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

PUBBLICAZIONE FINALE

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

PUBBLICAZIONE FINALE

TRIESTE, MARZO 2019

SECURITY PORTUALE - VARNOST PRISTANIŠČA

LEAD PARTNER / VODILNI PARTNER

Autorità di Sistema Portuale del Mare Adriatico Orientale Porto di Trieste

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

PARTNER DI PROGETTO / PROJEKTNI PARTNERJI

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

LUKA KOPER
Port of Koper

LUKA KOPER

UNIVERZA NA PRIMORSKEM IN IZVRŠNI / UNIVERSITÀ DEL LITORALE

Questo documento è un'iniziativa della partnership del progetto SECNET (elenco partner e riferimenti programma)

Il manoscritto in lingua italiana ed in lingua slovena è stato completato nel marzo 2019.

Autore: PP2 InCE

Assistente editoriale: Divulgando s.r.l.

Feedback di ogni tipo è il benvenuto.

Si prega di scrivere al Lead Partner del progetto: acozzi@porto.trieste.it

Questo documento è pubblicato

nel sito del progetto SECNET in https://www.ita-slo.eu/it/secnet

Il progetto SECNET: una sintesi

Il 31 marzo 2019 si conclude il progetto "SECNET – *Cooperazione istituzionale transfrontaliera per il rafforzamento della security portuale*", co-finanziato dal Programma di Cooperazione Interreg V A Italia-Slovenia 2014-2020.

L'obiettivo principale di SECNET, avviato a ottobre 2017 e guidato dall'Autorità di Sistema Portuale del Mare Adriatico Orientale è stato rafforzare la capacità istituzionale dei porti di Trieste, Venezia e Capodistria creando le basi per una governance coordinata e permanente della security portuale a livello transfrontaliero, anche con l'applicazione delle più recenti soluzioni digitali.

Nell'arco di un anno e mezzo i tre porti, con l'aiuto delle Università di Trieste e del Litorale e del Segretariato Esecutivo dell'Iniziativa Centro Europea, hanno confrontato le proprie strutture operative con le migliori pratiche internazionali ed hanno sviluppato in maniera congiunta piani di azioni e strategie di lungo periodo, aumentando il proprio coordinamento e cooperando a rafforzare la propria sicurezza e competitività. SECNET ha rafforzato così la capacità operativa e la governance transfrontaliera della sicurezza portuale anche al fine di soddisfare le raccomandazioni dell'UE per la protezione delle infrastrutture critiche e la relativa gestione del partenariato fra pubblico e privato. Sulla base della identificazione dei punti di forza e di debolezza delle strutture marittime dell'Alto Adriatico il progetto ha offerto la competenza tecnica per applicazioni ICT innovative e coordinate in materia di miglioramento della sicurezza informatica e della sicurezza dei perimetri portuali. Sono state messe in opera concrete azioni pilota, quali l'installazione di radar, sirene, telecamere, utilizzo di droni e test di penetrazione per la difesa da attacchi informatici, che rimangono come risultati di SECNET nella quotidianità delle operazioni portuali ed hanno innescato ulteriori sviluppi ora in corso.

I principali risultati del progetto sono stati presentati e discussi durante la conferenza finale, che si è svolta giovedì 28 marzo a Trieste e sono illustrati dalla presente pubblicazione di sintesi, che facilita anche l'accesso ai documenti originali prodotti lungo il percorso progettuale.

Le più recenti sfide, le minacce e le strategie per contrastarle nell'ambito della sicurezza fisica e della cyber security portuale, sono perciò l'orizzonte operativo del Protocollo congiunto per l'istituzionalizzazione di un sistema di cooperazione transfrontaliera nella security portuale, che i rappresentanti dei porti di Trieste, Venezia e Capodistria, e di altre amministrazioni ed aziende interessate, hanno firmato in questa occasione e che sono aperte all'adesione anche di altri *hub* marittimi come Monfalcone, Porto Nogaro e Chioggia.

Indice

1.

La sfida di security nell'economia portuale al tempo della trasformazione digitale ed il contributo del progetto SECNET

Secondo rilevazioni della Commissione Europea, l'impatto economico del *cyber-crime* è cresciuto di cinque volte fra il 2013 e il 2017 e potrebbe crescere ancora di quattro volte prima del 2020. L'80% delle imprese europee ne erano state colpite già nel 2016. Cittadini e Stati interi ne sono rimasti vittima a partire dal primo episodio noto, in Estonia nel 2007.

A maggio 2017, in occasione della verifica di medio termine della Strategia per il mercato unico digitale, **la Commissione ha identificato il contrasto delle minacce alla cyber-security come una delle tre priorità dell'UE nei prossimi anni**, avviando subito una proposta legislativa (illustrata in COM(2017) 477, 13.9.2017), che è giunta al voto della plenaria del Parlamento Europeo in questo mese di marzo 2019.

La proposta prevede di innovare e potenziare il mandato dell'ENISA (European Network and Information Security Agency), istituita nel 2004, facendone un soggetto operativo per l'azione comune e portando avanti il superamento della competenza esclusiva degli Stati Membri già avviato con la Direttiva (UE) 2016/1148 "**per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione**" (NIS Directive), il cui termine per la messa in opera era il 9 maggio 2018. ENISA svolgerà inoltre un ruolo chiave nella certificazione della *ICT security*, che tuttora segue molteplici criteri di certificazione, spesso validi solo a livello nazionale.

La creazione di un primo quadro di certificazione volontaria della cyber-security dei prodotti ICT nell'UE conferma l'importanza della dimensione europea anche in questo campo ed il rilievo dei contributi dal basso, che possono venire dalla cooperazione transnazionale e transfrontaliera di settore come nel caso del progetto SECNET.

La conferenza su **"Transport cybersecurity: raising the bar by working together",** organizzata il 23 gennaio scorso da ENISA a Lisbona con il sostegno della Commissione (DG MOVE) e di European Union Aviation Safety Agency (EASA), European Maritime Safety Agency (EMSA) e di EU Agency for Railways (ERA), ha confermato l'esigenza di accelerare ancora la cooperazione europea per la cyber-security in particolare nel mondo dei trasporti. Il dibattito ha focalizzato questioni come:

1. I cyber-attacchi mirati al sistema dei trasporti possono avere gravi conseguenze in vite umane e danni economici; il sistema trasportistico deve essere in grado di prevenire gli attacchi e, ove necessario, di reagire in prima persona.
2. La cyber-security richiede un metodo olistico, che non si rivolga solo ai sistemi connessi via inter-

net, ma anche al fattore umano, e che garantisca la cooperazione fra livello tecnico e livello operativo.

3. Nel solido quadro fornito dalla NIS Directive del 2016 il rafforzamento della cyber security per alcuni tipi di trasporto richiede normative specifiche.
4. Senza bisogno di normative, azioni concrete possono già essere svolte per affrontare le minacce *cyber*: scambio di informazioni, incremento delle risorse, promozione della consapevolezza, sviluppo delle competenze.
5. Il lavoro comune deve generare una "cultura della cybersecurity" propria del settore dei trasporti.
6. Poiché il trasporto è globale ed interconnesso, deve continuare ed essere incoraggiata la collaborazione con partner internazionali e con le organizzazioni internazionali pertinenti, anche oltre i confini dell'UE.

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.

Questo è il quadro di riferimento internazionale, nel quale si inseriscono i risultati raggiunti dal progetto SECNET, che fonda le raccomandazioni e gli obiettivi della sua strategia di cooperazione transfrontaliera non solo sulla sperimentazione realizzata con le sei azioni pilota, che hanno già rafforzato la sicurezza fisica e cyber dei tre porti partecipanti, ma anche su **una vasta documentazione dei quadri normativi in essere fra fine del 2017 e 2018 e sull'analisi dei fattori di forza e di debolezza dei tre sistemi portuali di Trieste, Koper-Capodistria e Venezia-Chioggia**, coordinata poi con la valutazione dei rischi e delle misure da adottare nel quadro del Piano d'Azione transfrontaliero elaborato già a metà progetto dall'Università di Trieste.

Poiché gran parte di tali elaborati riveste carattere sensibile, che ne impedisce la pubblicazione *tout court,* è utile ripercorrere gli argomenti sui quali SECNET ha messo a disposizione dei decisori politici, gestionali ed operativi questo vasto materiale di lavoro. Mentre lo studio comparativo curato dall'Università del Litorale di Koper/Capodistria sulle buone pratiche internazionali, europee e transfrontaliere è presentato in versione ridotta all'Allegato 6.1 di questa pubblicazione finale, merita evidenziare qui i contenuti del **"Rapporto consolidato sull'attuale situazione e le principali criticità riguardanti la security portuale nell'area di progetto"** (Deliverable 3.1.2.1), curato dallo staff di Luka Koper ed al quale hanno poi contribuito gli esperti di altri partner pertinenti.

Il Rapporto Consolidato sullo stato dell'arte nei porti dell'Alto Adriatico fornisce un utile **quadro della normativa esistente** a partire dai fondamenti giuridici e dagli standard di riferimento per le misure di sicurezza dei porti. Sono richiamate la normativa europea in materia di sicurezza marittima e quella di altri Paesi, USA in particolare. Viene presentata la legislazione nazionale vigente in Slovenia ed in Italia e gli atti interni adottati dalle Autorità portuali nell'esercizio della loro potestà. Sono poi comparate specificamente le norme nazionali ed europee per la protezione delle infrastrutture critiche e la loro applicabilità nella realtà transfrontaliera.

Una precisa illustrazione delle aree portuali e dei loro confini terrestri e marittimi include anche la presentazione delle zone a mare, dei canali di grande navigazione, degli impianti portuali e dei confini dove si esercita la security dei porti. Sono analizzati separatamente i grandi gruppi di rischio, che incombono sulle realtà portuali dell'Adriatico settentrionale e l'organizzazione del sistema integrato di sicurezza, al quale concorrono con distinte responsabilità organi diversi delle rispettive pubbliche amministrazioni nazionali e locali. Al riguardo sono stati valutati anche i controlli sugli accessi e la circolazione nei comprensori portuali, sia riguardo agli accessi via terra che a bordo nave, le procedure di entrata ed uscita delle merci, l'organizzazione dei centri operativi preposti alla sicurezza, i livelli di sicurezza a fronte delle violazioni registrate, le modalità di esercitazione, quelle di monitoraggio e la cooperazione con le istituzioni dello Stato.

Questa accurata analisi ha poi consentito la formulazione del Piano d'Azione sopra citato, che consente anche stimolanti comparazioni fra gli assetti di sicurezza fisica e di cyber-security nei tre porti partecipanti a SECNET, quali erano a metà del 2018!

2.

La cooperazione portuale transfrontaliera ed adriatica nei programmi INTERREG Italia – Slovenia della Cooperazione Territoriale Europea

Nella programmazione comunitaria 2007 – 2013 l'INTERREG Italia – Slovenia aveva perseguito la **priorità di "assicurare un'integrazione territoriale sostenibile"** anche attraverso l'"obiettivo specifico" descritto come "integrazione tra i sistemi di trasporto e diversificazione dei mezzi di trasporto". Il Programma si prefiggeva allora di "assicurare un'integrazione territoriale rispettosa dell'ambiente" attraverso lo "sviluppo di reti di trasporto sostenibili e interoperabili, nonché l'utilizzo di sistemi di trasporto multimodali, alternativi a quello su gomma"; di "migliorare l'accessibilità ed i sistemi di trasporto esistenti potenziando i collegamenti dei porti di Trieste e Koper all'Asse prioritario Lione – Torino – Milano – Trieste – Ljubljana – Budapest" (allora denominato Corridoio n.5); e di "incentivare il coordinamento tra tutti i porti dell'area di programma".

Alla fine di marzo 2015, considerata la numerosità e l'importanza dei progetti in materia trasportistica co-finanziati nel periodo, si tenne a Trieste un **evento di capitalizzazione** dei risultati e delle lezioni apprese, organizzato dal Segretariato dell'InCE insieme al Segretariato Congiunto del programma, che si articolava sulla presentazione di progetti transfrontalieri in corso (ADRIA A, IDAGO, TIP, TRADOMO) e di progetti analoghi realizzati nel quadro di altri programmi di scala transnazionale finanziati dal Fondo Europeo di Sviluppo Regionale ai fini dell'obiettivo Cooperazione Territoriale Europea (CTE). Dai gruppi di lavoro costituitisi successivamente sui temi dell'accessibilità, dell'intermodalità e della mobilità transfrontaliera vennero importanti indicazioni per la nuova programmazione, allora ancora in corso definizione.

Il Programma INTERREG Italia – Slovenia 2014 – 2020 non ha scelto fra i suoi "obiettivi tematici" quello della mobilità. Proprio dalla conferenza di Trieste sono venute però utili indicazioni per una **declinazione dei temi di interesse trasportistico trasversale agli obiettivi tematici scelti ed alle Priorità, che ne sono derivate**.

Le tematiche della mobilità avrebbero potuto generare con originalità progetti quali:

