Interreg

ITALIA-SLOVENIJA

UNIONE EUROPEA
EVROPSKA UNIJA

SECNET

Progetto standard co-finanziato dal Fondo europeo di sviluppo regionale
Standardni projekt sofinancira Evropski sklad za regionalni razvoj

COOPERAZIONE ISTITUZIONALE TRANSFRONTALIERA PER IL RAFFORZAMENTO DELLA SECURITY PORTUALE

ČEZMEJNO INSTITUCIONALNO SODELOVANJE ZA KREPITEV PRISTANIŠKE VARNOSTI

ZAKLJUČNA OBJAVA

Interreg

ITALIA-SLOVENIJA

UNIONE EUROPEA
EVROPSKA UNIJA

SECNET

Progetto standard co-finanziato dal Fondo europeo di sviluppo regionale
Standardni projekt sofinancira Evropski sklad za regionalni razvoj

COOPERAZIONE ISTITUZIONALE TRANSFRONTALIERA PER IL RAFFORZAMENTO DELLA SECURITY PORTUALE

ČEZMEJNO INSTITUCIONALNO SODELOVANJE ZA KREPITEV PRISTANIŠKE VARNOSTI

ZAKLJUČNA OBJAVA

TRST, MAREC 2019

SECURITY PORTUALE - VARNOST PRISTANIŠČA

VODILNI PARTNER / LEAD PARTNER

Autorità di Sistema Portuale del Mare Adriatico Orientale Porto di Trieste

AUTORITÀ DI SISTEMA PORTUALE
DEL MARE ADRIATICO ORIENTALE – PORTO DI TRIESTE

PROJEKTNI PARTNERJI / PARTNER DI PROGETTO

CEI
CENTRAL EUROPEAN INITIATIVE

SEGRETARIATO ESECUTIVO DELL'INIZIATIVA CENTRO-EUROPEA

UNIVERSITÀ DEGLI STUDI DI TRIESTE

UNIVERSITÀ DEGLI STUDI DI TRIESTE

AUTORITÀ DI SISTEMA PORTUALE DEL MARE ADRIATICO SETTENTRIONALE
PORTI DI VENEZIA E CHIOGGIA

AUTORITÀ DI SISTEMA PORTUALE DEL MARE ADRIATICO SETTENTRIONALE
PORTI DI VENEZIA E CHIOGGIA

LUKA KOPER
Port of Koper

LUKA KOPER

UNIVERZA NA PRIMORSKEM
UNIVERSITÀ DEL LITORALE
TURISTICA
FACOLTÀ DI STUDI PER IL TURISMO E LE PROFESSIONI TURISTICHE
FAKULTETA ZA TURISTIČNE ŠTUDIJE

UNIVERZA NA PRIMORSKEM IN IZVRŠNI / UNIVERSITÀ DEL LITORALE

Ta dokument je nastal na pobudo partnerjev projekta SECNET (seznam partnerjev in navezave na program).

Rokopis v Italijanskem in slovenskem jeziku je bil zaključen marca 2019.

Avtor: PP2 SEP

Pomočnik urednika: Divulgando s.r.l.

Vsakršne povratne informacije so dobrodošle.
Prosimo vas, da jih naslovite na vodilnega partnerja projekta: acozzi@porto.trieste.it

Ta dokument je objavljen na spletni strani projekta SECNET na naslovu https://www.ita-slo.eu/it/secnet

Projekt SECNET - povzetek

31. marca 2019 se je zaključil projekt "SECNET - Čezmejno institucionalno sodelovanje za krepitev pristaniške varnosti", sofinanciran iz Programa čezmejnega sodelovanja Interreg V-A Slovenija - Italija 2014 - 2020.

Glavni cilj projekta SECNET, ki se je začel oktobra 2017 pod vodstvom Pristaniške uprave Vzhodnega Jadrana, je bil okrepiti institucionalno sposobnost pristanišč Trst, Benetke in Koper ter s tem ustvariti podlago za usklajeno in trajno upravljanje pristaniške varnosti na čezmejni ravni, tudi z uporabo najsodobnejših digitalnih rešitev.
V letu in pol so tri pristanišča, s podporo Univerze v Trstu in Univerze na Primorskem ter Izvršnega sekretariata Srednjeevropske pobude, primerjala svoje operativne strukture z najboljšimi mednarodnimi praksami in skupaj razvila akcijske načrt in dolgoročne strategije ter s tem izboljšala svojo koordinacijo in s skupnimi močmi okrepila varnost in konkurenčnost. Projekt SECNET je okrepil operativno zmogljivost in čezmejno upravljanje pristaniške varnosti ter tako zadostil priporočilom Evropske unije za zaščito kritične infrastrukture in upravljanje javno-zasebnega partnerstva. Na podlagi ugotovljenih prednosti in slabosti pomorskih objektov v Severnem Jadranu je bilo v okviru projekta pridobljeno tehnično znanje za uporabo inovativne in usklajene IKT na področju informatike in varnosti ob zunanji meji pristanišč. Izvedene so bile konkretne pilotne aktivnosti, kot so postavitev radarjev, siren in kamer, uporaba dronov in izvedba testov vdorov za zaščito pred informacijskimi napadi, ki kot rezultati projekta SECNET ostajajo del vsakodnevne pristaniške prakse in so sprožile dodatni razvoj.

Temeljni rezultati projekta so bili predstavljeni in obravnavani na zaključni konferenci, ki je potekala 28. marca v Trstu, objavljeni pa so tudi v tej zgoščeni objavi, ki omogoča enostaven dostop do izvirnih dokumentov, izdelanih v času trajanja projekta.

Novi izzivi, grožnje in strategije za njihovo premagovanje v okviru fizične in kibernetske varnosti v pristaniščih so zato področja, ki so obravnavana v skupnem protokolu za institucionalizacijo sistema čezmejnega sodelovanja na temo pristaniške varnosti, ki so ga podpisali predstavniki pristanišč Trst, Benetke in Koper ter drugih zainteresiranih uprav in podjetij in h kateremu lahko pristopijo tudi druga pomorska vozlišča, kot so Tržič, Porto Nogaro in Chioggia.

Indice

1.

Varnostni izziv v pristaniškem gospodarstvu v času digitalnega preoblikovanja in prispevek projekta SECNET

Po ugotovitvah Evropske komisije se je gospodarski vpliv kibernetskega kriminala med letoma 2013 in 2017 za petkrat povečal in bi se do leta 2020 lahko povečal še za štirikrat. 80 % evropskih podjetij je utrpelo škodo zaradi napadov že leta 2016. Od prvega znanega napada v Estoniji leta 2007 so bili prizadeti tako državljani kot celotne države

Maja 2017 je ob vmesnem preverjanju strategije za enotni digitalni trg **Komisija uvrstila premagovanje groženj kibernetske varnosti v eno od treh prednostnih nalog EU za prihodnja leta** in takoj sprožila zakonodajni predlog (povzet v COM(2017) 477, 13.9.2017), o katerem so poslanci glasovali na plenarnem zasedanju Evropskega parlamenta marca 2019.

Predlog zajema prenovitev in okrepitev mandata Evropske agencije za varnost omrežij in informacij ENISA, ki je bila ustanovljena leta 2004, tako da bo postala nosilka skupnih aktivnosti in bo presežena izključna pristojnost držav članic, kar se je začelo izvajati že z Direktivo (EU) 2016/1148 "**o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji**" (Direktiva NIS) in bi se moralo zaključiti 9. maja 2018. ENIS bo imela ključno vlogo tudi v certificiranju varnosti IKT, ki že sedaj temelji na številnih certifikacijskih merilih, ki pogosto veljajo le na nacionalni ravni.

Oblikovanje prvega okvira prostovoljnega certificiranja kibernetske varnosti IKT izdelkov v EU potrjuje pomen evropske razsežnosti tudi na tem področju in pomembnost prispevkov od spodaj, ki so lahko sad transnacionalnega in čezmejnega sektorskega sodelovanja, kakor v primeru projekta SECNET.

Konferenca na temo "**Transport cybersecurity: raising the bar by working together**", ki jo je ENISA, s podporo Komisije (ED MOVE) in Evropske agencije za varnost v letalstvu EASA, Evropske agencije za varnost v pomorskem prometu EMSA in Evropske agencije za železniški promet ERA, organizirala 23. januarja 2018 v Lizboni, je potrdila potrebo po dodatni pospešitvi evropskega sodelovanja za kibernetsko varnost, zlasti na področju prevozov. Razprava se je osredotočala na teme, kot so:

1. kibernetski napadi na sistem prevozov imajo lahko hude posledice za človeška življenja in gospodarsko škodo; prometni sistem mora biti sposoben preprečevanja napadov in po potrebi osebnega odziva;
2. kibernetska varnost zahteva celostni pristop, ki se ne nanaša le na sisteme, povezane prek spleta, temveč tudi na človeški dejavnik, in zagotavlja sodelovanje med tehnično in izvedbeno ravnjo;

3. v trdnem okviru, ki ga zagotavlja Direktiva NIS iz leta 2016, zahteva krepitev kibernetske varnosti pri nekaterih vrstah prevoza posebne predpise;
4. s kibernetskimi grožnjami se je mogoče spopasti tudi brez predpisov, s konkretnimi aktivnostmi, in sicer z izmenjavo informacij, povečanjem sredstev, spodbujanjem osveščanja in razvojem kompetenc;
5. skupno delo mora poroditi lastno "kulturo kibernetske varnosti" v sektorju prevozov; ker so prevozi globalni in medsebojno povezani, je treba še naprej spodbujati sodelovanje z mednarodnimi partnerji in s pristojnimi mednarodnimi organizacijami, tudi onstran meja EU.
6. Sodelovanje med udeleženci Lizbonske konference se bo nadaljevalo z aktivnostmi, kot so spremljanje izvajanja Direktive NIS glede na posebne potrebe vsakega načina prevoza ter izmenjava informacij in dobrih praks, zlasti s stalnim ohranjanjem kibernetske varnosti med temami na dnevnem redu mednarodnih srečanj.
   La cooperazione fra i partecipanti alla conferenza di Lisbona avrà seguito con azioni come il monitoraggio della messa in opera della NIS Directive con riguardo alle specifiche esigenze di ciascuna modalità di trasporto e lo scambio di informazioni e di buone pratiche, in particolare mantenendo sempre la cyber-security fra i temi all'ordine del giorno degli incontri internazionali.

To je mednarodni referenčni okvir, v katerega se umeščajo rezultati projekta SECNET, katerega priporočila in cilji strategije čezmejnega sodelovanja temeljijo ne le na preizkušanju, ki je bilo izvedeno s šestimi pilotnimi aktivnostmi, ki so že okrepile fizično in kibernetsko varnost treh udeleženih pristanišč, temveč tudi na **obsežni dokumentaciji regulativnih okvirov med koncem leta 2017 in letom 2018 ter na analizi prednosti in slabosti treh pristaniških sistemov v Trstu, Kopru in Benetkah/Chioggi**, nadalje usklajeni s presojo tveganj in z ukrepi, ki jih je treba sprejeti v okviru čezmejnega akcijskega načrta, ki ga je na sredini projekta izdelala Univerza v Trstu.

Ker večina teh elaboratov vsebuje občutljive podatke, zaradi katerih se jih ne sme objaviti v celoti, je smiselno omeniti teme, v zvezi s katerimi je bilo to obsežno delovno gradivo v okviru projekta SECNET dano na voljo oblikovalcem politike, upravnim organom in izvajalcem. Primerjalna študija o mednarodnih, evropskih in čezmejnih praksah, ki jo je izdelala Univerza na Primorskem iz Kopra, je v skrajšani obliki predstavljena v Priloži 6.1 k tej končni objavi, na tem mestu pa velja opozoriti na vsebine "**Konsolidiranega poročila o obstoječem stanju in glavnih težavah na področju pristaniške varnosti na projektnem območju**" (izid 3.1.2.1), ki so ga pripravili zaposleni v Luki Koper in h kateremu so nato prispevali strokovnjaki drugih pristojnih partnerjev.

Konsolidirano poročilo o obstoječem stanju v pristaniščih Severnega Jadrana podaja uporaben **okvir obstoječe zakonodaje** pričenši s pravnimi temelji in referenčnimi standardi za varnostne ukrepe v pristaniščih. Povzeta je evropska zakonodaja o pomorski varnosti in zakonodaja drugih držav, zlasti ZDA.

Predstavljena je veljavna nacionalna zakonodaja v Sloveniji in Italiji ter notranji akti, ki so jih sprejeli pristaniški organi pri izvajanju svojih pristojnosti. Nato je izvedena primerjava med nacionalnimi in evropskimi predpisi za zaščito kritične infrastrukture in njihova uporabnost v čezmejnih okoljih.

Natančen opis pristanišč ter njihovih kopnih in morskih meja vključuje tudi predstavitev morskih območij, velikih plovnih kanalov, pristaniških objektov in meja, kjer se izvaja varovanje v pristaniščih. Ločeno so analizirane velike ogrožene skupine, ki so prisotne v pristaniščih Severnega Jadrana, in organiziranost integriranega varnostnega sistema, pri katerem z različnimi odgovornostmi sodelujejo različni upravni organi na nacionalni in lokalni ravni. V zvezi s tem so bili ocenjeni tudi preverjanja ob vstopanju na območje pristanišča tako po kopnem kot po morju in med zadrževanjem na slednjem, postopki za vstop in izstop blaga, organizacija operativnih centrov, pristojnih za varnost, stopnje varnosti v primeru zabeleženih kršitev ter načini urjenja, spremljanja in sodelovanja z državnimi institucijami.

Ta podrobna analiza je nato omogočila izdelavo zgoraj navedenega akcijskega načrta, ki omogoča tudi spodbudne primerjave med ureditvijo fizične in kibernetske varnosti v treh pristaniščih, udeleženih v projektu SECNET, kakor je bila zagotovljena na sredini leta 2018.

2.

Čezmejno pristaniško sodelovanje v jadranski regiji v okviru programov Evropskega teritorialnega sodelovanja INTERREG Slovenija - Italija

V evropskem programskem obdobju 2007 - 2013 je bila **prednostna naloga** INTERREG Slovenija - Italija "**zagotoviti trajnostno teritorialno integracijo**" tudi s "specifičnim ciljem", opisanim kot "povezovanje med prometnimi sistemi in diverzifikacija prevoznih sredstev". Tedaj je bil cilj programa "zagotoviti okolju prijazno teritorialno integracijo" prek "razvoja trajnostnih in interoperabilnih prometnih omrežij in z uporabo multimodalnih načinov prevoza, ki bi nadomestili cestni prevoz"; "izboljšati dostopnost in obstoječe načine prevoza z okrepitvijo povezav Tržaškega in Koprskega pristanišča s prednostno osjo Lion - Torino - Milan - Trst - Ljubljana - Budimpešta" (tedaj imenovano Koridor 5); in "spodbujati usklajevanje med vsemi pristanišči na programskem območju".

Glede na veliko število in pomembnost sofinanciranih projektov na področju prevozov v tistem obdobju, je konec marca 2015 v Trstu potekal **dogodek za kapitalizacijo** rezultatov in pridobljenega znanja, ki ga je priredil sekretariat SEP v sodelovanju s skupnim sekretariatom Programa, na katerem so bili predstavljeni čezmejni projekti v izvajanju (ADRIA A, IDAGO, TIP, TRADOMO) in podobni projekti, izvedeni v okviru drugih programov na transnacionalni ravni, financirani iz Evropskega sklada za regionalni razvoj za namene cilja evropskega teritorialnega sodelovanja. Delovne skupine, ki so se kasneje izoblikovale na temo dostopnosti, intermodalnosti in čezmejne mobilnosti, so podale pomembne zamisli za novo programsko obdobje, ki je bilo tedaj še v fazi opredelitve.

