# La security marittima del porto di Trieste valutata buona pratica europea

Dal 19 al 23 novembre 2018 la Commissione Europea ha condotto un'ispezione al porto di Trieste al fine di monitorare la corretta implementazione, da parte dell'Italia, delle norme in materia di *maritime security* sia per quanto attiene le navi e gli impianti portuali (Regolamento 725/2004) sia per l'intero comprensorio portuale (Direttiva 2005/65/EC).

L'attività di *maritime security* nasce nel 2006 per volontà degli Stati membri dell'Unione Europea, quale sistema armonizzato di prevenzione e protezione delle navi e delle strutture portuali contro minacce di atti illeciti intenzionali; essa si basa da allora anche sulle determinazioni già assunte a livello internazionale dall'Organizzazione Internazionale Marittima (IMO) a seguito dell'attacco alle Torri Gemelle (adozione del nuovo Capitolo XI-2 alla Convenzione SOLAS'74 e del International *Ship and Port Security Code*).

Il team della Commissione EMSA (*European Maritime Safety Agency)* in missione a Trieste, composto da sette ispettori di diversa nazionalità, ha individuato per l'attività "*port security*" l'intero comprensorio portuale e tre impianti specifici (*port facilities*), mentre, per la parte "*ship security*" sono state ispezionate quattro navi di diversa nazionalità, una extracomunitaria, due comunitarie ed una italiana. Gli esiti dell'ispezione sono stati estremamente positivi ed il rappresentante leader della Commissione Europea, nel suo discorso di chiusura, ha espresso **parole di elogio** sia per la Guardia Costiera - che ha operato nella duplice veste di Autorità Competente (Comando generale del Corpo delle Capitanerie di porto) e Designata (Capitaneria di Porto), nonché con propri ispettori a bordo delle unità ispezionate (*Duly Authorized Officers*) – sia per la Prefettura, la Polizia di Frontiera, l'Autorità Portuale e tutte le altre amministrazioni che, a vario titolo, partecipano alla implementazione della normativa di settore.

In occasione di questa ispezione il documento di *assessment* prodotto nell'ambito del progetto SECNET è stato ulteriormente riutilizzato e, visti i risultati raggiunti, si è rilevato molto utile per la valutazione complessiva dello stato di *security* del Porto di Trieste. Per la prima volta è stato coinvolto direttamente il CIO (*Chief Information Officer*) dell'AdSP MAO, che illustrando le componenti del documento e degli sviluppi successivi alla stesura ha riscontrato massimo gradimento da parte della Commissione, al punto che il leader della Commissione ha affermato che "le risultanze dell'ispezione ad uno degli impianti portuali saranno esportate quale best practice a favore degli altri Stati membri".

Grazie al progetto SECNET la Direzione di *Safety and Security* di AdSP MAO ha potuto infatti approfondire le tematiche legate alla *security* e *cyber security* realizzando la stesura di un dettagliato documento di *assessment* ("Valutazione di Sicurezza del Porto di Trieste – Allegato 4 Approfondimento, Cyber Risk Management"), che costituisce lo stato di fatto del Porto di Trieste. Questo elaborato è stato sottoposto a riuso dal DPO (Data Protection Officer) dell'AdSP MAO per le fasi propedeutiche agli adempimenti previsti per l'applicazione del GDPR (Regolamento (UE) 2016/679), che rientrano nell'ambito dell'azione pilota di cyber security (A.3.1.4) del progetto SECNET. Il progetto così ha permesso di ridurre il carico di lavoro interno e massimizzare l'efficienza nel raggiungimento di questi importanti obiettivi in termini di *security*. Ma le attività SECNET hanno consentito anche al AdSP MAO di acquisire il know-how propedeutico alla gestione di una infrastruttura tecnologica critica quale il SINFOMAR, il Port Community System del Porto di Trieste. Le competenze così sviluppate sono state un importante preparazione all'applicazione e al rispetto delle regole previste dalla direttiva NIS (Direttiva (UE) 2016/1148).