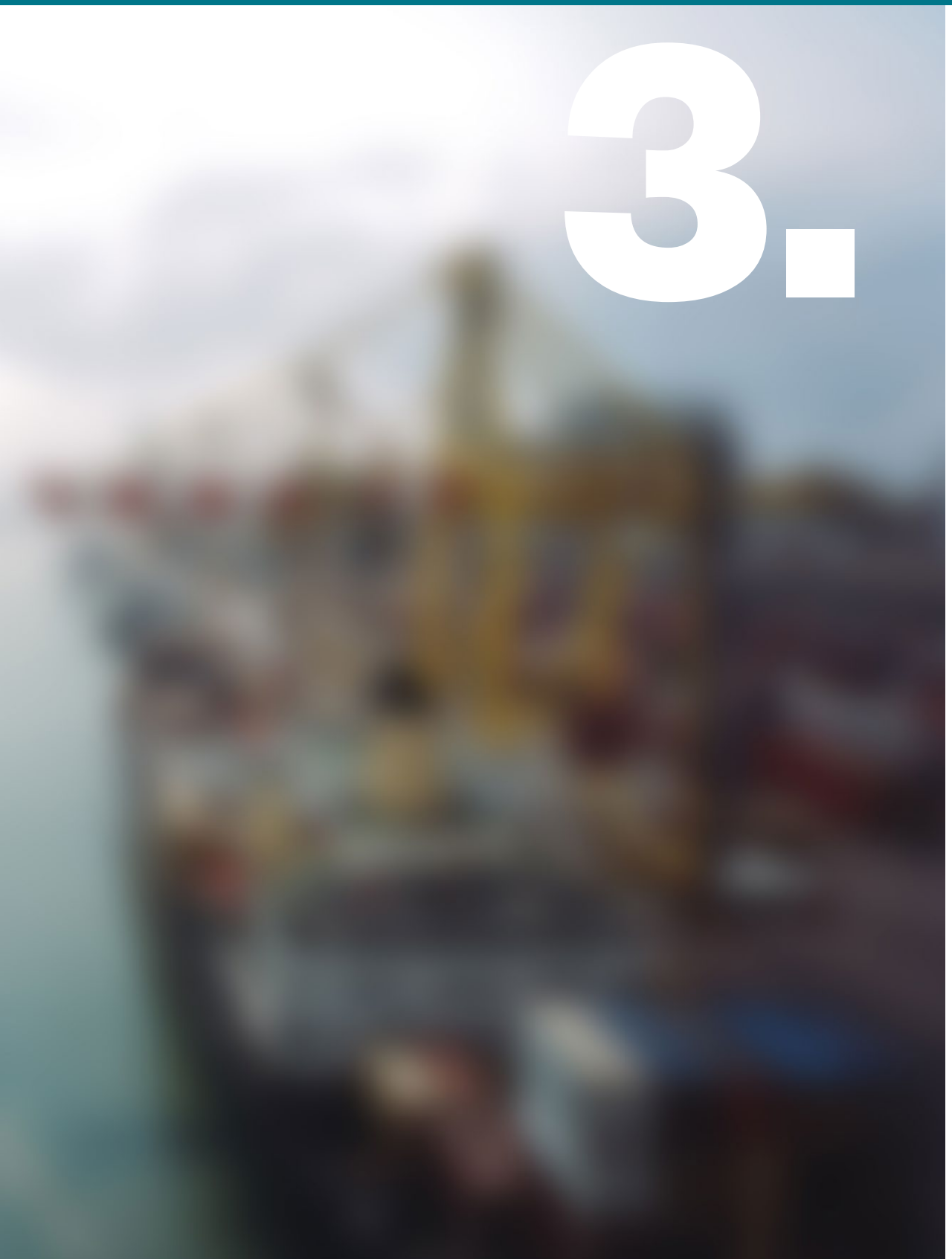
- per la Priorità 1 (innovazione tecnologica, di prodotto, di processo, organizzativa): trasporti verdi, innovazione sociale, tecnologie abilitanti per la mobilità sostenibile;
- per la Priorità 2 (economia a bassa emissione di carbonio): mobilità sostenibile e multi-modale, elaborazione partecipata di Piani di Mobilità Urbana Sostenibile (Sustainable Urban Mobility Plans - SUMP) in ottica Smart Cities, trasporto pubblico locale ed "ultimo miglio" transfrontaliero, eliminazione di "colli di bottiglia", sviluppo del car-sharing ad alimentazione elettrica, valutazione e pianificazione delle stazioni di ricarica elettrica, rivalutazione di mezzi di trasporto diversi (marittimi, aerei, anche riqualificando i piccoli aeroporti);
- per la Priorità 3 (protezione e promozione delle risorse naturali e culturali): marketing allargato fuori area programma, promozione dell'innovazione sociale (ad es. la modifica delle abitudini d'uso delle auto personali), infrastrutture comuni per la mobilità a breve, recupero di percorsi abbandonati di rilievo naturalistico e/o architettonico, potenziamento dei percorsi ciclabili transfrontalieri est-ovest;
- per la Priorità 4 (capacità della PA e governance transfrontaliera): collegamento fra le Pubbliche Amministrazioni, armonizzazione normativa, pianificazione congiunta, finanziamento coordinato.

E' in questo approccio **l'origine del progetto SECNET che implementa l'Obiettivo Tematico 11 della programmazione europea: "rafforzare la capacità istituzionale delle autorità pubbliche e delle parti interessate e un'amministrazione pubblica efficiente**" … "mediante la promozione della cooperazione giuridica e amministrativa e la cooperazione fra i cittadini e le istituzioni". Ovvero SECNET ha realizzato la traduzione operativa dell'Obiettivo Specifico 4.1 rafforzando "la cooperazione istituzionale attraverso la mobilitazione delle autorità pubbliche e degli operatori chiave dell'area del programma al fine di pianificare soluzioni congiunte per le sfide comuni"!

I progetti in materia di trasporto però, per quanto transfrontalieri, dovrebbero essere integrati nell'ambito di strategie più ampie quali le "strategie macroregionali europee". **L'area transfrontaliera Italia – Slovenia trova il suo quadro di riferimento più utile nella Strategia macroregionale delle Alpi, in quella del Danubio ed in quella Adriatico-Ionica.** Il contributo delle esperienze e dei risultati acquisiti con progetti di carattere transfrontaliero è infatti importante anche per alimentare il costante aggiornamento delle strategie macro-regionali dell'Unione Europea così come lo è per realizzarne gli obiettivi. I risultati del progetto SECNET perciò costituiscono un importante contributo ai Piani d'Azione delle strategie macro-regionali e meritano di essere comunicati ai coordinatori delle loro aree prioritarie pertinenti.

Per EUSAIR, la strategia adriatico-ionica, in particolare, SECNET è pienamente integrato fra le azioni previste dal **Pilastro n. 2 denominato "Connecting the region"**, che ha anche l'obiettivo specifico di "rafforzare la sicurezza marittima e sviluppare un sistema portuale regionale competitivo", con azioni quali "certificazioni comuni per la sicurezza, sostenibilità e digitalizzazione dei porti" e lo "sviluppo e ottimizzazione dei porti, delle infrastrutture e delle procedure", ad esempio con l'"implementazione di strumenti ICT per migliorare efficacia, efficienza e sicurezza delle operazioni portuali" e l'"armonizzazione delle procedure portuali tramite a strumenti ITS".

Il seguito di SECNET nella cooperazione istituzionalizzata dei porti di Trieste, Koper-Capodistria e Venezia, definita con il Protocollo sottoscritto in occasione della Conferenza Finale, può contribuire ulteriormente anche a capitalizzare risultati con altri progetti europei. La security portuale e il relativo uso delle ICT infatti non sono stati oggetto di molti progetti europei fino a quando non è emersa drammaticamente l'attualità di questa dimensione operativa nella fase attuale. **SECNET rappresenta perciò un'azione che ha ancora carattere pilota nel panorama della cooperazione territoriale europea.** Alcune sinergie con altri progetti co-finanziati dall'Unione Europea negli ultimi anni possono perciò essere esplorate, perseguendo la costruzione di rapporti di rete fra la partnership SECNET e quella di altri progetti noti per l'analogia delle esperienze di cooperazione transnazionale messe in opera, al fine di condividere le conoscenze sviluppate e di **creare i presupposti per una rete transnazionale di scambio di conoscenze di lungo periodo in materia di cyber security.**



3.

Presentazione del progetto SECNET: giustificazione, obiettivi, rilevanza della partnership

Il progetto SECNET ha avuto l'obiettivo di rafforzare la capacità di cooperazione istituzionale e la governance transfrontaliera nella security portuale attraverso la mobilitazione delle autorità pubbliche e degli operatori chiave dell'Area di Programma al fine di pianificare soluzioni congiunte per le sfide comuni.

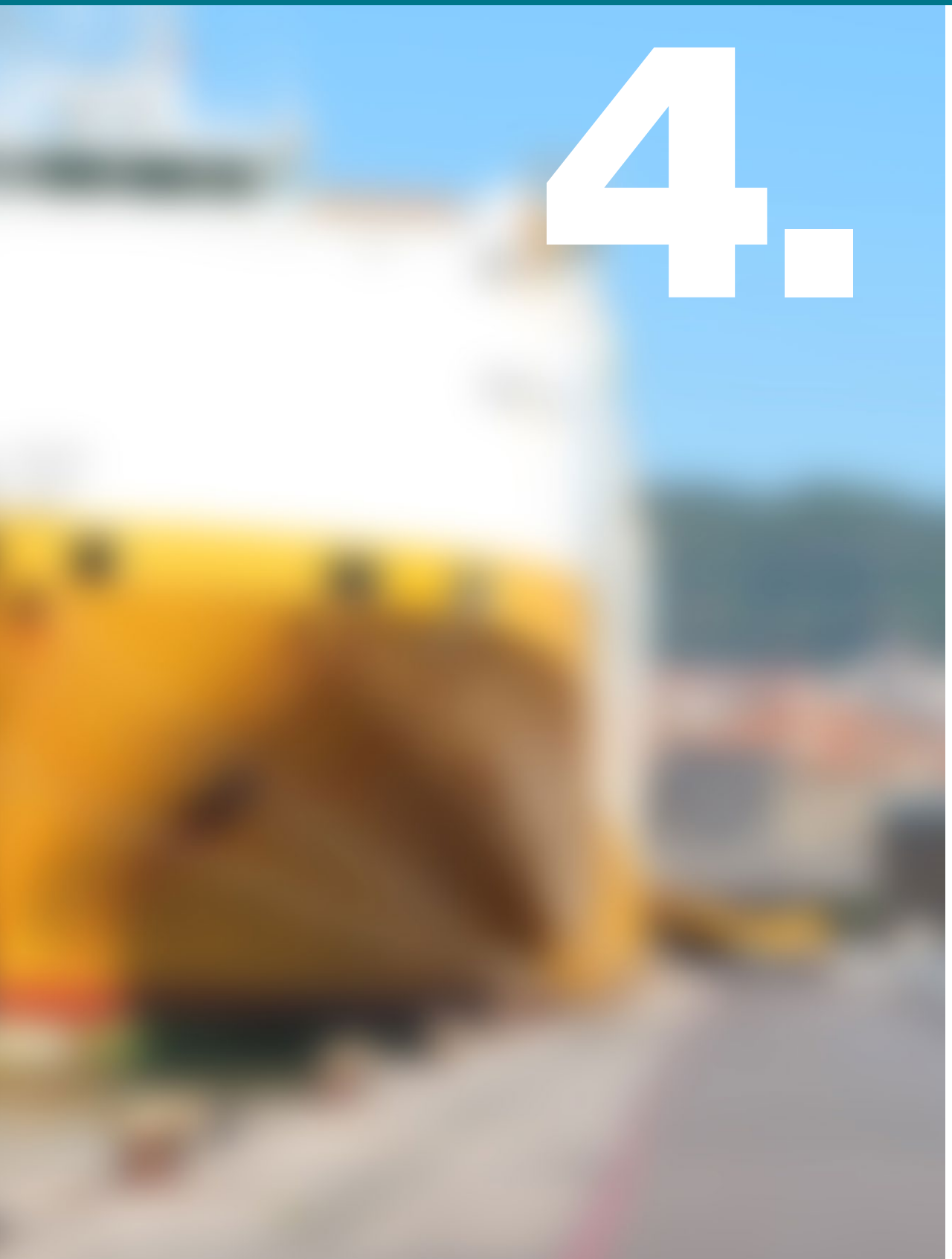
Le autorità portuali sono attori importanti nella formazione dell'identità culturale e della consapevolezza sociale delle comunità costiere legate all'economia marittima ed alle sue ricadute sul territorio. Nelle realtà di Trieste, Capodistria – Koper e Venezia il porto con il suo indotto emporiale è storicamente fattore identitario e motore della crescita e del benessere economico. Da esso traggono impulso professionalità specialistiche e competenze tecnologiche particolari, che sono spesso fondamentali vettori di processi olistici di innovazione.

Nella rapida evoluzione degli scenari del mercato globale, in cui operano le realtà portuali, sono presenti però anche fattori di rischio di natura sia materiale ed oggettiva, legati alle tipologie di traffico, sia soggettiva e geo-politica, determinati dall'uso distorsivo o illecito delle risorse tecnologiche disponibili.

Le autorità portuali sono oggi più che mai in passato poste a confronto con tali rischi su una scala sempre più estesa ed a reattività accelerata, che ne espande l'area territoriale di responsabilità. In un'area di confine all'interno dell'Unione Europea ciò impone coerenza fra le misure di governance locali / nazionali e le problematiche di rischio transfrontaliero, sia in considerazione della necessaria prevenzione dell'impatto dei rischi su scala ambientale sia in relazione alle possibili economie di scala derivabili dal coordinamento e dall'integrazione delle risorse e degli approcci.

L'area coinvolta dalle attività progettuali include i tre porti principali appartenenti alla rete TEN-T (Venezia, Trieste e Koper-Capodistria), che devono affrontare sfide comuni: garantire la sicurezza minimizzando il rischio e al contempo garantire un fluido e veloce transito della merce, tanto più suscettibile di generare economie di scala in relazione a flussi di traffico comuni, quando le stesse navi scalano in tutti i tre porti.

L'avanzamento di questo quadro nella realtà dell'Adriatico settentrionale compresa nell'area di programma della cooperazione fra Italia e Slovenia è stato perseguito da SECNET attraverso la partnership di autorità portuali ed università accompagnate da un'organizzazione internazionale con vasta esperienza nelle politiche di sviluppo delle reti trasportistiche in Europa centro-orientale. Ne è derivata anche una parallela evoluzione della consapevolezza di tutti i protagonisti dell'economia marittima dei territori coinvolti e della loro stessa società civile.



4.

Presentazione dei Partner

Autorità di Sistema Portuale
del Mare Adriatico Orientale (AdSP MAO)
www.porto.trieste.it

Iniziativa Centro Europea – Segretariato Esecutivo (INCE ES)
www.cei.int

Università di Trieste (UNITS)
www.units.it

Autorità di Sistema Portuale
del Mare Adriatico Settentrionale, Porti di Venezia e Chioggia
www.port.venice.it

Luka Koper
www.luka-kp.si

Università del Litorale (UP)
www.upr.si

Autorità di Sistema Portuale del Mare Adriatico Orientale (AdSP MAO)

Alberto Cozzi, Responsabile Progetti Europei / *acozzi@porto.trieste.it*
Fabio Rizzi, Responsabile Direzione Attività Portuali / *frizzi@porto.trieste.it*

L'Autorità di Sistema Portuale del Mare Adriatico Orientale (AdSP MAO), ai sensi della legge n. 84/1994 e modificazioni seguenti, ha compiti di "*[...] indirizzo, programmazione, coordinamento, promozione e controllo delle operazioni portuali di cui all'articolo 16, comma 1, e delle altre attività commerciali ed industriali esercitate nei porti, con poteri di regolamentazione e di ordinanza, anche in riferimento alla sicurezza rispetto a rischi di incidenti connessi a tali attività ed alle condizioni di igiene del lavoro in attuazione dell'articolo 24 [...]*" (art. 6)Si è dotata di un Piano Operativo Triennale, vero e proprio piano di investimenti attraverso il quale mette in opera strategie di rafforzamento e ammodernamento delle infrastrutture in un'ottica di sviluppo del traffico di merci e di passeggeri. Inoltre, ai sensi del D.lgs. 203/2007 riguardante la "*port security*", l'Autorità di Sistema Portuale è tenuta ad effettuare la Valutazione di Security del Porto. In più, ai sensi del Reg. (CE) 725/2004 AdSP MAO è tenuta alla redazione del Port Facility Security Assessment per ogni singolo terminal.

L'Autorità Portuale di Trieste ha curato la realizzazione e cura l'aggiornamento tecnologico dei sistemi (di cui è gestore) di video sorveglianza e di controllo accessi delle aree del demanio marittimo portuale. Nell'ambito delle proprie competenze, ha redatto la Valutazione di Security del Porto e partecipato, insieme alla Capitaneria di Porto, alla Guardia di Finanza, alla Polizia di Frontiera, all'Agenzia delle Dogane ed altre Istituzioni competenti, alla redazione del Piano di Security del Porto finalizzato all'intervento in caso di atti di interferenza illeciti.