Med "tematskimi cilji" Programa INTERREG Slovenija - Italija 2014 - 2020 ni bilo mobilnosti. Prav na konferenci v Trstu pa so se porodile koristne zamisli za **preusmeritev s tem horizontalnega interesa na področju prevoza na izbrane tematske cilje in iz tega izhajajoče prednostne naloge**.
Teme mobilnosti bi lahko porodile izvirne projekte, kot so:

- za prednostno nalogo 1 (inovativne tehnologije, produkte, procese, organizacije): okolju prijazne prevoze, socialne inovacije, tehnologije, ki podpirajo trajnostno mobilnost;
- za prednostno nalogo 2 (nizkoogljično gospodarstvo): trajnostna in multimodalna mobilnost, participatorna izdelava načrtov trajnostne urbane mobilnosti (Sustainable Urban Mobility Plans - SUMP) z vidika pametnih mest, čezmejni lokalni javni prevoz in prevozi do vrat, odprava ozkih grl, razvoj souporabe električnih vozil, ocena in načrtovanje polnilnih postaj za električna vozila, ocena različnih

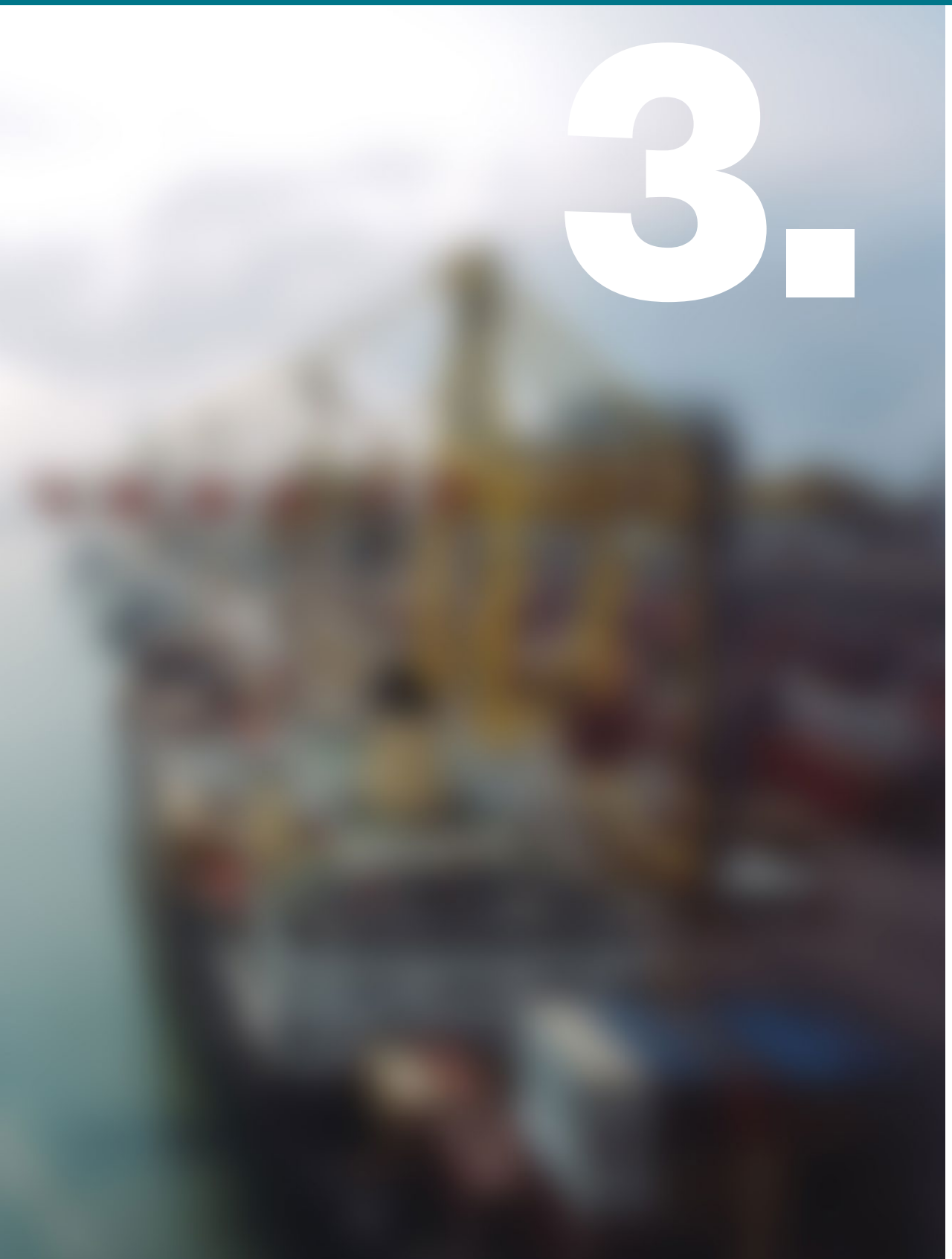
prevoznih sredstev (pomorskih, zračnih, tudi z obnovo manjših letališč);
- za prednostno nalogo 3 (zaščita in promocija naravnih in kulturnih virov): trženje, razširjeno zunaj programskega območja, promocija socialnih inovacij (npr. spreminjanje navad glede uporabe osebnih vozil), skupne infrastrukture za mobilnost na kratke razdalje, obnova opuščenih poti naravne in/ali arhitekturne vrednosti, krepitev čezmejnih kolesarskih stez v smeri vzhod-zahod;
- za prednostno nalogo 4 (sposobnost organov javne uprave in čezmejno upravljanje): povezava med organi javne uprave, usklajevanje zakonodaje, skupno načrtovanje, usklajeno financiranje.

Iz tega pristopa **izvira projekt SECNET, ki uresničuje tematski cilj 11 evropskega programa: "okrepiti institucionalno sposobnost javnih organov in zainteresiranih strank ter učinkovito javno upravo**"... "s spodbujanjem pravnega in upravnega sodelovanja ter sodelovanja med državljani in institucijami". V okviru projekta SECNET je bil v praksi izveden specifični cilj 4.1 s krepitvijo "institucionalnega sodelovanja z vključevanjem javnih organov in ključnih akterjev na programskem območju z namenom iskanja skupnih rešitev za skupne izzive".

Projekte na področju prevoza, četudi čezmejne, bi morali vključiti v širše strategije, kot so "evropske makroregionalne strategije". **Najuporabnejši referenčni okvir za slovensko-italijansko čezmejno območje so strategije za Alpsko, Podonavsko in Jadransko-Jonsko makro regijo**. Izkušnje in rezultati, pridobljeni s čezmejnimi projekti, so pomembni za stalno posodabljanje makroregionalnih strategij Evropske unije, pa tudi za doseganje ciljev slednjih. Rezultati projekta SECNET pomembno prispevajo k akcijskim načrtom makroregionalnih strategij in jih je kot take treba prenesti koordinatorjem ustreznih prednostnih območij.

Pri strategiji EU za Jadransko-jonsko makroregijo EUSAIR se SECNET v celoti umešča med aktivnosti 2. stebra, imenovanega "**Connecting the region**", katerega specifični cilj je tudi "krepitev varnosti v pomorskem prometu ter razvoj konkurenčnega regionalnega pristaniškega sistema" z aktivnostmi, kot so "skupno certificiranje varnosti, vzdržnosti in digitalizacije pristanišč" ter "razvoj in optimizacija pristanišč, infrastrukture in postopkov", na primer z "izdelavo orodij IKT za večjo učinkovitost, uspešnost in varnost pristaniških dejavnosti" ter "uskladitev pristaniških postopkov z orodji ITS".

Nadaljevanje projekta SECNET z institucionalnim sodelovanjem pristanišč Trst, Koper in Benetke, ki je bilo opredeljeno s protokolom, podpisanim na zaključni konferenci, lahko dodatno prispeva tudi h kapitalizaciji rezultatov z drugimi evropskimi projekti. Pristaniške varnosti in s tem povezane uporabe IKT ni obravnavalo veliko evropskih projektov, dokler se ni dramatično razkrila aktualnost te operativne razsežnosti v obstoječi fazi. **Projekt SECNET ima zato še vedno značaj pilotne aktivnosti na področju evropskega teritorialnega sodelovanja**. Nekatere sinergije z drugimi projekti, ki jih je v zadnjih letih sofinancirala Evropska unija, je mogoče raziskati in na podlagi izsledkov ustvariti mrežo odnosov med partnerji projekta SECNET in drugih projektov s podobnimi izkušnjami transnacionalnega sodelovanja, z namenom izmenjave pridobljenega znanja in **ustvarjanja podlage za vzpostavitev trajne transnacionalne mreže za izmenjavo znanj na področju kibernetske varnosti**.



3. Predstavitev projekta SECNET: utemeljitev, cilji, pomen partnerstva

Cilj projekta SECNET je bil okrepiti čezmejno institucionalno sodelovanje in upravljanje na področju pristaniške varnosti z vključitvijo javnih organov in ključnih akterjev na programskem območju z namenom iskanja skupnih rešitev za skupne izzive.

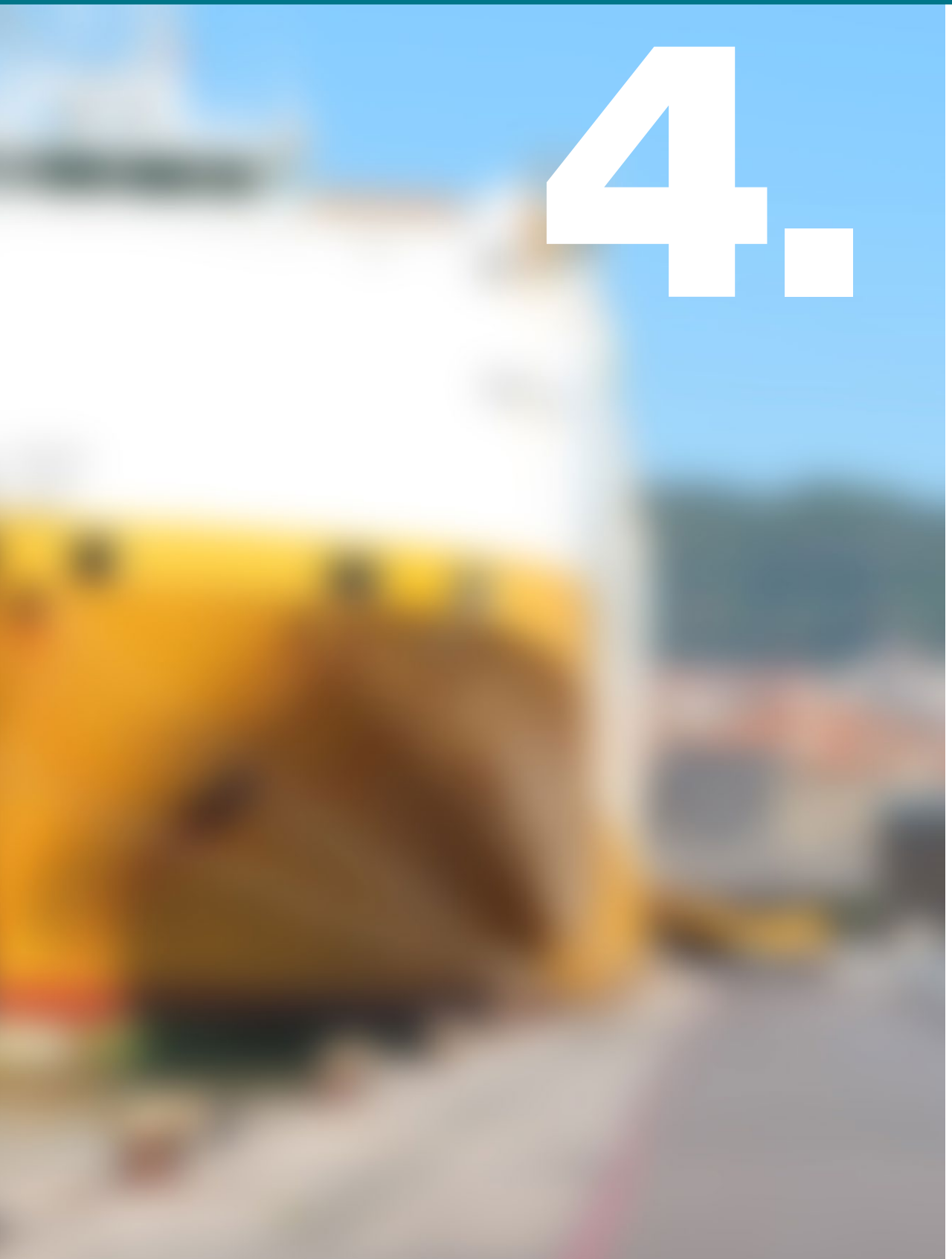
Pristaniški organi so pomembni akterji na področju snovanja kulturne identitete in družbene zavesti obalnih skupnosti, vezanih na pomorsko gospodarstvo in na vplive slednjega na ozemlje. V Trstu, Kopru in Benetkah je pristanišče in s tem povezano gospodarstvo že od nekdaj identitetni dejavnik in gonilna sila gospodarskega razvoja in blaginje. Iz njega izvirajo specializirani strokovni profili in posebna tehnološka znanja, ki so pogosto ključni nosilci celostnih inovacijskih procesov.

Vendar pa obstajajo v hitrem razvoju scenarijev svetovnega trga, na katerem poslujejo pristanišča, tudi dejavniki tveganja, ki so tako materialni in objektivni, vezani na vrste prometa, kot tudi subjektivni in geopolitični, katere določa izkrivljajoča uporaba razpoložljivih tehnoloških sredstev.

Pristaniški organi se danes, bolj kot kdajkoli prej, soočajo s temi tveganji v vse večjem obsegu in z vse hitrejšo odzivnostjo, zaradi česar se območje njihove odgovornosti povečuje. Na obmejnem območju znotraj Evropske unije je zato potrebno uskladiti upravljanje na lokalni in nacionalni ravni ter čezmejna tveganja, tako z vidika preprečevanja vpliva tveganj na okolje kot v zvezi z morebitnimi ekonomijami obsega, ki nastajajo pri usklajevanju in povezovanju sredstev in pristopov.

Območje, kjer potekajo projektne dejavnosti, obsega tri temeljna pristanišča, ki so vključena v omrežje TEN-T (Benetke, Trst in Koper) in ki se bodo morala soočiti s skupnimi izzivi: zagotoviti varnost, kolikor mogoče omejiti tveganje ter obenem omogočiti tekoč in hiter tranzit blaga, pri čemer je zaradi skupnih prometnih tokov, ob raztovarjanju ladij v vseh treh pristaniščih, nagnjenost k ustvarjanju ekonomij obsega še toliko večja.

Za krepitev teh vidikov v Severnem Jadranu, ki je del območja Programa sodelovanja med Slovenijo in Italijo, si prizadevajo partnerji projekta SECNET, med katerimi so pristaniški organi, dve univerzi in mednarodna organizacija z bogatimi izkušnjami na področju politik razvoja transportnih omrežij v Srednji in Vzhodni Evropi. Omogočen je bil tudi vzporedni razvoj osveščenosti vseh akterjev pomorskega gospodarstva na udeleženih območjih in njihove civilne družbe.



4.

Predstavitev partnerjev

Pristaniška uprava
Vzhodnega Jadrana (AdSP MAO)
www.porto.trieste.it

Srednjeevropska pobuda - Izvršni sekretariat (SEP ES)
www.cei.int

Univerza v Trstu (UNITS)
www.units.it

Pristaniška uprava
Severnega Jadrana, Pristanišči Benetke in Chioggia
www.port.venice.it

Luka Koper
www.luka-kp.si

Univerza na Primorskem (UP)
www.upr.si

Tržaška Pristaniška Uprava

Alberto Cozzi, vodja evropskih projektov / *acozzi@porto.trieste.it*
Fabio Rizzi, vodja področja za pristaniške dejavnosti / *frizzi@porto.trieste.it*

V skladu z Zakonom št. 84/1994 in naknadnimi spremembami je Pristaniška uprava Vzhodnega Jadrana (AdSP MAO) zadolžena za "*[...] usmerjanje, načrtovanje, usklajevanje, spodbujanje in nadzor pristaniških dejavnosti iz 1. odstavka 16. člena ter drugih trgovskih in industrijskih dejavnosti, ki se izvajajo v pristaniščih, z zakonodajnimi in uredbenimi pristojnostmi, tudi glede varnosti v zvezi s tveganji za nesreče, povezane s temi dejavnostmi, in glede higiene pri delu, v skladu s 24. členom [...]*" (6. člen). Pristaniška uprava Vzhodnega Jadrana je pripravila triletni operativni načrt naložb, na podlagi katerega se izvajajo strategije za krepitev in posodabljanje infrastrukture z namenom razvoja tovornega in potniškega prometa. Poleg tega je Pristaniška uprava na podlagi Uredbe z zakonsko močjo št. 203/2007 o pristaniški varnosti dolžna izdelati varnostno oceno pristanišča, v skladu z Uredbo (ES) 725/2004 pa tudi varnostno oceno vsakega terminala.

Tržaška pristaniška uprava je dala izdelati sisteme videonadzora in nadzora vstopa v območje pristanišča (katerih upravitelj je) ter skrbi za njihovo tehnološko posodabljanje. V okviru svojih pristojnosti je izdelala varnostno oceno pristanišča, skupaj z Luško kapitanijo, finančno policijo, mejno policijo, Carinsko upravo in drugimi pristojnimi institucijami pa tudi varnostni načrt pristanišča za ukrepanje v primeru protizakonitih dejanj.

Projekt SECNET je znotraj Pristaniške uprave Vzhodnega Jadrana pripomogel k boljšemu poznavanju tveganj, katerim so izpostavljena njena omrežja in podatkovne baze ter k zmanjšanju ranljivosti slednjih. Zahvaljujoč projektu SECNET je Pristaniška uprava Vzhodnega Jadrana lahko preizkusila nova orodja za zaščito zunanje meje in nadzor pristaniških območij z vgradnjo sirene, povezane s sistemom videonadzora in z uporabo dronov z različnimi vrstami senzorjev, ki omogočajo optimizacijo nadzora pristaniških območij.
S čezmejnim sodelovanjem s pristanišči iz Benetk in Kopra bo Pristaniška uprava Vzhodnega Jadrana lahko okrepila svojo varnost in povečala privlačnost, saj bodo orodja, ki bodo uporabljena na čezmejni ravni, zagotovila boljšo komunikacijo med tremi pristanišči, posledica tega pa bo učinkovitejši tranzit blaga. Kot upravi pristaniškega sistema bo Pristanišče Trst lahko preneslo in uporabilo znanja, pridobljena v okviru projekta SECNET, tudi v Pristanišču Tržič, ki je bilo s Predsedniško uredbo št. 57 z dne 29. marca 2018 dodeljeno k Pristaniški upravi Vzhodnega Jadrana.

Srednjeevropska pobuda - Izvršni sekretariat (SEP)

Ugo Poli, projektni vodja / poli*@cei.int*
Olga Izquierdo-Sotorrio, pristojna oseba za komunikacijo / s*otorrio@cei.int*
Alice Pappas, pristojna oseba za komunikacijo / *pappas@cei.int*

SEP (uradno Central European Initiative oziroma Srednjeevropska pobuda) je mednarodna organizacija, katere Izvršni sekretariat ima sedež v Trstu. Ustanovljena je bila novembra 1989, letos, ob svoji trideseti obletnici, pa združuje že sedemnajst držav članic, ki pokrivajo obsežno geografsko območje od Baltskega do Črnega in Jadranskega morja, katerega hrbtenica je Donava. Zaradi te značilnosti se Sekretariat SEP udeležuje aktivnosti tematskih delovnih skupin evropskih makroregionalnih strategij, zlasti v zvezi s prevozi, inovacijami in raziskavami, energijo in institucionalnim razvojem. Cilj SEP kot medvladnega regionalnega foruma je podpirati proces evropske integracije prek sodelovanja med institucijami, pa tudi med nevladnimi organizacijami njenih držav članic, tako na področju gospodarskega razvoja kot na področju temeljnih svoboščin. Pri opravljanju svoje misije, ki je znotraj akcijskega načrta razdeljena na triletja (www.cei.int/sites/default/files/file/PoA2018-2020), ima SEP vlogo donatorja, vendar pa razvija tudi projekte za izvajanje politik EU, financirane iz evropskih programov, in to ne le v okviru cilja evropskega teritorialnega sodelovanja kohezijske politike.

