim poudarkom na t.i. »mehkih tarčah«. To želi doseči z: (1) izboljšanjem sedanjih zmogljivosti izvajalcev javne in zasebne varnosti, s poudarkom na učinkovitejšemu izkoristku večje količine javnih baz podatkov in (2) vzpostavitvijo uspešnega okvirja sodelovanja s povečanjem racionalizacije in izrabe zmogljivosti, ki so na voljo. APPRAISE predlaga nov globalno

*avtorica je članica Slovenskega združenja korporativne varnosti

integriran, vključujoč in sodelovalni pristop za zagotavljanje varnosti mehkih tarč, ki temelji na združevanju, analizi, korelaciji in izmenjavi vseh ustvarjenih pomembnih podatkov. Celoten koncept APPRAISE je ponazorjen na shemi 1, kjer je zaznavanje fizične in kibernetske grožnje označeno z modro barvo, analitika velikih podatkov za inteligentno delovanje in napovedovalno analitiko, je prikazana s svetlo modro ter vizualizacijska in komunikacijska orodja, ki so ponazorjena z zeleno barvo. Shema prikazuje kateri od podatkov so v uporabi javnih in zasebnih varnostnih organizacijah ter javnosti, ki je tudi pomemben uporabnik dela teh informacij. V središču je prikazan vidik sodelovanja, ki se rezultira z uporabo ustreznih orodij, kot tehnična pomoč, pri zagotavljanju tega cilja. Za odkrivanje zgoraj omenjenih fizičnih in kibernetskih groženj APPRAISE uvaja nove rešitve in zmogljivosti, ki jih lahko uporabljajo varnostni strokovnjaki zasebnega in javnega okolja, odvisno od njihove razpoložljive infrastrukture. Ti vključujejo (i) rešitve videoanalize za omrežja CCTV za odkrivanje orožja in sumljivih predmetov, analize množice v realnem času in zaznavanje nenormalnega vedenja posameznikov in množice, (ii) (pol) avtomatski sistemi za nadzor širšega območja z uporabo brezpilotnih letal, (iii) odkrivanje terorističnih dejanj, kot so eksplozije in streli z uporabo zvočnih senzorjev, (iv) neposredne grožnje, kot so nelegalna uporaba materialov CBRN in uporaba dronov, kot sredstva napada, in (v) kibernetski napadi na nadzorno infrastrukturo. Poleg tega bodo za zbiranje informacij uvedene funkcije množičnega zbiranja informacij s strani udeležencev teh dogodkov. Vsa orodja za obdelavo podatkov bodo razmeščena bodisi na robu omrežja ali na lokalni strežniški ravni, kar bo zagotavljalo interoperabilnost z obstoječimi sistemi C2 in ohranjanje skladnosti GDPR v postopkih izmenjave podatkov. APPRAISE bo razvil tudi zmogljivosti, ki bodo varnostnim strokovnjakom omogočale izboljšanje njihovih operativnih zmogljivosti izvajanja (1) spletne analize vsebine, (2) oceno tveganja mehkih tarč, (3) pridobivanje obveščevalnih podatkov o grožnjah, in (4) pametno in učinkovito vizualizacijo podatkov v večdimenzionalnem sistemu, ki temelji na digitalnem dvojčku ter (5) sistemom za sprejemanje odločitev, ki temelji na podpori umetne inteligence. Spletni modul za analizo vsebine bo pridobival podatke (besedilne, vizualne in zvočne) iz javnih spletnih virov in virov iz temnega interneta ter na podlagi tega izvedel multimodalno analizo, da bi v njej pridobil kazalnike bližnjih napadov na mehke tarče. Za identifikacijo omrežij in določenih posameznikov bo opravljena analiza družbenih omrežij, kjer se bodo zaznavali indikatorji za organizacijo napadov ali s tem povezane propagandne kampanje. Rezultat modulov za odkrivanje groženj in spletnih modulov za analizo vsebine, bo skupaj s podatki o pametnih mestih, vizualiziran na digitalni osnovi in bo omogočal intuitivno zavedanje situacije v realnem času. Izboljšanje sodelovanja izvajalcev zasebne varnosti z organi za zagotavljanje javne varnosti je v središču projekta APPRAISE. Namen projekta je spodbujati izmenjavo informacij in krepiti operativno sodelovanje. Informacijski sistem, ki bo varen pred kibernetskimi vdori bo namenjen izmenjavi podatkov v standardizirani obliki. Vzpostavljeni multifunkcijski informacijski sistem bo v omejenem obsegu na voljo tudi izvajalcem zasebne varnosti z namenom zagotavljanja boljšega operativnega situacijskega zavedanja in možnosti večnivojskega izmenjevanja ključnih operativnih podatkov.