Il progetto SECNET ha contribuito ad approfondire, all'interno dell'AdSP MAO, la conoscenza dei rischi, cui sono esposte le sue reti e basi dati e ad attenuarne le vulnerabilità. Grazie a SECNET inoltre, l'AdSP MAO ha potuto sperimentare nuovi strumenti per la difesa perimetrale e la sorveglianza delle aree portuali, tramite l'installazione di una sirena collegata al sistema di video sorveglianza e l'utilizzo di droni, dotati di diverse tipologie di sensori, che permetteranno di ottimizzare il controllo delle aree portuali.
La cooperazione transfrontaliera con i porti di Venezia e Koper consentirà ad AdSP MAO sia di potenziare la propria security, sia di aumentare la propria attrattività, in quanto gli strumenti adottati a livello transfrontaliero consentiranno una migliore comunicazione tra i tre porti, che risulterà in una migliore efficienza dei transiti di merce. La dimensione di Autorità di Sistema consentirà al Porto di Trieste di trasmettere ed applicare le conoscenze apprese nella cornice del progetto SECNET anche allo scalo di Monfalcone, inserito sotto la competenza dell'AdSP MAO con Decreto del Presidente della Repubblica n. 57 del 29 marzo 2018.

Iniziativa Centro-Europea – Segretariato Esecutivo (INCE)

Ugo Poli, project manager / poli@*cei.int*
Olga Izquierdo-Sotorrio, communication officer / *sotorrio@cei.int*
Alice Pappas, communication officer / *pappas@cei.int*

InCE (ufficialmente Central European Initiative) è un'organizzazione internazionale, il cui Segretariato Esecutivo ha sede a Trieste. Fu costituita già nel novembre 1989 e quest'anno, nel suo trentesimo anniversario, conta diciassette Stati Membri (SM), che coprono un'area geografica estesa dal Mar Baltico al Mar Nero al Mar Adriatico, che ha la sua spina dorsale nel corso del Danubio. Grazie a questa caratteristica, il Segretariato dell'InCE partecipa all'attività dei gruppi di lavoro tematici delle strategie macro-regionali europee, in particolare riguardo a trasporti, innovazione e ricerca, energia e sviluppo istituzionale. Obiettivo dell'InCE come forum regionale intergovernativo, è sostenere il processo di integrazione europea attraverso la cooperazione fra le istituzioni, ma anche fra le organizzazioni non-governative dei suoi SM, sia nell'area dello sviluppo economico, che in quello delle libertà fondamentali. Per realizzare la sua missione, come articolata su base triennale dal Piano d'Azione (www.cei.int/sites/default/files/file/PoA2018-2020) l'InCE svolge un proprio ruolo di donatore, ma sviluppa anche progetti di messa in opera delle politiche dell'UE, che sono finanziati da programmi comunitari non solo nel quadro dell'obiettivo Cooperazione Territoriale Europea della politica di coesione.
Fra i 30 progetti europei realizzati dal 2004, sia in funzione di partner che di capofila, e fra i 16 progetti in corso, molti sono dedicati al settore trasporti.

Merita ricordare nel periodo 2007 – 2013 i grandi progetti realizzati come Lead Partner quali SEETAC ed ACROSSEE (Programma South-East Europe), ADRIA A (INTERREG CBC Italy-Slovenia), CERES (7th RTD Framework Programme).

Dei sedici progetti attualmente gestiti dallo staff InCE sono dedicati al settore Trasporti tre progetti del programma di cooperazione transnazionale Central Europe (COME-IN!, CONNECT2CE, SULPiTER), uno del programma MED (SUMPORT), due progetti del programma ADRION (INTER-CONNECT, ADRIPASS), il progetto NAMIRG finanziato da DG ECHO per il Maritime Incident Response Group del Nord Adriatico, ICARUS nel INTERREG Italia – Croazia sulla sostenibilità della mobilità costiera e naturalmente SECNET nel INTERREG Italia – Slovenia. Informazioni sui progetti sono reperibili in https://www.cei.int/eu-projects

In SECNET InCE ha coordinato le attività relative alla comunicazione, assicurando la corretta circolazione delle informazioni sui risultati raggiunti attraverso la newsletter, il sito di programma e le pagine SECNET sui social. Al fine di coinvolgere attivamente i gruppi obiettivo dei portatori di interessi InCE ha curato anche la preparazione degli eventi di consultazione sulla strategia SECNET di rafforzamento della security portuale tramite sistemi ICT, che si sono svolti nei primi mesi del 2019.

Le conoscenze di SECNET possono essere trasferite agli Stati Membri dell'InCE interessati, creando occasioni di replica di attività progettuali oltre l'area di programma.

Università di Trieste
Dipartimento di Scienze Economiche, Aziendali, Matematiche e Statistiche (DEAMS)

Giuseppe Borruso, professore / *giuseppe.borruso@deams.units.it*
Grazia Graziosi, ricercatrice / *ggraziosi@units.it*

L'Università degli Studi di Trieste è attualmente costituita da 10 dipartimenti, con una popolazione studentesca di circa 18.000 unità.

In SECNET, l'Università degli Studi di Trieste ha dedicato al progetto il suo solido apporto scientifico e accademico, messo a servizio del partenariato in tutte le fasi progettuali grazie al co-finanziamento del programma INTERREG, che ne ha consentito questa specifica attività di ricerca.

UNITS ha collaborato con l'Università del Litorale nell'attività A.WP3.1.2, dedicata all'analisi delle migliori pratiche a livello transfrontaliero, europeo e internazionale in merito alla security portuale ed ha coordinato la stesura del piano d'azione transfrontaliero per il rafforzamento della security portuale tramite l'uso di ICT e la sessione formativa, curata dall'Autorità Portuale di Venezia.

UNITS ha anche assistito l'Autorità Portuale di Trieste nella realizzazione delle sue azioni pilota ed ha elaborato la strategia transfrontaliera per il rafforzamento della security portuale tramite strumenti ICT, basata sui risultati del progetto.

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

James Orlandi & Valentina Zambetti, Area Ricerca e Sviluppo Progetti
james.orlandi@port.venice.it
valentina.zambetti@gmail.com

Andrea Rossi & Christian D'Antiga, Direzione Coordinamento Operativo Portuale
andrea.rossi@port.venice.it
christian.dantiga@port.venice.it

L'Autorità di Sistema Portuale del Mare Adriatico Settentrionale (AdSP MAS) è un ente pubblico non economico, istituito per effetto del D. Lgs. 4 agosto 2016 n. 169, che comprende i porti di Venezia e Chioggia. Si tratta di un unico sistema per il Porto Laguna di Venezia, cioè un unico contesto geografico, ambientale, sociale ed economico: un sistema di due porti per servire in modo complementare, ognuno con le proprie caratteristiche e specificità, un mercato di fatto coincidente.

Compito del sistema è indirizzare, programmare, coordinare, promuovere e controllare le operazioni portuali. Svolge la manutenzione delle parti comuni, mantiene i fondali, sorveglia la fornitura dei servizi di interesse generale, amministra in via esclusiva le aree e i beni demaniali, pianifica lo sviluppo del territorio portuale.

Inoltre coordina le attivita amministrative esercitate dagli enti pubblici nell'ambito portuale e promuove forme di raccordo con i sistemi logistici retro portuali e interportuali. Per aumentare i traffici del Porto di Venezia, AdSP MAS valuta il contesto economico internazionale, il bacino di influenza attuale e potenziale e lo stato dell'infrastruttura portuale. La sua azione e integrata con gli strumenti di pianificazione e gli indirizzi delle altre istituzioni pubbliche, dall'Unione Europea agli Enti locali.

Nell'ambito di SECNET, l'Autorità di Sistema Portuale del Mare Adriatico Settentrionale (avanti, AdSP MAS) ha accresciuto le proprie competenze grazie alla sessione formativa transfrontaliera ed ha contribuito alla stesura del piano d'azione congiunto(A.WP3.1.3) che è stato testato, in collaborazione con gli altri porti partner di progetto, nell'ambito delle due azioni pilota. In particolare, AdSP MAS ha sviluppato l'azione pilota relativa alla cyber security, nell'ambito della quale ha svolto uno studio per la messa in sicurezza della rete interna da attacchi informatici (A.WP3.1.4). Inoltre, AdSP MAS ha svolto delle analisi specifiche e sviluppo di applicazioni volte a ottimizzare il proprio Port Community System in merito alla security portuale e alla raccolta dei relativi dati, oltre a potenziare il proprio sistema di video sorveglianza (A.WP3.1.5). Infine, AdSP MAS ha coordinato il WP 3.2 e contribuito alla redazione del Protocollo congiunto con il quale si è impegnato, assieme agli altri porti, ad applicare la strategia transfrontaliera sviluppata sulla base dei risultati del progetto (WP 3.2).

LUKA KOPER

Roberto Richter, Senior project manager,
Department for strategic development / *roberto.richter@luka-kp.si*
Žiga Fišer, Head of Department for strategic development / *ziga.fiser@luka-kp.si*

Nell'ambito del progetto SECNET, LK ha coordinato il WP3.1, grazie anche alla sessione formativa transfrontaliera del quale ha accresciuto le proprie competenze, contribuendo inoltre alla stesura del Piano d'azione congiunto (A.WP3.1.3). Per le sue attività pilota LK ha effettuato un'analisi sulla messa in sicurezza della sua rete informatica al fine di impedire attacchi informatici al proprio sistema (A.WP3.1.4) ed ha aggiornato il proprio Port Community System per soddisfare i massimi standard in merito alla security portuale e alla raccolta dei relativi dati. Sulla base dei riscontri ottenuti dai cosiddetti test di penetrazione, sono stati poi svolti ulteriori test del sistema, per verificare la sua vulnerabilità dopo l'installazione degli aggiornamenti e l'attuazione delle misure di sicurezza aggiornate.

In aggiunta al lavoro svolto sul sistema informatico, le azioni pilota sono servite a LK anche per ampliare il proprio sistema fisico di sicurezza, intervenendo sulle attrezzature dedicate alla video-sorveglianza con l'approvvigionamento di sensori perimetrali per il controllo visivo e termico di mezzi stradali e ferroviari (A.WP3.1.5), prevenendo gli accessi non autorizzati.
Con l'aggiornamento del sistema radar, si sono ampliate anche le capacita di visione notturna del perimetro fornendo una nitidezza delle immagini per distanze anche superiori ad 1 km.

Infine, LK ha contribuito alla redazione del Protocollo congiunto con il quale si impegnerà, assieme agli altri porti, ad applicare la strategia transfrontaliera sviluppata sulla base dei risultati del progetto (WP 3.2). Con Il proprio budget LK ha inoltre coperto anche costi di personale interno per l'esecuzione delle attività di progetto, per il personale esterno dedito al supporto del Comitato di Pilotaggio (WP1), per le attività di comunicazione o dedicato alla promozione dei risultati ottenuti con SECNET (WP2), nonché per la realizzazione dell'azione pilota (WP 3.1) e per un contributo all'elaborazione della strategia transfrontaliera (WP 3.2).

A marzo 2019, le attività di SECNET sono state presentate anche ai soggetti interessati, con la visione dei risultati ottenuti e delle migliorie apportate alla sicurezza nell'area portuale e zone limitrofe.

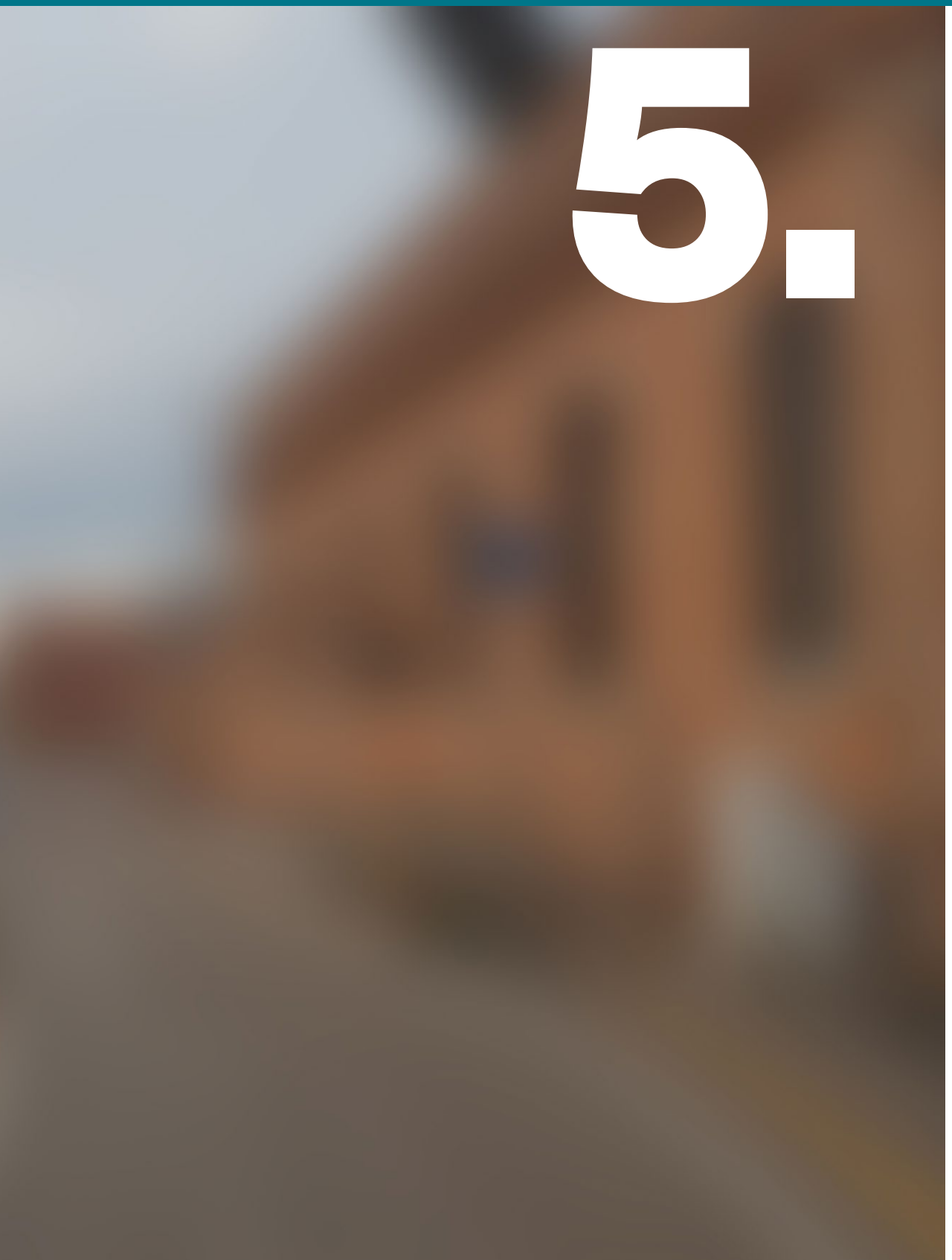
Università del Litorale - Univerza na Primorskem (UP)

Dejan Paliska, professor, project manager / *dejan.paliska1@gmail.com*
Ana Allegra, senior financial manager / *Ana.Allegra@fts.upr.si*

L'Università del Litorale (Univerza na Primorskem - UP) è un'università pubblica slovena con sede a Capodistria. UP ha undici componenti, comprese sette facoltà e due centri di ricerche. L'Università del Litorale ha molteplici esperienze in progetti europei: va ricordato in particolare il progetto SAFEPORT nell'ambito del quale ha sviluppato un sistema mobile per il controllo dell'inquinamento dell'aria LIDAR (Light Detection And Ranging), in stretta cooperazione con il Porto di Capodistria.