Mnogi od 30 evropskih projektov, ki so bili izvedeni od leta 2004, pri katerih je sodelovala kot partner ali vodilni partner, in 16 tekočih projektov so se oziroma se posvečajo področju prevozov.

Iz obdobja 2007-2013 velja omeniti pomembne projekte, kot so SEETAC in ACROSSEE (Program Jugovzhodna Evropa), ADRIA A (INTERREG CBC Slovenija - Italija) in CERES (Sedmi okvirni program Evropske skupnosti za raziskave, tehnološki razvoj in predstavitvene dejavnosti), ki jih je izvedla kot vodilni partner.

Od šestnajstih projektov, ki jih trenutno upravlja osebje SEP, se na področje prevozov nanašajo trije projekti iz programa transnacionalnega sodelovanja Srednje Evrope (COME-IN!, CONNECT2CE, SULPiTER), eden iz programa MED (SUMPORT), dva iz programa ADRION (INTER-CONNECT, ADRIPASS), projekt NAMIRG, financiran s strani Generalnega direktorata Evropske komisije za humanitarno pomoč in civilno zaščito DG ECHO za Maritime Incident Response Group iz Severnega Jadrana, ICARUS v okviru INTERREG Italija - Hrvaška o trajnostnem razvoju obalne mobilnosti in seveda SECNET v okviru Programa INTERREG Slovenija - Italija. Podrobnejše informacije o projektih so na voljo na spletni strani https://www.cei.int/eu-projects.

Pri projektu SECNET je bila SEP zadolžena za usklajevanje komunikacijskih aktivnosti, pri čemer je zagotavljala pravilno kroženje informacij o doseženih rezultatih z glasilom, programskim spletiščem in stranmi SECNET na družbenih omrežjih. Z namenom aktivnega vključevanja ciljnih skupin deležnikov je SEP organizirala tudi posvetovalne dogodke o strategiji SECNET za krepitev pristaniške varnosti s pomočjo sistemov IKT, ki so potekali v prvih mesecih leta 2019.

Znanje, pridobljeno v okviru projekta SECNET, je mogoče prenesti na zainteresirane države članice SEP z ustvarjanjem priložnosti za ponovitev projektnih aktivnosti zunaj programskega območja.

Univerza V Trstu
Oddelek Za Poslovne In Ekonomske Vede, Matematiko In Statistiko

Giuseppe Borruso, profesor / *giuseppe.borruso@deams.units.it*
Grazia Graziosi, raziskovalka / *ggraziosi@units.it*

Univerza v Trstu ima trenutno 10 oddelkov, ki jih obiskuje približno 18.000 študentov.

K projektu SECNET je Univerza v Trstu prispevala svoje dolgoletno strokovno in akademsko znanje, ki ga je zahvaljujoč sofinanciranju programa INTERREG, ki je to specifično raziskovalno dejavnost omogočilo, lahko zagotovila partnerjem v vseh projektnih fazah.

Oddelek UNITS je sodeloval z Univerzo na Primorskem pri aktivnosti A.DS3.1.2, namenjeni analizi najboljših praks s področja pristaniške varnosti na čezmejni, evropski in mednarodni ravni ter usklajeval pripravo čezmejnega akcijskega načrta za krepitev pristaniške varnosti z IKT ter usposabljanje, ki ga je pripravila Beneška pristaniška uprava.

Oddelek UNITS je tudi pomagal Tržaški pristaniški upravi pri izvedbi pilotnih aktivnosti in izdelal čezmejno strategijo za krepitev pristaniške varnosti z orodji IKT na podlagi rezultatov projekta.

Pristaniška Uprava Severnega Jadrana, Pristanišči Benetke In Chioggia

James Orlandi & Valentina Zambetti, Raziskave in razvoj projektov
james.orlandi@port.venice.it
valentina.zambetti@gmail.com

Andrea Rossi & Christian D'Antiga, Oddelek za usklajevanje pristaniških dejavnosti
andrea.rossi@port.venice.it
christian.dantiga@port.venice.it

Pristaniška uprava Severnega Jadrana (AdSP MAS) je neprofitna oseba javnega prava, ustanovljena na podlagi Uredbe z zakonsko močjo št. 169 z dne 4. avgusta 2016, ki zajema pristanišči iz Benetk in Chioggie. Gre za enotni pristaniški sistem v Beneški laguni z istim geografskim, okoljskim, družbenim in gospodarskim okvirom - sistem dveh pristanišč, ki se vsako s svojimi značilnostmi in posebnostmi dopolnjujeta pri oskrbi istega trga.

Naloga uprave je usmerjati, načrtovati, usklajevati, spodbujati in nadzirati pristaniške dejavnosti. Slednja skrbi za vzdrževanje skupnih delov, ohranja morsko dno, nadzira zagotavljanje storitev splošnega interesa, je zadolžena za izključno upravljanje pristaniških območij in dobrin ter za načrtovanje razvoja pristaniškega območja.

Poleg tega je pristojna tudi za usklajevanje upravnih dejavnosti javnih organov na območju pristanišča in za spodbujanje povezav z zalednimi in logističnimi sistemi. Zaradi povečanja prometa v Beneškem pristanišču je Pristaniška uprava Severnega Jadrana ocenila mednarodni gospodarski okvir, obstoječe in potencialno vplivno območje ter ohranjenost pristaniške infrastrukture. Njeno delovanje se dopolnjuje z orodji za načrtovanje in s smernicami drugih javnih institucij, od Evropske unije do samoupravnih lokalnih skupnosti.

V okviru projekta SECNET je Pristaniška uprava Severnega Jadrana (v nadaljevanju AdSP MAS) povečala svoje kompetence zahvaljujoč čezmejnemu usposabljanju in prispevala k pripravi skupnega akcijskega načrta (A.DS3.1.3), ki je bil v sodelovanju z drugimi projektnimi partnerji preizkušen v dveh pilotnih aktivnostih. AdSP MAS je razvila pilotno aktivnost v zvezi s kibernetsko varnostjo, v okviru katere je izvedla študijo za zaščito notranjega omrežja pred kibernetskimi napadi (A.DS3.1.4). Poleg tega je izvedla tudi posebne analize in razvila aplikacije za optimizacijo svojega sistema Port Community System v smislu pristaniške varnosti in zbiranja ustreznih podatkov, ter okrepila sistem videonadzora (A.DS3.1.5). Nazadnje je bila AdSP MAS zadolžena za koordinacijo DS 3.2 in je prispevala k pripravi skupnega protokola, s katerim se je, skupaj z drugimi pristaniščі, zavezala k izvajanju čezmejne strategije, razvite na podlagi rezultatov projekta (DS 3.2).

LUKA KOPER

Roberto Richter, višji projektni vodja,
Področje strateškega razvoja / *roberto.richter@luka-kp.si*
Žiga Fišer, Vodja področja strateškega razvoja / *ziga.fiser@luka-kp.si*

V okviru projekta SECNET je bila Luka Koper zadolžena za koordinacijo DS 3.1, kar je bilo mogoče tudi zahvaljujoč čezmejnemu usposabljanju, s katerim je povečala svoje kompetence, prispevala pa je tudi k pripravi skupnega akcijskega načrta (A.DS3.1.3). Za svoje pilotne aktivnosti je Luka Koper izvedla analizo o zaščiti svojega informacijskega omrežja z namenom preprečevanja kibernetskih napadov na svoj sistem (A.DS3.1.4) in posodobila sistem Port Community System za zadostitev najvišjih standardov s področja pristaniške varnosti in zbiranja ustreznih podatkov. Na podlagi povratnih informacij, pridobljenih s tako imenovanimi testi vdorov, so bili nato izvedeni dodatni testi sistema, da bi se preverilo njegovo ranljivost po namestitvi posodobitev in izvedbi posodobljenih varnostnih ukrepov.

Poleg del na informacijskem sistemu, je Luka Koper s pilotnimi aktivnostmi razširila svoj sistem fizične varnosti s posodobitvijo opreme za videonadzor in nabavo senzorjev za perimetralno zaščito, namenjenih vizualnemu in toplotnemu nadzoru cestnih in železniških vozil (A.DS3.1.5), s katerim bodo preprečeni nepooblaščeni vstopi v pristanišče.
S posodobitvijo radarskega sistema se je izboljšalo tudi sposobnost nočnega pregleda nad zunanjo mejo pristanišča, saj novi sistem zagotavlja jasno sliko tudi pri razdaljah, večjih od 1 km.

Nazadnje je luka Koper prispevala k pripravi skupnega protokola, s katerim se je, skupaj z drugimi pristanišči, zavezala k izvajanju čezmejne strategije, razvite na podlagi rezultatov projekta (DS 3.2). S svojim proračunom je Luka Koper pokrila tudi stroške zaposlenih za izvedbo projektnih aktivnosti ter za zunanje sodelavce za podporo koordinacijskega odbora (DS 1), za komunikacijske aktivnosti ali aktivnosti za promocijo rezultatov projekta SECNET (DS 2), kot tudi za izvedbo pilotne aktivnosti (DS 3.1) in prispevek pri pripravi čezmejne strategije (DS 3.2).

Marca 2019 so bile aktivnosti projekta SECNET predstavljene tudi zainteresiranim osebam s pregledom doseženih rezultatov in izboljšav na področju varnosti pristanišča in mejnih predelov.

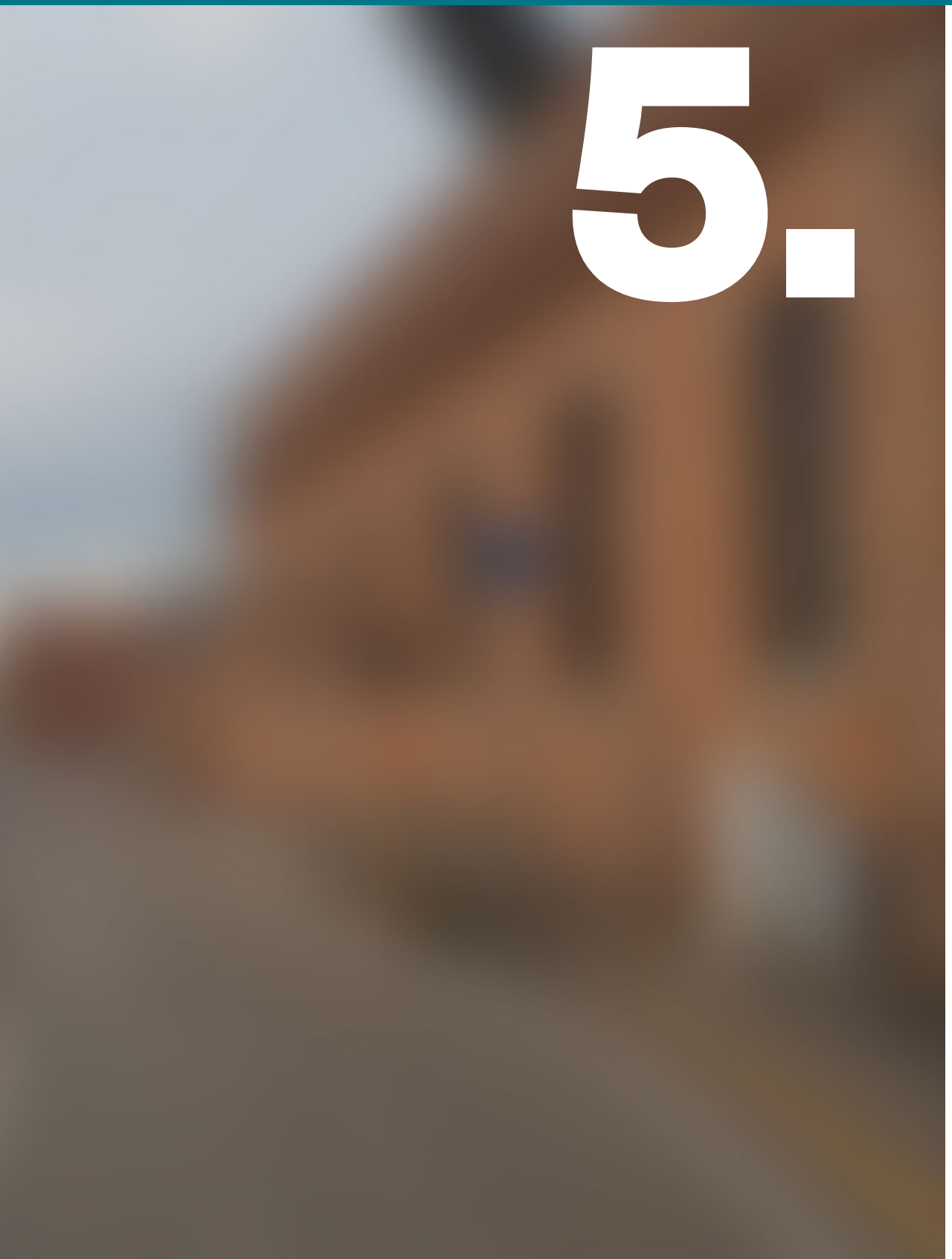
Univerza na Primorskem (UP) - Università del Litorale

Dejan Paliska, profesor, projektni vodja / *dejan.paliska1@gmail.com*
Ana Allegra, samostojna strokovna delavka / *Ana.Allegra@fts.upr.si*

Univerza na Primorskem je slovenska državna univerza s sedežem v Kopru. Ima enajst članic, od tega sedem fakultet in dve raziskovalni središči. Univerza na Primorskem ima bogate izkušnje na področju evropskih projektov. Omembe vreden je zlasti projekt SAFEPORT, v okviru katerega je, v tesnem sodelovanju z Luko Koper, razvila mobilni sistem za nadzor onesnaževanja zraka LIDAR (Light Detection And Ranging).

K projektu SECNET je Univerza na Primorskem prispevala z bogatim strokovnim in akademskim znanjem, ki so ga projektni partnerji lahko koristili v vseh fazah projekta. Njen proračun je omogočal financiranje zlasti zaposlenih (profesorji, raziskovalci itd.), ki so svoje znanje posvetili študijam in izvajanju drugih projektnih aktivnosti. UP je bila v sodelovanju z Univerzo v Trstu zadolžena za koordinacijo aktivnosti A.DS 3.1.2, namenjene analizi najboljših praks s področja pristaniške varnosti na čezmejni, evropski in mednarodni ravni.

UP je Luki Koper pomagala pri izvedbi pilotnih aktivnosti, za katere bo pripravila oceno in validacijo rezultatov, nazadnje pa je sodelovala tudi pri izdelavi čezmejne strategije za krepitev pristaniške varnosti.



5.

Potek priprave in cilji strategije SECNET za zagotovitev pristaniške varnosti na čezmejni ravni Slovenije in Italije

Čezmejna strategija in protokol za krepitev pristaniške varnosti, izdelana v okviru projekta SECNET, sta namenjena ne le pristaniškim organom, ki so partnerji projekta, temveč tudi drugim tovornim pristaniščem v območju Programa INTERREG Slovenija - Italija 2014 - 2020 (Chioggia, Porto Nogaro in Tržič) ter poglavitnim deležnikom pristaniškega gospodarstva (pomorska uprava, pristaniški delavci, vkrcevalci in ustanove, pristojne za civilno zaščito in varovanje okolja).

Strategija vsebuje priporočila za izvedbo usklajenih ukrepov uporabe pametne tehnologije in uskladljivih postopkov za povečanje učinkovitosti čezmejne pristaniške varnosti na kratki, srednje dolgi in dolgi rok. Partnerji so se s podpisom protokola na zaključni konferenci zavezali k njegovemu uresničevanju, k njemu pa lahko pristopijo tudi druga tovorna pristanišča in njihovi deležniki.

Strategija, ki so jo izdelali partnerji projekta SECNET, je bila središče vključevanja in izmenjave z deležniki s področja pristaniške varnosti, pri čemer so bile organizirane tri usklajene delavnice, ena v Trstu, ena v Kopru in ena v Benetkah, ki so bile namenjene javnim in zasebnim pristaniškim delavcem ter institucijam, ki so odgovorne za varnost na referenčnih območjih pristanišč. Delavnic so se udeležili:

- tovorna pristanišča na programskem območju (Tržič, Porto Nogaro in Chioggia),
- pristaniški delavci na terminalih,
- špediterji in pomorske agencije,
- druga pristaniška podjetja, vključno z zadrugami,
- nekatera podjetja, vključno z MSP, ki so posebej pomembna za pristaniške in pomorske dejavnosti, pa tudi ladjedelniška industrija,
- vse institucije, ki sodelujejo pri civilni zaščiti na zadevnem območju,
- uslužbenci lokalnih javnih organov, ki so pristojni za pristaniška območja.

Dela v okviru delavnic so potekala interaktivno, tako da so udeleženci lahko ne le zastavljali vprašanja in dajali pripombe, temveč predstavili tudi svoje izkušnje, potrebe in pričakovanja na temo pristaniške varnosti.

Na delavnici, ki je potekala **18. februarja v Trstu**, je AdSP MAO predstavila tudi ukrepe za zagotovitev v**arnosti ob zunanji meji pristanišča***,* ki se že izvajajo (namestitev sistema javljanja in nadzora območja ob zunanji meji pristanišča z droni); postopke, vezane na aktivnosti, ki so bile preizkušene v okviru

projekta SECNET in jih sedaj vključujejo v pristaniške varnostne načrte; usposabljanja za izvajalce glede uporabe dronov v kritičnih razmerah.

V zvezi s kibernetsko varnostjo so bila opazna prizadevanja AdSP MAO tako za odzivanje na neprestani in hitri razvoj referenčnega regulativnega okvira kot tudi za vzpostavitev lažje komunikacije z občani v zvezi z dogajanjem v pristanišču, z načrtovanjem nove IT platforme na podlagi podatkov o pretovoru blaga ter gibanju vozil in oseb.