V projektu bodo organizirani pomembni pilotni primeri, ki bodo predstavljali različne oblike možnih tipov javnih prireditvenih prostorov. Le ti bodo naslednji (1) meddržavni primer organizacije velikega kolesarskega tekmovanja v Baskiji med Francijo in Španijo; (2) ATP teniški turnir v Torinu v Italiji; (3) trgovsko zabaviščni kompleks BTC-City v Ljubljani in (4) mednarodna sejemska infrastruktura v Gdansku na Poljskem.

Slovenski partnerji tega projekta so Ministrstvo za notranje zadeve-Policija, BTC City in Institut za korporativne varnostne študije.

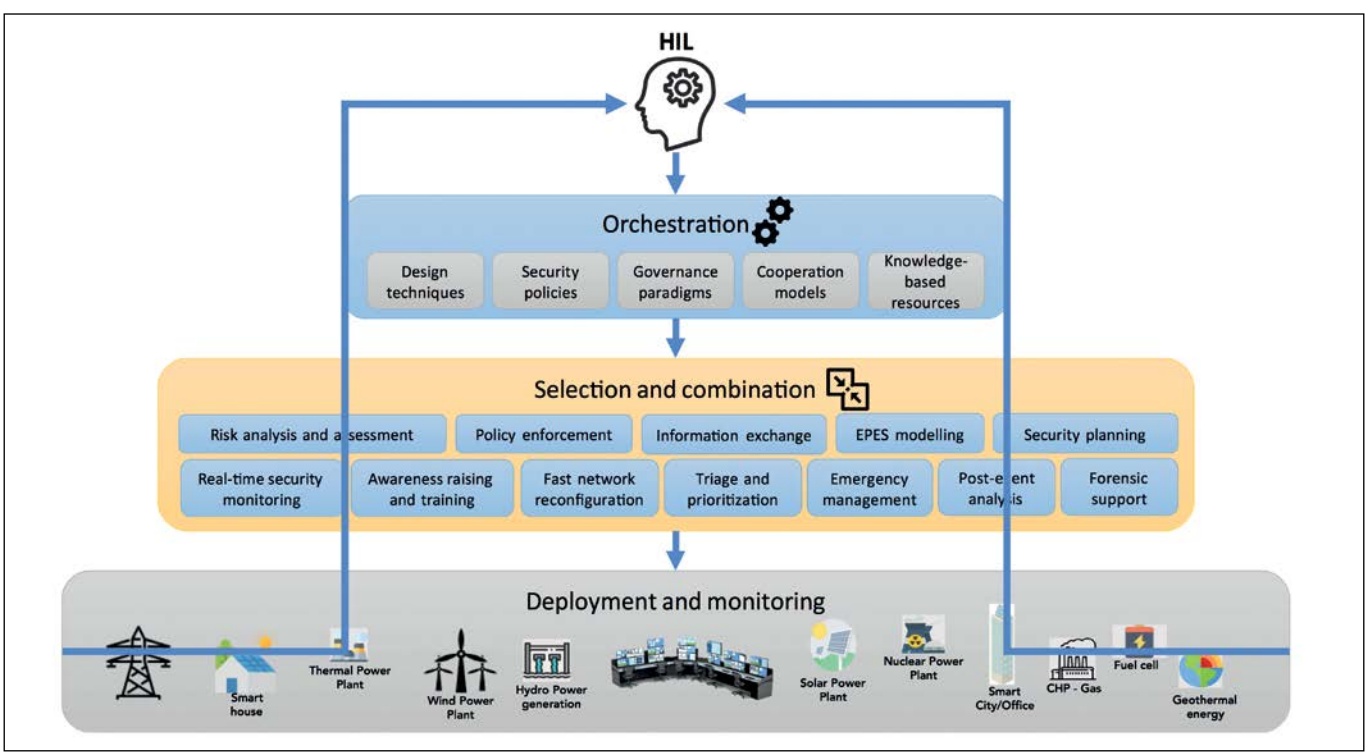


Shema 1 – koncept APPRAISE

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021981".

CyberSEAS

Cilj projekta CyberSEAS (Cyber Securing Energy Data Services) je izboljšati splošno odpornost verig oskrbe z energijo in jih zaščititi pred motnjami, ki izkoriščajo okrepljene interakcije, modele razširjene vključenosti zainteresiranih strani in potrošnikov, kot poti za zapletene kibernetske napade. Tveganja še dodatno izpostavljajo prisotnost slabih osnov pri razvoju sistemov in vse večjo povezljivost energetske infrastrukture, v katerem imajo pomembno mesto shrambe podatkov in vedno večje število deležnikov, ki so vključeni v elektro-energetski sistem. Projekt ima tri strateške cilje: 1) boj proti kibernetskim tveganjem, povezanim z napadi, ki imajo najpomembnejši vpliv na elektro-energetski sistem; 2) zaščita potrošnikov pred kršitvami osebnih podatkov in kibernetskimi napadi; in 3) povečanje varnosti skupnega podatkovnega prostora vezanega na delovanje elektro-energetskega sistema. Vsi trije cilji so enako pomembni, saj kibernetski kriminalci spreminjajo taktiko v prid večstopenjskim napadom, pri katerih je kraja občutljivih