In SECNET l'Università del Litorale ha dato al progetto un solido apporto scientifico e accademico, messo a servizio del partenariato in tutte le fasi progettuali. Il suo budget ha consentito di finanziare per lo più spese di personale interno (professori, ricercatori, ecc.), che hanno dedicato le proprie competenze agli studi ed alla realizzazione delle altre attività progettuali. In particolare UP in collaborazione con l'Università di Trieste, ha coordinato l'attività A.WP3.1.2, dedicata all'analisi delle migliori pratiche a livello transfrontaliero, europeo e internazionale in merito alla security portuale.

UP ha inoltre assistito Il Porto di Capodistria nella realizzazione delle sue azioni pilota e ne effettuerà la valutazione e validazione dei risultati ed ha infine collaborato alla elaborazione della strategia transfrontaliera per il rafforzamento della security portuale.



5.

Il percorso di elaborazione e le finalità della Strategia SECNET per la security portuale nella dimensione transfrontaliera di Italia e Slovenia

L'elaborazione di una **Strategia** e di un **Protocollo transfrontalieri** per il rafforzamento della security portuale realizzata nel progetto SECNET è rivolta non solo alle autorità portuali partner del progetto, ma anche agli altri porti commerciali dell'Area di Programma dell'INTERREG Italia – Slovenia 2014 – 2020 (Chioggia, Porto Nogaro e Monfalcone) ed ai principali portatori di interessi dell'economia portuale (Autorità Marittima, operatori portuali, caricatori ed enti preposti alla protezione civile e difesa ambientale).

La Strategia contiene infatti raccomandazioni per l'attuazione di misure coordinate di applicazione di tecnologie intelligenti e di procedure concordabili al fine di rendere la security portuale transfrontaliera più efficiente nel breve, medio e lungo termine. Il Protocollo alla firma dei partner di progetto in occasione della Conferenza Finale reca infatti l'impegno alla sua attuazione ed è aperto all'adesione degli altri porti commerciali ed ai relativi stakeholders.

La Strategia elaborata dalla partnership SECNET è stata al centro di **attività di coinvolgimento e condivisione con gli *stakeholder* della security portuale** attraverso l'organizzazione di tre workshop coordinati, a Trieste, Koper – Capodistria e Venezia, rivolti agli operatori portuali pubblici e privati ed alle istituzioni responsabili della sicurezza nel territorio di riferimento dei porti. Sono stati coinvolti:

- I porti commerciali dell'area di programma (Monfalcone, Porto Nogaro e Chioggia)
- Operatori portuali terminalisti
- Spedizionieri ed agenzie marittime
- Altre imprese portuali, incluse le cooperative di lavoro
- Alcune aziende, incluse PMI, particolarmente significative per l'operatività in ambito portuale e marittimo, ma anche l'industria navalmeccanica
- Tutti gli enti partecipanti al sistema di protezione civile del territorio pertinente
- Funzionari degli enti pubblici territoriali pertinenti le aree portuali

I workshop hanno avuto una forma interattiva, che ha consentito ai partecipanti di formulare non soltanto domande ed osservazioni, ma anche di presentare le proprie esperienze, bisogni e proposte sul tema della security portuale.

Nel workshop che si è svolto a **Trieste il 18 febbraio** AdSP MAO ha presentato anche le misure già in attuazione per la **security perimetrale** (installazione del sistema di allerta e sorveglianza aerea del pe-

rimetro portuale mediante droni); le procedure relative ad azioni sperimentate con SECNET in corso di inserimento nei piani di *security* e *safety* portuale; i percorsi di formazione degli operatori avviati per l'utilizzo dei droni in condizioni critiche.

Riguardo alla cyber security è stato evidenziato lo sforzo di AdSP MAO sia per corrispondere alla continua e rapida evoluzione del quadro normativo di riferimento, sia per facilitare la comunicazione alla cittadinanza su quanto accade nelle aree portuali con la progettazione di una nuova piattaforma IT sui dati relativi al movimento di merci, mezzi e persone.

Dai partecipanti alla consultazione sono emerse osservazioni e proposte riguardo a:

- la necessità che le regole per l'utilizzo di nuove strumentazioni di sorveglianza delle aree portuali siano coordinate con le Forze dell'Ordine competenti;
- la forte diversità geomorfologica dei porti partecipanti al progetto SECNET come potenziale ostacolo alla messa in opera di linee guida congiunte;
- l'esigenza di coinvolgere il livello decisionale centrale;
- le esperienze in corso in alcune imprese terminaliste del Porto di Trieste per l'*assessment* del livello di sicurezza cibernetica di impianti ed attrezzature in uso, accompagnato da *penetration test* per la rilevazione e mitigazione di eventuali criticità e vulnerabilità;
- la crucialità della sensibilizzazione e formazione dei dipendenti, poiché è generalmente condivisa l'opinione che il principale punto di debolezza sia rappresentato dagli utenti delle infrastrutture IT;
- l'istituzione di un comitato dei responsabili ICT dei vari soggetti, pubblici e privati, della comunità portuale.

Anche l'incontro che si è svolto a **Koper – Capodistria il 15 marzo** ha raccolto importanti indicazioni in materia di sicurezza del porto da parte di interlocutori dal ruolo ben definito quali i rappresentanti della polizia nazionale e locale, l'amministrazione comunale, le imprese di fornitura e manipolazione di carburanti nell'area portuale, che si sono confrontati con i responsabili della sicurezza di Luka Koper su temi come lo stato della sicurezza nell'area portuale, le nuove tecnologie di protezione, le misure di sicurezza preventiva adottate nell'area portuale contro le intrusioni, il furto di dati e quant'altro possa minacciare la sicurezza nel porto o nella città di Capodistria.

La Strategia transfrontaliera così verificata, è stata redatta sulla scorta degli studi previsti dalle attività del progetto SECNET (analisi delle buone pratiche in ambito transfrontaliero, europeo ed internazionale, sessione di formazione transfrontaliera, piano d'azione congiunto) e delle sue azioni pilota, reca un quadro delle principali sfide alla cyber security nel settore portuale mettendo in evidenza le criticità rilevabili nel presente contesto normativo e provvede raccomandazioni e linee guida per l'applicazione di soluzioni congiunte relative alla cyber security ed alla difesa perimetrale delle aree portuali.

La Strategia, pubblicata qui di seguito nella sua versione integrale, rappresenta una *road map* per i futuri interventi promuovibili dai partner di progetto, e più in generale dagli stakeholder dell'area di programma, al fine di incrementare la sicurezza fisica e cyber delle aree portuali, apportandovi un ulteriore fattore di competitività.

Il Protocollo sulla dimensione transfrontaliera della security portuale testimonia l'impegno dei firmatari a recepire e applicare le raccomandazioni della Strategia e a scambiarsi dati e procedure sulla security portuale nell'ottica di un'armonizzazione della governance transfrontaliera e di una cooperazione istituzionale permanente. I partner di progetto ne promuoveranno i contenuti anche al di fuori dell'area di programma, in particolare con il porto di Fiume, in quanto appartenente alla North Adriatic Port Association (NAPA) e con i porti dei Paesi membri dell'Iniziativa Centro Europea.

La "Strategia transfrontaliera per il rafforzamento della security portuale tramite l'uso di ICT" (Testo integrale – Deliverable 3.2.3.1)

1. Introduzione

I porti costituiscono nodi intermodali cruciali nella rete di trasporto merci e passeggeri dell'Unione Europea (UE) e, oltre ad essere importanti punti di controllo delle frontiere, svolgono un ruolo essenziale nel commercio internazionale.

Nel 2015, il valore dello scambio di merci trasportate via mare nell'UE ammontava a 1.777 miliardi di euro, pari a circa il 51 per cento degli scambi di merci nell'intera UE[1] (Eurostat, 2016). Nel 2016, i porti marittimi dell'UE-28 hanno movimentato 3,9 miliardi di tonnellate di merci via mare[2], con un leggero incremento dello 0,5 per cento rispetto al 2015, ma solo dello 0,01 per cento, rispetto al 2006. Tuttavia, dal 2009, il volume di merci trasportate via mare è cresciuto ben dell'11,4 per cento (Eurostat, 2018).

La Conferenza delle Nazioni Unite sul commercio e lo sviluppo (UNCTAD) prevede che, nel medio termine, il commercio marittimo mondiale continuerà la propria espansione, con volumi in crescita stimati ad un tasso annuale del 3,2 per cento tra il 2017 e il 2022 (UNCTAD, 2017).

I flussi di merci via mare sono in continua espansione ed il trasporto marittimo conferma la sua importanza vitale per il funzionamento della nostra società, così come per la nostra economia.

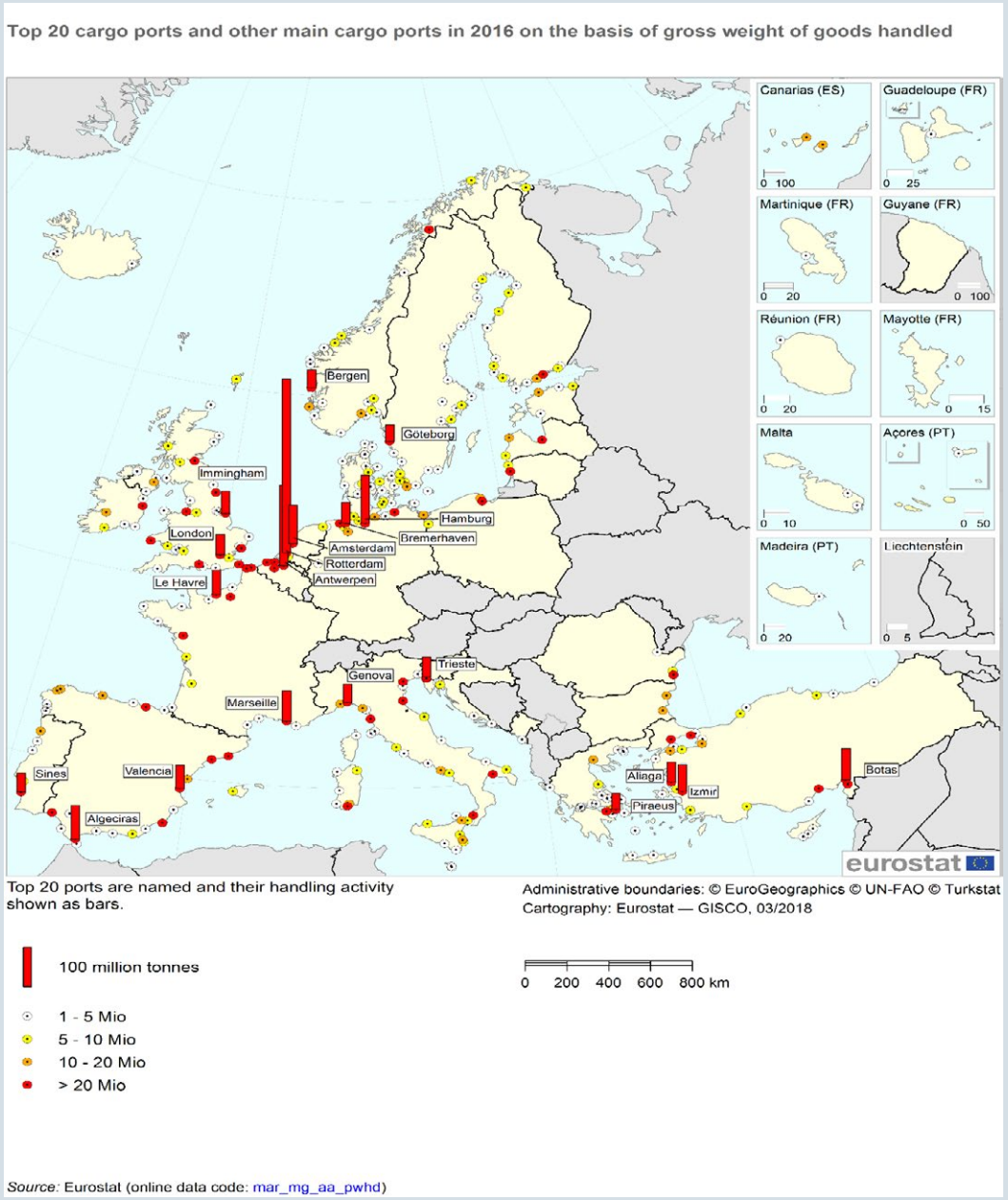
La sicurezza dei porti e la loro efficienza operativa è quindi di fondamentale importanza non solo per il trasporto marittimo, ma anche per il ruolo strategico in termini di sicurezza, a livello regionale, nazionale ed europeo. La sicurezza portuale diventa così un'opportunità per automatizzare e semplificare le procedure e le operazioni portuali (Andritsos, 2013), anche con l'utilizzo di tecnologie dell'informazione e della comunicazione (ICT). In particolare, le nuove tecnologie stanno trasformando tutte le operazioni marittime, dalla navigazione alla gestione del trasporto merci, quali le pratiche di sdoganamento, la determinazione dei tempi, le consegne, la disponibilità di stoccaggio nei magazzini, lo stivaggio a bordo delle navi, e tutta la gestione delle comunicazioni e informazioni relative alla movimentazione delle merci e delle persone, cui sono collegate notevoli quantità di dati legati a transazioni monetarie, suscettibili di attacchi informatici.Per garantire sicurezza ed efficienza nelle operazioni portuali ed un efficace controllo dei flussi di persone e merci, il presente documento individua le principali sfide della sicurezza nel settore marittimo e le linee guida per la realizzazione di una cooperazione transfrontaliera permanente, che, in termini generali, possono riassumersi nelle seguenti azioni:

1) Sensibilizzazione sull'importanza di una appropriata sicurezza nelle operazioni marittime da destinare ai principali attori del settore portuale, attraverso una adeguata, e personalizzata, formazione transfrontaliera degli addetti alla sicurezza portuale;
2) Coordinamento transfrontaliero della security portuale, che definisca regole comuni e coinvolga, oltre ai responsabili istituzionali della sicurezza, anche gli stakeholder privati;
3) Scambio di informazioni e di dati, anche attraverso la creazione di una piattaforma in cui raccogliere e condividere esperienze legate all'uso degli strumenti ICT.

1 In particolare, il 53% delle importazioni europee è entrato nell'UE via mare, mentre le spedizioni hanno rappresentato il 48% delle esportazioni dell'UE verso paesi terzi.

2 Si veda la figura 1 per un maggior dettaglio sulla movimentazione delle merci nei porti Europei nell'anno 2016.

Fig. 1. Porti Europei e movimentazione delle merci.



2. Le principali sfide della sicurezza nel settore marittimo

2.1 Il contesto normativo

L'entrata in vigore nel novembre del 2002 del *Maritime Transportation Security Act* (MTSA) ed il successivo Atto sulla *Security and Accountability For Every Port* (SAFE Port Act, 2006) hanno evidenziato ampi margini di miglioramento nel campo della sicurezza portuale, a partire dallo svolgimento di valutazioni sulla vulnerabilità delle strutture portuali allo sviluppo ed attuazione di piani di sicurezza per limitare l'accesso alle aree protette al solo personale autorizzato.

In linea con il MTSA, il Regolamento UE n. 725/2004 del Parlamento europeo e del Consiglio, relativo al miglioramento della sicurezza delle navi e degli impianti portuali, introduce misure volte a rafforzare la sicurezza dei trasporti marittimi, nazionali e internazionali, obbligando i paesi membri ad una valutazione dei rischi di sicurezza. Ad integrazione di questo documento, la direttiva 2005/65/CE del Parlamento europeo e del Consiglio indirizza i paesi membri verso l'elaborazione e l'aggiornamento di piani di sicurezza portuale che individuino, per ciascun livello di sicurezza, a) le procedure da seguire; b) le misure da attuare; c) le azioni da intraprendere.

