DS 3.2.3.1

Čezmejna strategija za krepitev pristaniške varnosti z uporabo IKT

Kazalo

1. Uvod

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

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

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

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

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

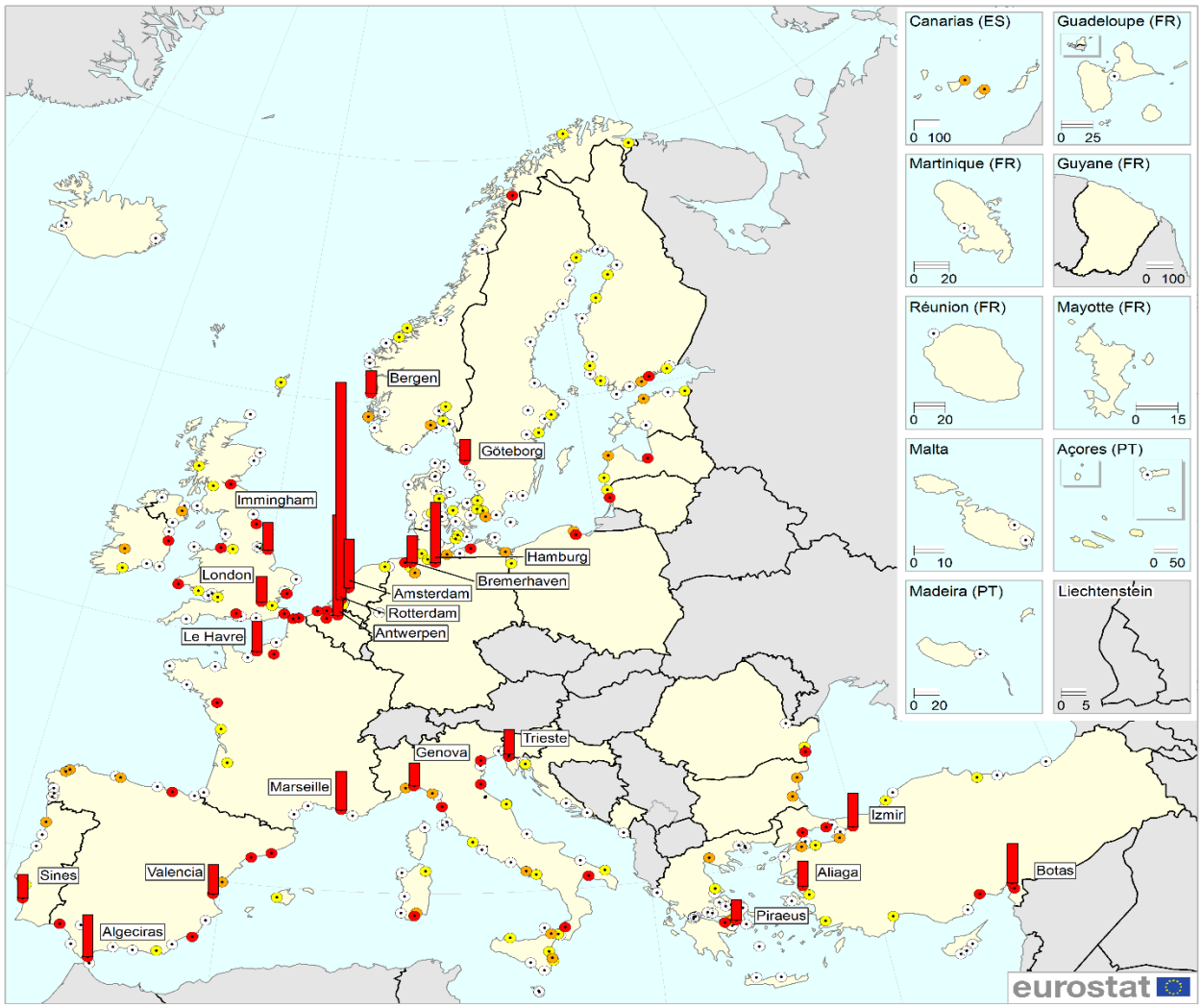
Za zagotovitev varnosti in učinkovitosti pri pristaniških dejavnostih ter učinkovit nadzor pretoka blaga in oseb, so v tem dokumentu predstavljeni poglavitni izzivi varnosti na področju pomorstva in smernice za vzpostavitev trajnega čezmejnega sodelovanja, ki jih je v splošnem mogoče povzeti z naslednjimi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

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

[1] EU je po morju uvozila za 53 odstotkov vsega uvoženega blaga, izvozila pa za 48 odstotka v države nečlanice.
[2] Podrobnejši podatki o pretovoru blaga v evropskih pristaniščih v letu 2016 so na voljo na sliki 1.

Slika 1. Evropska pristanišča in pretovor blaga.