Udeleženci posveta so s tem v zvezi podali naslednje pripombe in predloge:

- pravila za uporabo novega orodja za nadzor pristaniških območij je treba uskladiti s pristojnimi organi pregona;
- velika geomorfološka raznolikost pristanišč, ki sodelujejo pri projektu SECNET, kot potencialna ovira pri izvajanju skupnih smernic;
- potreba po vključitvi centralne ravni odločanja;
- izkušnje na nekaterih terminalih Tržaškega pristanišča za oceno ravni kibernetske varnosti obstoječih sistemov in opreme v kombinaciji s testi vdorov za ugotavljanje in blaženje morebitnih slabosti in ranljivosti;
- ključna vloga osveščanja in usposabljanja zaposlenih, saj prevladuje splošno mnenje, da so najšibkejši člen uporabniki IT infrastrukture;
- ustanovitev odbora odgovornih oseb za IKT različnih javnih in zasebnih subjektov v pristaniški skupnosti.

Tudi na srečanju, ki je potekalo 1**5. marca v Kopru**, so sogovorniki z natančno opredeljenimi vlogami, kot so predstavniki nacionalne in okrajne policije, občinska uprava, podjetja za oskrbo in rokovanje z gorivi na pristaniškem območju, podali pomembna mnenja s področja pristaniške varnosti in se soočili z odgovornimi osebami za varnost v Luki Koper v zvezi s temami, kot so obstoječa varnost v pristanišču, nove varnostne tehnologije, preventivni varnostni ukrepi, ki jih v pristanišču izvajajo za preprečevanje vdorov, kraja podatkov in morebitni drugi dejavniki, ki lahko ogrozijo varnost v pristanišču ali v mestu Koper.

Tako preverjena čezmejna strategija, izdelana na podlagi študij, ki so bile predvidene v okviru aktivnosti projekta SECNET (analiza dobrih praks na čezmejni, evropski in mednarodni ravni, čezmejno usposabljanje, skupni akcijski načrt) in njegovih pilotnih aktivnosti, vsebuje pregled temeljnih izzivov, s katerimi se spopada kibernetska varnost v pristaniškem sektorju, poudarja slabosti v regulativnem okviru ter ponuja priporočila in smernice za uresničevanje skupnih rešitev v zvezi s kibernetsko varnostjo in zaščito zunanje meje pristanišča.

Strategija, ki je v celoti objavljena v nadaljevanju, predstavlja *časovni načrt* za prihodnje ukrepe, ki bi jih lahko spodbujali projektni partnerji in splošneje deležniki s programskega območja za povečanje fizične in kibernetske varnosti pristanišč in uvedbo dodatnega dejavnika konkurenčnosti.

Ta protokol o čezmejni razsežnosti pristaniške varnosti priča o prizadevanjih podpisnikov za sprejem in izvajanje priporočil strategije ter za izmenjavo podatkov in postopkov o pristaniški varnosti z vidika usklajevanja čezmejnega upravljanja in trajnega institucionalnega sodelovanja. Projektni partnerji bodo promovirali njegove vsebine tudi zunaj programskega območja, zlasti s Pristaniščem Reka kot članom Združenja pristanišč Severnega Jadrana in s pristanišči držav članic Srednjeevropske pobude.

»Čezmejna strategija za krepitev pristaniške varnosti z uporabo IKT«

(celotno besedilo - izid 3.2.3.1)3.2.3.1)

1. Uvod

Pristanišča so ključna intermodalna vozlišča v tovornem in potniškem prometnem omrežju Evropske unije (EU). Poleg tega, da so pomembne kontrolne točke na meji, imajo tudi pomembno vlogo v mednarodni trgovini.

Leta 2015 je EU po morju izmenjala za okoli 1.777 milijard Evrov blaga, kar je približno 51 odstotkov celotne trgovine EU z blagom[1] (Eurostat, 2016). Leta 2016 so morska pristanišča EU (28) po morju pretovorila 3,9 milijarde ton blaga[2] , z rahlim povečanjem za 0,5 odstotkov v primerjavi z letom 2015, vendar le za 0,01 odstotek v primerjavi z letom 2006. Kljub temu se je leta 2009 delež pomorskega tovornega prometa povečal za kar 11,4 odstotke (Eurostat 2018).

Po napovedih Konference Združenih narodov za trgovino in razvoj (UNCTAD) je pričakovana srednjeročna rast obsega svetovnega prevoza blaga po morju med letoma 2017 in 2022 3,2 odstotka (UNCTAD, 2017).

Pomorski blagovni tokovi se stalno širijo, pomorski promet pa potrjuje svojo ključno vlogo v delovanju naše družbe in našega gospodarstva.

Varnost pristanišč in učinkovitost njihovega poslovanja je torej ključnega pomena ne le za pomorski promet, temveč tudi za strateško vlogo v smislu varnosti na regionalni, nacionalni in evropski ravni. Pristaniška varnost tako postaja priložnost za avtomatizacijo in poenostavitev postopkov in dejavnosti v pristaniščih (Andritsos, 2013), pri čemer si je mogoče pomagati tudi z informacijsko in komunikacijsko tehnologijo (IKT). Nove tehnologije spreminjajo vse pomorske dejavnosti, od plovbe do upravljanja tovornega prometa, kot so carinjenje, določanje rokov, dostava, prostor za shranjevanje v skladiščih, skladiščenje na ladjah ter upravljanje vseh komunikacij in informacij o gibanju blaga in oseb, s katerim so povezane velike količine podatkov, ki se navezujejo na denarne posle, ki so dovzetni za kibernetske napade.

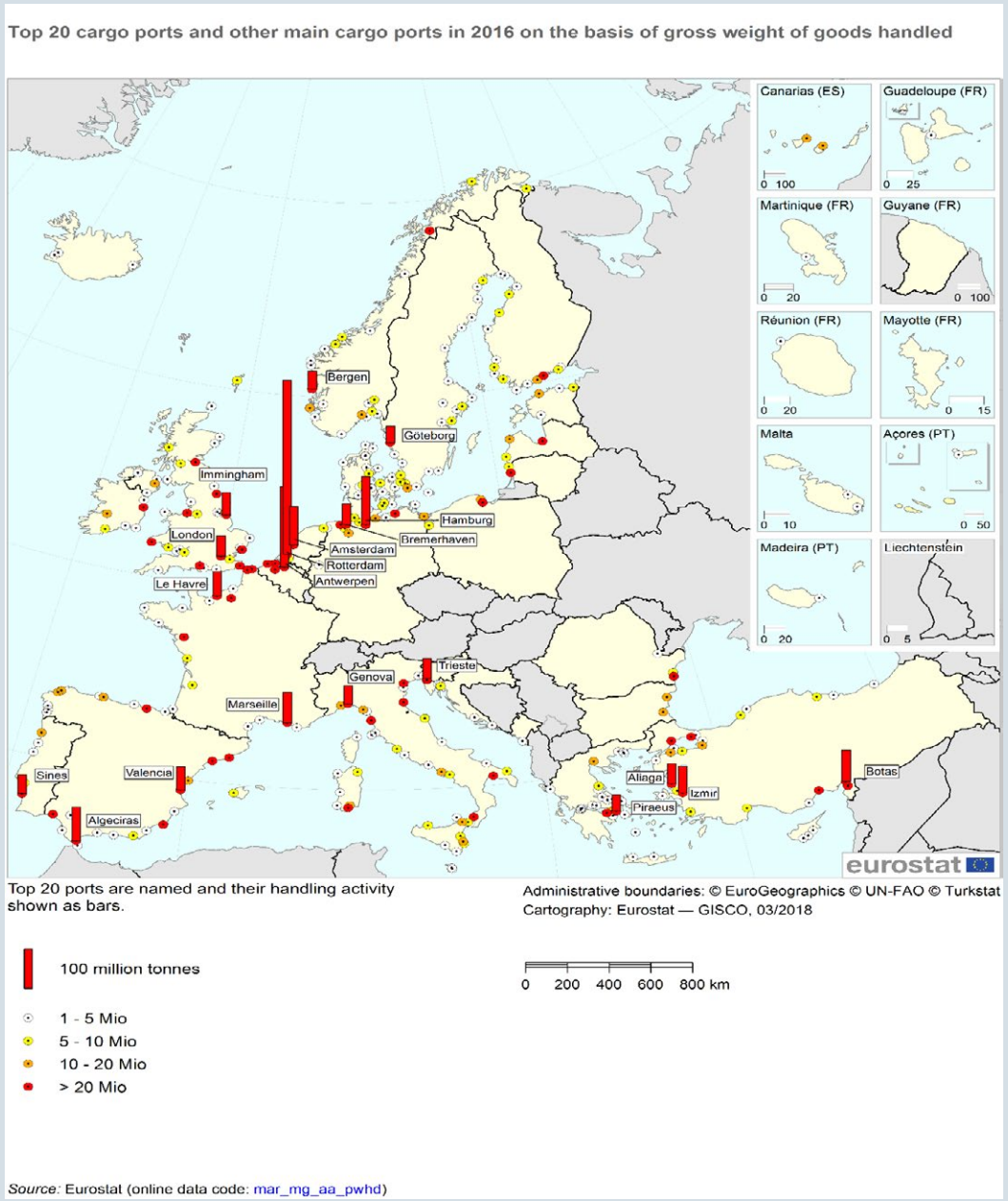
Za zagotovitev varnosti in učinkovitosti pri pristaniških dejavnostih ter učinkovitega nadzora nad pretokom blaga in oseb, so v tem dokumentu predstavljeni poglavitni izzivi varnosti na področju pomorstva in smernice za vzpostavitev trajnega čezmejnega sodelovanja, ki jih je v splošnem mogoče povzeti z naslednjimi aktivnostmi:

1) osveščanje poglavitnih akterjev iz pristaniškega sektorja o pomenu primerne varnosti pri pomorskih dejavnostih z ustreznim individualnim čezmejnim usposabljanjem pristojnih oseb za pristaniško varnost;
2) čezmejno usklajevanje pristaniške varnosti, kjer se bo določilo skupna pravila in pri katerem bodo, poleg pristojnih oseb za varnost na institucionalni ravni, sodelovali tudi deležniki iz zasebnega sektorja;
3) izmenjava informacij in podatkov, tudi z vzpostavitvijo platforme, kjer se bodo stekale in izmenjevale izkušnje, povezane z uporabo orodij IKT.

1 EU je po morju uvozila za 53 odstotkov vsega uvoženega blaga, izvozila pa za 48 odstotkov v države nečlanice.

2 Podrobnejši podatki o pretovoru blaga v evropskih pristaniščih v letu 2016 so na voljo na sliki 1.

Slika 1. Evropska pristanišča in pretovor blaga.



2. 2. Poglavitni izzivi varnosti na področju pomorstva

2.1 Regulativni okvir

Ko je novembra 2002 vstopil v veljavo Zakon o varnosti pomorskega prometa (Maritime Transportation Security Act - MTSA), zatem pa leta 2006 še Zakon o varnosti in odgovornosti za vsako pristanišče (Security and Accountability For Every Port - SAFE Port Act), je to pomenilo velik korak naprej na področju pristaniške varnosti, od ocene ranljivosti pristaniških objektov do razvoja in izvedbe varnostnih načrtov za omejitev vstopa v zaščitena območja le za pooblaščene osebe.

V skladu z MTSA, Uredba (EU) št. 725/2004 Evropskega parlamenta in Sveta o povečanju zaščite na ladjah in v pristaniščih uvaja ukrepe za okrepitev varnosti nacionalnega in mednarodnega pomorskega prometa, pri čemer države članice obvezuje k oceni varnostnih tveganj. Kot dopolnitev tega dokumenta, Direktiva 2005/65/ES Evropskega parlamenta in Sveta usmerja države članice k izdelavi in posodobitvi pristaniških varnostnih načrtov, ki za vsak nivo varnosti določajo: a) postopke, ki jim je treba slediti; b) ukrepe, ki jih je treba izvajati; c) dejavnosti, ki jih je treba uvesti.

Analiza vidikov informacijske varnosti na področju pomorstva, ki jo je izvedla Evropska agencija za varnost omrežij in informacij (ENISA), priznava strateško vlogo pomorske infrastrukture, ki jo je treba zaščititi, če se želi spodbujati in izboljšati dobrobit evropske družbe. Evropska komisija je sprejela Sporočilo[3] o izboljšanju zaščite evropske kritične informacijske infrastrukture pred morebitnimi terorističnimi napadi z evropskim programom za zaščito kritične infrastrukture in direktivo[4] o ugotavljanju in določanju evropske kritične infrastrukture.

Obveznosti glede varnosti za družbe, ladje, pristaniške objekte, pristanišča in storitve upravljanja ladijskega prometa se v skladu s pravnimi akti Evropske unije nanašajo na vse postopke, vključno z radijskimi in telekomunikacijskimi sistemi, informacijskimi sistemi in omrežji, ki imajo bistveno vlogo pri zagotavljanju lažjega čezmejnega pretoka blaga, storitev in ljudi (Direktiva 2016/1148/EU).

Del obveznih postopkov, ki jih je treba upoštevati, vključuje poročanje o vseh incidentih, Generalni direktorat za mobilnost in promet (GD MOVE) pa je v sodelovanju z Evropsko agencijo za pomorsko varnost (EMSA) sprejel konkretne ukrepe za lažjo izmenjavo podatkov med pomorskimi organi držav članic prek platforme SafeSeaNet[5]. Glavni cilj te platforme je spodbujanje zbiranja, razširjanja in usklajene izmenjave pomorskih podatkov, kar omogoča lažjo komunikacijo med organi na lokalni, regionalni in centralni ravni, obenem pa zagotavlja enotni sistem za spremljanje ladijskega prometa in obveščanje ter tako prispeva k preprečevanju incidentov na morju.

3 COM(2006) 789 z dne 12. 12. 2006
4 Direktiva 2008/114/ES z dne 8. 12. 2008
5 Direktiva 2010/65/EU

2.2 Ugotovljeni izzivi:

Glede fizične varnosti pristanišč so največji izzivi naslednji:

1. varno in učinkovito delovanje evropskih pristanišč v smislu trajnostnega transporta;
2. pretok tovora in potnikov brez prekinitev;
3. preprečevanje:
   - napadov na pristaniške objekte visoke vrednosti (kritična infrastruktura);
   - nezakonito priseljevanje;
   - preprodaja drog, orožja in prepovedanih snovi.

V skladu s standardom ISO 28001 so scenariji groženj, ki jih je treba upoštevati pri presoji varnosti, naslednji:

1. Vdor in/ali izguba nadzora nad dobrino (vključno s prevozom) v dobavni verigi. To bi lahko poškodovalo ali uničilo dobrino, poškodovalo ali uničilo zunanji cilj z uporabo dobrine (ali blaga) ali povzročilo civilne in/ali gospodarske nemire, kot so zajemanje talcev ali ubijanje ljudi.
2. Uporaba dobavne verige kot sredstva za tihotapljenje, kot so, na primer, nezakonito trgovanje z orožjem, teroristi ali drugi storilci kaznivih dejanj, znotraj ali zunaj zadevne države.
3. Nedovoljeno spreminjanje informacij: lokalni ali oddaljeni dostop do informacijskih sistemov v dobavni verigi z namenom prekinitve dejavnosti ali olajšanja protizakonitih dejavnosti.
4. Celovitost tovora: nedovoljeno poseganje, sabotaža in/ali kraja za namene terorizma ali drugih kaznivih dejanj.
5. Nedovoljena uporaba: razvoj dejavnosti v mednarodni dobavni verigi zaradi lažje izvedbe terorističnih incidentov (npr. uporaba prevoznega sredstva kot orožja).

Glede kibernetske varnosti so v poročilu o vidikih informacijske varnosti v pomorstvu (ENISA, 2011) navedene težave v zvezi z informacijsko varnostjo v pristaniščih, ki jih je mogoče povzeti kakor sledi:

6. *Slaba osveščenost o informacijski varnosti v pomorstvu oziroma namenjanje nezadostne pozornosti slednji*, kar ima za posledico neustrezno pripravljenost na spopadanje z informacijskimi tveganji. Posledično lahko učinki potencialnega informacijskega napada na pristaniške sisteme IKT povzročijo večjo škodo kot v drugih sektorjih, kjer je osebje pripravljeno za odziv na tovrstne dogodke.

7. *Kompleksnost sistemov IKT v pomorstvu*, ki zajemajo tudi zelo specifične elemente, katerih hitri tehnološki razvoj je v določenih primerih povzročil zmanjšanje pozornosti na njihovo ranljivost. Pomemben primer je vse večje število pristaniških infrastruktur, ki uporabljajo sisteme IKT, na primer naprave SCADA[6] , ki so povezane z internetom brez zaščitenih omrežij. Ranljivosti, ki jih te vrzeli povzročijo v varnosti sistemov IKT, lahko vplivajo ne le na storitve, ki jih ti sistemi podpirajo, temveč tudi na tiste, ki so običajno skupne, kot so podatkovne baze, sistemi za gostovanje občutljivih informacij ipd. Ugotovljeno je bilo tudi, da standardizacija dobrih praks za zagotovitev ustrezne zaščite sistemov IKT ne obstaja. Smernice s področja varnosti se pogosto nanašajo le na osnovne ukrepe in med številnimi orodji IKT ne najdejo ustreznice ali pa ne pokrivajo vse ustrezne tehnologije.