podatkov predpogoj za pravi napad. Le to jim omogoča, da povečajo škodo in dobiček, medtem ko so tradicionalni kibernetski napadi na infrastrukturo odražajo skozi neposredne napade na infrastrukturo in so običajno ciljno usmerjeni v onemogočanje nadzornih sistemov in manj v podatke. Akterji groženj, zlasti veliki, kot so nacionalne države, izvajajo tudi zapletene napade, ki spodbujajo odvisnosti od dobavne verige, in ta trend se še naprej povečuje, kot je bilo poudarjeno v analizi, ki jo je julija 2020 opravil NATO. V zadnjem obdobju, pa je potrebno vedno močneje upoštevati scenarije, kjer so uporabniki sistemov vedno bolj vključeni v delovanje teh sistemov. V teh primerih podatki o porabnikih postajajo vse bolj občutljivi. Za dosego teh ciljev CyberSEAS ponuja odprt in razširljiv ekosistem s 30 prilagodljivimi varnostnimi rešitvami, ki zagotavljajo učinkovito podporo ključnim dejavnostim, zlasti: (1) ocene tveganja; (2) interakcijo s končnimi napravami; (3) varen razvoj in uvajanje novih storitev in naprav; (4) varnostno spremljanje dogodkov v realnem času; (5) izboljšanje spretnosti in ozaveščenost; (6) certificiranje, upravljanje in sodelovanje. Rešitve CyberSEAS so potrjene za doseganje stopnje tehnološkega razvoja na nivoju TRL-7 s poskusnimi kampanjami, sestavljenimi iz več kot 100 scenarijev napadov, preizkušenih v treh laboratorijih, preden se bodo preselili v eno od šestih pilotnih infrastruktur.



Shema 2 - The CyberSEAS ekosistem

"The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560".

Slovenski pilot tega mednarodnega projekta je izredno močan in je sestavljen iz organizacij ELES, PETROL, INFORMATIKA s podporo vseh elektro distribucijskih podjetij, SI-CERT in Instituta za korporativne varnostne študije.