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. Poglavitni izzivi varnosti na področju pomorstva

2.1 Regulativni okvir

Ko je novembra 2002 vstopil v veljavo Zakon o varnosti pomorskega prometa (*Maritime Transportation Security Act* - MTSA), zatem pa leta 2006 še Zakon o varnosti in odgovornosti za vsako pristanišče (*Security and Accountability For Every Port* - SAFE Port Act), je to pomenilo velik korak naprej na področju pristaniške varnosti, od ocene ranljivosti pristaniških objektov do razvoja in izvedbe varnostnih načrtov za omejitev vstopa v zaščitena območja le za pooblaščene osebe.
V skladu z MTSA, Uredba (EU) št. 725/2004 Evropskega parlamenta in Sveta o povečanju zaščite na ladjah in v pristaniščih uvaja ukrepe za okrepitev varnosti nacionalnega in mednarodnega pomorskega prometa, pri čemer države članice obvezuje k oceni varnostnih tveganj. Kot dopolnitev tega dokumenta, Direktiva 2005/65/ES Evropskega parlamenta in Sveta usmerja države članice k izdelavi in posodobitvi pristaniških varnostnih načrtov, ki za vsak nivo varnosti določajo: a) postopke, ki jim je treba slediti; b) ukrepe, ki jih je treba izvajati; c) dejavnosti, ki jih je treba uvesti.

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

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

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

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

2.2 Ugotovljeni izzivi:

Glede fizične varnosti pristanišč so največji izzivi naslednji:

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

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

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

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

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

2) *Kompleksnost sistemov IKT v pomorstvu,* ki zajemajo tudi zelo specifične elemente, katerih hitri tehnološki razvoj je v določenih primerih povzročil zmanjšanje pozornosti na njihovo ranljivost. Pomemben primer je vse večje število pristaniških infrastruktur, ki uporabljajo sisteme IKT, na

primer naprave SCADA[6], ki so povezane z internetom brez zaščitenih omrežij. Ranljivosti, ki jih povzročijo te vrzeli v varnosti sistemov IKT, lahko vplivajo ne le na storitve, ki jih ti sistemi podpirajo, temveč tudi na tiste, ki so običajno skupne, kot so podatkovne baze, sistemi za gostovanje občutljivih informacij ipd. Ugotovljeno je bilo tudi, da ne obstaja standardizacija dobrih praks za zagotovitev ustrezne zaščite sistemov IKT. Smernice s področja varnosti se pogosto nanašajo le na osnovne ukrepe in med številnimi orodji IKT ne najdejo ustreznice ali pa ne pokrivajo vse ustrezne tehnologije.

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

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

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

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

7) *Potreba po pobudah, ki bi spodbujale sodelovanje, izmenjavo informacij in deljenje izkušenj* med zainteresiranimi akterji. Pobud za sodelovanje je malo. Med njimi velja omeniti pobudo Port ISAC[7] (Information Sharing and Analysis Center), katere cilj je vzpostaviti sodelovanje med

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

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

subjekti iz javnega in zasebnega sektorja za spodbujanje izmenjave informacij, mnenj in izkušenj o vprašanjih informacijske varnosti in o dobrih praksah.

3. Čezmejno usklajevanje za krepitev pristaniške varnosti

Na podlagi pomanjkljivosti, ugotovljenih v prejšnjem delu besedila, si čezmejna strategija za krepitev pristaniške varnosti s pomočjo orodij IKT želi uresničiti v nadaljevanju naštete pobude.

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

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

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

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

razvoju Centrov za izmenjavo in analizo informacij ISAC je treba določiti pomembne deležnike iz javnega in zasebnega sektorja ter med njimi vzpostaviti zaupanje.

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

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

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

4. Zaključki

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

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

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

Večja varnost pomeni manjšo možnost hudih incidentov, boljši nadzor vstopa, zaščito računalniških omrežij, hitrejšo zaznavo groženj in večjo odpornost.
Večja odpornost pomeni nizek učinek v primeru prekinitve in hitro obnovo običajnih dejavnosti, z ohranitvijo konkurenčnosti pristanišč.

Opredelitev pojmov:

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

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

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

Bibliografija

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

Ahokas, J. Kiiski, T. Malmsten, J. and 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, str. 267-274 Fraunhofer. *http://publica.fraunhofer.de/documents/H-47052.html*, ISBN: 978-3-8396-0604-9

Boyes, H. Isbell, R. and Luck A. (2016). *Code of Practice Cyber Security for Ports and Port Systems*. Institution of Engineering and Technology, London, Združeno kraljestvo. *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*

Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

Evropska komisija (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*

Evropska komisija (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,* str. 2-135, Združeni narodi, Ženeva. *https://unctad.org/en/Pages/Publications/Review-of-Maritime-Transport-(Series).aspx,* ISBN 978-92-1-112922-9