8. *Razdrobljenost pomorskih organov*: v pomorstvu obstajajo različne ravni upravljanja informacijske varnosti in s tem povezanih tveganj. Med temi je nekaj medvladnih organizacij, kot so Mednarodna pomorska organizacija (IMO), Svetovna carinska organizacija (WCO), Mednarodni pomorski urad (IMB) in Mednarodna pomorska varnostna korporacija (IMSC). Pomanjkanje uskladitve med temi organizacijami in obstoječimi organizacijami na evropski in nacionalni ravni povzroča neskladnosti v obravnavi pomorske varnosti. Razdrobljenost pomorskih politik v državah članicah pa povzroča težave pri opredelitvi odgovornosti in vlog na področju informacijske varnosti. Naraščajoča privatizacija nekaterih evropskih pristanišč, četudi le delna, poraja različne pomisleke v zvezi s smernicami, ki se uporabljajo na področju pomorske varnosti, katere morda ne sovpadajo s tistimi, ki so predvidene v Evropi, temveč so večinoma odvisne od posameznega lastnika in njegove zrelosti pri obravnavi vprašanj, povezanih z informacijsko varnostjo. Očitna je torej potreba po globalnem pristopu in konstruktivnem dialogu med vladami držav članic in pomorskimi organi.

9. *Premajhno upoštevanje informacijske varnosti v pomorskih predpisih*: obstoječi regulativni okvir daje velik poudarek na varnost (safety) in fizično varnost (phisical security) pristanišč, kakor na primer Mednarodni kodeks o zaščiti ladij in pristanišč (ISPS), vendar pa povsem zanemarja vidik informacijske varnosti in preprečevanja morebitnih kibernetskih napadov s protizakonitimi dejanji.

10. *Pomanjkanje enotnega pristopa do informacijskih tveganj*: pomorski organi pri obravnavi informacijske varnosti upoštevajo le del dejanskih tveganj, kot so prekinitev telekomunikacij ali razširjanja informacij v zvezi s tovorom, pri opredelitvi ukrepov, ki so potrebni za preprečevanje in upravljanje vseh vrst informacijskih incidentov, pa zanemarjajo vse pomembne vidike varovanja kritične pomorske infrastrukture (Critical Information Infrastructure Protection – CIIP).

11. *Pomanjkanje finančnih sredstev za zagotovitev informacijske varnosti*, kar je posledica tudi razdrobljenega in pomanjkljivega regulativnega okvira pri obravnavi teh vprašanj in pri določanju smernic, ki jih je treba upoštevati.

12. *Potreba po pobudah, ki bi spodbujale sodelovanje, izmenjavo informacij in deljenje izkušenj* med zainteresiranimi akterji. Pobud za sodelovanje je malo. Med njimi velja omeniti pobudo Port ISAC[7] (Information Sharing and Analysis Center), katere cilj je vzpostaviti sodelovanje med subjekti iz javnega in zasebnega sektorja za spodbujanje izmenjave informacij, mnenj in izkušenj o vprašanjih informacijske varnosti in dobrih praksah.

6 Kratica SCADA iz angleškega izraza Supervisory Control And Data Acquisition se nanaša na programsko opremo za nadzorovanje in pridobivanje podatkov.

7 Za podrobnejše informacije o pobudi ISAC si oglejte spletno stran http://www.cpni.nl/informatieknooppunt/werkwijze-isacs

3. Čezmejno usklajevanje za krepitev pristaniške varnosti

Glede na pomanjkljivosti, ki so bile ugotovljene v prejšnjem delu besedila, se želi s čezmejno strategijo za krepitev pristaniške varnosti s pomočjo orodij IKT uresničiti v nadaljevanju naštete pobude.

1) *Trajno omizje za izmenjavo dobrih praks z namenom izvajanja pobud za osveščanje o pomenu ustrezne varnosti pri pomorskih dejavnostih,* namenjeno za poglavitne akterje iz pristaniškega sektorja. Izdelati je treba smernice za načrtovanje, organizacijo in upravljanje pobud, namenjenih osveščanju o najprimernejših orodjih za zaščito vseh pomorskih dejavnosti pred morebitnimi napadi. Podrobno opredeljene dobre prakse in smernice morajo zagotoviti *varno načrtovanje* za vse kritične sestavine pomorskega sistema, s pristopom, temelječim na tveganju, ki omogoča razumevanje kompleksnosti pomorskega okolja in potrebe po čezmejnem sodelovanju.

2) *Stalno usposabljanje o pristaniški varnosti.* Poleg ciljno usmerjene akcije za osveščanje je treba delavcem v pomorstvu zagotoviti ustrezno individualno usposabljanje o specifičnih vidikih varnosti. Te dejavnosti bi povečale izkušenost celotnega sektorja, vključno s kibernetsko varnostjo, pri čemer bi se izkoristilo tudi podobne pretekle izkušnje iz drugih sektorjev, kot so, zgolj kot primer, sektor telekomunikacij, energetike, financ in drugi. Posebna pozornost bo namenjena *presoji obstoječih informacijskih tveganj, povezanih s trenutno izvedbo sistemov IKT*, pa tudi ugotavljanju vseh kritičnih dejavnosti v pomorskem sektorju, ki zajemajo presojo kritičnih pomorskih storitev in dobrin, grožnje, s katerimi se te spopadajo, njihovo izpostavljenost tveganju in izvajanje pripravljalnih vaj na temo upravljanja tveganj. Zato morajo dobavitelji pomorske IKT, delavci v pomorstvu, pristaniški organi in oblikovalci politik s skupnimi močmi ugotoviti, prepoznati in upravljati dejanska tveganja v skladu z njihovimi poslovnimi cilji in z regulativnim okvirom.

3) *Razvoj sistema v podporo pri odločanju v procesih prostorskega načrtovanja (SDSS).* Priporoča se izdelava sistema v podporo pri odločanju v procesih prostorskega načrtovanja, ki bo namenjen za vprašanja v zvezi z varnostjo, vendar ga bo v prihodnje mogoče razširiti, tako da bo omogočal upravljanje različnih vidikov, povezanih s pristaniščem. Znotraj tega sistema bodo povezane informacijske komponente, digitalne podatkovne baze, zlasti geografske, nadzorni sistemi in sistemi za vizualizacijo (3D slike, video kamere, posnetki v realnem času, zračni in satelitski posnetki), tako da bo izdelano orodje v podporo pri sprejemanju odločitev glede varnosti v pristaniščih. Za spodbujanje in olajšanje komunikacije o varnosti, vključno z informacijsko, ter izboljšanje izmenjave informacij in statističnih podatkov med pristaniškimi organi in zainteresiranimi akterji s področja pomorstva bo ustvarjena namenska platforma, kakršne so, na primer, tiste, ki jih izdeluje CPNI (Centre for the Protection of National Information Infrastructure[8]). Ta omrežja so lahko ključnega pomena pri odkrivanju obstoječih in prihodnjih informacijskih groženj. Pri razvoju Centrov za izmenjavo in analizo informacij ISAC je treba določiti pomembne deležnike iz javnega in zasebnega sektorja ter med njimi vzpostaviti zaupanje.

4) *Ustanovitev čezmejnega koordinacijskega centra za pristaniško varnost* (CCTSP)[9]. Center bo sestavljala specializirana delovna skupina, ki bo razvila vrsto natančno opredeljenih smernic o varnosti in dobrih praks za tehnološki razvoj in izvedbo sistemov IKT v pomorskem sektorju. Ta delovna skupina bi morala vključevati ne le poglavitne organe držav članic, ki sodelujejo v pomorskem sektorju, temveč tudi predstavnike najpomembnejših pristaniških oblasti, ladjarske družbe, dobavitelje pomorske infrastrukture ter raziskovalne ustanove (telekomunikacijske infrastrukture, strojna oprema IKT in programska oprema, SCADA, univerze in raziskovalne ustanove ipd.). Center se bo ukvarjal s sistematizacijo prejšnjih točk ter z morebitno *vzpostavitvijo partnerstev med javno-zasebnim sektorjem* v pomorstvu (npr. ladjarske družbe, pristaniški organi itd.) in s tem povezanimi deležniki (na primer zavarovalnice ali zavarovalni posredniki), da bi spodbudil sprejemanje varnostnih ukrepov, s tem pa odpravil ovire, ki jih predstavlja nezavedanje o tveganjih, vključno s kibernetskimi. Poleg tega lahko boljša izmenjava informacij in statističnih podatkov o informacijski varnosti zavarovalnicam pomaga izboljšati njihove aktuarske modele, zmanjša tveganja in zato udeleženim delavcem v pomorstvu zagotovi boljše pogodbene pogoje zavarovanja. To je primer, kako lahko boljše sodelovanje in večja varnost, vključno z informacijsko, povečata gospodarske koristi vseh udeleženih strank.

5) *Izvedba skupnih usposabljanj in navzkrižnega udeleževanja lokalnih usposabljanjih tako glede informacijske varnosti kot glede varnosti ob zunanji meji.* Te aktivnosti, ki jih je treba načrtovati v srednje in dolgoročnem časovnem okviru, bodo obenem omogočile preizkušanje lokalnih težav na kraju samem in izmenjavo izkušenj na čezmejni ravni, s tem pa vzpostavite sodelovanje, ki bo omogočalo povečanje kompetenc in okrepitev pristaniške varnosti.

6) *Skupna udeležba pri sofinanciranih projektih.* Za nadaljevanje čezmejnega sodelovanja na področju varnosti v pristaniščih je mogoče črpati sredstva iz več evropskih virov financiranja, tako v sedanjem kot v naslednjem evropskem programskem obdobju (2021-2027).

4. Zaključki

Evropska unija je močno odvisna od morskih pristanišč, ki urejajo izmenjavo blaga in ljudi na trgu znotraj in zunaj Unije. 74 odstotkov uvoženega in izvoženega blaga ter 37 odstotkov izmenjav znotraj Unije (Evropska komisija, 2013) poteka skozi morska pristanišča, ki zagotavljajo ozemeljsko kontinuiteto Unije ter povezavo obrobnih in otoških območij, tudi zahvaljujoč lokalnemu pomorskemu prometu. Poleg tega evropska pristanišča zagotavljajo kar 1,5 milijona delovnih mest, skoznje pa letno potuje 400 milijonov potnikov (Evropska komisija, 2015).

Glavni izziv za pristaniške varnostne sisteme je združiti varne pristaniške dejavnosti in učinkovit nadzor meja oziroma z drugimi besedami, za zagotovitev napredne varnosti, brez prekomernih stroškov, je treba:

- obravnavati varnost kot del strateškega upravljanja pristanišča;
- vključiti varnostne rešitve v operativne postopke z večjo avtomatizacijo pri spremljanju in usklajevanju aktivnosti;
- podpirati razvoj kompetenc na področju varnosti v pristaniščih in izkoristiti sposobnost organizacij, ki sodelujejo;
- spodbujati učinkovito sodelovanje med vsemi zainteresiranimi strankami, ki so udeležene pri pristaniški varnosti na regionalni, nacionalni in evropski ravni.

Večja varnost pomeni manjšo možnost hudih incidentov, boljši nadzor vstopa, zaščito računalniških omrežij, hitrejšo zaznavo groženj in večjo odpornost.

Večja odpornost pomeni nizek učinek v primeru prekinitve in hitro ponovno vzpostavitev normalnega poslovanja, z ohranitvijo konkurenčnosti pristanišč.

8 Za podrobnejše informacije si oglejte spletno stran www.cpni.nl

9 V pričakovanju ustanovitve so za člane čezmejnega koordinacijskega centra za pristaniško varnost (CCTSP) za največ 18 mesecev izbrani predstavniki partnerjev projekta SECNET.

Opredelitev pojmov:

pomorska varnost: kombinacija preprečevalnih ukrepov za zaščito ladij in pristanišč pred grožnjami namernih protizakonitih dejanj;

informacijska varnost: sposobnost omrežja ali informacijskega sistema, da se na določeni stopnji zaupanja upre naključnim dogodkom ali škodljivim dejanjem, ki ogrožajo razpoložljivost, verodostojnost, celovitost in zaupnost shranjenih ali prenesenih podatkov ter odgovarjajočih storitev, ki jih ta omrežja in informacijski sistemi ponujajo oziroma dostop do katerih omogočajo;

kibernetsko tveganje: vsako tveganje, povezano s finančno izgubo, motnjo ali oškodovanjem podobe organizacije, ki je posledica odpovedi informacijskih sistemov (Institute of Risk Management).

Bibliografija

AA.VV. (2018). *The Guidelines on Cyber Security Onboard Ships* (2018). Produced and supported by Bimco, Clia, Ics, Intercargo, Intermanager, Intertanko, Iumi, Ocimf e Worl Shipping Council.
http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on--cyber-security-onboard-ships.pdf?sfvrsn=16

Ahokas, J. Kiiski, T. Malmsten, J. e Ojala L. (2017). Cybersecurity in Ports: a Conceptual Approach. Proceedings of the Hamburg International Conference of Logistics
https://tore.tuhh.de/bitstream/11420/1451/1/ahokas_kiiski_malmsten_ojala_cybersecurity_hicl_2017.pdf

Andritsos, F. (2013). *EU port security & growth.* Proceedings of the 8th Future Security Research Conference, p. 267-274 Fraunhofer. *http://publica.fraunhofer.de/documents/H-47052.html*, ISBN: 978-3-8396-0604-9

Boyes, H. Isbell, R. e Luck A. (2016). *Code of Practice Cyber Security for Ports and Port Systems*. Institution of Engineering and Technology, London, United Kingdom.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546160/cyber-security-for-ports-and-port-systems-code-of-practice.pdf

Direttiva 2016/1148/UE del Parlamento Europeo e del consiglio, del 6 luglio 2016 recante «Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione».

European Commission (2013). *Port 2030. Gateways for the Trans European Transport Network.* Directorate General for Mobility and Transport, Directorate B – European Mobility Network, Unit B3 – Ports and Inland Navigation
http://ec.europa.eu/transport/modes/maritime/ports_en.htm

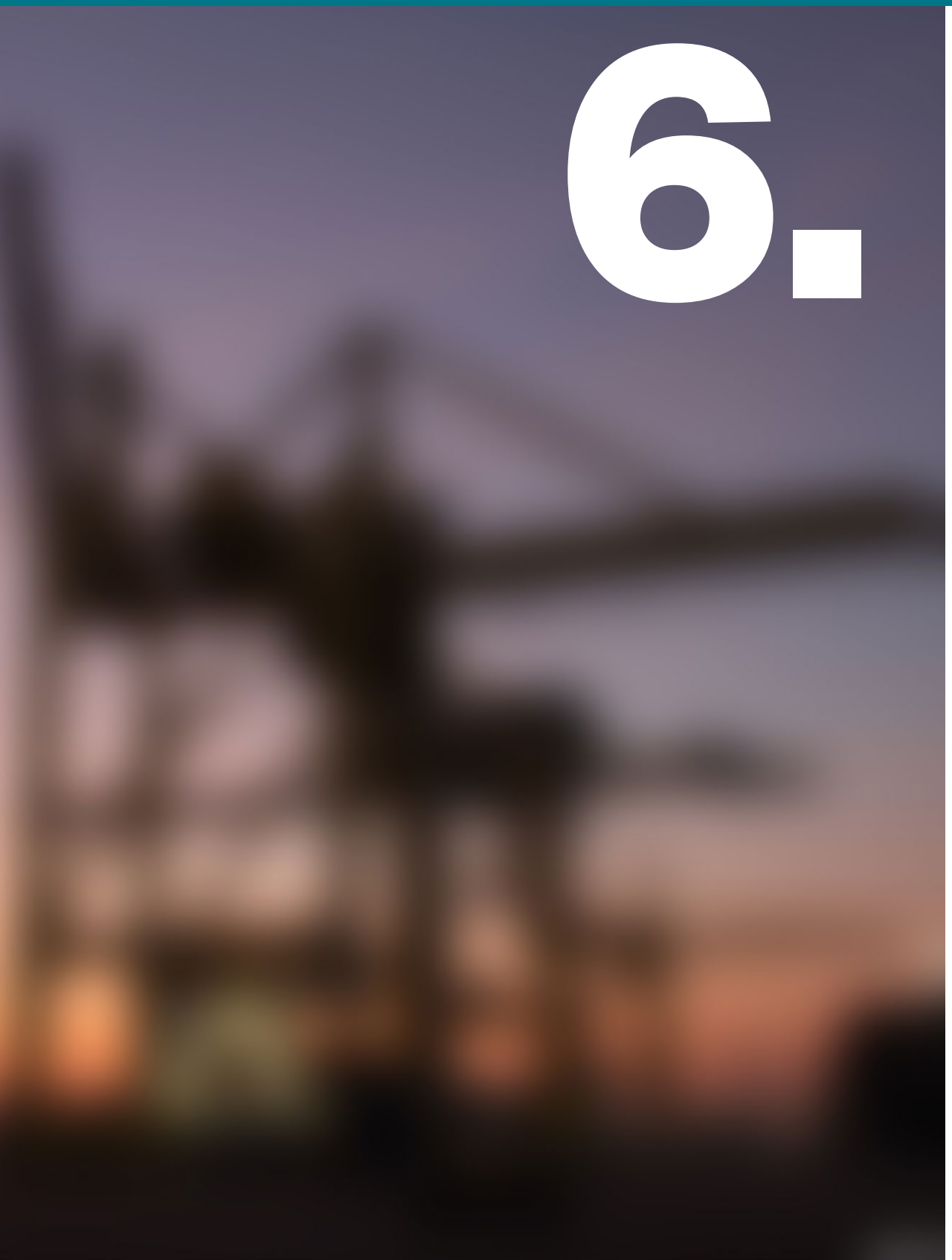
European Commission (2015). Exchange of views between ports CEOs and Transport Commissioner Bulc. *https://ec.europa.eu/transport/modes/maritime/ports/ports_en*

Eurostat, 2016.*World Maritime Day.* News realease 184/2016 - 28 September 2016. Eurostat Press Office. *eu.europa.eueurostat.*
https://ec.europa.eu/eurostat/documents/2995521/7667714/6-28092016-AP-EN.pdf/f9834e75-8979-4454-9d04-a32f0757926a

Eurostat, 2018. *Maritime ports freight and passenger statistics*. Statistics Explained.
https://ec.europa.eu/eurostat/statistics-explained/index.php/

European Union Agency for Network and Information Security (ENISA), 2011. *Analysis of Cyber Security Aspects in the Maritime Sector*. *https://www.enisa.europa.eu/news/enisa-news/stuxnet-analysis*

United Nations Conference on Trade and Development (UNCTAD), 2017. *Review of maritime transport,* p. 2-135, United Nations, Geneva. *https://unctad.org/en/Pages/Publications/Review-of-Maritime-Transport-(Series).aspx,* ISBN 978-92-1-112922-9



6.