PRECINCT

Kritične infrastrukture EU so vse bolj ogrožene zaradi kibernetsko-fizičnih napadov in naravnih nevarnosti. Raziskave in nastajajoče rešitve se osredotočajo na zaščito posameznih KI, vendar so medsebojni odnosi med posameznimi kritično-infrastrukturnimi sektorji postali vse bolj zapleteni. Ukrepi na primer v pametnih mestih, obvladovanje kaskadnih učinkov in omogočanje hitrega okrevanja, pa postajajo vse pomembnejši in zelo zahtevni. Cilj projekta PRECINCT je povezati zasebne in javne deležnike informacijske tehnologije na geografskem območju s skupnim pristopom upravljanja kibernetske in fizične varnosti, ki bo državljanom in infrastrukturi prinesel ustrezne mehanizme zadostne zaščite.

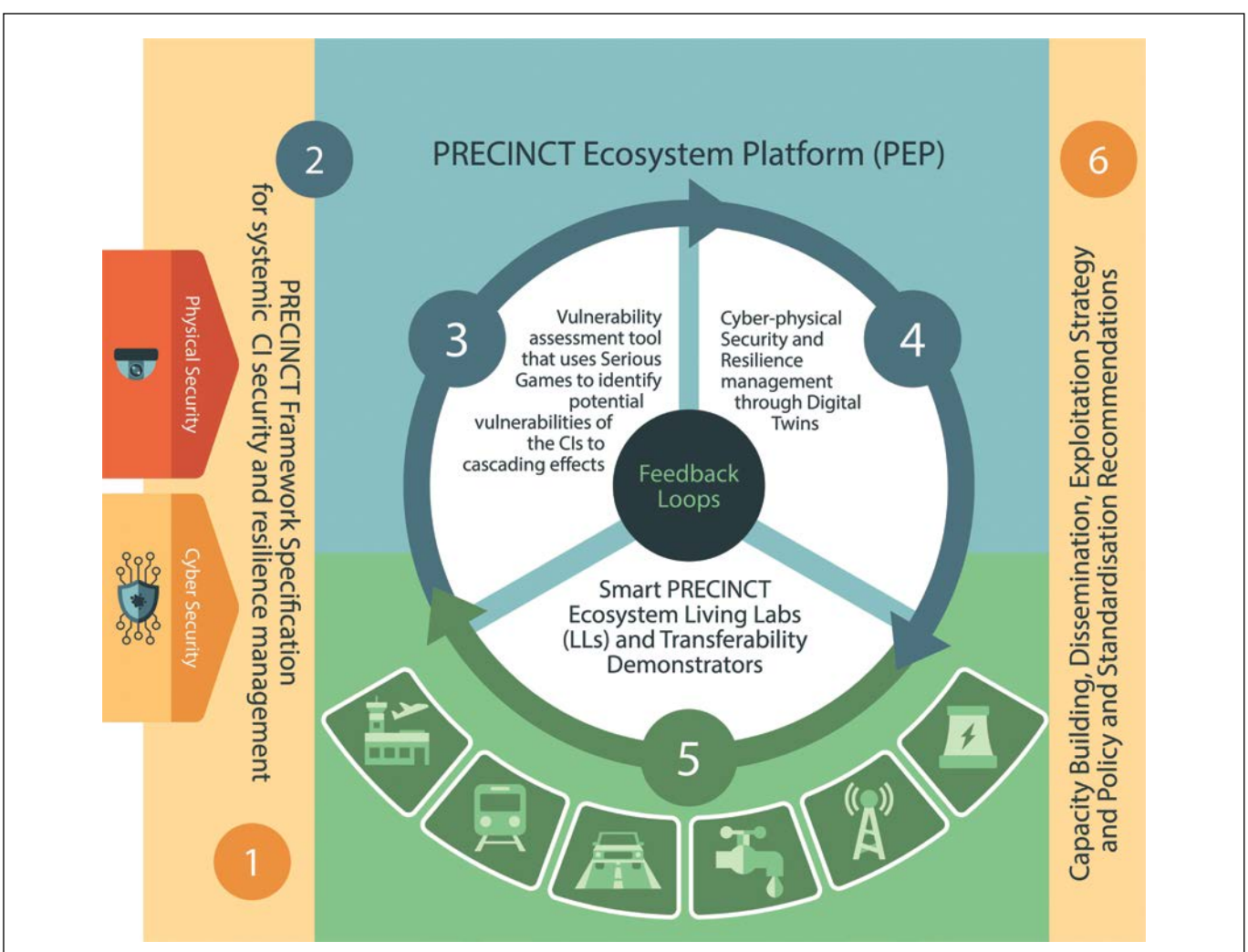
Projekt bo predstavil koncept pametnih odpornih okoli, ki bodo razviti v štirih živih laboratorijih. Kaskadni učinki bodo obravnavani skozi različne scenarije, ki bodo simulirali grož-