L'analisi degli aspetti di sicurezza informatica nel settore marittimo affidata all'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) riconosce il ruolo strategico delle infrastrutture marittime, la cui protezione è necessaria per sostenere e migliorare il benessere della società europea. In particolare, la Commissione europea ha adottato una Comunicazione[3] per migliorare la protezione delle infrastrutture critiche europee da potenziali attacchi terroristici attraverso il programma europeo per la protezione delle infrastrutture critiche e la direttiva[4] sull'individuazione e la designazione delle infrastrutture critiche europee.

Gli obblighi di sicurezza per le compagnie, le navi, gli impianti portuali, i porti e i servizi di gestione del traffico navale, ai sensi degli atti giuridici dell'Unione Europea, riguardano tutte le operazioni, compresi i sistemi di radio e telecomunicazione, i sistemi informatici e le reti, che svolgono un ruolo essenziale nell'agevolare i movimenti transfrontalieri di beni, servizi e persone (Direttiva 2016/1148/UE).

Parte delle procedure obbligatorie da seguire prevede la segnalazione di tutti gli incidenti, e la Direzione Generale per la mobilità e il trasporto (DG MOVE) in collaborazione con l'Agenzia europea per la sicurezza marittima (EMSA) hanno intrapreso azioni concrete per facilitare lo scambio di dati tra le autorità marittime degli Stati membri, attraverso la piattaforma SafeSeaNet[5]. Questa piattaforma ha quale obiettivo principale quello di promuovere la raccolta, la diffusione e lo scambio armonizzato di dati marittimi, facilitando la comunicazione tra le autorità a livello locale, regionale e centrale, offrendo un sistema comunitario di monitoraggio del traffico navale e di informazione, e contribuendo così alla prevenzione di incidenti in mare.

3 COM(2006) 789 dd. 12.12.2006
4 Direttiva 2008/114/EC dd. 08.12.2008
5 Direttiva 2010/65/UE

2.2 Le sfide rilevate:

Per quanto riguarda la security fisica dei porti, le maggiori sfide sono le seguenti:

1. Funzionamento sicuro ed efficiente dei porti europei nel contesto del trasporto sostenibile.
2. Flussi di merci e passeggeri senza interruzioni.
3. La prevenzione di:
    - attacchi a strutture portuali di alto valore (infrastrutture critiche);
    - immigrazione illegale;
    - traffico di droga, armi e sostanze illecite.

In particolare, con riferimento alla normativa ISO 28001, gli scenari delle minacce da considerare nella valutazione della sicurezza sono:

1. Intrusioni e/o perdita del controllo di un bene (inclusi i trasporti) all'interno della supply chain. Ciò potrebbe danneggiare o distruggere il bene, danneggiare o distruggere il bersaglio esterno usando il bene (o le merci), causare disordini civili e/o economici, come la presa di ostaggi o l'uccisione di persone.
2. Utilizzo della catena di approvvigionamento come mezzo di contrabbando, come ad esempio il traffico di armi illegali, terroristi o altri soggetti criminali, all'interno o all'esterno del paese dato.
3. Manomissione delle informazioni: accesso locale o remoto ai sistemi informativi della catena di approvvigionamento allo scopo di interrompere le operazioni o facilitare attività illegali.
4. Integrità del carico: manomissione, sabotaggio e/o furto a scopo di terrorismo o di altri atti criminali.
5. Uso non autorizzato: sviluppo di operazioni nella catena di approvvigionamento internazionale per facilitare un incidente terroristico (ad esempio usando il mezzo di trasporto come arma).

Per quanto riguarda la cyber security, il rapporto sugli aspetti di sicurezza informatica nel settore marittimo (ENISA, 2011) identifica le aree problematiche di sicurezza informatica nel contesto portuale, che possono essere così riassunte:

1. *Scarsa consapevolezza / attenzione verso la sicurezza informatica marittima* che si traduce in una inadeguata preparazione a fronteggiare rischi informatici. Di conseguenza, gli effetti di un potenziale attacco informatico verso i sistemi ICT portuali potrebbero creare danni maggiori rispetto ad altri settori in cui il personale è preparato nel rispondere ad eventi di questo tipo.
2. *Complessità dei sistemi ICT nel contesto marittimo* che includono anche elementi molto specifici, il cui rapido sviluppo tecnologico ha, in alcuni casi, ridotto l'attenzione sulla loro vulnerabilità. Un esempio rilevante è il numero sempre crescente di infrastrutture portuali che utilizzano sistemi ICT, ad esempio dispositivi SCADA[6], connessi a Internet senza l'impiego di reti protette. Le vulnerabilità create da queste lacune nella sicurezza dei sistemi ICT possono influire non solo sui servizi supportati da questi sistemi, ma anche su quelli comunemente condivisi quali database, sistemi che ospitano informazioni sensibili, ecc.. Inoltre, è stato notato che non esiste una standardizzazione delle buone pratiche per garantire un'adeguata protezione dei sistemi ICT. Le linee guida in materia di sicurezza sono spesso riferite solo a misure di base e non trovano corrispondenza nella complessità degli strumenti ICT o non coprono tutta la tecnologia pertinente.
3. *Frammentazione delle autorità marittime*: esistono diversi livelli di governance nel settore marittimo rispetto ai temi di sicurezza informatica e rischi connessi. Tra questi ritroviamo alcune organizzazioni intergovernative quali l'Organizzazione marittima internazionale (IMO), l'Organizzazione mondiale delle dogane (OMD), l'Ufficio marittimo internazionale (IMB) e l'International Maritime Security Corporation (IMSC). La mancanza di un coordinamento tra queste organizzazioni e quelle esistenti a livello europeo e nazionale comporta disarmonia nell'affrontare la sicurezza marittima. Inoltre, la frammentazione delle politiche marittime nei paesi membri rende difficile definire le responsabilità ed i ruoli in materia di sicurezza informatica. Infine, la crescente privatizzazione, seppur parziale, di alcuni porti europei solleva diverse preoccupazioni in merito alle linee guida seguite nell'ambito della sicurezza marittima che potrebbero non coincidere con quelle previste in Europa, ma dipendere principalmente dal loro titolare proprietario e dal suo livello di maturità nell'affrontare le tematiche sulla sicurezza informatica. È evidente quindi la necessità di un approccio globale e di un'interazione costruttiva tra il governo degli Stati membri e le autorità marittime.
4. *Bassa considerazione della sicurezza informatica nella regolamentazione marittima*: l'attuale contesto normativo pone molta attenzione verso la sicurezza (*safety*) e la sicurezza fisica (*physical security*) delle aree portuali, come ad esempio il codice internazione per la sicurezza delle navi e degli impianti (ISPS), ma tralascia quasi del tutto l'aspetto della sicurezza informatica e della prevenzione di possibili attacchi informatici tramite atti illeciti.
5. *Assenza di un approccio unitario verso i rischi informatici*: le autorità marittime stanno gestendo la sicurezza informatica considerando solo una parte dei rischi effettivi, come l'interruzione di telecomunicazioni o la divulgazione di informazioni relative ai carichi merci, trascurando tutti gli aspetti rilevanti della protezione dell'infrastruttura marittima critica (Critical Information Infrastructure Protection – CIIP) per l'identificazione delle misure necessarie a prevenire e gestire tutte le tipologie di incidenti informatici.
6. *Carenza di incentivi economici per la realizzazione della sicurezza informatica*, anche a causa di un quadro normativo frammentario ed insufficiente nell'affrontare questi temi e nell'indicare le linee guida da seguire.
7. *Necessità di iniziative volte alla collaborazione, allo scambio di informazioni e alla condivisione di esperienze* tra gli attori interessati. Si segnalano poche e scarse iniziative collaborative; tra queste, l'iniziativa Port ISAC[7] (Information Sharing and Analysis Center) mira a stabilire una collaborazione tra soggetti pubblici e privati per favorire lo scambio di informazioni, opinioni ed esperienze su questioni di sicurezza informatica e buone pratiche.

6 L'acronimo SCADA, dall'inglese Supervisory Control And Data Acquisition, si riferisce a software di controllo di supervisione e acquisizione dati.

7 Per ulteriori informazioni sull'iniziativa ISAC si veda http://www.cpni.nl/informatieknooppunt/werkwijze-isacs

3. Il coordinamento transfrontaliero per il rafforzamento della security portuale

Date le criticità rilevate nella precedente sezione, la strategia transfrontaliera per il rafforzamento della security portuale con l'utilizzo degli strumenti ICT mira ad implementare le iniziative elencate di seguito.

1) *Tavolo permanente per la condivisione di buone pratiche, per l'attuazione di iniziative di sensibilizzazione sull'importanza di una adeguata sicurezza nelle operazioni marittime* da destinare ai principali attori del settore portuale. È opportuno provvedere alla stesura di linee guida per pianificare, organizzare e gestire iniziative volte ad aumentare la consapevolezza verso gli strumenti più congrui per proteggere tutte le operazioni marittime da potenziali attacchi. L'insieme dettagliato delle buone pratiche e delle linee guida deve garantire la *sicurezza di progettazione* per tutte le componenti critiche del sistema marittimo, attraverso un approccio basato sul rischio, al fine di comprendere la complessità dell'ambiente marittimo e della necessità di una cooperazione transfrontaliera.

2) *Formazione continua sulla sicurezza portuale*. Oltre ad una mirata campagna di sensibilizzazione, gli operatori marittimi devono ricevere *adeguata e personalizzata formazione* sugli aspetti specifici della sicurezza Queste azioni aumenterebbero l'esperienza complessiva del settore, inclusa la *cyber security*, anche utilizzando precedenti ed analoghe esperienze di altri settori, quali a titolo esemplificativo quello delle telecomunicazioni, dell'energia, della finanza, e così via. Ciò andrà in particolare focalizzato sulla *Valutazione dei rischi informatici esistenti associati all'attuale implementazione dei sistemi ICT*, nonché l'identificazione di tutte le attività critiche all'interno del settore marittimo, che comprendono la valutazione dei servizi e dei beni marittimi critici, le minacce che affrontano, la loro esposizione al rischio e l'attuazione di esercizi di preparazione sulla gestione del rischio. È necessario, quindi, uno sforzo congiunto tra fornitori di ICT marittime, operatori marittimi, autorità portuali e responsabili delle politiche al fine di mappare, riconoscere e gestire i rischi effettivi, in linea con i loro obiettivi di business e il contesto normativo.

3) *Sviluppo di un Sistema di Supporto alle Decisioni Spaziali (SDSS)*. Viene raccomandata la realizzazione di un Sistema di Supporto alle Decisioni Spaziali, finalizzato alle problematiche di sicurezza, ma scalabile, in aggiornamenti successivi, alla gestione dei diversi aspetti legati alla portualità. All'interno di tale sistema andranno integrate le componenti informatiche, banche dati digitali, in particolar modo geografiche, sistemi di sorveglianza e visualizzazione (immagini 3D, videocamere, riprese da droni in real time, immagini aeree e satellitari) al fine di disporre di uno strumento agile di supporto alle decisioni in termini di sicurezza portuale.

   Per promuovere e facilitare la comunicazione sulla sicurezza, inclusa quella informatica, e migliorare lo scambio di informazioni e statistiche tra le autorità portuali e gli attori marittimi interessati, si procederà con la creazione di una apposita *piattaforma*, come ad esempio quelle realizzate dal CPNI (Centre for the Protection of National Information Infrastructure[8]). Tali reti possono rivelarsi fondamentali nell'aiutare a identificare le minacce informatiche presenti e future. Lo sviluppo degli ISAC richiede però l'identificazione delle parti interessate rilevanti dei settori pubblico e privato e l'instaurazione di una relazione di fiducia tra questi soggetti.

4) *Istituzione di un Centro di Coordinamento Transfrontaliero per la Security Portuale (CCTSP)*[9]. Il Centro sarà costituito da un gruppo di lavoro specializzato che sviluppi una serie dettagliata di linee guida sulla sicurezza e buone pratiche per lo sviluppo tecnologico e l'implementazione dei sistemi ICT nel settore marittimo. Questo gruppo di lavoro dovrebbe includere non solo le principali autorità degli Stati membri coinvolte nel settore marittimo, ma anche i rappresentanti delle principali autorità portuali, le compagnie di navigazione, i fornitori di infrastrutture a marittime, nonché le strutture di ricerca (infrastrutture di telecomunicazione, hardware ICT e software, SCADA, università ed enti di ricerca, ecc.). Il *Centro* si occuperà della messa a sistema dei punti precedenti e della possibile *creazione di partenariati tra pubblico-privato* nel settore marittimo (ad esempio compagnie di navigazione, autorità portuali, ecc.) e parti interessate collegate (ad esempio compagnie o intermediari di assicurazione) al fine di incentivare l'adozione di misure di sicurezza, eliminando la barriera della mancanza di consapevolezza sui rischi, inclusi quelli cibernetici. Inoltre, un migliore scambio di informazioni e statistiche sulla sicurezza informatica può aiutare gli assicuratori a migliorare i loro modelli attuariali, ridurre i propri rischi e quindi offrire migliori condizioni di assicurazione contrattuale agli operatori marittimi coinvolti. Questo è un esempio di come una maggiore cooperazione e una migliore sicurezza, compresa quella informatica, possano aumentare i benefici economici di tutte le parti interessate.

5) *Realizzazione di esercitazioni congiunte e partecipazioni incrociate ad esercitazioni locali sia di security perimetrale sia informatica*. Tali attività, da pianificare con un orizzonte temporale di medio e lungo periodo, consentiranno al contempo di testare sul campo le criticità locali e uno scambio di esperienze a livello transfrontaliero, attivando un circolo virtuoso di accrescimento delle competenze e rafforzamento della security portuale.

6) *Partecipazione congiunta a progetti co-finanziati*. Per proseguire la cooperazione transfrontaliera nell'ambito della security portuale, è possibile attingere a molteplici fonti di finanziamento europee, sia nell'attuale sia nella prossima programmazione comunitaria (2021-2027)

4. Conclusioni

L'Unione Europea è fortemente dipendente dai porti marittimi che regolano gli scambi di merci e persone nel mercato interno e al di fuori dell'Unione. Il 74% delle merci importate ed esportate e il 37% degli scambi all'interno dell'Unione (European Commission, 2013) transitano nei porti marittimi, i quali garantiscono la continuità territoriale dell'Unione e il collegamento delle aree periferiche e insulari, grazie anche al traffico marittimo locale. I porti europei inoltre permettono il transito annuale a 400 milioni di passeggeri e generano lavoro per ben 1,5 milioni di lavoratori impiegati (European Commission, 2015).

La sfida principale per i sistemi di sicurezza portuali è coniugare operazioni portuali sicure e controllo efficiente delle frontiere; in altre parole, per fornire una sicurezza avanzata, senza penalizzazioni in termini di costi, si deve:

8 Per maggiori informazioni si veda www.cpni.nl

9 Nelle more di istituzione e per una durata massima di 18 mesi fanno parte del CCTSP i rappresentanti dei partner di progetto SECNET.

