WP3.2.3.1

Strategia transfrontalieria per il rafforzamento della security portuale tramite l'uso di ICT

Indice

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.

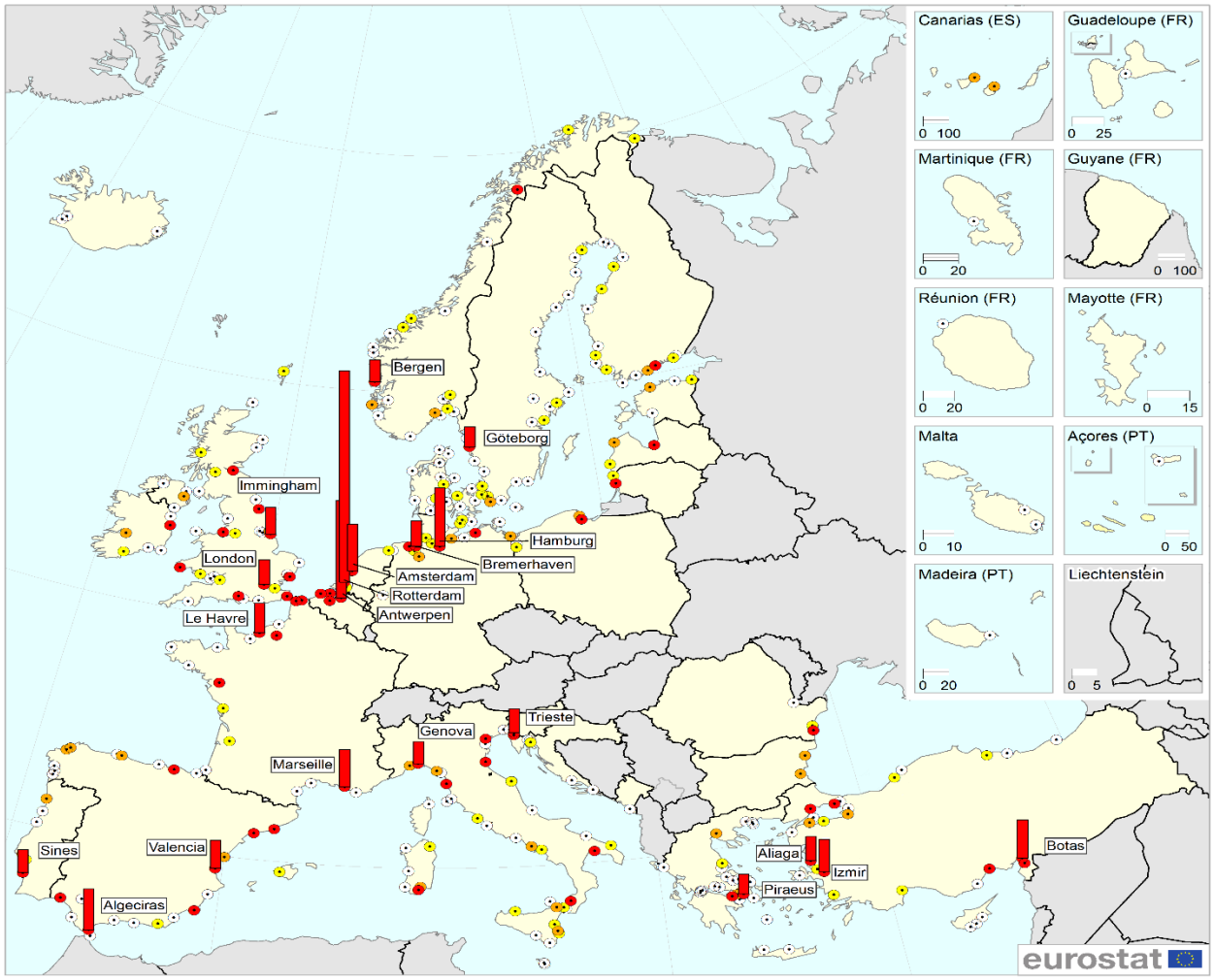
Per garantire sicurezza ed efficienza nelle operazioni portuali ed un efficace controllo dei flussi di persone e merci, il presente documento individua le principali sfide della sicurezza nel settore marittimo e le linee guida per la realizzazione di una cooperazione transfrontaliera permanente, che, 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.

Top 20 cargo ports and other main cargo ports in 2016 on the basis of gross weight of goods handled



Top 20 ports are named and their handling activity shown as bars.

Administrative boundaries: © EuroGeographics © UN-FAO © Turkstat
Cartography: Eurostat — GISCO, 03/2018

100 million tonnes

1 - 5 Mio
5 - 10 Mio
10 - 20 Mio
> 20 Mio

0 200 400 600 800 km

Source: Eurostat (online data code: mar_mg_aa_pwhd)

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,

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

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.

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

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

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)

[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.

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:

- ✓ 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/Maritime_ports_freight_and_passenger_statistics*

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