Priloge

6.1 Študija najboljših praks pri sistemih IKT, uporabljenih za zagotavljanje pristaniške varnosti (Povzetek poročil o najboljših praksah na krajevni in mednarodni ravni - izidi 3.1.2)

6.2 Čezmejno usposabljanje SECNET – Benetke, 28. februar 2018 (zgoščeno poročilo - izidi 3.1.3.2)

6.3 Pilotne aktivnosti kibernetske in fizične varnosti v pristaniščih Koper, Trst in Benetke (zgoščene predstavitve - izidi 3.1.4 in 3.1.5.)

6.4 Protokol o vzpostavitvi sistema čezmejnega sodelovanja na področju pristaniške varnosti

Priloga 6.1

Študija najboljših praks pri sistemih IKT, uporabljenih za zagotavljanje pristaniške varnosti

(Povzetek poročil o najboljših praksah na krajevni in mednarodni ravni - izidi 3.1.2)

V okviru DS 3.1, namenjenega razvoju »pametne čezmejne pristaniške varnosti«, je Univerza na Primorskem na koncu leta 2017 in v prvih mesecih leta 2018 izvedla obsežno študijo dobrih praks na področju fizičnih in digitalnih sistemov za zagotavljanje pristaniške varnosti na krajevni in čezmejni (D.3.1.2.2) ter evropski in mednarodni ravni (D.3.1.2.3). Avtorji raziskave so profesorji Dejan Paliska, Daša Fabjan, Peter Kopič, Ana Allegra, Julija Švagelj Mežnar s Klaro Dodič Pegan in Asto Domian z Univerze na Primorskem.

Glavni cilj raziskave je bil ugotoviti dobre prakse na področju fizične in kibernetske varnosti v pristaniščih, ter zagotoviti izmenjavo ugotovljenih dobrih praks. Ugotovljene dobre prakse, ki so se izkazale za učinkovite za povečanje fizične in kibernetske varnosti pristanišč, so bile primerjalno predstavljene z možnostjo uporabe v treh pristaniščih partnerjih projekta SECNET.

Raziskava temelji na obsežnem pregledu in analizi virov, dostopnih na spletu, intervjujih s predstavniki pristanišč in razdeljevanjem dveh vprašalnikov evropskim pristaniščem. Na podlagi rezultatov je bilo mogoče izoblikovati splošen okvir obstoječega stanja na področju fizične in kibernetske varnosti v pristaniščih in primerjati dobre prakse v sodobnih evropskih pristaniščih s tistimi v Kopru, Trstu in Benetkah. V prvem vprašalniku so bili zajeti organizacijski vidik fizične varnosti v pristaniščih v različnih državah, vrste groženj, s katerimi so se v pristaniščih v preteklih petih letih dejansko soočili in ukrepi, ki so jih posamezna pristanišča na podlagi takih dogodkov vpeljala. Z vprašalnikom o kibernetski varnosti se je raziskava osredotočila na zbiranje informacij o postopkovnem in organizacijskem vidiku kibernetske varnosti ter o tehničnih in tehnoloških rešitvah za njeno izboljšanje.

Kljub želji po večjem odzivu (na vprašalnik o fizični varnosti je odgovorilo le osem pristanišč, ki niso bila udeležena v projektu SECNET, na vprašalnik o kibernetski varnosti pa sedem), se je na vprašalnik vendarle odzvalo nekaj najpomembnejših evropskih pristanišč tako po količini pretovora kot po tehnološki opremljenosti, in sicer Valencia, Barcelona, Antwerpen, Ravena, Ancona, Costanza, Burgas in Varna.

Poudariti velja, da gre pri informacijah o tveganjih na področju varnosti in o tehnični opremi pristanišč lahko za občutljive podatke.

Vprašalnik o fizični varnosti je bil namenjen zbiranju informacij o nesrečah in dobrih praksah s področja varnosti pristanišč. Sestavljen je iz treh delov vprašanj: uvodni del je namenjen zbiranju splošnih podatkov o pristanišču, drugi del vsebuje vprašanja o tehnologijah in sistemih, ki se uporabljajo v pristaniščih in zajema informacije o potencialnih tveganjih ter o nesrečah, ki so se pripetile v zadnjih petih letih. Zadnji del vprašalnika je namenjen zbiranju informacij o dobrih praksah na področju varnosti pristaniških objektov.

Območja vseh pristanišč, ki so bila zajeta v raziskavi, so bila ograjena z mrežasto ograjo ali zidom. V večini primerov so bila opremljena s kamerami, stolpi in razsvetljavo. Pogosto so imela tudi senzorje gibanja, manj pogosto infrardeče senzorje in toplotne kamere. Najbolje opremljeno med obravnavanimi je bilo pristanišče v Antwerpnu, ki ima, poleg toplotnih kamer na vhodu v pristanišče, tudi kamere za prepoznavanje registrskih tablic vozil (ANPR, *Automatic Number Plate Recognition*). Pristanišča, udeležena v projektu, imajo podobno opremo kot tista, ki so izpolnila vprašalnik in v varnostni opremi pristaniškega območja ni velikih razlik.

Vsa pristanišča uporabljajo vsaj sistem za prepoznavanje oseb, ki vstopajo v pristanišče. Večina pristanišč uporablja le ID kartice oziroma značke za prepoznavanje oseb, nekatera pa dva ali več sistemov. Pristanišči v Barceloni in Antwerpnu uporabljata tudi biometrične čitalce.

Pristanišča imajo različne pristope za preverjanje tovora, vozil, ladij in infrastrukture. Pristanišče v Barceloni ima v ta namen zaposlene delavce ter skupino ustrezno izurjenih psov za iskanje prepovedanih drog in eksploziva (K9 team). Druga pristanišča, kot sta na primer tisti v Antwerpnu in Costanzi, uporabljajo predvsem tehnične sisteme.

Kakor pri opremi za preverjanje tovora, vozil, ladij in infrastrukture, so tudi oprema in sistemi za hitro ukrepanje odvisni od specifičnih značilnosti posameznega pristanišča. Poleg lastnih varnostnih služb se lahko pristanišča obrnejo tudi na druge nacionalne reševalne službe, ki imajo lastno opremo. Zato je oprema pristanišč odvisna od organizacije storitev na nacionalni in regionalni ravni. Običajno imajo pristanišča vozila za prvo pomoč in gašenje požara.

Vsa pristanišča, ki so prejela vprašalnik, se srečujejo z zelo podobnimi varnostnimi tveganji. Najpogostejša od teh so povezana s trgovino z ljudmi in s slepimi potniki. Med najpogostejšimi tveganji so tudi kraje in ropi, vandalizem in drugi prestopki, kršitve trgovinske zakonodaje in tihotapljenje prepovedanega ali zakonsko urejenega blaga. Eno od pristanišč je navedlo tudi kršenje zračnega prostora oziroma nedovoljeno preletavanje pristaniškega območja z dronom.

Raziskava je razkrila, da so največja omejitev pri izvedbi novih tehnologij in sistemov za zagotavljanje fizične varnosti pristanišč potrebna finančna sredstva. Najsodobnejše tehnologije in sistemi (na primer skeniranje vozil, zabojnikov in oseb) so zelo dragi in si jih zato lahko privoščijo le največja pristanišča. Nekatera pristanišča so opozorila tudi na težave v zvezi z ograditvijo prostora (na primer, pristanišče v Antwerpnu je »odprto« pristanišče, ki se ga ne sme v celoti ograditi in zato preverjanja ob vstopu vanj niso mogoča), z zaposlenimi (potrebnega osebja ni mogoče zaposliti ali pa ni na voljo specializiranih kadrov), tehnično zapletenimi situacijami (uporaba novih tehnologij v pristaniškem območju, vendar nezmožnost preverjanja vsakega posameznega zabojnika) in varnostnimi preverjanji lastnih zaposlenih ter zaposlenih drugih podjetij, ki sodelujejo s pristaniščem (na primer voznikov tovornjakov). Kljub težavam, vsa pristanišča stalno izboljšujejo svoje varnostne in nadzorne sisteme in tehnologije.

Ugotovljenih je bilo nekaj dobrih praks s področja pristaniške varnosti, saj pristanišča na splošno namenjajo precej pozornosti sistemu zgodnjega prepoznavanja varnostnih tveganj. Med najbolj razširjenimi so pametni sistemi videonadzora, prepoznavanje registrskih tablic, preverjanje istovetnosti ob vstopu v pristanišče in sistem za alarmiranje. Veliko truda se namenja tudi povezavi različnih sistemov z enotnim nadzornim centrom in s sistemi za obveščanje v izrednih primerih. Pristanišča s potniškimi terminali namenjajo dodatno pozornost preverjanju vstopa in iskanju tihotapcev prepovedanih drog ali orožja.

Med vsemi pristanišči, ki so izpolnjevala vprašalnik, je najnaprednejše s tehnološkega vidika in najbolje organizirano na področju pristaniške varnosti pristanišče v Antwerpnu, ki je leta 2012 sodelovalo pri se-

stavi evropskega priročnika (DG MOVE) za usposabljanje in urjenje na področju pomorske varnosti[10]. Priročnik obravnava vse vidike usposabljanja in urjenja s praktičnega in teoretičnega vidika ter zajema vse izkušnje in znanje, pridobljene tekom časa. Pristanišča, ki so kot partnerji sodelovala v projektu SEC-NET, so priročnik uporabila za načrtovanje in izvajanje pilotnih projektov.

Podobna praksa se uporablja tudi v drugih velikih pristaniščih, kakršno je na primer Port of Long Beach, ki je izdelalo lastno varnostno strategijo na podlagi uporabe geografskega informacijskega sistema GIS, povezave z nadzornimi kamerami in popolnega nadzora pristaniškega območja v realnem času z možnostjo takojšnjega preverjanja nesreč ter s stalnim, rednim izvajanjem reševalnih vaj in vaj s področja preprečevanja tveganj, katerih se morajo udeležiti vsi člani pristaniške skupnosti (pristaniška varnostna služba, potapljači, policija, gasilci itd.)[11].

Pomembna dobra praksa je tudi obveščanje in spodbujanje osveščenosti o tveganjih, kar je mogoče že s tiskanjem brošur na temo varnosti, ki se jih razdeli zaposlenim v pristanišču in voznikom težkih vozil, ki vstopajo v pristanišče.

Raziskava o kibernetski varnosti za zaščito pristaniških sistemov IKT je bila razdeljena na prvi del z informacijami o organizaciji kibernetske varnosti in postopkih za njeno okrepitev, drugi del z informacijami o orodjih in tehničnih rešitvah ter tretji del, namenjen dobrim praksam s področja kibernetske varnosti.

Med pristanišči, ki so prejela vprašalnike, se s certifikatom ISO/IEC 27001, ki potrjuje usposobljenost za upravljanje in zaščito informacij, ponašata je Livorno in Valencia. Pristanišče v Valencii je pridobilo tudi certifikat ISO/IEC 28000, ki sicer ne obravnava neposredno kibernetske varnosti v pomorski dobavni verigi, vendar pa v splošnem opredeljuje metodologijo za oceno varnostnih tveganj. Valencia je tudi edino pristanišče, ki zahteva izpolnjevanje standardov ISO/IEC 27001 in spoštovanje varnostne politike pri izmenjavi in arhiviranju informacij tudi od zasebnikov (prevoznikov, špediterjev, agentov itd.). Tudi pristanišči Varna in Burgas imata podobne zahteve s strani svojih partnerjev, medtem ko pristanišči v Livornu in Raveni zahtevata od podjetij sprejem podobne varnostne politike, četudi ne nujno enake njihovi lastni. Pristanišče v Barceloni trenutno nima nikakršne varnostne politike pri opravljanju dejavnosti svojih partnerjev.

Osveščenost o kibernetskih tveganjih in razumevanje pomena kibernetske varnosti pri upravljanju in dejavnostih, ki potekajo v pristaniščih, se med pristanišči zelo razlikuje. Večina pristanišč, ki so izpolnila vprašalnik, ima načrt kibernetske varnosti, ki je dostopen vsem zaposlenim ter ureja odgovornosti in obveznosti posameznikov. V pristaniščih Valencia, Varna, Burgas in Koper so bili uvedeni tudi načini ravnanja v primeru kibernetskih nesreč, ki zajemajo prepoznavanje poskusov vdora v sistem in alarmiranje ekipe, ki je na voljo ves dan, vse dni v letu. Vendar pa le dve pristanišči (Koper in Burgas) sistematično analizirata napade. Zbrani podatki razkrivajo, da niti polovica intervjuvanih pristanišč ne izdeluje redne ocene tveganj za kibernetsko varnost. Le redka pristanišča v varnostno oceno vključijo dobavitelje strojne in programske opreme. Testi vdora v sistem se opravljajo redno le v dveh španskih pristaniščih, v Varni in Kopru.

Vprašalniki razkrivajo, da imajo pristanišča, ki imajo med zaposlenimi referenta za varnost pristanišča (PSO), ki je pristojen tudi za kibernetsko varnost, aktivnejši in celovitejši pristop do varnosti v tem sektorju. Pristanišči v Kopru in v Barceloni sta edini med tistimi, ki so izpolnila vprašalnik, ki izvajata redna usposabljanja na področju kibernetske varnosti za svoje zaposlene in ki organizirata tudi redna urjenja. Imenovanje varnostnega odbora (PSC) nima pomembnega vpliva na dejavnost, povezano s kibernetsko varnostjo.

10 http://www.portofantwerp.com/sites/portofantwerp/files/print_exer_complete_1.pdf
11 https://www.portoflosangeles.org/idx_security.asp

Rezultati vprašalnika razkrivajo, da vsa pristanišča uporabljajo protivirusne programe in požarne zidove ter da imajo vsa ločeno Wi-Fi omrežje za goste in za zaposlene. Večina pristanišč ima ločeno notranjo omrežje in uporablja sisteme za odkrivanje (IDS) in preprečevanje vdorov (IPS).

Poleg tehničnih ukrepov, je pri zagotavljanju kibernetske varnosti pomembno upoštevati tudi posamezne zaščitne ukrepe, s katerimi pristanišča zmanjšujejo tveganja, omejujejo škodo uspešno izvedenega napada in omogočajo hitro ponovno vzpostavitev sistema. V zvezi s tem vsa intervjuvana pristanišča izdelujejo varnostne kopije podatkov, redno posodabljajo varnostne sisteme in nameščajo posodobitve programske opreme.

Glede osveščanja in usposabljanja zaposlenih je večina intervjuvanih pristanišč povedala, da sta obveščanje in usposabljanje zaposlenih o morebitnih posledicah kibernetskega napada zelo pomembna. Enako velja tudi za osveščanje zaposlenih o morebitnih nevarnostih pri uporabi prenosnikov zunaj delovnih prostorov, na katerih se hranijo občutljivi podatki. Vendar pa pristanišča različno ocenjujejo potrebo po posebnem usposabljanju s področja kibernetske varnosti.

Vzpostavitev posebnih organov za zagotavljanje kibernetske varnosti pozitivno vpliva na krepitev kibernetske varnosti same. Ugotovljeno je bilo, da imajo pristanišča, ki imajo med zaposlenimi referenta za varnost pristanišča (PSO), ki je pristojen tudi za kibernetsko varnost, aktivnejši in celovitejši pristop tudi do tega vprašanja.

Na splošno pa se pogosto spregleda in zanemarja človeški dejavnik in kibernetsko »higieno«, temveč se daje prednost naložbam v tehnično opremo. Izraelski pristaniški organi poročajo o dobrih praksah na to temo. Vsake tri mesece pošljejo svojim zaposlenim elektronsko sporočilo z obljubo denarne nagrade ali nagradnega potovanja. Če zaposleni kliknejo povezavo v sporočilu, so preusmerjeni na spletno stran, kjer so poučeni o tem, da gre za preverjanje spoštovanja predpisov glede varnosti. Nato se od zaposlenih zahteva, da znova preberejo predpise o kibernetski varnosti. Na ta način se v pristanišču skrbi za osveščanje o vidiku kibernetske varnosti in spremlja učinkovitost posameznih ukrepov.

Zaposleni morajo biti udeleženi v kibernetski varnosti in morajo poročati o vseh ranljivih točkah in sumljivih okoliščinah, sicer se lahko ranljivosti spregleda ali pa lahko hekerji izvedejo napad preko zaposlenih. V idealnih okoliščinah bi moral vsak zaposleni že od vsega začetka poznati varnostne ukrepe, nato bi moral prestati ustrezno usposabljanje in zatem redno urjenje. Do enakih zaključkov so prišli tudi avtorji poročila ENISA (Report on "Analysis of cyber security aspects in the maritime sector", November 2011). Med kratkoročnimi ukrepi za krepitev kibernetske varnosti poročilo navaja tudi povečanje osveščenosti vseh deležnikov na področju pomorskega prevoza. Na prvem mestu sta vzpostavitev dialoga in izmenjava podatkov o kibernetskih nesrečah med vsemi člani pristaniške skupnosti in med pristanišči. V ta namen je bil ustvarjen portal, na katerem se izvajajo testi za prenos poročil o kibernetskih nesrečah v pomorstvu (http://www.csoalliance.com/page/maritime-cyber-crime-reporting-portal).

Izboljšanje kibernetske varnosti v pristaniščih ni enostaven proces. Že ugotovitev morebitnih ranljivosti in izvedba pravilnih rešitev sta lahko velik izziv za pristanišče in za druge člane pristaniške skupnosti. Kibernetska varnost je zapleteno in večnivojsko, izrazito tehnično področje, ki zahteva specifično znanje in izkušnje.