- affrontare la gestione della sicurezza come parte della gestione strategica del porto;
- integrare soluzioni di sicurezza nei processi operativi con maggiore automazione nel monitoraggio e nel coordinamento delle attività;
- sostenere lo sviluppo delle competenze in materia di sicurezza nei porti e sfruttare la capacità delle loro organizzazioni che collaborano;
- promuovere una collaborazione efficiente tra tutte le parti interessate coinvolte nella sicurezza portuale a livello regionale, nazionale ed europeo.

Maggiore sicurezza significa ridotta probabilità di incidente grave, migliore controllo degli accessi, protezione delle reti informatiche, tempestività del rilevamento delle minacce più efficiente e maggiore resilienza.

Maggiore resilienza significa basso impatto di interruzione e rapido recupero alle normali operazioni, perservando la competitività dei porti.

Definizioni:

Sicurezza marittima: la combinazione di misure preventive volte a proteggere la navigazione e gli impianti portuali dalle minacce di atti illeciti intenzionali.

Sicurezza informatica: la capacità di una rete o di un sistema di informazione di resistere, a un dato livello di fiducia, a eventi accidentali o azioni dannose che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati archiviati o trasmessi e dei relativi servizi offerti o accessibili tramite tali reti e sistemi informativi.

Rischio cyber: qualsiasi rischio legato a perdite finanziarie, turbative o danni all'immagine di un'organizzazione derivante da un'avaria nei suoi sistemi informatici (Institute of Risk Management).

Bibliografia

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

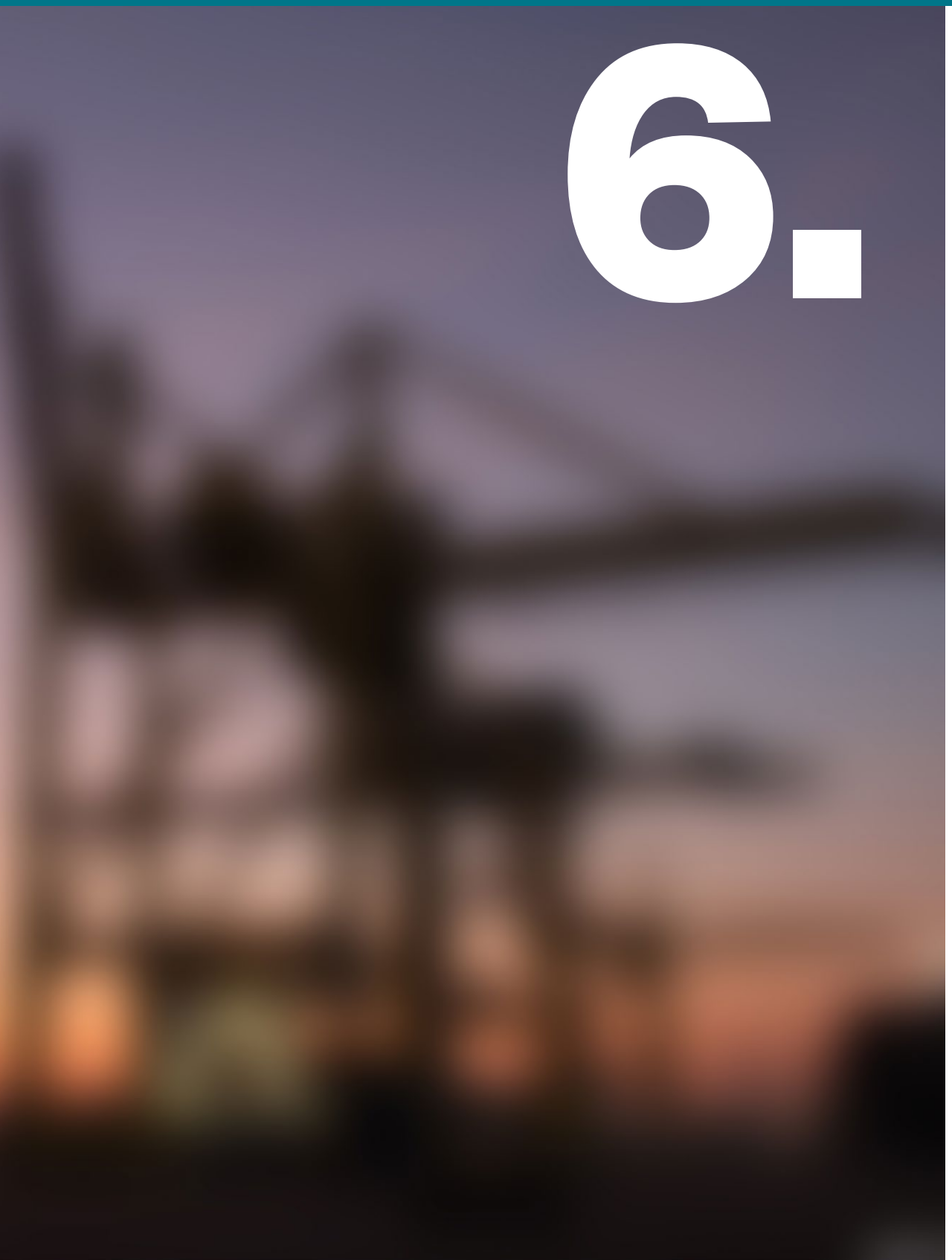
European Commission (2015). Exchange of views between ports CEOs and Transport Commissioner Bulc. *https://ec.europa.eu/transport/modes/maritime/ports/ports_en*

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.

ALLEGATI

6.1 Studio delle best practices nei sistemi ICT utilizzati per la security portuale (Sintesi dei rapporti sulle migliori pratiche locali ed internazionali - Deliverables ex 3.1.2)

6.2 Training transfrontaliero SECNET – Venezia 28 febbraio 2018 (Rapporto sintetico - Deliverable 3.1.3.2)

6.3 Azioni pilota di cyber security e di security fisica nei porti di Koper – Capodistria, Trieste, e Venezia (Schede sintetiche - Deliverables ex 3.1.4 e 3.1.5.)

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

Allegato 6.1

Studio delle *best practices* nei sistemi ICT utilizzati per la security portuale

(Sintesi dei rapporti sulle migliori pratiche locali ed internazionali - Deliverables ex 3.1.2)

Nel quadro del WP 3.1 dedicato allo sviluppo di "Security portuale transfrontaliera intelligente" l'Università del Litorale di Capodistria / Koper ha realizzato, fra la fine del 2017 ed i primi mesi del 2018, un ampio studio sulle buone pratiche in termini di sistemi fisici e digitali utilizzati per la security portuale a livello locale e transfrontaliero (D.3.1.2.2) ed a livello europeo e internazionale (D.3.1.2.3). Autori della ricerca sono i proff. Dejan Paliska , Daša Fabjan, Peter Kopič, Ana Allegra, Julija Švagelj Mežnar con Klara Dodič Pegan ed Asta Domian dell'Università del Litorale.

L'obiettivo principale della ricerca è stato conoscere le buone prassi nell'ambito della sicurezza fisica e cibernetica del porto, come anche lo scambio delle buone prassi identificate. Le buone prassi identificate, che si sono dimostrate efficaci nell'aumento della sicurezza fisica e cibernetica dei porti, sono presentate comparativamente con riferimento alla possibilità di implementazione nei tre porti partner del progetto SECNET.

La ricerca si basa su una vasta panoramica ed un'analisi di fonti accessibili in rete, interviste con i rappresentanti dei porti e somministrazione di due questionari a porti europei. I risultati permettono di acquisire un quadro generale sullo stato attuale nell'ambito della sicurezza fisica e cibernetica dei porti e di comparare le buone prassi di porti europei moderni con quelle dei porti di Capodistria, Trieste e Venezia. Nel primo questionario sono stati ricompresi l'aspetto organizzativo della sicurezza fisica dei porti in diversi paesi, le tipologie di minacce effettivamente intervenute nei cinque anni precedenti e le misure, che i singoli porti hanno introdotto in seguito a tali eventi. Con il questionario sulla sicurezza cibernetica la ricerca si è concentrata invece sulla raccolta di informazioni relative alla concezione procedurale ed organizzativa della sicurezza cibernetica e sulle soluzioni tecniche e tecnologiche per il suo miglioramento.

Nonostante l'auspicio di un'adesione maggiore (al questionario sulla sicurezza fisica hanno risposto otto porti estranei al progetto SECNET, a quello sulla cyber security, invece, sette), hanno risposto alcuni dei più importanti porti europei, tanto per volumi dei trasbordi quanto per attrezzature tecnologiche ovvero Valencia, Barcellona, Anversa, Ravenna, Ancona, Costanza, Burgas e Varna.

E' opportuno ricordare che le informazioni sui rischi in materia di sicurezza ed attrezzature tecniche dei porti possono essere dati sensibili.

Il questionario sulla sicurezza fisica è stato dedicato alla raccolta di informazioni su incidenti e buone prassi in materia di sicurezza dei porti. E' composto da tre sezioni di domande: la parte introduttiva è dedicata alla raccolta dei dati generali sul porto, nella seconda parte vi sono domande su tecnologie e sistemi utilizzati nei porti e comprende l'informazione sui rischi potenziali e sugli incidenti accaduti negli ultimi cinque anni.

L'ultima parte del questionario è dedicata alla raccolta di informazioni sulle buone prassi nel settore della sicurezza degli impianti portuali.

Le aree di tutti porti, inclusi nella ricerca, sono risultate essere recintate con reti o muri; nella maggior parte dei casi sono dotate di videocamere, torrette e illuminazione. Spesso sono allestite anche con sensori di movimento, meno spesso con sensori ad infrarossi e camere termiche. Tra i porti intervistati quello meglio attrezzato è il porto di Anversa che, oltre alle camere termiche alle entrate al porto, ha anche telecamere per il riconoscimento delle targhe automobilistiche (ANPR, *Automatic Number Plate Recognition*). I porti inclusi nel progetto hanno attrezzature simili agli altri porti che hanno compilato il questionario e non vi sono grandi differenze nelle attrezzature di sicurezza dell'area del porto.

Tutti i porti utilizzano almeno un sistema di riconoscimento personale per chi entra nell'area portuale. La maggior parte dei porti utilizza solo carte ID - badge di riconoscimento personale - altri, invece, utilizzano due o più sistemi. I porti di Barcellona e di Anversa utilizzano anche lettori biometrici.

I porti adottano diversi approcci per il controllo di carichi, veicoli, navi e infrastrutture. Il porto di Barcellona dispone a tal fine personale e un gruppo di cani opportunamente addestrati per la ricerca di sostanze stupefacenti o esplosivi (K9 team). Altri porti, come ad esempio Anversa e Costanza, utilizzano principalmente sistemi tecnici.

Come per l'attrezzatura per il controllo di merci, veicoli, navi e infrastrutture anche l'allestimento ed i sistemi per misure rapide di contrasto dipendono da caratteristiche specifiche di ogni porto. Oltre ai propri servizi di sicurezza, i porti possono contare anche su altri servizi nazionali di soccorso, che sono dotati di attrezzature proprie. Per tale motivo l'attrezzatura dei porti dipende dal livello di organizzazione dei servizi a livello nazionale e regionale. Di solito i porti sono dotati di veicoli di pronto intervento e antincendio.

Tutti i porti, cui è stato somministrato il questionario, corrono rischi per la sicurezza molto simili. I più frequenti sono connessi con il traffico di persone e clandestini. Tra i rischi più frequenti vi sono anche furti e rapine, atti vandalici ed altre infrazioni, violazione della legislazione commerciale e contrabbando di merci vietate o legalmente regolamentate. Un porto ha riferito anche di violazioni dello spazio aereo ovvero di sorvoli non autorizzati dell'area portuale con un drone.

La ricerca ha messo in luce che il vincolo maggiore nell'implementazione delle nuove tecnologie e di sistemi per la sicurezza fisica delle aree portuali è la disponibilità dei fondi finanziari necessari. Le tecnologie ed i sistemi più moderni (ad esempio scansione di veicoli, container e persone) sono estremamente costosi e possono permetterseli solo i porti più grandi. Alcuni porti hanno messo in luce anche difficoltà relative alla loro delimitazione territoriale (ad esempio il porto di Anversa è un porto "aperto" che non può essere recintato in tutto il suo perimetro e non è possibile fare controlli all'accesso), al personale (non è possibile assumere il personale necessario o mancano profili professionali specializzati), a complessità tecniche (implementazione di nuove tecnologie nell'area portuale, ma impossibilità di controllare ogni singolo container) ed ancora ai controlli di sicurezza dei dipendenti e dei dipendenti di società che collaborano con il porto (ad esempio i conducenti di camion). Nonostante le difficoltà, tutti i porti stanno migliorando costantemente i propri sistemi e le tecnologie di sicurezza e controllo.

Sono state identificate alcune buone prassi nell'ambito della sicurezza portuale poiché in generale i porti dedichino molta attenzione al sistema di riconoscimento precoce dei rischi per la sicurezza. Sistemi di video sorveglianza intelligenti, riconoscimenti delle targhe, identificazione ai punti di accesso e sistema di allerta sono quelli più diffusi. Molto impegno è rivolto anche alla connessione di sistemi diversi con un centro di controllo unificato e con sistemi di comunicazione di emergenza. I porti con terminal passeggeri dedicano ulteriore attenzione al controllo degli accessi e all'individuazione di contrabbandieri di sostanze stupefacenti o armi.

Il porto di Anversa, tra tutti i porti che hanno partecipato al questionario, è quello più avanzato dal punto di vista tecnologico e meglio organizzato nell'ambito della sicurezza portuale. Nel 2012 ha cooperato nella redazione del manuale europeo (DG MOVE) per l'addestramento e le esercitazioni nell'ambito della sicurezza marittima[10]. Il manuale tratta tutti gli aspetti dell'addestramento e dell'esercitazione dal punto di vita pratico e teorico e comprende tutte le esperienze ed il know-how acquisiti nel tempo. I porti partner di SECNET hanno utilizzato il manuale per la pianificazione e l'attuazione dei progetti pilota.

Una prassi simile è in uso anche in altri grandi porti, come ad esempio nel Port of Long Beach, che realizza la propria strategia di sicurezza basandosi sull'implementazione del GIS (sistema informativo geografico), collegandosi con le camere di sorveglianza ed offrendo un controllo totale dell'area portuale in tempo reale con possibilità di accertamento immediato degli incidenti, nonché con l'attuazione costante e periodica di esercitazioni di salvataggio e prevenzione dei rischi, a cui partecipano tutti i membri della comunità portuale (servizio di sicurezza del porto, subacquei, polizia, vigili del fuoco, ecc.)[11] .

Ma una importante buona prassi è anche l'informazione e la promozione della consapevolezza dei rischi, già con la stampa di brochure sul tema della sicurezza da consegnare ai dipendenti del porto ed ai conducenti dei mezzi pesanti, che entrano nell'area portuale.

La ricerca sulla cyber security per la protezione dei sistemi portuali ICT è stata suddivisa fra una prima parte di informazione sull'organizzazione della sicurezza cibernetica e sulle procedure per aumentarla; una seconda parte sulle informazioni relative a strumenti e soluzioni tecnici ed un'ultima parte dedicata alle buone prassi di cyber security.