nje v multimodalnem prometu, energiji, oskrbi z vodo in IKT/telekomunikacijah. Te kritične infrastrukture temeljijo na medsebojni odvisnosti med temi vidnimi in zelo medsebojno povezanimi okolji, ki zajemajo kibernetske fizične in hibridne scenarije groženj. Zahteve za pristop k celovitemu upravljanju kibernetsko-fizične varnosti, vključno z javno-zasebnimi partnerstvi, bo iskal poti za doseganje harmonije med organizacijo družbe in gospodarskim razvojem. Pomembno bo doseči optimalno ravnovesje med tveganjem, stroški in zahtevami glede varnosti ter odpornosti. To bo v nadaljevanju nudilo ustrezno podlago za obveščanje o taktičnih in strateških možnostih naložb na posameznem območju. V ta namen bo PRECINCT gradil na nedavnih in naprednih pristopih KI v štirih predlaganih živih laboratorijih. Projekt bo zagotovil modelno podprto in vključujočo platformo za kibernetsko-fizično varnost in upravljanje odpornosti za pametne in odporne regije. Glavni rezultati projekta, prikazani na shemi 3, so:

(1) Okvirna specifikacija PRECINCT za sistematično upravljanje varnosti in odpornosti kritičnih infrastruktur, ki izpolnjuje industrijske zahteve, pridobljene s strani zainteresiranih deležnikov v živih laboratorijih in vključuje nove vpoglede iz referenčnih projektov EU. (2) Sodelujoča platforma za kibernetsko-fizično varnost in upravljanje odpornosti, ki sodeluje med različnimi ustanovami in omogoča zainteresiranim stranem, da razvijejo ekosisteme PRECINCT, ki podpirajo umetno inteligenco, in storitve podpore za večjo odpornost. (3) Orodje za ocenjevanje ranljivosti, ki uporablja simulacijska orodja za preigravanje scenarijev, ki omogoča ugotavljanje potencialnih ranljivosti kritične infrastrukture do kaskadnih učinkov in za ugotavljanje izboljšav odpornosti na ravni vsake posamezne kritične infrastrukture ter usklajenih ukrepov. (4) PRECINCT digitalni dvojčki za predstavitev topologije in metapodatkov kritičnih infrastruktur, ki ustrezajo ustreznim profilom odvisnosti, z uporabo strojnega učenja z zaprto zanko (ML) za odkrivanje nepravilnosti in opozorilnih pogojev ter za optimizirano aktiviranje odzivnih in omilitvenih ukrepov ter avtomatizirano forenziko. (5) Ekosistemi Smart PRECINCT, razporejeni v štirih velikih živih laboratorijih in v demonstratorjih potrditve prenosljivosti, bodo na podlagi meritev zagotovili dokaze o ciljnih prednostih. (6) PRECINCT-ovi trajnostni učinki, vključno z izgradnjo zmogljivosti, razširjanjem, izkoriščanjem, strategijo odpornosti ter priporočili politike in standardizacije.

Slovenski partnerji tega projekta so Mestna občina Ljubljana z Mestnim redarstvom, Telekom Slovenija, Elektro Ljubljana, Slovenske železnice, Ljubljanski potniški promet (LPP), Prometni inštitut in Institut za korporativne varnostne študije.

O vseh projektih, ki začnejo s svojim delovanjem v mesecu septembru in oktobru vas bomo redno obveščali. ■



Shema 3 - The PRECINCT ecosystem

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021668".