V raziskavi so podana podrobna priporočila, povzeta po drugih mednarodnih virih, kakršna sta «Understanding Cyber Risk: Best Practice for Canada's Maritime Sector» (Transport Canada, 2016) in «Code of practice – Cyber Security for Ports and Ports Systems» (Boyes s sod., 2016), ki ocenjujeta morebitne ranljivosti in navajata dobre prakse pri njihovem reševanju.

V zaključku raziskave je bila potrjena določena stopnja nehomogenosti v opremi in organiziranosti pristanišč na področju fizične in kibernetske varnosti, obenem pa tudi izpostavljenost zelo podobnim varnostnim

tveganjem.

Kljub temu pa še vedno ne obstaja enotna evropska strategija za zagotavljanje pristaniške varnosti, temveč večina pristanišč samostojno financira varnostne projekte. Državne oblasti prispevajo malo ali nič k zaščiti teh kritičnih infrastruktur.

Ugotavljanje nehomogenega, kompleksnega, večnivojskega in tehnično naprednega značaja pristaniške varnosti potrjuje, da je izmenjava dobrih praks in informacij med pristanišči ključnega pomena in da je sodelovanje med pristanišči in njihovimi strokovnjaki, ki je bilo vzpostavljeno s projektom SECNET, nedvomno korak naprej v tej smeri.

Bibliografija in viri

Boyes, H., Roy, I. in Luck, A. (2016). *Code of practice – Cyber Security for Ports and Ports Systems*. IET, UK Department for Transport.

European Union Agency for Network and Information Security - ENISA. (2011)

Cyber Security Aspects in the Maritime Sector. Heraklion, Greece:.

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infra...

https://www.portoflosangeles.org/idx_security.asp

http://www.portofantwerp.com/sites/portofantwerp/files/print_exer_complete_1.pdf

Transport Canada. (2016). *Understanding Cyber Risk: Best Practice for Canada `s Maritime Sector*.

Priloga 6.2

Čezmejno usposabljanje SECNET - Benetke, 27. februar 2018

(Zgoščeno poročilo - izid 3.1.3.2)

Beneško pristanišče, kot partner projekta SECNET, je gostilo čezmejni seminar o varnosti in kibernetski varnosti v pristaniščih, ki je bil predviden v okviru projekta. Seminar je bil predpriprava na skupni akcijski načrt za krepitev zaščite informacijskih omrežij (kibernetske varnosti) in fizične varnosti pristanišč pred vstopom nepooblaščenih oseb, ki so ga izdelala tri pristanišča, udeležena v projektu (Trst, Koper in Benetke). Na podlagi prednostnih nalog, ugotovljenih v akcijskem načrtu, je bila predvidena tudi izvedba konkretnih pilotnih aktivnosti.

Z organizacijo seminarja o fizični in kibernetski varnosti, katerega so se kot predavatelji udeležili nekateri od najpomembnejših mednarodnih strokovnjakov s tega področja, je projekt SECNET zadostil zelo razširjeni potrebi med osebami, odgovornimi za varnost pristanišč v Severnem Jadranu. Čezmejnega usposabljanja se je tako udeležilo več kot 50 referentov, ki delujejo na področju upravljanja pristaniške varnosti v pristaniščih Severnega Jadrana.

Seminar je otvoril generalni sekretar Pristaniške uprave Severnega Jadrana, Martino Conticelli, ki je spomnil na zgodovino razvoja varnostnih ukrepov v pristanišču, od sistemov za fizično zaščito in nadzor območja do vse naprednejših tehnologij. Danes je kibernetska varnost ključni dejavnik, kateremu Benetke že dlje časa namenjajo kar največjo pozornost. Ni naključje, da so inšpektorji Evropske komisije med inšpekcijskim nadzorom konec leta 2017 ugotovili, da je treba **nekatere postopke, ki jih uporabljajo na terminalih Beneškega pristanišča, uporabiti kot dobro prakso tudi v drugih evropskih pristaniščih**. Conticelli je nazadnje poudaril pomen sodelovanja med pristanišči na tem področju, saj je le tako mogoče doseči učinkovitejše in bolj konkurenčne standarde.

Usposabljanje je bilo razdeljeno na tri tematske sklope, pri katerih so sodelovali pomembni univerzitetni profesorji in strokovnjaki. **Kapitan fregate Vincenzo Paolo Leone**, vodja poveljstva luških kapitanij (VI. oddelek), je predstavil najpomembnejše študijske primere v praksah evropskih pristanišč pri upravljanju fizične in kibernetske varnosti, ki so bile ugotovljene ob inšpekcijskih pregledih Evropske komisije. Leone je poudaril strateški pomen kibernetske varnosti in ga podkrepil tudi z neposrednimi izkušnjami pri svojem delu pri Evropski komisiji in ameriški obalni straži. Napovedal je razvoj novega orodja za zbiranje analitičnih podatkov o upravljanju kibernetskih tveganj, ki bo kmalu razširjeno na pristaniške uprave EU.

Prof. Roberto SETOLA, koordinator podiplomskega študija "Homeland Security" na Biomedicinski univerzi v Rimu, je predstavil nove tehnologije za zagotavljanje fizične varnosti (sistemi videoanalize, droni, skenerji itd.) in kibernetske varnosti pristaniških dejavnosti ter poudaril, da stroški varnosti niso »stroški«, temveč naložba, potrebna za rast pristaniškega gospodarstva.

Prof. Fabio Garzia z Univerze La Sapienza iz Rima (Oddelek za varnostno inženirstvo) je poročal o integriranem multidisciplinarnem upravljanju varnosti v pristaniških območjih z železniškimi

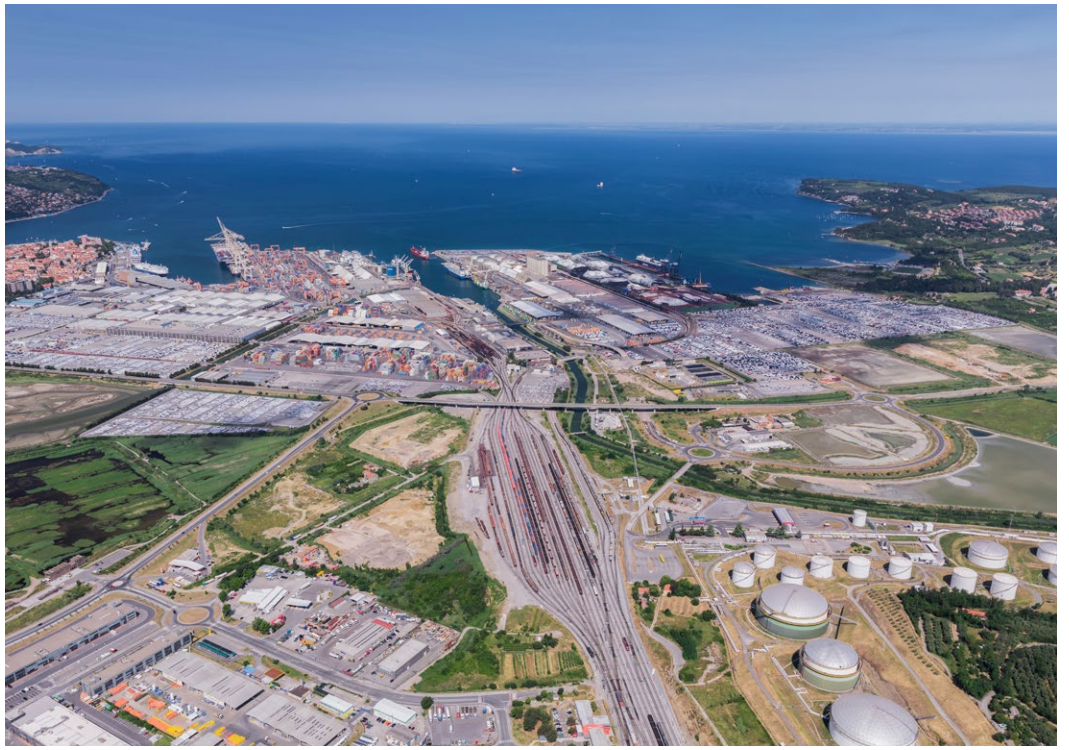
povezavami, kar so kot prednostno poudarili tudi številni drugi govorci.

Koordinatorja usposabljanja sta bila Martina Gržančić, samostojna strokovna delavka na področju strateškega razvoja v Luki Koper, in Ivano Di Santo, predsedujoči Tržaški pristaniški upravi.

Priloga 6.3

Pilotne aktivnosti kibernetske in fizične varnosti v pristaniščih Koper, Trst in Benetke

(Zgoščene predstavitve - izidi 3.1.4 in 3.1.5)



Luka Koper

✓ CYBERSECURITY – PENETRATION TESTS

Cilj te pilotne aktivnosti je preveriti in zatem preprečiti kibernetske napade na pristaniški in na vse z njim povezane sisteme, pri tem pa ugotoviti njegove ranljivosti in posodobiti njegovo podatkovno bazo.

V okviru te aktivnosti so bili izvedeni tako imenovani testi vdorov v sistem (penetration tests), pri katerih gre za: nadzor varnosti po metodi »črne škatle«, kjer je vključeno preverjanje možnosti nepooblaščenega dostopa do podatkov in do spreminjanja slednjih; ustreznost shranjevanja podatkov v lokalnih delovnih postajah za preprečevanje nadaljnje zlorabe sistema; prevzem identitete obstoječih uporabnikov v sistemu; spremembe pravic uporabnikov in oceno funkcij.

Zajeto je tudi preverjanje varnosti operacijskih sistemov strežnika z aplikacijo MS Windows Server. V tem primeru so bili upoštevani vsi veljavni certifikati informacijske varnosti, pri čemer je bilo preverjeno

stanje kontrolne točke in Microsoft GOLD.

Do konca februarja 2019 bodo predvidoma opravljena nadaljnja testiranja sistema, s katerimi se bo preverilo, ali so bile ranljivosti, ki so bile ugotovljene s testi vdorov, učinkovito odpravljene, v skladu s predvidenimi načeli.

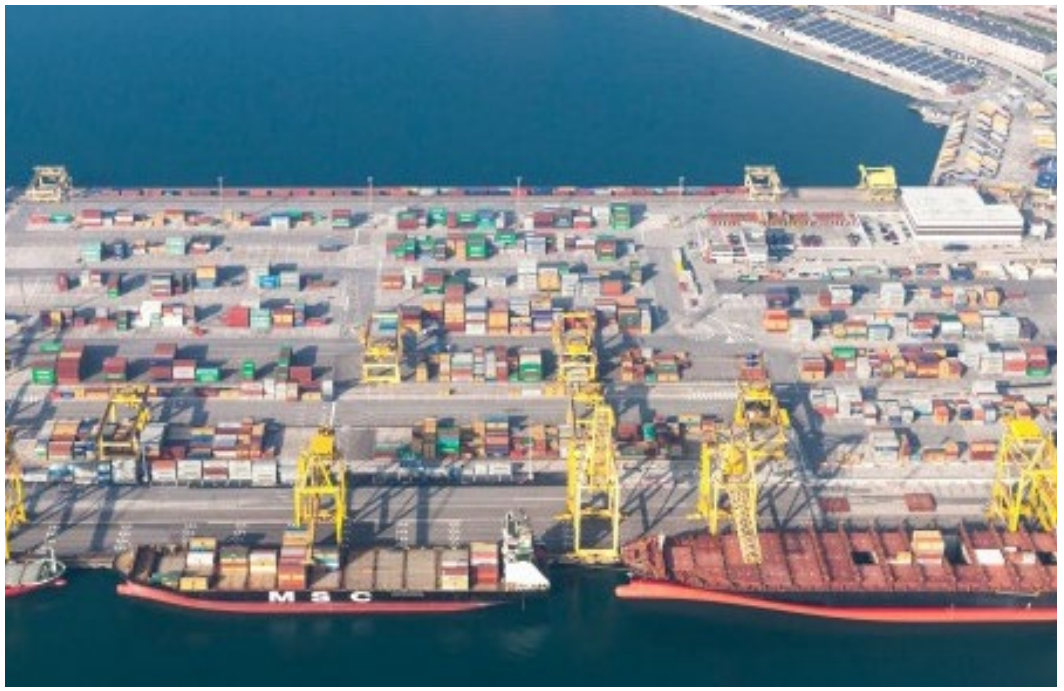
✓ VARNOST OB ZUNANJI MEJI - RADAR

S to pilotno aktivnostjo bo območje koprskega pristanišča, Luke Koper, kjer je pretok blaga, vozil in ljudi največji, opremljeno z izpopolnjenim radarskim varnostnim sistemom, ki se ga bo uporabilo po potrebi.

Vzporedno z razvojem različnih varnostnih tehnologij se razvija tudi vrsta tehnologij za premagovanje ali onemogočanje pregrad za zaščito varnosti in celovitosti pristaniškega sistema. V ta namen je Luka Koper d.d. strateška mesta na območju pristanišča opremila s sodobnim infrardečim radarskim sistemom z dodatnimi termografskimi kamerami z visoko ločljivostjo za 360-stopinjski ogled določenih območij v pristanišču. S temi kamerami lahko nadzorni center zaznava vse vire toplote in vse premike v radiju 1.500 m v vseh vremenskih razmerah, tako podnevi kot ponoči.

Sistem je povezan s strežniki, ki omogočajo shranjevanje in razpošiljanje velikih količin podatkov, ki jih zajema zgoraj navedena oprema, s posnetki visoke ločljivosti, ki se snemajo neprestano.

Predvidena je tudi predpriprava in združljivost videonadzornega sistema, s katerim bo nadzorni center pristanišča lahko v realnem času ter v vseh vremenskih in svetlobnih razmerah spremljal pogoje varovanja in nadzora na določenih območjih Luke Koper.



Pristaniška uprava Severnega Jadrana (Pristanišče Trst)

✓ CYBER SECURITY – PORT IN NUMBERS

Zamisel za to pilotno aktivnost se je porodila zaradi potrebe Pristaniške uprave po integrirani platformi za upravljanje podatkov, ki jih pridobiva s strani heterogenih sistemov. Ta platforma bo uporabnikom omogočala natančen vpogled v dogajanje v pristanišču in na postajališčih zunaj slednjega (t.i. buffer ali vmesna območja) v realnem času.

Pristaniška uprava Vzhodnega Jadrana ima dva informacijska sistema: i) Port Community System - Sinfomar; ii) sistem za nadzor vstopa I-gate, ki bo v kratkem nadgrajen v sistem Vi-gate. Ti dve platformi vsebujeta veliko in kompleksno zbirko podatkov, z vzajemno obdelavo katere bi bilo mogoče zagotoviti boljši nadzor nad vstopi in gibanjem na območju pristanišča tudi z vidika podpore pri sprejemanju upravnih odločitev in ravnanja v izrednih razmerah.

V okviru projekta SECNET je bilo mogoče razviti tovrsten portal, poimenovan PIN - Port In Numbers, s pomočjo katerega bo lahko uporabnik, v skladu z veljavno zakonodajo, zlasti pa z Zakonom o elektronskem poslovanju v javni upravi, z orodjem povleci in spusti (draft & drop) ali z vlečenjem na zaslonu, občutljivem na dotik (v primeru dostopa s tabličnega računalnika ali pametnega telefona), ustvaril lastno zaslonko sliko s povzetkom informacij.

Ta platforma je močno orodje za komuniciranje s skupnostjo, in to ne le pristaniško, temveč s celotnim mestnim tkivom, ki je povezano s pristaniškim območjem. Cilj platforme je tudi prikaz podatkov prek vmesnikov, ki so enostavni za branje in razumevanje. Podatki, ki jih platforma obdeluje, so, na primer, število oseb, ki so vstopile v pristanišče, z njimi povezana prevozna sredstva in hkrati tista, ki jih obravnava sistem Port Community System, ki izvirajo iz vmesnih (buffer) območij ali neposredno z avtocestnih povezav, podrobni podatki o deklariranem blagu na krovu vozil, vključno z nevarnim tovorom, razdelje-

nim po mednarodnih destinacijah. Programska oprema bo ustvarjala grafične prikaze, ki jih bo mogoče predvajati na televizijskih sprejemnikih z internetno povezavo tudi zunaj pristanišča, kar bo občanom omogočalo vpogled v ad hoc pripravljene številke in grafikone.

Vse strani z uporabniškimi funkcijami bodo na voljo v italijanščini in angleščini.

✓ CYBER SECURITY - GDPR

Ta pilotna aktivnost se osredotoča na storitve svetovanja glede varnosti in skladnosti s predpisi, njen cilj pa je prilagoditev IT infrastrukture Pristanišča Trst ob upoštevanju napovedi iz:

i. Uredbe (EU) št. 2016/679 o varstvu posameznikov pri obdelavi osebnih podatkov (t.i. GDPR);

ii. Uredbe z zakonsko močjo št. 196/2003 (t.i. Zakon o varstvu osebnih podatkov), zlasti glede smernic o spremljanju dostopa sistemskih skrbnikov.

Pilotna aktivnost se osredotoča na dve poglavitni področji:

1. storitve na zahtevo: oziroma vse podporne storitve z visoko dodano vrednostjo, namenjene za naslednja področja:
   - navodila za usmerjanje postopka analize in upravljanje tveganj (Security Risk Management);
   - preverjanje obstoječega stanja izvedbe in skladnosti z obstoječo zakonodajo s področja kibernetske varnosti (Gap Analysis);
   - odpravljanje kritičnih točk z namenom povečanja varnosti pri uporabi (Remediation Consulting).
2. Trajne storitve: oziroma vse storitve, ki zagotavljajo neprekinjeno poslovanje na sedežu pristaniške uprave z namenom zaščite in/ali podpore na specifičnih področjih varnosti/skladnosti s predpisi, kot so:
   - zagotavljanje vzdrževanja skladnosti, zagotovljene s sistemi pristaniške uprave, z namenom nadzora nad jamstvom ustreznosti doseženega stanja tekom časa (Compliance Maintenance Support);
   - upravljanje akcij presoje varnosti in skladnosti z veljavno zakonodajo ali s sprejetimi notranjimi standardi (Security & Compliance Audit).