Tra i porti a cui sono stati somministrati i questionari solo Livorno e Valencia posseggono il certificato ISO/IEC 27001, che qualifica la gestione e la protezione delle informazioni. Il porto di Valencia è anche certificato ISO/IEC 28000, che non tratta specificamente la cyber security nella catena di approvvigionamento marittimo, ma definisce in generale la metodologia di valutazione dei rischi alla sicurezza. Valencia è anche l'unico porto, che richiede l'adempimento degli standard ISO/IEC 27001 ed il rispetto della politica di sicurezza nello scambio ed archiviazione delle informazioni anche alle aziende private (trasportatori, spedizionieri, agenti, ecc.). Anche i porti di Varna e Burgas richiedono adempimenti simili dai propri partner, mentre i porti di Livorno e Ravenna esigono dalle aziende di dotarsi di una politica di sicurezza simile, anche se non necessariamente uguale, alla loro. Il porto di Barcellona riferisce di non utilizzare attualmente alcuna politica di sicurezza per lo svolgimento delle attività dei propri partner.

Sono diversi i livelli di consapevolezza nei confronti dei rischi cibernetici e la comprensione dell'importanza della sicurezza cibernetica nella gestione e nelle procedure attuate dai porti. La maggior parte dei porti intervistati si è dotata di un piano di sicurezza cibernetica, accessibile a tutti i dipendenti e regolamenta le responsabilità e gli obblighi dei singoli. Nei porti di Valencia, Varna, Burgas e Capodistria sono state introdotte anche procedure comportamentali in caso di incidenti cibernetici, che comprendono il riconoscimento dei tentativi di intrusione nel sistema e la trasmissione di allarme al team, disponibile 24 ore su 24, 7 gg su 7. Ma solo due porti (Capodistria e Burgas) analizzano gli attacchi in modo sistematico. I dati raccolti indicano che nemmeno la metà dei porti intervistati svolge regolarmente una valutazione dei rischi per la sicurezza cibernetica. Solo pochi porti includono i fornitori di software e hardware nella valutazione della sicurezza. I test di intrusione al sistema vengono svolti regolarmente solo nei due porti spagnoli, a Varna ed a Capodistria.

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

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

I questionari rivelano che i porti con in organigramma un agente di sicurezza del porto (PSO) per la cyber security hanno anche un approccio più attivo ed integrato alla sicurezza in questo settore. Tanto il porto di Capodistria quanto quello di Barcellona sono gli unici fra i rispondenti, che attuavano programmi di formazione regolare in cyber security per i dipendenti e che organizzano regolarmente esercitazioni. La nomina di un comitato di sicurezza (PSC) non ha impatti significativi sull'attività connessa con la sicurezza cibernetica.

In base ai risultati del questionario è stato possibile osservare che tutti i porti utilizzano programmi antivirus, firewall e hanno una rete WI-FI per gli ospiti separata da quella dedicata ai dipendenti. La maggior parte dei porti ha la rete interna segmentata e utilizza sistemi di rilevamento (IDS) e di prevenzione delle intrusioni (IPS).

Oltre alle misure tecniche, nel garantire la sicurezza cibernetica è importante considerare anche singole misure di protezione, con le quali i porti riducono i rischi, limitano i danni di un attacco andato a buon fine e permettono un rapido ripristino del sistema. In tale contesto tutti i porti intervistati producono copie di sicurezza dei dati, aggiornano regolarmente i sistemi di sicurezza e implementano l'upgrade dei software.

Nell'ambito della sensibilizzazione e della formazione dei dipendenti, la maggior parte degli intervistati ha dichiarato che l'informazione e la formazione del personale in merito alle possibili conseguenze di un attacco cibernetico siamo molto importanti. Lo stesso vale anche per la sensibilizzazione del personale sui possibili pericoli nell'utilizzo di PC portatili al di fuori degli spazi aziendali, nei quali vengono conservati dati sensibili. I porti, però, valutano in modo diverso l'affermazione che tutti i dipendenti debbano assolvere un corso di formazione per la cyber security.

La creazione di organi deputati alla sicurezza cibernetica influisce positivamente sul rafforzamento della cyber security. E' stato, inoltre, accertato che i porti che hanno nell'organigramma un agente di sicurezza del porto (PSO) deputato alla cyber security, hanno anche un approccio più attivo ed integrato a questo problema.

In generale però il fattore umano e l'"igiene" cibernetica" vengono spesso trascurati o messi da parte, prediligendo investimenti nell'attrezzatura tecnica. Le autorità portuali israeliane relazionano su buone prassi in tale ambito. Ogni tre mesi inviano un'e-mail ai dipendenti con la promessa di un premio in denaro o un viaggio in regalo. Se i dipendenti cliccano sul link che appare, vengono reindirizzati sulla pagina web, sulla quale viene specificato che si tratta di una verifica del rispetto delle norme sulla sicurezza. I dipendenti sono, poi, pregati di rileggere le norme sulla cyber sicurezza. In questo modo nel porto viene sensibilizzato l'aspetto della cyber sicurezza e monitorata l'efficacia delle singole misure.

I dipendenti devono essere coinvolti nella sicurezza cibernetica e devono comunicare eventuali punti vulnerabili e circostanze sospette, in caso contrario i punti deboli del sistema potrebbero essere trascurati o addirittura i cyber-hacker potrebbero sferrare un attacco per mezzo degli stessi dipendenti. Idealmente ogni dipendente dovrebbe conoscere sin dall'inizio le misure di sicurezza, poi dovrebbe essere idoneamente formato ed in seguito regolarmente addestrato. Anche ENISA (Report on "Analysis of cyber security aspects in the maritime sector", November 2011) è arrivata alle stesse conclusioni. Tra le misure a breve termine per il rafforzamento della cyber security nella sua relazione si trova anche l'aumento del livello di consapevolezza di tutti gli stakeholder in materia di trasporto marittimo. Al primo posto vi è l'instaurazione del dialogo e lo scambio dei dati sugli incidenti cibernetici tra tutti i membri della comunità portuale e porti. A tal fine è stato creato il portale sul quale si svolgono test per la trasmissione di relazioni su cyber incidenti nel settore marittimo (http://www.csoalliance.com/page/maritime-cyber-crime-reporting-portal).

Il miglioramento della cyber security nei porti non è per nulla un processo facile. Già l'identificazione delle potenziali vulnerabilità e l'implementazione delle soluzioni corrette possono rappresentare una grande sfida per il porto ed altri membri della comunità portuale. Inoltre, il settore della cyber security è complesso e multilivello, specificatamente tecnico e richiede know-how specifico.

La ricerca presenta in dettaglio le raccomandazioni pertinenti estratte da altre fonti internazionali come »Understanding Cyber Risk: Best Practice for Canada `s Maritime Sector« (Transport Canada, 2016) e »Code of practice – Cyber Security for Ports and Ports Systems« (Boyes s sod., 2016) dedicate alla stima delle potenziali vulnerabilità ed alla rappresentazione delle buone prassi nella loro soluzione.

La conclusione della ricerca ha confermato una certa disomogeneità nell'attrezzatura e nell'organizzazione dei porti nel settore della sicurezza fisica e cibernetica, ma al contempo anche l'esposizione a rischi di sicurezza molto simili.

Eppure non esiste ancora una strategia europea unitaria per la sicurezza portuale; la maggior parte dei porti finanzia autonomamente i progetti di sicurezza. Le autorità statali contribuiscono poco o nulla alla protezione di queste infrastrutture critiche.

L'accertamento del carattere disomogeneo, complesso, multilivello e tecnicamente sofisticato della sicurezza portuale conferma che lo scambio di buone prassi e di informazioni tra i porti è di fondamentale importanza e che la cooperazione tra i porti ed i loro esperti perseguita dal progetto SECNET ha rappresentato sicuramente un passo avanti in questa direzione.

Bibliografia e fonti

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*.

Allegato 6.2

Training transfrontaliero SECNET Venezia 27 febbraio 2018

(Rapporto sintetico - Deliverable 3.1.3.2)

Il Porto di Venezia, quale partner del progetto SECNET, ha ospitato il seminario transfrontaliero relativo a security e cyber security portuali, previsto dal progetto. Il seminario ha avuto un ruolo propedeutico alla elaborazione da parte dei tre porti partecipanti (Trieste, Capodistria e Venezia) di un Piano d'Azione congiunto per il potenziamento della difesa delle reti informatiche (cyber security) e della difesa fisica delle aree portuali dall'accesso di soggetti non autorizzati. Sulla base delle priorità individuate dal Piano d'Azione è poi prevista anche l'implementazione di concrete azioni pilota.

Con l'organizzazione del seminario sulla security fisica e cibernetica, al quale hanno partecipato come relatori alcuni tra i massimi esperti internazionali in materia, SECNET ha corrisposto ad un'esigenza molto diffusa fra i responsabili della sicurezza dei porti nord adriatici: al training transfrontaliero erano presenti oltre 50 funzionari impegnati nella gestione della sicurezza portuale provenienti da scali del Nord Adriatico.

Ad aprire i lavori **il Segretario Generale dell'Autorità di Sistema Portuale del Mare Adriatico Settentrionale, Martino Conticelli**, che ha ricordato la storia dello sviluppo delle misure di sicurezza portuale, passate dai sistemi di presidio e di controllo fisico del territorio a tecnologie sempre più avanzate. Oggi la cyber security è un fattore cruciale, al quale Venezia dedica da tempo la massima attenzione. Non per caso l'ispezione della Commissione Europea di fine 2017 ha determinato i membri del gruppo ispettivo a ritenere che **alcune procedure già in uso nei terminal del porto di Venezia vadano adottate come buone pratiche anche da altri scali europei**. Conticelli ha infine confermato l'importanza della cooperazione tra i porti su questo fronte, necessaria per raggiungere standard più efficaci ed insieme più competitivi.

L'evento formativo, che è stato articolato in tre sessioni tematiche, ha potuto contare sulla partecipazione di docenti universitari ed esperti di assoluta rilevanza. Il **Capitano di Fregata Vincenzo Paolo Leone**, Capo Unità al Comando Generale del Corpo delle Capitanerie di Porto (VI° Reparto), ha presentato casi di studio maggiori nelle prassi dei porti europei per la gestione della sicurezza fisica ed informatica, come emerse dalle ispezioni condotte dalla Commissione Europea. Leone ha inquadrato la rilevanza strategica della cyber security, condividendo anche esperienze dirette del suo lavoro per la Commissione Europea e per la U.S. Coast Guard. Leone ha annunciato in anteprima la elaborazione di un nuovo strumento per la raccolta di dati più analitici sul *cyber-risk management*, che verrà presto diffuso alle Autorità di Sistema dell'UE.

Le nuove tecnologie per la sicurezza fisica (sistemi di video-analisi, droni, scanner, ecc.) e per la cyber security delle operazioni portuali sono state presentate dal **Prof. Roberto SETOLA**, coordinatore del Master "Homeland Security" all'Università Campus Bio-Medico di Roma, che ha sottolineando quanto il costo della security non rappresenti una "spesa", ma un investimento necessario alla crescita delle economie portuali.

Al **Prof. Fabio Garzia** dell'Università La Sapienza di Roma (Dipartimento di Ingegneria della Sicurezza) è spettato poi il compito di relazionare sulla gestione multidisciplinare integrata della sicurezza nelle aree portuali di manovra ferroviaria, priorità richiamata anche negli interventi di molti operatori presenti.

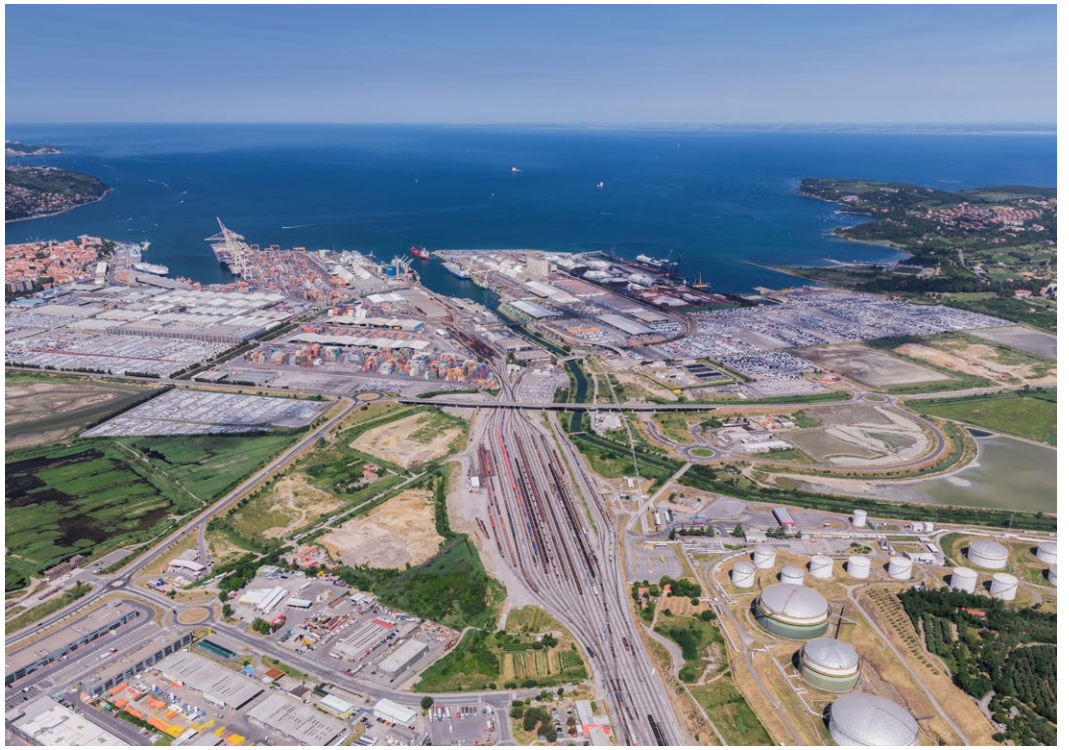
Coordinatori del training sono stati Martina Gržančić, Senior Expert al Dipartimento di Sviluppo Strategico di Luka Koper ed Ivano Di Santo, CIO all'Autorità di Sistema Portuale di Trieste.

.

Allegato 6.3

Azioni pilota di cyber security e di security fisica nei porti di Koper – Capodistria, Trieste, e Venezia

(Schede sintetiche - Deliverables ex 3.1.4 e 3.1.5.)



Luka Koper

✓ CYBERSECURITY – PENETRATION TESTS

Questa azione pilota è finalizzata a verificare e successivamente a prevenire attacchi informatici al sistema portuale ed a tutti i sistemi ad esso collegati, verificandone le vulnerabilità ed aggiornandone il database.

In particolare, l'azione prevede lo svolgimento di cosiddetti test di penetrazione del sistema che consistono in: un controllo di sicurezza secondo il principio della "Scatola Nera" in cui vengono inclusi i controlli sulle possibilita di accesso non autorizzato ai dati o alla loro modifica; l'adeguatezza della conservazione dei dati presso postazioni di lavoro locali, per evitare ulteriori abusi del sistema; assunzione di identita degli utenti esistenti nel sistema; modifiche dei privilegi degli utenti e valutazione delle funzionalità.

Inoltre, vengono inclusi anche controlli di sicurezza dei sistemi operativi del server con l'applicazione MS

Windows Server. In questo caso sono stati presi in cosniderazione tutte le certificazioni di sicurezza IT applicabili, verificando lo stato del punto di controllo e di Microsoft GOLD.