Zahvaljujoč projektu SECNET je bil sestavljen pomemben dokument za presojo, in sicer »Ocena varnosti v Pristanišču Trst - Priloga 4 Podrobna obravnava, Obvladovanje kibernetskih tveganj (Valutazione di Sicurezza del Porto di Trieste – Allegato 4 Approfondimento Cyber Risk Management)«, ki povzema obstoječe stanje v Pristanišču Trst. Ta elaborat je uporabila tudi odgovorna oseba za varstvo podatkov (Data Protection Officer - DPO) Pristaniške uprave Vzhodnega Jadrana v pripravljalnih fazah na uresničitev zahtev Uredbe GDPR, ki je nedavno stopila v veljavo.

Ob inšpekcijskem nadzoru Evropske agencije za varnost v pomorskem prometu (EMSA) novembra 2018 je vodja službe za informatiko Chief Information Officer - CIO) Pristaniške uprave Vzhodnega Jadrana predstavil sestavine dokumenta in naknadni razvoj, kar se je izkazalo za zelo koristno pri skupni presoji varnosti Pristanišča Trst in je poželo veliko odobravanja s strani Evropske komisije.

✓ VARNOST OB ZUNANJI MEJI - SIRENA

Cilj te pilotne aktivnosti je namestiti v predele pristanišča, kjer poteka večina dejavnosti, sistem alarmiranja ob izrednih dogodkih, ki ga nova prostocarinska cona do sedaj ni imela.
V okviru te aktivnosti sta predvideni dobava in namestitev dveh t.i. oddajnih enot, ki ju tvorita aluminijasti usmerjeni sireni, na strehi dveh različnih stavb v novem pristanišču, tako da bo zagotovljena pokritost zvočnega signala na vseh terminalih in v z njimi povezanih delovnih območjih.
Za vklop in upravljanje sistema alarmiranja je zadolžen nadzorni center v Lloydovem stolpu zunaj ograjenega delovnega območja. Zato je v pilotni aktivnosti predvidena tudi namestitev programske opreme z ustreznim radijskim sprožilnikom, ki omogoča sproženje sistema alarmiranja ter nadzor siren in ponavljalnikov v vnaprej določenih časovnih intervalih zaradi preverjanja delovanja (napetost, baterije in troblja) in kakovosti radijskega prenosa.
Predvidena je tudi priprava sistema, ki bo uporabnikom omogočal popoln oddaljeni nadzor siren s podatkovnim omrežjem pristaniške uprave.
Izbrane so bile usmerjevalne sirene za omejitev zvočnega onesnaževanja zunaj pristaniškega območja.

✓ *VARNOST OB ZUNANJI MEJI - DRONI*

Cilj te pilotne aktivnosti je povečati učinkovitost in uspešnost neposrednega preverjanja delovanja pristanišč ter posledično izboljšati sposobnost ukrepanja pristaniške uprave pri opravljanju svojih nalog vzdrževanja in pristaniške varnosti, zlasti z rednim nadzorom na pristaniškem območju s pomočjo dronov (v tehničnem žargonu daljinsko vodeni zrakoplovni sistemi - SAPR).
Drone je pristaniška uprava kupila z lastnimi sredstvi (30.000 Eur) in jih predelala glede na okoljske pogoje v Pristanišču Trst (prisotnost anten, radarskih sistemov, ladij različnih velikosti in tonaž, superstruktur kot so žerjavi ipd.) s sredstvi iz projekta SECNET. Ti sistemi zajemajo digitalne podatke o videonadzoru, ki jih nato obdela kontrolna postaja na sedežu Pristaniške uprave Vzhodnega Jadrana, postavitev katere, vključno s programsko opremo in tehnično podporo, je bila mogoča zahvaljujoč sredstvom iz projekta SECNET.

Pristaniška uprava Vzhodnega Jadrana je omogočila tudi usposabljanje za lastne zaposlene na dveh tečajih, ki ju je delno financirala Dežela Furlanija - Julijska krajina prek Evropskega socialnega sklada (10.000 Eur).

Pristaniška uprava Vzhodnega Jadrana (pristanišče Benetke)

✓ *VARNOST OB ZUNANJI MEJI*

Pilotna aktivnost, ki jo je začela Pristaniška uprava Severnega Jadrana, se je porodila iz potrebe po okrepitvi fizične varnosti in spremljanja uporabe nekaterih vhodov v pristanišče z dopolnitvijo obstoječega sistema za nadzor vstopa z dodatno komponento za odčitavanje registrskih tablic in posodobitvijo obstoječe opreme za obravnavo zahtevkov in izdajo dovolilnic za začasni vstop. V pilotni aktivnosti bodo zajeti prehodi Pristanišča Benetke, natančneje prehoda Sant'Andrea, 34/17 in San Nicolò.

Z aktivnostjo, ki bo potekala v okviru projekta SECNET, bo sistem za nadzor vstopa opremljen s komponento za nadzor prometa motornih vozil, ki bo omogočal potrditev prehoda vozil tako s samodejnim odčitavanjem registrskih tablic kot tudi s klasičnimi značkami, pa tudi upravljanje in spremljanje uporabe parkirišč, ki so predvidena na območju pristanišča.

Na operativni ravni je bila pilotna aktivnost razdeljena na izvedbo dela, ki je zajemal programsko opremo, ter na fizično postavitev kamer in opreme za spremljanje.
Z avtomatizacijo, uvedeno s projektom SECNET, je Pristaniška uprava Severnega Jadrana izboljšala načine spremljanja vstopa v beneško pristanišče, s tem pa skrajšala upravni postopek za izdajo dovolilnic in izboljšala nadzor prehoda.

Priloga 6.4

Protokol o vzpostavitvi sistema čezmejnega sodelovanja na področju pristaniške varnosti

Progetto SECNET

Cooperazione istituzionale transfrontaliera per il rafforzamento della security portuale

Protocollo per l'istituzionalizzazione di un sistema di cooperazione transfrontaliera nell'ambito della security portuale

Projekt SECNET

Čezmejno institucionalno sodelovanje za krepitev pristaniške varnosti

Protokol o vzpostavitvi sistema čezmejnega sodelovanja na področju pristaniške varnosti

In conformità al principio di mutuo vantaggio e sviluppo comune e al fine di rafforzare e sviluppare la cooperazione transfrontaliera, Luka Koper d.d., l'Autorità di Sistema Portuale del Mare Adriatico Orientale e l'Autorità di Sistema Portuale del Mare Adriatico Settentrionale, di seguito denominate "le parti", sottoscrivono il presente protocollo con l'obiettivo di rafforzare la cooperazione transfrontaliera nella security portuale, sviluppata nell'ambito del progetto SECNET, co-finanziato dal Programma Interreg V-A Italia-Slovenia 2014-2020.

V skladu z načelom obojestranske koristi in skupnega razvoja ter z namenom krepitve in razvijanja čezmejnega sodelovanja, Luka Koper d.d., Pristaniška uprava Vzhodnega Jadrana in Pristaniška uprava Severnega Jadrana, v nadaljevanju "stranke", sklepajo ta protokol z željo po okrepitvi čezmejnega sodelovanja na področju pristaniške varnosti, vzpostavljenega v okviru projekta SECNET, sofinanciranega s sredstvi Programa Interreg V-A Slovenija - Italija 2014-2020.

Articolo 1
Obiettivi comuni

La cooperazione transfrontaliera attuata nel progetto SECNET ha evidenziato come la sicurezza dei porti e la loro efficienza operativa siano di fondamentale importanza non solo per il trasporto marittimo, ma anche per il ruolo strategico dei porti in termini di sicurezza, a livello regionale, nazionale ed europeo. La sicurezza portuale diventa così

1. člen
Skupni cilji

Tekom čezmejnega sodelovanja v okviru projekta SECNET je bilo ugotovljeno, da sta varnost pristanišč in učinkovitost njihovega poslovanja ključnega pomena ne le za pomorski promet, temveč tudi za strateško vlogo pristanišč v smislu varnosti na regionalni, nacionalni in evropski ravni. Pristaniška varnost tako postaja priložnost za

un'opportunità per automatizzare e semplificare le procedure e le operazioni portuali, anche con l'utilizzo di tecnologie dell'informazione e della comunicazione (ICT).

avtomatizacijo in poenostavitev postopkov in dejavnosti v pristaniščih, pri tem pa si je mogoče pomagati tudi z informacijsko in komunikacijsko tehnologijo (IKT).

Per questo motivo, le parti faranno tutti gli sforzi per stabilire una cooperazione adeguata nel campo della security portuale.

Iz tega razloga si bodo stranke prizadevale za vzpostavitev ustreznega sodelovanja na področju pristaniške varnosti.

Articolo 2
Cooperazione

2. člen
Sodelovanje

Le parti convengono di cooperare tra loro nelle seguenti attività:

Stranke se strinjajo, da bodo sodelovale pri naslednjih aktivnostih:

1) condivisione di buone pratiche nella gestione dei rischi inerenti la sicurezza perimetrale e cyber security, inclusa la protezione dei dati personali, compatibilmente con il necessario profilo di riservatezza richiesto;

1) izmenjava dobrih praks pri obvladovanju tveganj v zvezi z varnostjo ob zunanji meji pristanišča in s kibernetsko varnostjo, vključno z varstvom osebnih podatkov, v skladu z zahtevano stopnjo zaupnosti;

2) iniziative congiunte di formazione e sensibilizzazione sull'importanza di una adeguata sicurezza nelle operazioni marittime da destinare ai principali attori del settore portuale;

2) skupne pobude usposabljanja in osveščanja o pomenu ustrezne varnosti pri pomorskih dejavnostih za najpomembnejše akterje iz pristaniškega sektorja;

3) realizzazione di esercitazioni congiunte

3) izvedba skupnih usposabljanj in

e/o partecipazioni incrociate ad esercitazioni locali sia di security perimetrale sia informatica;

navzkrižno udeleževanje pri lokalnih usposabljanjih tako glede informacijske varnosti kot glede varnosti ob zunanji meji;

4) partecipazione congiunta a progetti co-finanziati per proseguire la cooperazione transfrontaliera nell'ambito della security portuale

4) skupna udeležba pri sofinanciranih projektih z namenom nadaljnjega čezmejnega sodelovanja na področju pristaniške varnosti.

Articolo 3
Contatti amministrativi

3. člen
Upravni stiki

Le parti convengono di individuare dei punti di contatto interni per la realizzazione delle attività di cui all'articolo 2.

Stranke se strinjajo, da bodo opredelile notranje kontaktne točke za izvedbo aktivnosti iz člena 2.

Articolo 4
Rapporto con altri accordi e obblighi delle parti

4. člen
Razmerje do drugih sporazumov in obveznosti strank

Questo Protocollo e le sue modalità esecutive non pregiudicano l'esecuzione di obblighi derivanti da altri accordi multilaterali o bilaterali che sono stati o saranno firmati e approvati dalle parti.

Ta protokol in načini njegovega izvajanja ne bodo vplivali na druge obveznosti, določene z drugimi večstranskimi ali dvostranskimi sporazumi, ki so ali jih bodo stranke sklenile in odobrile.

Con la stipula del presente Protocollo, ciascuna parte si impegna ad attuarne i contenuti. Nessuna delle parti coinvolte ha verso le altre obblighi finanziari e ciascuna parte sostiene i propri costi di attuazione del

S sklenitvijo tega protokola vsaka stranka prevzema dolžno prizadevanje za njegovo izvedbo. Nobena stranka nima do druge finančnih obveznosti in vsaka stranka nosi svoje stroške izvedbe tega Protokola.

presente Protocollo.

Articolo 5 Modifiche	5. člen Spremembe
Questo Protocollo può essere modificato su richiesta scritta di una delle parti, e scritto di comune accordo delle parti. Le modifiche saranno fatte per iscritto ed entreranno in vigore il giorno della firma delle parti e costituiscono parte integrante del presente Protocollo	Spremembe tega protokola so mogoče na pisno zahtevo ene od strank in jih sestavijo stranke v skupnem dogovoru. Spremembe morajo biti pisne in v veljavo stopijo na dan podpisa s strani strank ter so sestavni del tega protokola.
Articolo 6 Entrata in vigore	6. člen Začetek veljave
Questo Protocollo d'intesa entrerà in vigore il giorno della firma.	Ta protokol o sodelovanju začne veljati z dnem podpisa.
Questo Protocollo è concluso per un periodo di 3 anni e dopo tale periodo verrà automaticamente rinnovato per altri periodo di 3 anni, a meno che una delle parti informi le altre circa la propria volontà di ritirarsi.	Ta protokol se sklepa za 3 leta, po tem obdobju pa se samodejno podaljša za nadaljnja 3 leta, v kolikor ena od strank ne sporoči drugim strankam, da protokola ne namerava podaljšati.
Questo Protocollo comprende un preambolo e 6 articoli, in lingua italiana e slovena.	Ta protokol obsega uvod in 6 členov, v italijanskem in slovenskem jeziku.

Trieste, 28 marzo 2019

V Trstu, 28. marca 2019

Autorità di Sistema Portuale del Mare Adriatico Orientale Zeno D'Agostino, Presidente	Autorità di Sistema Portuale del Mare Adriatico Orientale Zeno D'Agostino, Predsednik
Firma,	Podpis,

Autorità di Sistema Portuale del Mare Adriatico Settentrionale - Porti di Venezia e Chioggia

Pino Musolino, Presidente

Firma, _____

Autorità di Sistema Portuale del Mare Adriatico Settentrionale - Porti di Venezia e Chioggia

Pino Musolino, Predsednik

Podpis, _____

7

Luka Koper, pristaniški in logistični sistem, d.d.

Dimitrij Zadel, Presidente del Consiglio di Amministrazione

Firma, _____

Luka Koper, pristaniški in logistični sistem, d.d.

Dimitrij Zadel, Predsednik Uprave

Podpis, _____

8

Kratice

OKRAJŠAVA	RAZLAGA
EU	Evropska unija
IKT	Informacijska in komunikacijska tehnologija
SEP	*Srednjeevropska pobuda*
INTERREG	Programme for the European Territorial Cooperation (program za evropsko teritorialno sodelovanje)
ETS	*Evropsko teritorialno sodelovanje*
TEN-T	*Trans-European Transport Network (Vseevropsko prometno omrežje)*
ADSP MAO	Pristaniška uprava Vzhodnega Jadrana
WP	Work Package (DS - Delovni sklop)
UNITS	*Università degli Studi di Trieste (Univerza v Trstu)*
ADSP MAS	Pristaniška uprava Severnega Jadrana
LK	Luka Koper
UP	*Univerza na Primorskem*
NAPA	North Adriatic Port Association (Združenje pristanišč Severnega Jadrana)
UNCTAD	United Nations Conference on Trade and Development (Konferenca Združenih narodov za trgovino in razvoj)
MTSA	Maritime Transportation Security Act (Zakon o varnosti pomorskega prometa)
SAFE PORT ACT	Security and Accountability For Every Port
ENISA	*European Network and Information Security Agency (Evropska agencija za varnost omrežij in informacij)*
DG MOVE	Direzione Generale per la mobilità e il trasporto (Generalna direkcija za mobilnost in promet)
EMSA	*European Maritime Safety Agency (Evropska agencija za varnost v pomorskem prometu)*
SCADA	*Supervisory Control And Data Acquisition*
IMO	International Maritime Organization (Mednarodna pomorska organizacija)
OMD/WCO	*World Customs Organization (Svetovna carinska organizacija)*
IMB	*International Maritime Bureau (Mednarodni pomorski urad)*
IMSC	International Maritime Security Corporation (Mednarodna pomorska varnostna korporacija)
CIIP	*Critical Information Infrastructure Protection (Zaščita kritične informacijske infrastrukture)*
ISAC	*Information Sharing and Analysis Center (Center za izmenjavo in analizo informacij)*
SDSS	*Spatial Decision Support System (Sistem v podporo pri odločanju v procesih prostorskega načrtovanja)*
CPNI	Centre for the Protection of National Information Infrastructure (Center za zaščito nacionalne informacijske infrastrukture)
CCTSP	Centro di Coordinamento Transfrontaliero per la Security Portuale (Čezmejni koordinacijski center za pristaniško varnost).
DPO	*Data Protection Officer (pooblaščena oseba za varstvo osebnih podatkov)*
GDPR	Splošna uredba EU o varstvu podatkov
ANPR	Automatic Number Plate Recognition (Samodejno prepoznavanje registrske tablice)
GIS	Geografski informacijski sistem
PSO	*Port Security Officer (referent za varnost pristanišča)*
PSC	*Port Security Committee (odbor za varnost pristanišča)*

CEI
CENTRAL EUROPEAN INITIATIVE
SEGRETARIATO ESECUTIVO
DELL'INIZIATIVA CENTRO-EUROPEA

AUTORITÀ DI SISTEMA PORTUALE
DEL MARE ADRIATICO SETTENTRIONALE
PORTI DI VENEZIA E CHIOGGIA

Autorità di Sistema Portuale
del Mare Adriatico Orientale
Porto di Trieste
AUTORITÀ DI SISTEMA PORTUALE
DEL MARE ADRIATICO ORIENTALE
PORTO DI TRIESTE
(LEAD PARTNER / VODILNI PARTNER)

UNIVERSITÀ
DEGLI STUDI DI TRIESTE
UNIVERSITÀ DEGLI STUDI DI TRIESTE

LUKA KOPER
Port of Koper
LUKA KOPER

UNIVERZA NA PRIMORSKEM IN IZVRŠNI
UNIVERSITÀ DEL LITORALE

Mare Adriatico
Jadransko morje



SECURITY PORTUALE - VARNOST PRISTANIŠČA

KONTAKT / CONTATTI

Autorità di Sistema Portuale
del Mare Adriatico Orientale – Porto di Trieste
Dott. Alberto Cozzi
acozzi@porto.trieste.it
T. +39 040 673 2617

facebook.com/secnet
twitter.com/Secnet Project
linkedin.com/in/secnet-project

www.ita-slo.eu/**SECNET**