È inoltre previsto entro fine febbraio 2019 lo svolgimento di ulteriori test del sistema, con lo scopo di verificare se le vulnerabilità riscontrate durante i test di penetrazione siano state eliminate efficacemente e secondo i criteri previsti.

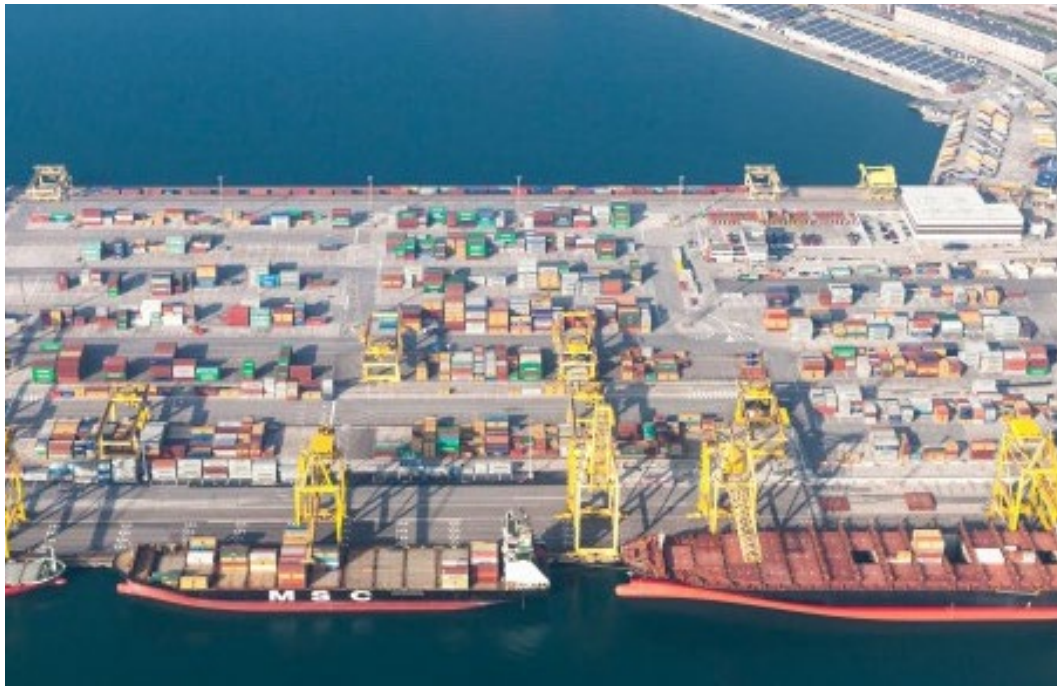
✓ SICUREZZA PERIMETRALE - RADAR

Questa azione pilota è finalizzata a dotare l'area del porto di Capodistria, nella quale si concentra la maggior parte dei passaggi di merci, mezzi di trasporto e persone, di un sistema sofisticato di allertamento radar da utilizzare in caso di necessità.

Con l'evoluzione delle varie tecnologie sulla sicurezza si sviluppano parallelamente anche tutta una serie di tecnologie atte a superare o ad eludere le barriere poste per salvaguardare la sicurezza e l'integrità del sistema portuale. A tal proposito, Luka Koper d.d. ha dotato punti strategici all'interno dell'area portuale di un moderno sistema radar ad infrarossi, con l'integrazione di videocamere termografiche ad alta risoluzione, per la visione a 360° di aree specifiche nella zona portuale. Con queste videocamere, si permette al Centro di controllo di rilevare tutte le fonti di calore e movimenti nel raggio di 1.500m, in tutte le condizioni meteo, sia con visione diurna, sia con quella notturna.

Il sistema viene integrato con il collegamento a dei server in grado di immagazzinare e distribuire le grandi quantità di dati acquisite dalle attrezzature di cui sopra, con i filmati ad alta risoluzione generati 24h su 24h.

È inoltre prevista la predisposizione e compatibilità del sistema di video sorveglianza, per consentire alla postazione del Centro di controllo portuale, di visionare in tempo reale e in ogni tipo di condizione meteo e di luminosità, quelle che sono le condizioni di sicurezza e sorveglianza, nelle specifiche aree del porto di Capodistria.



Autorità di Sistema Portuale del Mare Adriatico Settentrionale (Porto di Trieste)

✓ CYBER SECURITY – PORT IN NUMBERS

Questa azione pilota nasce dall'esigenza dell'Autorità di Sistema Portuale di dotarsi di una consolle di gestione dei dati provenienti da sistemi eterogenei. Tale piattaforma mira a permettere al fruitore di avere una esatta visione, in tempo reale, di quanto accade nelle aree portuali e nelle aree di sosta esterne al porto (c.d. buffer).

Attualmente, l'AdSP MAO dispone di due sistemi informatici: i) il Port Community System – Sinfomar; ii) il sistema di controllo degli accessi, I-gate, che a breve si evolverà nel sistema Vi-gate. Queste due piattaforme contengono un elevato e complesso set di dati, il cui studio correlato permetterebbe di massimizzare il controllo delle presenze in porto, anche nell'ottica di un supporto alle decisioni gestionali e di trattamento delle emergenze.

Il progetto SECNET permette lo sviluppo di tale portale, denominato *PIN - Port In Numbers*, che, in linea con la normativa vigente e in particolare con il Codice dell'Amministrazione Digitale, dovrà permettere all'utente, attraverso meccanismi di *drag & drop* o di trascinamento di tipo *touch* (in caso di accesso da tablet o smartphone) di creare una propria schermata di sintesi delle informazioni.

Questa piattaforma rappresenta uno strumento di forte comunicazione verso la collettività, intesa non solo come comunità portuale, ma anche come tessuto cittadino integrato con le aree portuali. Ha inoltre l'obiettivo di esporre i dati attraverso interfacce di semplice lettura e di facile comprensione. I dati elaborati sono, ad esempio, il numero di soggetti che hanno fatto accesso in porto, i mezzi associati e contemporaneamente quelli gestiti nell'ambito del Port Community System, provenienti dalle *buffer areas*, oppure direttamente dalle arterie autostradali, il dettaglio delle merci a bordo dichiarate, comprensivo di

quelle pericolose, e divise per destinazione internazionale. Il software applicativo genererà output grafici riproducibili su tv connesse ad internet, anche non appartenenti al mondo portuale, tali da poter permettere ad un cittadino comune di percepire i numeri ed i grafici preconfezionati ad hoc.

Per tutte le funzioni utente le pagine saranno disponibili in lingua italiana ed inglese.

✓ CYBER SECURITY - GDPR

Questa azione pilota è focalizzata sui servizi di Security & Compliance Consulting e in particolare mira ad assicurare l'adeguamento dell'infrastruttura IT del Porto di Trieste rispetto alle previsioni di cui a:

i. il Regolamento (UE) n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (c.d. GDPR);

ii. il D. Lgs. n. 196/2003 (c.d. Codice della Privacy), in particolare per quanto riguarda la direttiva sul monitoraggio degli accessi degli amministratori di sistema.

L'azione pilota è strutturata in due aree principali:

1. Servizi On Demand: ossia tutti i servizi di supporto ad alto valore aggiunto definiti per le seguenti aree di intervento:

   - istruzioni operative per governare il processo di analisi e gestione del rischio (*Security Risk Management*);
   - verifica dell'attuale stato di implementazione e coerenza con le normative esistenti in materia di cyber security (*Gap Analysis)*;
   - adeguamento dei punti di criticità emersi per l'innalzamento della sicurezza applicativa (*Remediation Consulting)*.

2. Servizi Continuativi: ossia tutti i servizi che assicurano la continuità operativa presso la sede dell'Autorità di Sistema Portuale, al fine di offrire un servizio di presidio e/o di supporto dedicato a specifici ambiti della sicurezza/compliance, quali:

   - gestione del mantenimento dello stato di conformità raggiunto dai sistemi dell'AdSP, al fine di supervisionare la garanzia nel tempo dello stato di adeguatezza di quanto implementato (*Compliance Maintenance Support*);
   - gestione delle campagne di audit di sicurezza e conformità rispetto alle normative vigenti o agli standard interni definiti (*Security & Compliance Audit*).

Grazie al progetto SECNET è stato quindi redatto un importante documento di assessment, la "Valutazione di Sicurezza del Porto di Trieste – Allegato 4 Approfondimento, Cyber Risk Management", che ricostruisce lo stato di fatto del Porto di Trieste. Questo elaborato è stato utilizzato anche dal Data Protection Officer (DPO) dell'AdSP MAO per le fasi propedeutiche all'applicazione del GDPR di recente entrato in vigore.

In occasione di un'ispezione della European Maritime Safety Agency (EMSA), svoltasi a novembre

2018, il CIO (Chief Information Officer) dell'AdSP MAO ha illustrato le componenti del documento e gli sviluppi successivi alla stesura, che si sono rivelati molto utili per la valutazione complessiva dello stato di security del Porto di Trieste e ha riscontrato grande apprezzamento da parte della Commissione europea

✓ SICUREZZA PERIMETRALE - SIRENA

Questa azione pilota è finalizzata a dotare le aree portuali nelle quali si concentra la maggior parte delle operazioni di un sistema di allertamento da utilizzare in caso di emergenze, di cui finora il Punto Franco Nuovo risultava sprovvisto.
In particolare l'azione prevede la fornitura e l'installazione di due c.d. gruppi di emissione, costituiti da sirene elettroniche direzionali in alluminio, sui tetti di due diversi edifici del Porto Nuovo, in modo da garantire la copertura del segnale acustico in tutti i terminal e le aree operative ivi compresi.
Il sistema di allertamento è attivato e gestito dalla sala di controllo ubicata nel complesso della Torre del Lloyd, esterno al perimetro delle aree operative. Pertanto, l'azione comprende anche l'installazione di un software applicativo, con relativo attivatore via radio, in grado di azionare il sistema di allertamento e controllare le unità sirene e ripetitori ad intervalli di tempo prestabiliti per verificare lo stato funzionale (stato alimentazione, stato batterie e stato trombe) e la qualità della tratta radio.
È inoltre prevista la predisposizione di un sistema volto a consentire agli utenti il completo controllo da remoto delle sirene tramite la rete dati dell'Autorità di Sistema Portuale.
Sono state scelte trombe direzionali per limitare l'inquinamento acustico all'esterno dell'area portuale.

✓ SICUREZZA PERIMETRALE - DRONI

Questa azione pilota mira a rendere più efficienti ed efficaci le operazioni di verifica diretta del funzionamento degli impianti portuali e quindi migliorare la capacità di intervento dell'Autorità di Sistema Portuale di nello svolgimento dei propri compiti di manutenzione e security portuale, in particolare attraverso periodiche azioni di vigilanza dell'ambito portuale svolte con l'ausilio di droni (in gergo tecnico, sistemi di pilotaggio a controllo remoto – SAPR).
I droni sono stati acquistati dall'Autorità di Sistema Portuale con fondi propri (30.000 euro) e in seguito adattati alle condizioni ambientali operative del Porto di Trieste (presenza di antenne, sistemi radar, navi di varia dimensione e stazza, sovrastrutture come le gru, ecc.), grazie ai fondi del progetto SECNET. Tali sistemi acquisiscono dati di videosorveglianza in formato digitale che vengono poi elaborati da una postazione di controllo situata nella sede della AdSP MAO e il cui allestimento, comprensivo della dotazione software e della relativa assistenza tecnica, è stato reso possibile dai fondi del progetto SECNET.
L'AdSP MAO ha inoltre promosso iniziative di formazione rivolte ai propri dipendenti, e strutturate in due corsi, in parte finanziati dalla Regione Friuli Venezia Giulia mediante il Fondo Sociale Europeo (10.000 euro).

Autorità di Sistema Portuale del Mare Adriatico Settentrionale (Porto di Venezia)

✓ SICUREZZA PERIMETRALE

L'azione pilota avviata da AdSP MAS nasce dalla necessità di incrementare la sicurezza fisica e il monitoraggio dell'utilizzo di alcuni varchi dell'area portuale, attraverso l'implementazione dell'attuale sistema di controllo accessi con l'aggiunta di una componente per la lettura delle targhe e l'aggiornamento dell'attuale componente di richiesta e gestione del rilascio dei permessi di accesso temporaneo. I varchi interessati dall'azione pilota sono i varchi dell'area portuale di Venezia e precisamente il varco Sant'Andrea, il varco 34/17 e il varco San Nicolò.

Con l'intervento realizzato in SECNET, il sistema di controllo accessi sarà dotato di una componente per il controllo del traffico veicolare che permetterà di validare il transito dei mezzi sia attraverso la lettura automatica delle targhe sia attraverso i più tradizionali "badge" nonché di gestire e monitorare l'impiego delle aree di parcheggio a disposizione all'interno dell'area portuale.

A livello operativo, l'azione pilota si è articolata nell'implementazione della parte software dell'intervento e nell'installazione fisica di telecamere e dispositivi per permettere il monitoraggio.
Con le automazioni apportate dal progetto SECNET, AdSP MAS ha migliorato le modalità di monitoraggio degli accessi nell'area portuale veneziana, garantendo al contempo la riduzione dei tempi amministrativi per il rilascio dei permessi nonché un maggiore controllo dei transiti.

Allegato 6.4

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

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

ACRONIMI

Abbreviazione	Spiegazione
AdSP MAO	Autorità di Sistema Portuale del Mare Adriatico Orientale
AdSP MAS	Autorità di Sistema Portuale del Mare Adriatico Settentrionale
ANPR	*Automatic Number Plate Recognition*
CCTSP	Istituzione di un Centro di Coordinamento Transfrontaliero per la Security Portuale
CIIP	*Critical Information Infrastructure Protection*
CPNI	*Centre for the Protection of National Information Infrastructure*
CTE	Cooperazione Territoriale Europea
DG MOVE	Direzione Generale per la mobilità e il trasporto
DPO	*Data Protection Officer*
EMSA	Agenzia europea per la sicurezza marittima
ENISA	Agenzia europea per la sicurezza delle reti e dell'informazione
GDPR	*EU General data protection regulation*
GIS	Sistema informativo geografico
ICT	Information and Communication Technology
IMB	Ufficio marittimo internazionale
IMO	Organizzazione marittima internazionale
IMSC	*International Maritime Security Corporation*
INCE	Iniziativa Centro - Europea
INTERREG	*Programme for the European Territorial Cooperation goal*
ISAC	*Information Sharing and Analysis Center*
LK	Luka Koper
MTSA	*Maritime Transportation Security Act*
NAPA	*North Adriatic Port Association*
OMD	Organizzazione mondiale delle dogane
PSC	*Port Security Committee*
PSO	*Port Security Officer*
SAFE Port Act	*Security and Accountability For Every Port*
SCADA	Supervisory Control And Data Acquisition
SDSS	Sistema di Supporto alle Decisioni Spaziali
TEN-T	*Trans-European Transport Network*
UE	Unione Europea
UNCTAD	Conferenza delle Nazioni Unite sul commercio e lo sviluppo
UNITS	Università degli Studi di Trieste
UP	*Univerza na Primorskem (Università del Litorale)*
WP	*Work Package*

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 IZVRŠNI
UNIVERSITÀ DEL LITORALE

Mare Adriatico
Jadransko morje



SECURITY PORTUALE - VARNOST PRISTANIŠČA

CONTATTI / KONTAKT

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**